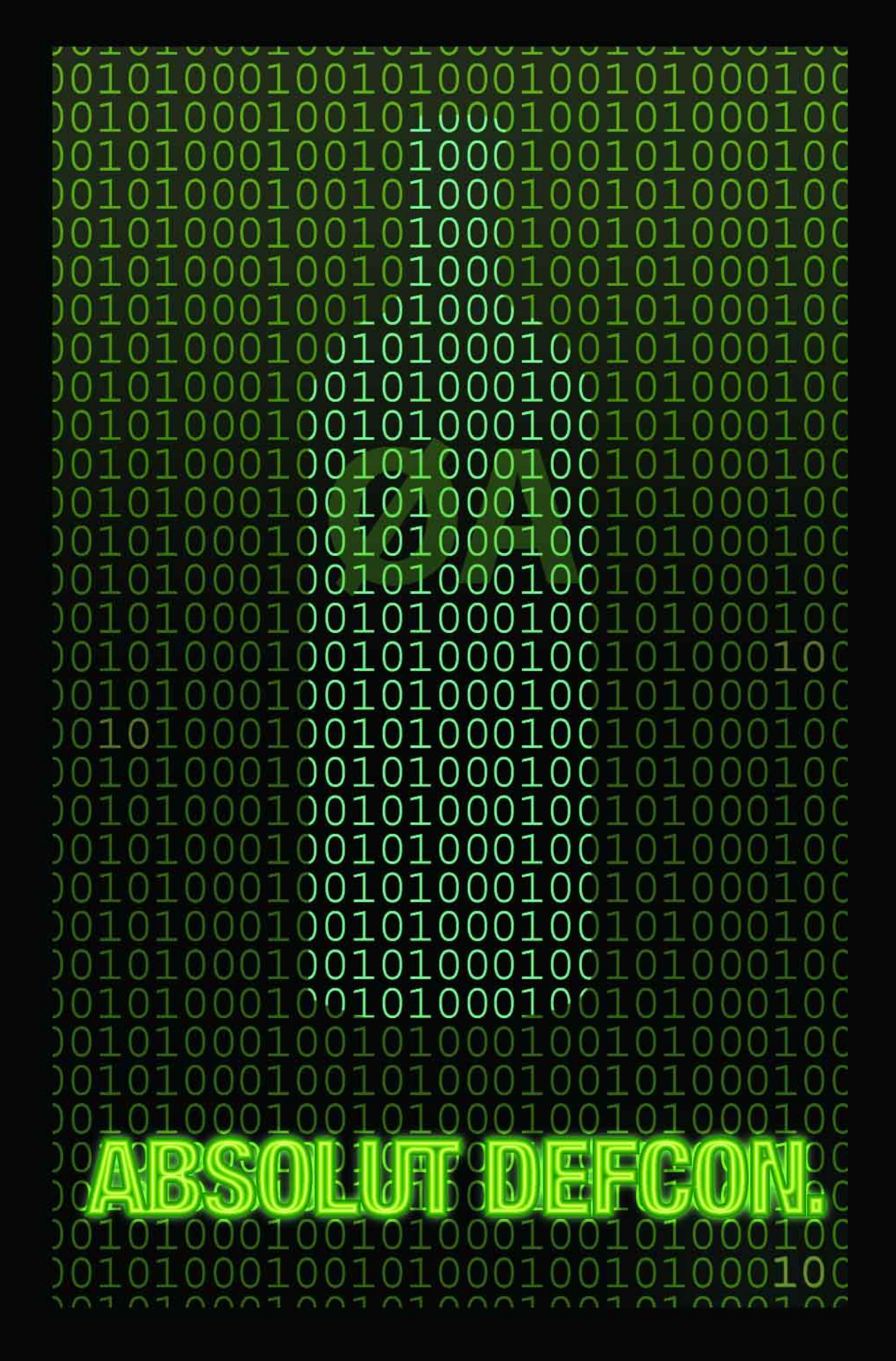

ABSOLUT DEFCON

Thanks to:

Major Malfunction, Zac, Ping, Lockheed, CMoS, Tina, Bro, McNabstra, Sleestak, B.K., Agent X, TechnoWeenie, Gonzo, Josh, DC Forums, Evil Pete, Skroo, Spun, CHS, Priest, Bink, the Ghetto Hacker staff who ran CTF, Zziks, Evil, ChrisH, Xylorg, Flea, Justabill, Pescador, Queeg, Teklord, Cyber, Mel, Ming of Mongo, Grifter, Monk, Nichole, LRC, Xam, RussR, Zain, Shatter, Caezar, Pappy, Cat Okita, The People, Waz, Priest, Artimage, Anti-Bill, Nulltone & Simon for the DEFCON Forums, Hdink, Moloch, LA2600, ISN and BugTraq, Scott Post, Rooster, Charel, The Alexis Park Staff, Winn, Dr. Kool, Dead Addict, tdragon, Ghent, SD, Bodoman, BAWUG, KenO- the original Fed, Metalhead the original goon, Netstumber, Uncle Ira's Fun Farm 'O Death, the whole FreeBSD project, the Hektik crew and 2600SLC for the scavenger hunt, the OpenSSH and OpenSSL projects, D A/V Las Vegas (lighting support), Las Vegas Sound & Video, Dan Bernstein for QMail and DJBDNS, the JAP team for making web browsing more anonymous, and all the people who sent in suggestions after reading my letter to the community.

© Dead Dreamer

Welcome - DEF CON ØA

Thanks for coming to DEF CON ØA! (That's 10 in Hex for you slow ones)

New:

First off, some new stuff to check out this year: We have speakers going Friday to Sunday, and we start an hour later each day than last year to let everyone recover from the night before. Gone are the days when we thought we could run this sucker 24 hours a day. We need sleep too! Be careful with your ninja throwing badges. We put holes in the corners in case you want to screw them to your car or something.

You will notice the wireless network has grown, we have more space, and the rave room is gone. We are turning it into a lounge to hang out in. Also there are two vendor areas instead of one, split in two locations. New contests, updated stuff, and we hope DEF CON TV will run with less glitches this year.

As always the CON is what you make of it. Help someone out with a question, and they might return the favor to someone else. The karma wheel rolls on! Having a party? The Staff loves parties, and needs excuses to unwind, so invite 'em if you got room.

Looking Back:

This is the Tenth year of DEF CON. It has come a long way in that time. When I started the first DEF CON I had never been to Las Vegas, and I had never been to a "Hacker" convention. The short version of the story is that I was left to put together a party for some fido-style networks I belonged to (Remember CyberCrime, HiT Net, etc?), and in the end I invited everyone, even the Secret Service. Because I knew of no convention on the West Coast (Not that Vegas is on the coast), and because I had never been to Las Vegas, I decided to do it here. There was also the tie in with the movie War Games. I live in Seattle, and so did the character John Lightman in the movie. When picking a location to Nuke he picked Las Vegas. Sounded good to me!

At that first DEF CON there were about 110 people, and we all had a great time. It was held in one room, with just a few speakers. I got to meet all the people I had met on-line, and we had this sense of camaraderie. It was this camaraderie that made DEF CON grow exponentially. We quickly went from 110 to about 250 to about 550, and so on. This paralleled the same growth trends of the internet. Pretty soon the whole world was changing— what we did was no longer obscure and unknown. Movies started popping up, from the awful "The Net" to "Hackers" (With characters based on the real members of the MOD) and pretty soon it was el1t3 to be a haxor.

Since those early days, computer security has gone from some soopah seekret skill learned in the "scene" to something you can study on-line for free. You no longer have to break into systems to learn un*x because there are plenty of free operating systems. It seems that almost every original motivation to hack has changed over the last decade. PCs are cheap, un*x free, internet access can be had at the cost of 4 espressos, and security information is free on-line. This ever increasing complexity of security had another side effect: Back in "the day" it was possible to have a real good handle on all technology. If you understood phone switching, x.25 packet networking, un*x and the Internet you would be a ninja compared to the other kids. Now you could spend you life just trying to keep up in all those areas. Everyone started having to specialize in order to stand out, or even just keep up. With the speed of technology now I don't see that trend ever slowing down! The result of all of this is that, much like what happened on USENET when AOL connected to the net, the scene fragmented and split into a lot of smaller pieces in order to deal with the increasing noise level. Just like the good conversation from USENET moved to mailing lists, the good hacking information moved to more private groups and tended not to be discussed in the open.

OK enough of that! What going to happen next?

Looking Forward:

Well, I can't see into the future, but this is what I am guessing: People continue to not give a crap about security. They haven't for ten years, so why start now? It hasn't slowed down the delivery time of pron, spam, or ebay. The people who should really care about it, like the Government, the Military, Hospitals and Banks, will continue to have hard times. The market will take 4 years or more to recover, and there will be a lack of cool Gen-X jobs all around. Sort of like how it was six or seven years ago. I predict there will be more politically motivated hacking. I've said it for years, but I think we are reaching critical mass for the number of people who can get on-line and learn to hack. Some of these people are going to be motivated by politics.

Yes, that is all coolio, but what about DEF CON? Well we have some changes n the works. I've said it for about the last year, but we are actually getting around to doing it now. I have been thinking about how to do more stuff for the scene, and have come up with the following ideas. We'll see what works and what doesn't on-line over the next few months. We are going to run a few mailing lists, start a Speak Freely encrypted voice bridge and voice chat server, try and run a small-file size anonymous re-mailer, run a JAP remix chain (If anyone of us can learn to read German and set that sucker up) on some of our bandwidth, and re-build the media server. Basically we want to do things that, however small, increase people thinking about privacy and freedom.

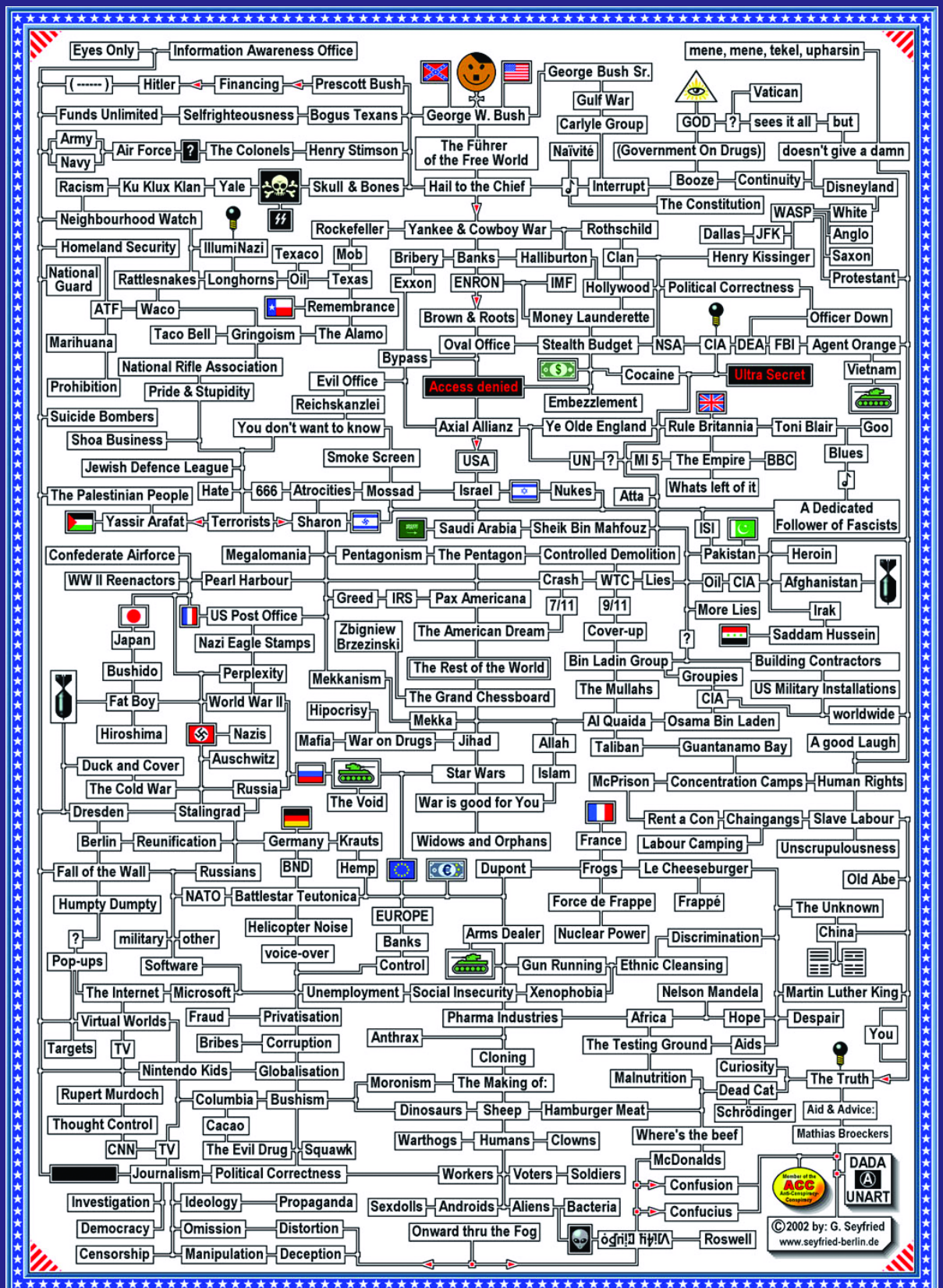
OK, so those are my big monumental words on this year's convention. As usual PLEASE DON'T BREAK THINGS, and if you see someone breaking things stop them or point them out to a Goon. We do like the hotel and would like to come back. This con is a collaborative effort, and it takes us all to make sure we all have fun. See you by the pool.

— The Dark Tangent

P.S. - "So is it 'DEF CON', 'DefCon', 'Def Con' or 'DEFCON'?" you ask. My answer is "Yes"

Cover image by Darrington

World Conspiracy Theory



A Blast From the Past.

I wrote this for New Media Magazine in 1994.

Well I'm all updated with OS/2 3.0, yessirree-bob. I've been using this fine product for several years. Every once in a while I switch back to windoze just to make sure I've made the right choice. If I have a few crashes in OS/2 I figure I'd have about 30 in windoze. I was pleased to find that 3.0 comes with all types of goodies, but most importantly for me it has an "InterNet Access Kit" which provides a WWW browser, Gopher, FTP, etc. in a nice graphical format. Much like Chamileon, but not nearly as expensive.

What to do with my new toy? Well I've never had a Web Broswer at home, so I jumped online and went searching for a friends home page. Aleph One maintains the DEF CON web site, but also has an excellent home page with pointers going to several other great pages and links. Where else will you find an index to all previous issues of PHRACK? While some people might not "get it", check out HTTP://dfw.net/~aleph1 next time you can. Makes me want to start my own page.

While checking out the new IBM/Sears Advantis network I tried the newsreader. Pretty good for free, too bad it isn't threaded, though. I was in comp.security when I came accross a warning post from the ILF (Internet Liberation Front) warning coprorate America to back off. It seems these security professionals are getting sick of the control being passed to all the major telco companies who can only see as far as the next profit. Faster then Microsoft can say "AntiTrust Violation" the ILF claims they can penetrate your firewall router. Stealing more corporate secrets than there are bugs in sendmail the ILF will cause the only thing the companies understand, financial expense, should they not "get out of dodge." Wether or not the ILF is for real, it is echoing the feelings of many people who do not see the net as the latest fad but a great resource that shouldn't be destroyed by commercializing. If Canter and Segil can become "good guys" by posting for their law practice to every newsgroup reguardless of it's topic, and then complaining about cencorship, the future may be bleak indeed. Now if only I can get a book contract writing about "The commercial opportunities on the net" like they did, my financial worries would be over.

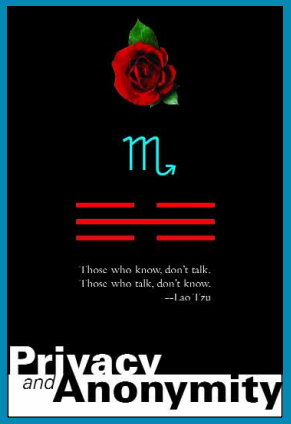
Besides the normal spate of chain letters, improper cross posting, off topic messages and the average net-splits it looks like it's shaping up to be an ok year.

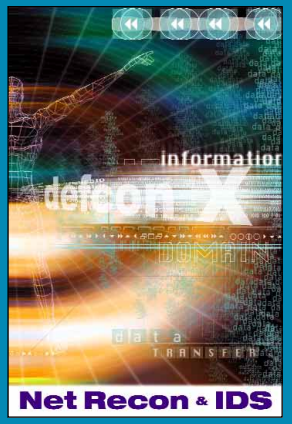
The Dark Tangent.

WHERE THINGS ARE

ALEXIS PARK
RESORT & SPA • LAS VEGAS

Friday August 2





time			
11:00 - 11:50	**Attacking Printers** *Dennis Mattison*	**Stealth Data** *Khan*	**XProbe** *Ofir Arkin*
12:00 - 12:50	**DC Phone Home** *Chris Davis*	**Tracing Anon Email** *Len Sassaman*	**Perl OS Tool** *Fred Trotter*
13:00 - 13:50	**FTPd** *Jay Beale*	**Patriot and YOU** *Jennifer Granick*	**IDS Correlation** *Dan Burroughs*
14:00 - 14:50	**Windows Server Security** *Humperdink*	**Net Cash** *Ryan Lackey*	**Extensible IDS** *Ian Peters*
15:00 - 15:50	**Hiding Data** *Thomas Munn*	**Hiding Data** *Thomas Munn*	**Reduce Net Abuse** *Jaeson Schultz*
16:00 - 16:50	**Hacking of America** *John Dodge*	**Mixminion** *Roger Dingledine*	**GNURadio** *Steve Schear*
17:00 - 17:50	**OSS Phone Systems** *Rich Bodo*	**Gnunet** *Christian Grothoff*	**Applescript in Security in OSX** *Agent OJ*
18:00 - 18:50	**Closed**	**Post 9/11 Privacy** *John Q. Newman*	**Closed**

PERFORMING @ DEFCON 2002

Black & White Ball

Saturday, August 3
8pm- 4am

"The music is abominable"
– Winn Schwartau

Here is the line up for the Black and White Ball this year which will be running from 8pm - 4am.

The Minibosses
DJ Jerkface
CMOS
HiBias
Jackalope Ov Orbis
Corrupt Data
Kris Klink
Prophei

Despite the changes happening to the DJ area, the Black and White Ball will still be happening this year. Traditionally folks would dress up and we'd provide the entertainment, but over the years less and less people came in costume. This year we'd like to encourage folks to dress up for the event. Anything goes, you can play it straight and throw on your best outfit, or go completely sideways and wear your purple and silver zoot suit or dress up like one of the ghosts from Pac-Man.

If you remember a few years ago we had a screening of "Enemy of the State" with the writer giving commentary. This year we are not as cool. Instead we have three movies to play Friday and Saturday night in Apollo. I have asked five Goons to select one of their favorite moves, and tell me why they think it is so cool. Below are the results, and the order in which they will be shown. If the popcorn maker is working you can expect free popcorn as well. Tired? Want to hide from the parties? Stop by for a late night movie.

Note, that these movies are separate than what you will see on DEF CON TV.

DEF CON Presents:
Night at the Movies, Part II

Friday Night:

#1 – The Dark Tangent picks: **Animation Compilation**
This is an original compilation of many flash animations that we found to be cool. While many of you have seen some of these before, we hope to expose you to some you may not have seen. Besides who can really get enough of "Beer Good, Napster Bad!" and "Killer Bean 2" ? Run off a laptop, this may be a bit sketchy!

#2 – Josh picks: **Colossus: The Forbin Project**
Colossus is a movie which expressed fears of a computer taking over the world. Written in the early 70's(??) it was ahead of its time. I think it would be a classic. I think Uncle Ira from MECO may have the original Colossus somewhere in his barn. (Ed: Count the number of audio samples you recognize that have been sued in techno / industrial songs)

#3 – Gonzo (The Original Goon) picks: **Fight Club (1999)**
We are young and have what we want. We are confused and disillusioned with the white bread single serving corporate lifestyle and have no problems of our own so we dwell on other peoples problems and misfortunes. We need the support of others. We are spiritually empty and we are pissed off. We need a release that only the collapse of society would appease. I am Jack's extreme exhaustion after only the first 24 hours of Defcon...

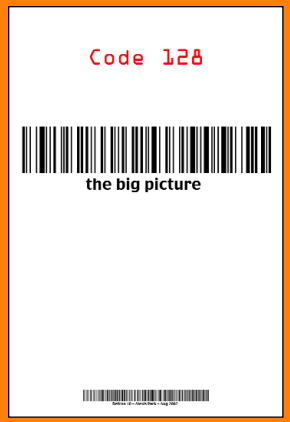
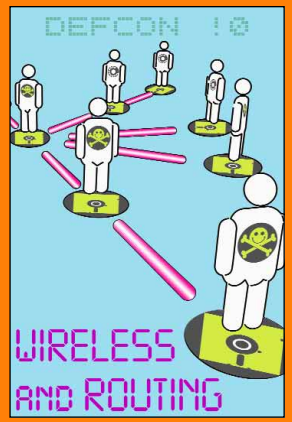
Saturday Night:

#1 – Major Malfunction form UK Pirate Radio picks: **Dark Star**
So you socialed your way into a really high power .com job and are in way over your head (but still have more clue than the rest of them put together, despite lack of training/qualifications)... The company is dynamic and powerful but out of control and ultimately doomed... The guys at the top don't know what they're doing, or why they're doing it, but they're prepared to throw the best possible hardware at the problem and damn the costs/consequences... Your only hope is to find the reclusive uber-geek that started the whole thing and pick his brains... This film is the ultimate metaphor for the .com era...

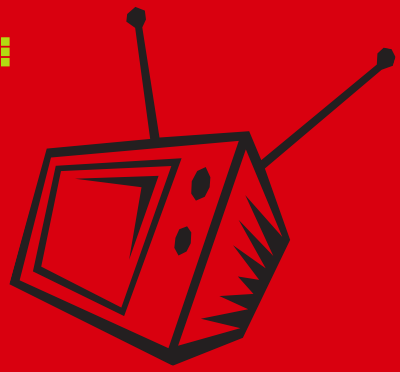
#2 – Uncle Ira (From the Fun Farm 'O Death) picks: **Blade Runner**
1982 Harrison Ford Classic! A dark portrayal of the near future, based on a Phillip K. Dick novel– Do Androids Dream of Electric Sheep? A police officer, played by Ford, is tasked to retire (kill) androids who want to meet their creator. A dark, Film Noir, cyberpunk classic! Directed by Ridley Scott.

#3 – TBA

Saturday August 3

time				
11:00 - 11:50	**Politics of Vulnerabilities** *Scott Blake*	**Web Application Brute Forcing** *David Endler & Michael Sutton*	**Mobile VPNs** *Brett Eldridge*	**Hardening Solaris** *Chris Hurley*
12:00 - 12:50	**The Other Side of InfoSec** *Wilco van Ginkel*	**Attacking Embedded Systems** *FX*	**Wireless Networking** *Bruce Potter*	**Bastille Linux** *Jay Beale*
13:00 - 13:50	**The Hacker Nation** *Simple Nomad*	**Lockpicking Demo** *Gingerbread Man*	**Router Security & Forensics** *Nicholas Fischbach & Sébastian Lacoste-Séris*	**SQL Injection** *Kevin Spett*
14:00 - 14:50	**Consumer Media Protections** *Adam Bresson*	**.Net Security Issues** *Cyrus Pekiri*	**Replacing Tripwire** *Matthew Marsh*	**Hacker Meetings** *Skroo / Grifter*
15:00 - 15:50	**Elcomsoft Update** *Joe Burton*	**Terminal Servers** *Ian Vitek*	**Seattle Wireless Project** *Ken Caruso*	**Intelligence Gathering** *Vic Vandal*
16:00 - 16:50	**TCPA** *Lucky Green*	**Lockpicking** *Laz*	**Securing Wireless** *zSnark*	
17:00 - 17:50	**Vulnerability Disclosure** *Tom Parker*	**Security at Kernel Level** *Philippe Biondi*	**DDoS Mitigation** *Greg Miles aka Doc*	
18:00 - 18:50	**Hacking: The Next Ten Years** *Richard Thieme*	**SNMP** *DJSS*	**Black Ops TCP/IP** *Dan Kaminsky*	

DEFCON TV



This is the third year of DEF CON TV, and we hope to have it all sorted out starting by the speaking Friday morning. We have found out the hard way about signal degradation over coax, poor video tape quality, etc. This year there will be dedicated channels for the three speaking areas as well as a movie channel. While you won't be able to ask a question, you can stay in the privacy of your room and watch. If all works out there will be three speaking channels during the day, one movie channel, and a miscellaneous channel we have not assigned yet.

Channel # 17 – (Parking Lot Tent) Speaking area

Channel # 29 – (Roof Tent) Speaking area

Channel # 32 – (Movies)

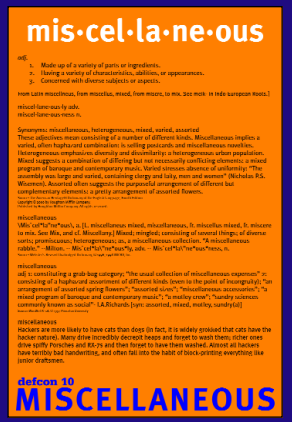
Channel # 33 – (Apollo Feed) Speaking area

Channel #42 – Announcements and strange things randomly

Channel # 32 – Movie Channel. Starting Friday evening after we get things sorted out this channel starts. Once the movies are selected we will try to get them listed on Channel #42.

These are not the same movies being played in Apollo on Friday and Saturday night.

Sunday
August 4



time			
11:00 - 11:50	**Advances in Trojans** *Roelof Temmingh*	**No IP Address** *Mick Bauer*	**NLP Intro** *Error*
12:00 - 12:50	**Spiders** *Michael Schrenk*	**LIDS** *Huagang Xie*	**FreeBSD Exploits** *Rich Murphey*
13:00 - 13:50	**Shell Code** *Fozzy*	**Next Gen Data Forensics** *Thomas Rude*	**Biometrics** *Nate Rotschafer*
14:00 - 14:50	**Steganographic Trojans** *Michael Rogers*	**Covert Channels** *Andrew Hintz*	**Selling Out** *hellNbak*
15:00 - 15:50	**Intro to Computer Virii** *Robert 'v1ru5' Lupo*	**FBSD Security** *Sean Lewis*	**Security Wolves Among Us** *Gobbles*
16:00 - 16:50	**Hacking of America** *John Dodge*	**Mixminion** *Roger Dingledine*	**GNURadio** *Steve Schear*

DEFCON

How Would You Like You

I get a lot of spam - a whole lot. Each day, as I read my e-mail I find anywhere from fifty to two hundred of these steaming little pieces of... spam, waiting for me, all in their places with bright shiny faces. I once hosted some adult web sites. As you may imagine, this means that I am on every possible list of people who crave the latest info on Hot Steamy Sex, Biggest Paying Casinos, Improving Cash-flow, Herbal Viagra... Nigerian functionaries want me to help them smuggle millions. Everyone wants to increase my web traffic and my penis size.

One would imagine that I, more than anyone would hate spam. One would be wrong.

Why, you ask? Why do I not tremble with rage as the flood of crap envelopes my screen? Why do I not seethe at the horrible violation of my space – the intrusion into my life of unwanted ads, scams and whatnot? Why?

In a word, perspective.

It's not that I don't have a lot of hate in me. Many people, places and things receive my ire. I hate income tax. I hate policemen who hide behind trees with radar guns rather than doing their jobs. I hate Nebraska. I hate these things and people, and many more, because currently, or in the past they have caused me very real pain, and do no good for me or anyone else. I do not hate spam. Spam annoys me. I wish it would stop, but I don't hate it.

Spam is blamed for so many evils that I am constantly amazed at the continued sense of humor shown by the people at Hormel, who have unwittingly given a name to it, and not sued anyone. Not that I particularly like mystery meat – but nobody is stuffing pounds of it under my front door. Spam killed Usenet! Spam sucks up millions of dollars of bandwidth! Spam violates me! (Now that would make for an interesting adult web site) Spam steals my valuable time! Spam ate my homework! Spam, spam, spamity spam...

Let's examine some of this drivel.

How much time does spam waste? In my case, about twenty seconds a day. In less time than I spend reading a single e-mail, I delete all my spam, and we have already established that I get a LOT of spam. And I don't use any filtering. More on that later... They say you can't judge a book by its cover, but I have no such trouble with e-mail. If it has no sender address, out it

spam, were able to access Usenet through a GUI. Usenet stinks like it does because the people who used to make it worthwhile got tired of being outnumbered and took their topics to private mail lists where moderation can mean something. Canter and Siegel were nothing special. They were, as Agent Smith would say, "the sound of inevitability." Usenet and e-mail were ripe for mass marketing, and SOME asshole had to be the first to try it. But make no mistake: Usenet was on its last legs already.

So, why do we hate spam all out of proportion to its effects? In part, because we can. If you say you hate income tax, there will be some that think you are one of those wacky militia nuts who rant about the fringe on flags and conspiratorial instructions on the back of street-signs. If you say you hate spam, everyone is right there with you. Even the people who make money off spam (or try) won't take the time out of their day to defend it.

Spam is a self-contained particle of annoyance that is extremely easy to put one's finger on. It is SO pointless that it makes the perfect straw to snap camel vertebrae with. We live in a world where the big pressures fly under the radar. If people actually took a good look at how insane it is to spend eight to ten hours in a cubicle every day, typing and staring at a little box, they would swallow their tongues and die. They avoid this death by convincing themselves they like/need the job. The biggest hassles in their lives are rationalized thoroughly. The proper holes are sealed up, and the steam must come out somewhere. So it comes out the little holes.

Why do people get blind rage when someone changes lanes in front of their car? Because their jobs suck, and AT&T screwed up their cable modem, and their crazy Auntie Penelope came to visit and won't leave, and their house has structural damage from termites, and the neighbor's kids dug up the rose bush, and to top it all off – YOU had the unmitigated gall to get in front of MY car when I'M IN A HURRY, DAMMIT!!!

It's the same thing with spam.

This all gives rise to that famous old battle cry, "There ought to be a LAW!' And of course, like most every time you hear that - no, if there's any sanity in the world, there shouldn't be a law. Laws are serious business. Every law is a restriction on freedom. A law is a necessary evil, and you better be damn sure its necessary before you call for one. Not that that stops anyone.

Not only should there not be a law, I say filters are a big waste of effort. Whether at the reader program or on the

Spam? Spam?

by Ming

goes. If I see 'Viagra' or 'casino' or 'income' it gets a quick look at the subject line, and out it goes. If it says 'Hi' or 'Hey' or 'I love you'... out it goes. I can run through this at lightning speed in a text based mailer, and almost as fast on a graphical one, once I configure it to NOT display every message that is highlighted. 99.9% of all my spam is deleted without a peek inside. The few that get by are the ones that touch my curiosity. I am developing a certain fondness for that poor Nigerian guy who can't move his millions. The Spanish Prisoner scam is 400 years old and going strong.

How much does spam really invade your inner sanctum? Really? Regular junk mail gets physically delivered to your home. Telemarketers interrupt your dinner to sell you aluminum siding. Actual walking, talking humans come to your door to beg for all manner of real and imagined charities. Spam is just pixels on a screen and is wiped away at the touch of a button. If this aspect of spam causes you more than a slight itch, then you can consider all that money you give your shrink, to be money well spent.

Wasted bandwidth? I have two words for you. Dancing Baby.

My favorite is, "Spam Killed Usenet!" This is untrue in many ways. First of all, Usenet is still there, serving up bad porn and stale warez like never before. I will admit it isn't like it was, but it wasn't spam that killed it, it was AOL. Compuserve, Prodigy, (not the band) Netcom and Earthlink. Usenet was terribly unwieldy to manage and to use. It was a horrible, clunky, nightmarish pain in the ass. I loved it. The user-hostile interface put up enough of a barrier to monkeys that for one brief shining moment, there was a world-wide forum of mostly intelligent communication, free to anyone who could figure it all out. Then the big ISPs came to the party and the whole thing caved in. The only way that spam entered into it, is that all of a sudden, people who were dumb enough to fall for the server side, spam filters rarely work as intended. If you add up the time spend configuring software, setting up rules, fielding the angry tech calls from people who can't get mail from their favorite mailing list, writing special purpose rules to work around individual problems, etc... you and your users could have used the time to delete several million junk e-mails manually. Or gone to a lot of movies. Or read the entire series of The X-Men from issue one to the present. Don't start. You will get spam, and you won't get that important e-mail you've been waiting for. You will give up, and turn off the filter eventually.

I don't have time to even get started on such do-gooder fiascos as ORBS and the Realtime Blackhole List. You'll notice that that trick didn't work. Let's just say a heavier hand has never tried to smash a gnat.

Anything you do to stop spam will be more trouble than it is worth, and in the end, it won't be effective at all. There will always be spam, because spam works. If even a tiny percentage of the Internet population falls for that crap, it will make money. And even if it doesn't directly make money, it makes a hell of a pyramid scam. How many spams have you received offering CDs full of e-mail addresses? As usual with such things, the people doing most of the scamming are the marks for most of the scams. It is almost a sort of self-acting poetic justice.

So just stop already!

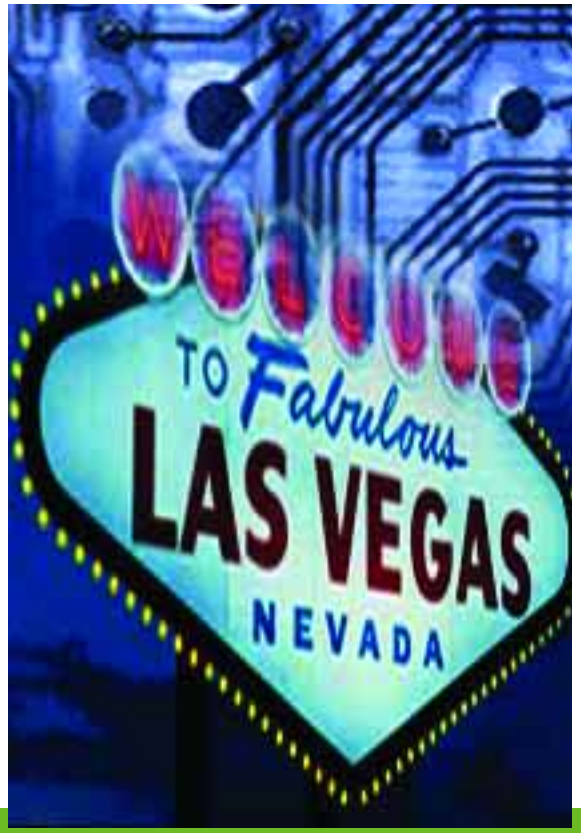
If you need a real problem, I have a whole bag of them for you. The DMCA and its siblings are taking a huge chunk of your rights and handing them to Mickey Mouse (trademark of Disney) and very few people seem to care. That's a little more important than spam. In some jurisdictions, no judge has ever refused a wire-tap request. That is also a little more disturbing than a couple 'make money fast' messages. I'm sure you can think up a few more examples for yourselves.

I'm just saying that a lot less of my time and yours would be wasted if people could realize that spam is far less of a problem than pigeon crap.

scavengerDCXhunt

The Main URL is

http://www.scavengerhunt.org/



Under the link above is “stats” page, this is key. Throughout the hunt we will be constantly updating this page. We want people to know what teams are playing and what their current point level is. I’m hoping this will make things a little more competitive. I know that there were people walking around last year that were sure they were going to win, but when all was said and done they didn’t even place in the top three. If you know you’re 50 points away from first place, you’re probably going to try and get those last 50 points before the day is up. At least that’s the theory. Oh, by the way, we’ll be keeping a hard copy record of all the points, so if you were thinking of going CTF on the site, you’d be wasting your time.

The Hunt Box. While there is no link to it now, after the hunt we are hoping this page will be packed with good stuff. Whenever we have an item or task that is marked with “Proof” it means we need picture or video evidence of completing the task or receiving an item. We’ll be setting up a box equipped with a video capture card and we’re also hoping to grab all the images people take while hunting for items. This will all be added here after the hunt so people can see all the things that people did, or teams can relive their experiences.

Speaking of teams. Above you can see a link called “teams”. We will be accepting pre-registration for the hunt, so if you want to come up with a team name and submit pictures of your team ahead of time, we’ll post it there. I think this will be good so that people can see who they’re competing against before they even get to Vegas. This should prompt Nancy Kerrigan style attacks, which is always good.

˜The Rules˜

1. Teams will consist of no more than 5 people. The team with the most points by noon on Sunday wins the hunt.

2. Items must be brought to an official Scavenger Hunt Crew member. Members will be wearing authorized badges. The points will be logged at the **Scavenger Hunt table.**

3. Only one item will be counted per team, “Proof.” in listing means videotape or photograph the action so that we know that you really did it, otherwise bring the actual item in question or talk to a crew member about where to do it? Where applicable, an audio recording may suffice.

4. 2600SLC and the Hektik crew may publish any writing, video or photo brought to us, or taken by us. We would like copies of video footage and images for our archives.

5. Bonus Items are high value endeavors that can be obtained through special hand delivered notes upon completing a task. They could be puzzles or excursions? Not all items will have bonus items. However, each item will have the same Tier 2 item tied to it, this way it’s fair.

6. The first team to find a listed or bonus item will receive the value of the item plus 5 additional points.

Applescript (in)Security in OS X

Agent OJ, Team2600

AgentOJ, a Macintosh programmer for Team2600, will be speaking on Applescript in the OS X environment, covering both attack and defense tools using Applescript. Topics covered will include: Applescript as an information gathering tool (system info, list of users, open services, etc). Applescript as an attack tool (applescript trojans, destructive scripts, exploiting scriptable applications, and a proof of concept applescript trojan). Applescript as a defense tool (log checking, locking down an OS X system, automating network security scripts, and a proof of concept applescript defense suite). General applescript security practices will also be covered.

XProbe, The Year After

Ofir Arkin, Founder, The Sys-Security Group

Xprobe, written and maintained by Fyodor Yarochkin & Ofir Arkin, is an active operating system fingerprinting tool based on Ofir Arkin's "ICMP Usage in Scanning" research project (http://www.sys-security.com). Last year at the Black hat briefings, July 2001, the first generation of Xprobe was released.

The tool's first generation (Xprobe v0.0.1) relies on a hard coded static-based logic tree. Although it has a lot of advantages (1-4 packets only, accurate, fast, efficient, etc.) the tool suffers from a major drawback - its logic is static.

At Defcon 10 we will be releasing Xprobe2, a complete re-written active operating system fingerprinting tool with a different approach to operating system fingerprinting. Xprobe2 rely on fuzzy signature matching, probabilistic guesses, multiple matches simultaneously, and a signature database.

As with the previous year– Don't miss the demonstration!

Stealthful Sniffing, Logging, and Intrusion Detection: Useful and Fun Things You Can do Without an IP Address

Mick Bauer, Upstream Solutions, Inc.

Centralized event-logging and automated intrusion detection are required tools for good network security. But what can you do to prevent your loggers and IDS probes from falling victim to the same attacks they're supposed to warn you about? As it happens, one cool thing you can do is run such systems without IP addresses. In my presentation I'll describe the benefits and drawbacks of this technique, and demonstrate how it can be used in conjunction with Snort, syslog-ng, and other standard *nix tools to build stealthful loggers and IDSes.

Bastille Linux 2.0: Six Operating Systems and Still Going!

Jay Beale, JJB Security Consulting & Training & Bastille Linux

Bastille Linux is a security tightening program that has proven capable of thwarting or containing many of the vulnerabilities discovered in operating systems. Originally written for Red Hat Linux, Bastille has now been ported to six operating systems, including HP-UX. This talk will talk about what Bastille does, what we've done to it in the last year, and what we're working on next. Most importantly, it will teach you something about hardening systems and beating worms, even if you're an old spacedog of a sysadmin.

Attacking and Securing FTP

Jay Beale, JJB Security Consulting & Training & Bastille Linux

The Unix FTP servers have been called 'the IIS of the Unix world' for their frequent and potent vulnerabilities. Each has provided remote exploits, usually at the root privilege level, on a consistent and frequent basis. WU-FTPd is the most popular Unix FTP server by far, shipping by default on most Linux distributions, and even on Solaris, and being installed most commonly on the rest of the Unix platforms. This talk will demonstrate working exploits on WU-FTPd, then show you how to configure WU-FTPd to defeat them. While the talk will use WU-FTPd as the primary example, we'll also discuss ProFTPd, the other major FTP daemon for Unix.

The Politics of Vulnerabilities

Scott S. Blake, CISSP, Vice President, Information Security, BindView Corporation

The vulnerability reporting process is rife with competing interests. Research is conducted by software vendors themselves, paid consultants, government agencies, professional and academic researchers, as well as people who make their living in other ways. Each of these groups have particular interests in the process. The vendor of the targeted software has their concerns. The public at large has an interest in the process (and its results), but it is unclear what the public should be concerned with. This talk explores vulnerability reporting from all angles, including that of the public good. Attendees will learn a rudimentary cognitive framework for understanding the powers in play in vulnerability reporting and apply that to understand the present and the future of security.

Security at Kernel Level

Philippe Biondi, Cartel Sécurité

Security is a problem of trust. Having a system that offers services to Internet and that can be trusted is very hard to achieve. Classical security models focus on the physical limit of the machine. We will see that it can be interesting to move the trust limit between user space and kernel space and that it is still possible to enforce a security policy from this trusted place. We will also see some practical aspects with a review of some implementations that exist for Linux kernels.

It is Now Safe to Compile Your Phone System

Rich Bodo, Managing Director, Open Source Telecom Corporation

The telephony industry was late to adopt open-source software and commodity protocols. The open-source

Defcon ØA Speakers and Topics

development community is rapidly correcting that problem. Everyone from enthusiasts to Fortune 500 companies are now deploying open-source telephony software, from PBX's to voice messaging systems to VoIP gateways. This lecture will focus on the practical. We'll provide demos of the major open-source telephony systems, a brief tutorial on rapid application development, and a discussion of the effect these systems will have on the future the industry. Special attention will be paid to Bayonne and other GNU projects, and their relationship to the more ambitious GNUComm and GNU Enterprise meta-projects.

Attendees should leave with an understanding of the general capabilities of the major existing open-source telephony projects and a working knowledge of basic application development with the GNU telephony subsytem.

DEF CON 10 Talk: Consumer Media Protections

Adam Bresson

Did you buy The Fast and the Furious Soundtrack only to find out you couldn' t archive the songs to MP3s on your PC? Companies including Vivendi Universal, AOL Time Warner and Sony employ different protection methods on DVDs, video games and CDs. Many consumers argue that these protections abrogate their legal rights. I'll be presenting a broad overview of these Consumer Media Protections (CMPs) and will conduct demonstrations of how to identify and bypass them. I will focus on bit-level video game, video signal and audio CMPs. Whichever side of the legal argument you fall on learn the law, learn your rights and speak-up.

Correlation and Tracking of Distributed IDS

Daniel Burroughs, Institute for Security, Technology Studies, Dartmouth College

Standard approaches to intrusion detection and response attempt to detect and prevent individual attacks. However, it is not the attack but rather the attacker against which our networks must be defended To do this, the information that is being provided by intrusion detect systems (IDS) must be gathered and then divided into its component parts such that the activity of individual attackers is made clear. By applying techniques from radar tracking, information warfare, and multi-sensor data fusion to info gathered from distributed IDS, we hope to improve the capabilities for early detection of distributed/coordinated attacks against infrastructure and the detection of the preliminary phases of distributed denial of service attacks.

Community Wireless Networks, Friend or Foe to the Telecom Industry

Ken Caruso, Co-Founder of Seattlewireless.net project

Ken will talk about different types/implementations of community wireless networks. He will also discuss why companies in the industry like, dislike and do know what to make of the community wireless movement. Most importantly he will tell you why this movement is important and what role it has promoting privacy, community owned infrastructure, and peer to peer communications

Freenet, Past, Present, and Future Direction

Ian Clarke, FreeNet Project

Freenet is a system designed to allow people to publish and read information on the Internet with reasonable anonymity for both producers and consumers of information. To achieve this, Freenet uses a totally decentralized emergent architecture. This talk will describe the interesting aspects of Freenet, the challenges we have faced, and what the future holds for the project.

The Mixminion Anonymous Remailer Protocol

Roger Dingledine, The Free Haven Project

Mixminion is a message-based anonymous remailer protocol intended to take the place of the old Mixmaster network. Mixminion provides secure single-use reply blocks (Mixmaster provides no support for replies, instead relying on the older and less secure Cypherpunk remailers), and introduces nymservers that allow users to maintain long-term pseudonyms using single-use reply blocks as a primitive. It also integrates directory servers that allow users to learn public keys and performance statistics of participating remailers. I'll cover a variety of serious anonymity issues with Mixmaster and other deployed networks and published designs, and also describe some of the many surprising anonymity risks that come from adding these new services.

SNMP Attacks/Security

DJ Sweet Sensation

Should Organizations Employ Hackers?

John L. Dodge, Steve S. Mautsatsos & Bernadette H. Schell

This DefCon10 presentation, while drawing from the study, will discuss the implications of employing hackers in the work place. The book *Hacking of America* (Greenwood, 2002) reports on the Laurentian University study of the hacker community and in particular the conference participants of DefCon8 and H2K. The study data was collected though a 20 page self-report questionnaire completed by hackers at these conferences. It was also supplemented by selected in-depth interviews. John Dodge is a Full Professor of E-Business at Laurentian University, Canada, Bernadette Schell is the Dean of Business Information Technology at the University Of Ontario Institute Of Technology (UOIT), Canada and Steve Moutsatsos is a partner with the law firm Weaver Simmons.

Mobile VPN Vulnerabilities & Solutions

Brett Eldridge, Netscreen

A real life solution to the mobile VPN problem will be presented. It uses OpenBSD on a laptop with a IPsec tunnel to a gateway. The real benefit to the audience is that potential security vulnerabilities will be discussed (e.g., sending IKE ID in the clear, allowing udp/500 to the gateway from all IP addresses, the use of Aggressive vs. ID Prot mode in Phase 1).

In addition, potential solutions to those vulnerabilities will be presented.

Web Application Brute Forcing 101 - "Enemy of the State (Mechanism)"

David Endler, Director, iDEFENSE Labs & Michael Sutton, Sr. Security Engineer, iDEFENSE Labs

This presentation focuses on the ease with which many web application Session IDs can be brute-forced, allowing an attacker to hijack a legitimate web user's online session (e.g. Slashdot, Apache, Register.com, PHPNuke, etc.). While a somewhat narrow area of web application security, the simplicity of the attacks and the prevalence of these vulnerabilities on the Internet make this an important topic. Malicious users can easily try (usually automated) combinations of well-known usernames and passwords, or indeed attempt all possible combinations of the accepted Session ID character set. However, the scope of a brute force attack can be greatly reduced when Session IDs are predictable in nature. The presentation will include an overview of the issues involved in exploiting predictable or "reverse-engineerable" Session IDs in popular web applications, including a demonstration with several real-world exploitation examples. It will conclude with a description of techniques both users and web developers can use to protect against these types of attacks.

Neuro-Linguistic Programming (NLP)

Error

This talk is primarily about psychology and relates to typical programming in no way. Neuro-Linguistic Programming is best described as new age pseudo science by some and the future of psychology to others.

Through this talk on NLP you will learn about the ability to control and otherwise manipulate as well as teaching via "knowledge encoded linguistic algorithms." You should also gain the ability to do a "cold read." You will also learn about "NLP modeling." Some should walk away with a greater understanding of human psychological patterns.

Layer 2, Routing Protocols, Router Security & Forensics

Nicolas Fischbach, Manager, IP Engineering Department, COLT Telecom & co-founder, Sécurité.Org and Sébastien Lacoste-Séris, Security Officer & Manager, IP Research & Development Department, COLT Telecom AG & co-founder, Sécurité.Org

Our talk will cover the (in)security of layer 2 protocols (CDP, xTP, HSRP, VRRP, VLANs, etc) and its consequences. We will also discuss routing protocols attacks and how to (try to) protect your infrastructure. The architecture, security, secure management and forensics of routers and switches will also be covered. This last part of the talk will be complementary to the presentation from FX of Phenoelit.

Advanced Shellcodes

FozZy, Hackadamy, Hackerz Voice Newspaper & DMPFrance

Shellcodes are tiny machine language programs designed to be injected inside a vulnerable process and executed with its privileges. They traditionally do simple actions, like execing a shell or writing to a file. They can be easily defeated by host intrusion prevention and detection systems like filesystem ACL, kernel system calls ACL, non-privileged chrooted processes, etc. Is it possible to bypass these security measures, or at least take advantage of what they permit ? In this talk FozZy will present how to design small polymorphic shellcodes downloading encrypted modules or binaries and executing them directly in memory. (ever got a shell without running /bin/sh ? ;) Trough live demos with HIDS and NIDS on, we'll see the limits of current security systems on open-source OSes.

Attacking Networked Embedded Systems

FX, Phenoelit & FtR, Phenoelit

Servers, workstations and PCs are the common targets of an average attacker, but there is much more to find in todays networks. Every device that has a processor, some memory and a network interface can become a target. Using printers and other common devices as examples, we will show how to exploit design failures and vulnerabilities and use the target as an attack platform. We will also release some tools, methods and sample code to entertain the audience and aid further vulnerability research in this area.

High Security Locks, and Access Control Products

Mr. Michael Glasser CRL, aka. Laz

The topic of the talk will be covering both high security locks, and access control products. The locks covered will be including, Medeco, Mul-T-Lock, Assa, Fichet, Concept, Miwa and others. The access control technology will cover, Proximity cards, Mag stripe cards, Biometrics, keypad technology, and others.

Questions will be answered on other topics, such as safes, standard locks, lock picking, CCTV, computer security, and other security issues.

Wolves Among Us

GOBBLES Security

GOBBLES Security members will be giving a presentation called "Wolves Among Us", which will discuss the evil motivations of certain members and organizations of the security industry, the big companies that are underqualified for security and yet reap such incredible revenue for their services, the way the media is uninformed and further intentionally writes incorrect information concerning hackers, and more. Concrete examples will be cited, and then discussion on the greater ramifications of those examples will be held.

Defcon ØA Speakers and Topics

Defcon ØA Speakers and Topics

The USA PATRIOT Act and You

Jennifer Stisa Granick, Esq., Litigation Director, Center for Internet and Society, Stanford Law School

This presentation will update attendees on changes to the law under the USA PATRIOT Act, with special emphasis on how the changes may effect political activists and the investigation and prosecution of computer crimes.

GNUNet

Christian Grothoff, Department Of Computer Sciences, Purdue University

GNUNet is an anonymous peer-to-peer networking infrastructure. GNUnet provides anonymity, confidentiality, deniability and accountability, goals that were thought to be mutually exclusive. In GNUnet, users can search for files without revealing the query to anybody. Intermediaries can not decrypt the query or the reply, but they can verify that the reply is a valid answer for the query. This allows GNUnet to deploy a trust-based accounting scheme that does not require end-to-end knowledge about transactions and that is used to limit the impact of flooding attacks.

Anonymity in GNUnet is based on the idea that it a host is anonymous if the perceived sender of the message looks sufficiently like a router. Based on this realization, GNUnet nodes can individually trade-off anonymity for efficiency without affecting the anonymity of other participants. GNUnet is written in C and licensed under the GNU Public License. GNUnet is officially part of the GNU project

Selling Out For Fun and Profit

hellNbak, NMRC

Recent events in the security industry have caused multiple groups to cry foul and claim that many so called hackers have sold out. A war of words has erupted between those crying foul and those who have apparently sold out. Most recently, Gweeds presented a talk at H2K2 that touched on many nerves when he pointed fingers at specific people in the security industry.

While the talk given by Gweeds was based mostly on made up stories and FUD he touched on some points that deserve a bit of attention. Additionally, the articles written in The Register by Thomas Greene points out that the media in general has a responsibility to verify facts -- something does not seem to be happening.

The talk presented by hellNbak will address these issues along with some of the dirty little secrets in the security industry. In general, Hackers hack for the quest of knowledge and the ability to be places that others cannot go. Based on this, Hacktivism, cyberterrorism, and selling out is a myth and until hackers are hacking for a real cause it always will be.

DC Phone Home

Aaron Higbee, Foundstone & Chris Davis, Senior Security Consultant, RedSiren

DC Phone Home (DreamCast Phone Home, a pun on the well-known film ET: The Extraterrestrial) is a project that challenges conventional enterprise security models by showing the ease by which an attack to an organization's network resources and infrastructure can be performed from an internal perspective. Simply put, once the DreamCast is deployed, it 'phones home' joining an organization's internal network with a remote network. We show that this type of attack can be performed easily with a variety of available hardware and software and in such a way that is not easily discovered by an organization's employees or security resources. Our presentation will include development descriptions and demonstrations of the attack tools that we have developed and are continuing to develop. The attack tools are comprised of a SEGA Dreamcast, a Compaq iPAQ handheld device, and a bootable x86 CD-ROM which can perform the attack using any available PC. Using open-source tools that we have ported to these platforms, we have created devices that 'phones home' over known protocols.

Covert Channels in TCP and IP Headers

Drew Hintz, guh.nu

How would you communicate securely in a country where encryption is outlawed or where key escrow is mandatory? How can you prevent the Feds from forcing you to turn over your encryption keys? Simple. Don't let your adversaries know that you're transmitting encrypted information. Using covert channels you can completely hide the fact that you're transmitting encrypted information. During this presentation we'll give an introduction to covert channels in TCP and IP headers, release a few vulnerabilities in current TCP timestamp covert channels, and demonstrate and release software that enables covert communication via TCP and IP headers.

Securing your Windows Internet Server

Humperdink, Sr. Security Engineer, Covert Systems

I will show people how to secure different Windows servers using common sense and a variety of different tools. The fundamentals can be applied to any Windows server whether it is NT 4 / 2000 / .NET as well as IIS or Exchange. I will also walk people thru many good security tools that are a must have for any Windows server. I will actually secure a server at the talk that will later be placed on the CTF network. I will announce a FTP location at my talk where all of the tools I will feature can be downloaded from.

Hardening Solaris Installs

Chris Hurley, SecurityTribe

A step by step guide to hardening a Solaris installation. Focusing primarily on Solaris 8 but with concepts that apply to all Solaris/Unix installs, attendees will learn the steps that need to be taken to lock down a Solaris installation. While recognizing the best practice of pre-deployment hardening, the concepts presented also apply to already live Solaris installations. Rather than focusing on known attacks and reacting to them, this presentation will better equip system/security administrators to proactively reduce the risk of a successful attack against their systems.

Black Ops of TCP/IP: Work NAT, Work. Good NAT. Woof

Dan Kaminsky, DoxPara Research

Communication under TCP/IP networks has become extraordinarily popular; still, there remains significant problems that as of yet have remained unsolved within its layered rules. So, lets break the rules, elegance (and possibly security) be damned. Significant new techniques and code will be unveiled to answer the following questions:

A) Instant Portscan
- Is it possible to discover instantaneously what network services have been made available, even on massive networks?

B) Guerrilla Multicast
- Is it possible to send a single packet to multiple recipients, using today.s multicast-free Internet?.

C) "NATless NAT"
- Is it possible to share a globally addressable IP address without translating private IP ranges a la NAT?
- Is it possible to allow incoming connections to an IP multiplexed in this manner?

D) NAT Deadlock Resolution
- Is it possible to establish a TCP connection between two hosts, both behind NATs?

Various interesting uses of these new packet-level primitives should be discussed, and OpenSSH will trotted out as the method of bringing some degree of security unto the resulting chaos.

Wireless Networking

Tony 'Xam' Kapela, Bruce Potter, Adam Shand

Wireless networks have seen explosive growth in the last year. Wardriving a city last July resulted in only a handful of access points. Now there are hundreds if not thousands of access points in every city in the nation. And during the same time holes have been shot in all major wireless security protocols. People deploying wireless technologies are either unaware of the risk involved or have decided the productivity gain out weighs the risk. We feel it is more of the former than the later. This presentation will discuss contemporary issues in wireless network security. While we will discuss some of the basic foundations of wireless security such as WEP, the talk will be more focused on the state of the art. The speakers all have heavy backgrounds in community wireless networking using open standards and living in hostile environments. They will draw upon their knowledge to give the audience an idea of where they can expect wireless security to go in the next year.

Stealth Data Dispersal: ICMP Moon-Bounce

Saqib A. Khan, M.S., SecurityV, Inc

This research is targeted at demonstrating that small amounts of data can be dispersed over IP based networks, utilizing the data payloads of existing protocols. Such data is expected to be kept alive on the ether until one chooses to retrieve it. The crux of the scheme is the fact that this type of data dispersal is expected to be extremely difficult to detect. Such a scheme also raises some very interesting aspects regarding using Internet traffic itself as virtual mass storage system, etc.

As an example, a specific technique created by the author, the "ICMP Moon-Bounce", will be presented that accomplishes our data dispersal goal.

Anonymous, Secure, Open Electronic Cash

Ryan Lackey, founder & CTO, HavenCo

Electronic cash has been the lynchpin of cypherpunk software goals for decades -- yet, there is no viable electronic cash system in the marketplace. We will describe the theory, applications, past attempts, politics, failures, and successes in the field. We present a specification and implementation of a new system which is secure, open, extensible, Free, and which will hopefully avoid the technical and strategy mistakes which plagued earlier systems. We will solicit developer involvement in creating applications which use this infrastructure. We hope this infrastructure is a first step toward limiting the power of governments and other oppressors vs. individuals and small groups throughout the world. It is also an example of how to provide a critical infrastructure application, in an open-source form, in the post-dotcom world, and a generally-applicable demonstration of how security hardware and software can be used in applications to win user trust.

BSD Security Fundamentals

Sean Lewis, subterrain.net

FreeBSD security fundamentals will cover some security basics as well as advanced topics on FreeBSD host and network security. Emphasis will be on hardening a FreeBSD machine from the inside-out, locking down ports, services, filesystems, network activity, etc. Some of the material presented in this talk will be BSD-agnostic, and some will apply to a UNIX environment in general. Review of several recent UNIX security vulnerabilities and valuable information on monitoring and safeguarding your system as well as your network.

Defcon ØA Speakers and Topics

Network Printers and Other Network Devices, Vulnerabilities and Fixes

LittleWolf

Like computers on large heterogeneous environments, networked printers and other peripherals have vulnerabilities that can lead to exposure of data, denial of service, and as a gateway for attacks on other systems. Yet, while many organizations seek to protect their computers, they ignore printers and other peripherals. We will discuss general attacks against printers and other peripherals, with specifics on known (and some newly discovered) vulnerabilities in several brands of printers, and propose possible solutions to keep both computers and networked peripherals from attack. The talk is technical but not microcode technical, and the audience needs only to bring their brains, though familiarity with the various printers and other peripheral devices available on the market is a plus.

Trusted Computing Platform Alliance: The Mother(board) of all Big Brothers

Lucky Green, Cypherpunks.to

The Trusted Computing Platform Alliance, which includes Intel, AMD, HP, Microsoft, and 180 additional PC platform product vendors, has been working in secrecy for 3 years to develop a chip which will begin shipping mounted on new PC motherboards starting early next year.

This tamper-resistant Trusted Platform Module (TPM) will enable operating system and application vendors to ensure that the owner of the motherboard will never again be able to copy data which the media corporations or members of the TCPA don't wish to see copied, or to utilize the TCPA's software applications without pay.

Lucky Green will explain the history of the TCPA and the alliance's efforts, identify the dominant players in the TCPA and their objectives, discuss how the members of the TCPA will be able to limit and control a user's activities by remote, show how TPM's might permit a software vendor to exploit a bug in the GNU General Public License (GPL) to defeat the GPL, and detail previously unthinkable software licensing schemes which the TCPA enables.

Lucky will then analyze the bill currently pending in the U.S. Congress (S. 2048 S.2048) that will make it illegal to sell PC hardware in the future that does not comply with the TCPA's specifications.

Introduction to Computer Viruses: Understanding the Fundamentals of How to Identify, Remove and Defend Against Hostile Code

Robert 'V1ru5' Lupo

This talk will cover:

- How different computer viruses work "boot sector, file infector, multi-parti, VBS, Java, the different OS viruses, etc..."
- How to remove different computer viruses with and without anti-virus software.
- How to defend against computer viruses and hostile code.
- Computer viruses and different operating systems.
- The future of computer viruses and hostile code.

Replacing TripWire with SNMPv3

Matthew G. Marsh, Chief Scientist, NEbraskaCERT

This talk demonstrates how to use SNMPv3 software (specifically illustrated using Net-SNMP) both with minor custom configurations and also with specialized MIBs and Agents to provide file data and file hashes on demand over secure channels. I also discuss the use of the TCP Inform Trap as a syslog style message transfer mechanism. I spend the majority of the time showing how the authentication and privacy features of SNMPv3 provide robust bi-directional security message transfers. Along the way I demonstrate how to use the split between the authentication and privacy features to provide double blind random file hashes of a managed system. Use of trigger settings to capture file changes will be discussed. I provide the example MIBs and related Agent code for general Unix platforms running Net-SNMP and where possible discuss how to get the code working on Microsoft or other platforms. Time permitting I will digress into ways to integrate these techniques into common Network Management platforms.

Anatomy of Denial of Service Mitigation Testing

Gregory S. Miles Ph.D., CISSP, IAM, aka 'DOC', CIO, Security Horizon, Inc

DOC has had the privilege of working on a project that was focused on looking at new product technologies relating to DOS and DDOS mitigation. Several commercial companies were formed who's entire focus was to find solutions to DOS and DDOS issues. Different types of detection were used in each product from pure rate analysis to statistical analysis and anomaly detection. This talk will focus on the testing methodology, testing results, lessons learned, and thoughts on the direction that this technology will be moving.

Disclosure: The Mother of All Vulnerabilities

Michael I. Morgenstern, Global InterSec, Moderator; Richard Schaeffer, National Security Agency; Marcus H. Sachs, Office of Cyber space Security; O. Sami Saydjari, SRI International; Steve Lipner, Microsoft Corp; Tom Parker, Global InterSec

Michael Morgenstern will be leading a panel comprised of several individuals from the 'other side' of Information Security. Panel highlights will include:

- An overview on vulnerability disclosure in the past
- Potential impacts of irresponsible disclosure and "new threats" (terrorism etc).
- An overview on vulnerability disclosure in the past
- Potential impacts of irresponsible disclosure and "new threats" (terrorism etc).
- What "responsible disclosure" means.
- The ideal disclosure metric, is it plausible?

- Ways in which communities can work together better.

There will be time for questions during and after the presentation

Using Filesystem Crypto and Other Approaches to Protect Your Data/Privacy on BSD and LINUX

Thomas J. Munn, CISSP & tgr2mfx

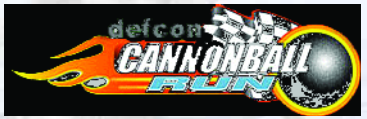
This talk will cover using the LOOP-AES package to encrypt data on a removable, USB hard disk in linux.

The presentation will focus on using encryption to protect your data, via using GNUPG, removable keychain, and a removable hard disk, to encrypt your home directory. It will focus on how to install the USB device, include a script for getting things going "automagically", and installing the LOOP-AES patch to both a stock and a custom kernel. The bsd portion of the talk will cover the use of tightvnc, ssh tunnels, 802.11 and vnconfig to keep personal data personal in a business environment.

FreeBSD Exploits & Remedies

Rich Murphey, PhD

This talk continues the review of system hardening and security management presented in the Black Hat talk, "Locking Down Your FreeBSD Install". We walk though well-known exploits for the FreeBSD 4.5 release, showing the mechanisms and effects on the system. We then discuss the way in which the vulnerability is assessed and monitored, and the ways in which the system can be hardened or access controls can be refined to reduce the risk of exposure. For each of these, we show the key features of the bundled tools for monitoring and controlling access.



Post 9/11 Privacy

John Q. Newman

Hacking .NET Server

Dr. Cyrus Peikari, CTO, VirusMD & Seth Fogie, Director of Engineering, VirusMD

Windows .NET Server is Microsoft's new contender against Linux in the server market. Scheduled for release in 2003, .NET Server (which was originally released for beta testing under the codename "Whistler") is re-engineered from the Windows 2000 Server codebase. .NET Server's survival will probably depend on how users perceive its security. Bill Gates himself realized this when he released his "Trustworthy Computing" memo in Jan. 2002. His ultimatum echoed what hackers have been saying for years: get secure or fail.

This speech will focus on the new security features in .NET Server -- and how to break them. The purpose is to identify early weaknesses while the OS is still a release candidate so that developers and network administrators can make informed decisions before deployment. This talk is technical, using live examples and some source code, but there will also be enough general information to benefit anyone interested in .NET Server security. Coverage includes weaknesses and exploits in the following areas:

- Windows Product Activation (WPA) on .NET Server
- New Encrypting File System (EFS) changes
- .NET Server Smart Card support
- Kerberos implementation
- Wireless standard implementation
- Remote Desktop Security
- Death of the Microsoft Security Partners Program (MSSP)
- Microsoft security partners full disclosure "gag rule"

An Extensible Gateway IDS

Ian Peters, Rubicon

IDSs have traditionally been seen as purely information resources, requiring human intervention in order to act on alerts. Recently, support for modifying firewall rules and killing active connections have begun to appear in IDSs, but these suffer from shortcomings. A desire has been recently expressed by many people for an active, 'Gateway' IDS (GIDS), allowing filtering and routing of traffic to be performed by a gateway computer using both traditional firewall-style rules, and also NIDS-style analysis. Rubicon was developed to supply this functionality, and more, in an extensible manner. This talk will discuss some shortcomings of current NIDS products, and hence the need for GIDS, the design and development of Rubicon, and the future for GIDS in general and Rubicon in particular.

Dmitry Sklyarov and the DMCA: 12 Months Later

William Reilly & Joe Burton

Joe Burton will discuss the events that lead to Dmitry's arrest last July in Las Vegas for violating the DMCA. Joe will also discuss the legal issues surrounding the case, the current status of the criminal proceedings in California and some thoughts on the future of the DMCA. Joe has been one of the nation's leading critics of the aggressive civil and criminal application of the DMCA's anti-circumvention provisions. Bill Reilly will discuss how non-US software developers and others can avoid falling into US digital jurisdiction by analyzing how the Federal government brought charges against Dmitry. Joe and Bill will also discuss how the DMCA, the USA Patriot Act and other recent legal developments are increasing the liability for network administrators and network security specialists.

Defcon ØA Speakers and Topics

Steganographic Trojans

Michael Rogers, Exceptional Software Strategies, Inc

As anti-virus manufacturers develop more efficient techniques for stopping an infection, potential attackers must become more cunning and resourceful in their deployment methodologies; they must create "invisible" code...but how? What are the possibilities of developing an invisible virus or Trojan?

The purpose of this talk is to explain the research we have collected, and to identify potential distribution methods, including JPEG, MPEG, and MP3, which may utilize steganographic hiding techniques to obfuscate the source code of various programs such as viruses and Trojans.

N Stage Biometric Authentication

Nate Rotschafer, MCP, University of Nebraska at Omaha

The topic will be about using biometric authentication as part of a multiple stage authentication mechanism. This discussion will explore various applications and flaws with the technology along with some of my ongoing research into a replay attack on the devices by capturing what "goes down the wire".

Next Generation Data Forensics & Linux

Thomas Rude, CISSP, aka Farmerdude, RedHat, Inc.

The field of data forensics ('computer forensics' as commonly referred to) is rapidly changing. Historically data forensics was focused on the imaging, analysis, and reporting of a stand-alone personal computer (PC) hard drive perhaps 1 gigabyte (GB) in size using DOS-based tools. However, due to a number of changes and advances in technology an evolution has begun in the field of data forensics. So where do we stand today? Increasingly, forensic examiners are faced with analyzing 'non-traditional' PCs, corporate security professionals are doubling as in-house forensic examiners and incident first responders, and critical data is residing in volatile system memory. This is the 'Next Generation of Data Forensics.' What is the Next Generation Data Forensics platform of choice? Linux. Why Linux? There are a number of key functionalities within the Linux operating system environment that make it the best platform for data forensics. Among them:

- everything, including hardware, is recognized as a file
- support for numerous filesystem types
- ability to mount a file via the 'loopback driver'
- ability to analyze a live system in a safe and minimally invasive manner
- ability to redirect standard output to input, or 'chaining'
- ability to monitor and log processes and commands
- ability to review source code for most utilities
- ability to create bootable media, including floppies and compact discs

Anonymity Services and the Law: How to Safely Provide Anonymous Technology on the Internet

Len Sassaman, The Shmoo Group

Anonymity technologies can be an essential life-saving tool for whistle blowers, human rights workers, political dissidents of oppressive regimes, and can provide a safe mechanism for the free-sharing of controversial ideas while protecting an individual's "true name" reputation. Due to the possibility of abuse of these systems, however, anonymity services are often criticized by law enforcement agencies and ISPs.

This presentation will examine some of the challenges that anonymity service providers face when their systems are used for controversial purposes, and will explore ways to mitigate the risk of operating an anonymity service.

GNU Radio

Steve Schear

Wireless communication devices have traditionally been exclusively hardware in nature. Software has augmented and is now replacing basic functional elements of radio systems. The conclusion of this process is a radio where almost all functions are performed by software. GNU Radio is a collection of software that when combined with minimal hardware, allows the construction of radios where the actual waveforms transmitted and received are defined by software. What this means is that it turns the digital modulation schemes used in today's high performance wireless devices into software problems.

Introduction to Writing Spiders and Web Agents

Michael Schrenk

You can have a lot of fun with the Internet by ditching your browser in favor of writing special purpose programs that look for— or do— very specific things on the Internet. This session will equip you with techniques to extract and interact with data from web sites without a browser, parse and filter data, follow links, deal with encryption and passwords, and manage terabytes of information. You'll also learn why writing these programs is a useful activity, and walk away with ideas and abilities to write useful spiders or web agents of your own design.

Extreme IP Backtracing

Jaeson Schultz & Lawrence Baldwin

A prudent System Administrator will review system logs. While performing this log analysis, administrators may detect nefarious activity of various types (port probes, exploit attempts, DOS/DDOS). Of course, what you receive in the system logs doesn't contain the offender's name and telephone number. Rather, most Firewalls and Intrusion Detection Systems will log an IP address, or at best, a reverse DNS lookup of the IP address. This presentation outlines several "Road-Tested" techniques for tracing IP addresses back to a responsible party. Included are many real-world examples from our research; Step-by-step traces ranging from the trivial to the impossible.

Widdershins: The Hacker Nation

Simple Nomad, NMRC

Post 9-11 knee-jerk legislation such as the U.S. Patriot Act. Calls for new legislation requiring ISPs to retain 90 days worth of email. The European Union collecting Internet communications. The continued fall of the nation state, and continued rise of the transnationals. Echelon. Carnivore.

Last year's Widdershins talk outlined a need for hackers to band together, put aside petty differences, and start thinking about what we can do as not just hacker but humans to help the war on privacy. It appears to many that the war may be over, and we seem to have lost.

This year we have to face the fact that the playing field has shifted. We can no longer stand on the sidelines. The time is now. The ability to communicate privately and securely on the Internet is rapidly dwindling. Therefore NMRC will be announcing and recommending some new software to help answer the threat to our online privacy.

Resurrecting the Scene through Local 'Hacker' Meetings

Skrooyoo, LA2600 & Grifter, SLC2600

Many people are interested in bringing their local underground community closer together by organising meetings for those in the area. While this is certainly a good idea, doing it successfully is not as simple as it sounds.

SQL Injection

Kevin Spett, SPIDynamics

SQL injection is a technique for exploiting web applications that use client-supplied data in SQL queries without stripping potentially harmful characters first. Despite being remarkably simple to protect against, there is an astonishing number of production systems connected to the Internet that are vulnerable to this type of attack. The objective of this talk is to educate the professional security community on the techniques that can be used to take advantage of a web application that is vulnerable to SQL injection, and to make clear the correct mechanisms that should be put in place to protect against SQL injection and input validation problems in general.

Making a Non-portable Computer System Portable

TechnoDragon

This will cover a range of information from wearable systems to homebrew mp3 players for cars to even network intrusion devices. Things such as user input, displays, storage and data access, along with remote / wireless access will also be covered.

Setiri: Advances in Trojan Technology

Roelof Temmingh, Technical Director &Founding Member SensePost & Haroon Meer, Technical Security Specialist, SensePost

The presentation will describe the inner workings of the Trojan "Setiri". Setiri leads a new wave of Trojan Horse technology that defeats most conventional security devices including personal firewalls, NAT, statefull inspection firewalls, IDS, proxy type firewalls and content level checking. The presentation will focus on the setting up of a bi-directional communication stream in non-conducive environments, rather than describing the features of the Trojan.

The presentation will include an online demonstration - a well-protected PC located inside a heavily protected environment will be Trojaned with Setiri. The computer will be taken over by a Controller that is situated outside of the network. At the same time network traffic will be manually inspected.

1992 ... 2002 ... 2012 ... Hacking: The Next Ten Years

Richard Thieme, Thiemeworks

Ten years ago hacking was a frontier; ten years from now, hacking will be embedded in everything we do, defined by the context in which it emerges. Real hackers will be pushing the frontiers of information networks, perception management, the wetware/dryware interface, and the exploration of our galactic neighborhood. Mastery means not only having the tools in your hands but knowing that you have them ... and using them to build the Big Picture. Richard Thieme illuminates how to do that.

Operating System Fingerprinting Library

T3 - Fred Trotter, CISSP, Verisign & threatguard.com

This is a fingerprinting library designed to bring together the fingerprinting capabilities of NMAP, QueSO and X (at least version 1). Using this library you should be able to add operating system sensitive code to your favorite Perl, Java, C or C++ code.

At the most basic level the goal of this library is to provide a mechanism so that you can add code to your programs that reads

```
if(OS.Family == Windows Family)
{ 'do something'}
if((OS.Name == Linux) && (OS.Kernel ⇢ 2.2))
{ 'do something else'}
```

At the same time the library will give you control over the execution of individual OS Fingerprint Tests. If you are interested in writing OS sensitive code or researching OS fingerprinting then this talk. (and the code) are for you. Everything will be released GPL.

The Other Side of Information Security

Wilco van Ginkel, Ubizen

Until now, the focus of Information Security within organisations was mainly technical. Organisations are becoming more and more aware of the fact that this technical side - although very important - is just one part of the total security solution. Currently, organisations are increasingly changing their focus to the organisational side of Information Security. In order to control the organisational issues of Information Security, an organisational oriented approach is

Defcon 0A Speakers and Topics

needed. Such an approach will be the subject of this talk and will give the audience an overview, ideas, references, hints & tips of this organisational side. Items to be discussed are:

- Risk Management
- Security Policies & Procedures
- Security Standards
- Security Awareness
- Security Auditing & Monitoring
- Where Organisational meets Technical

Intelligence Gathering

Vic Vandal, 504/NOLAB

This comprehensive talk covers the tools and techniques used in corporate espionage, information warfare, and private investigation. It also includes an overview of laws that one must be aware of before employing such tools and techniques.

Vic has been employed as an "InfoSec Samurai" by various government entities for the past 13 years. He was "drafted" (kicking and screaming) into the InfoSec discipline to develop proprietary security software for a specific government agency, and the rest is history. Some of the sensitive federal data he has helped protect has belonged to the CIA, DEA, Secret Service, Treasury Dept, Commerce Dept, and every other federal agency in existence. He has also done the same for the Department of Defense, Navy, Marines, and Army. He has worked extensively in every area of information security. Any more 411 and he'd have to kill you (heh).

Citrix and Terminal Services

Ian Vitek, iXsecurity

Citrix and Terminal Services are becoming very popular. Ian Vitek will speak about:

- Scanning and finding Terminal Services and Published Applications. This will include statistics of open and vulnerable servers.
- Connection to Published Applications. This can be harder than you think. Most of the servers have Published Applications. You can't just see them.
- Breaking out from the given environment and elevation of rights.
- Demonstration. The way administrators set up their Citrix servers every so often the Citrix client can't enumerate Published Applications or connect to them from Internet. Tools for enumerating and connecting to Published Applications will be released.

Linux Kernel Security with LIDS

Huagang Xie, IntruVert Networks

The talk will discuss the backgroup, current architecture and use the LIDS. And also will talk about what kind of attacks LIDS can detect and prevent and finally will get into details how to build a secure linux system with LIDS.

Building Secure Wireless Networks

zSnark

Wireless has become quite popular in network scenarios from the basic home network to the corporate LAN to the point-to-point backbone tying together offices or job sites. Wireless security and security breaches have been getting lots of press as have various vendors' multitude of proposals for cute proprietary ways to solve some of the problems in currently available products (primarily 802.11) by retrofitting them with better encryption, better authentication, tightly integrated access control, etc. What is lacking is a well-defined practical approach for the administrator in deploying (or the auditor in testing) a wireless network with currently available technology. This talk will begin with an overview of my present threat model and the details of various attacks against typical wireless networks. Following this I will give a walk-through of building a secure 802.11 LAN as well as the monitoring and auditing necessary to keep it secure. Time permitting I will also bring up a guest or two to discuss several "theoretical" attacks and other things yet to be revealed.

The Dark Tangent's Paranoia Notes

While I could talk all day, here is the short form. Investigate these things, and run them if you want. I am going to only mention the Windoze applications.

Clean up your System

- **Ad Aware** [Anti SpyWare]
  Run this after every new software install, and don't forget to get the latest SpyWare definition files. Also read the alt.security.spyware newsgroup.
  http://www.lavasoftusa.com/
- **Anti Virus** [Pick your favorite Flavor]
  Remember to get virus definition updates.
- **Eraser 5.3** [One of the best secure delete programs]
  Take time to schedule your favorite files and directories for daily wiping. *http://www.tolvanen.com/eraser/*
- **Run BHOcaptor & StartCapror**
  Use these to see what Browser Help Objects have been installed and what programs run on start up. Great way to quickly kill things you don't want to run.
  http://www.xcaptor.org/

Protect your System

- **BestCrypt** [Container Encryption]
  Enable the keyboard filter to slow down keylogging attacks. Use the hidden container in container utility for the real paranoid. I suggest creating CD ROM sized containers, format them NTFS and enable compression. When all done burn them to ROM, or use them on your CD-RW. If someone steals the CD, who cares? I have had 12Gig containers, and never had a problem with this program. *http://www.jetico.com/*
- **Personal Firewall** [Tiny, Norton Internet Security]
  Make super restrictive rules to only let your mail program talk to your mail server, etc. Set up your internet options to use the JAP proxy for http. https and FTP (See below) that way when things you don't want access the net at least your identity is hidden. I've used the NIS firewall (Back when it was called AtGuard) for years and have had no problems. Downside, it costs. *http://www.norton.com*
- **Full Drive Encryption** [PointSec]
  Full drive encryption is nice. You can loose your laptop and not worry about someone getting your porn. What's better? Using full drive encryption with Container Encryption so when you move data off your laptop it is encrypted as well. *http://www.pointsec.com*

Protect your Communication

- **Opera** [Web Browser]
  This is a fast and customizable web browser. I like it much better than Netscape or Internet Exploder. If you set up the privacy, multimedia and network options correctly you can gain some privacy. *http://www.opera.com/*
- **Eudora** [Email client]
  For Windows this is *the* email client to use. Ever heard of an Exchange virus working on Eudora?
  http://www.eudora.com/
- **PGP** [File encryption utility OpenPGP, GPG, Legacy PGP Desktop]
  While a bit of a pain to set up and get your key signed, it is worth it in the long run. Encrypt as much email as you can stand. You never know when a mail server will get busted into and your messages hovered up. Especially now with all the Patriot Act stuff going on. *http://www.gnupg.org/* or *http://www.openpgp.com/*
- **JAP** [Java Anonymous Proxy]
  Use this to create an encrypted web and ftp proxy connection to a re-mix cascade. This is better that a normal proxy in that it mixes traffic and helps defeat traffic analysis. Update to the latest jap.jar file (1.067) to add dummy traffic. Disable ActiveX, Java and Jscript to keep your true IP hidden. I want to create JAP mix cascades in the USA, but the documentation is mostly all in German, so I haven't figured how to set it up yet. Let me know if you do! *http://anon.inf.tu-dresden.de/index_en.html*

- **Use Anonymous Remailers** [Mixmaster]
  While remailers and nym servers are due for a tech update, they still work well. While the hassle factor is high, there is no real alternative after ZKS killed their Freedom product. Look into them, or attend the privacy talks at DEF CON.
- **Use SSH** [Putty, WinSSH]
  I use Challenge Response a lot, and I've found that Putty is the only windows client that handles it OK with the SSH v2 protocol. I hope other clients support that in the future.
- **Run FreeNET** [or GNUNet (un*x only), etc]
  These are networks that sit on top of the internet. They provide a more private and anonymous world of web like freesites, file sharing and chat systems. It reminds me a lot of my old BBS days, and how small that community was. You can actually make a difference and help out in this fledgling area.
  http://www.freenetproject.org or *http://www.ovmj.org/GNUnet/*

That is the short list. We are not even going to go into permission settings, options, etc. for the browsers and email clients. I hope this give you're a place to start if you never have thought about this stuff too much.

It's All a Hack

by Ming

It is very seldom, if ever, that anyone thinks up something so entirely new that it doesn't owe something to a previous invention. Isaac Newton once said, "If I have seen further, it is by standing on the shoulders of giants."[1] And that's something, coming from an ego the size of Newton's. As one might well imagine, giants are not always happy about people standing on their shoulders, and so this must often be done in a stealthy manner.

This is where hackers come in. A lot.

If hacking is the misapplication of technology, then all technology comes from hacking. And not just for large values of 'all'; I mean the whole thing. If no one used things for unintended purposes, we would still be throwing rocks at wildebeests and eating bugs with our hands.

When the Wright brothers built the first airplane that worked worth a damn, they built it largely out of bicycle parts. They didn't just get the idea all at once one day in the form of an AutoCad file... they sat around their bicycle shop, looking at bicycle parts all day, and the whole thing fell together around the parts. Smart guys, using stuff at hand in new ways. They did plenty of new work on the project. They fabricated new parts, and did some great work improving the power to weight ratio of the engine, but it was all inspired by ordinary stuff they dealt with every day.[2]

Most people are perfectly content to use the items they have around them, in just the way they were intended (with the possible exception of the screwdriver). If the available tools and prescribed methods can't do the job, then the job doesn't really need to be done, and anyway "Friends" is on in a few minutes... Wilbur and Orville were not like these people. Bicycles did not fly, and the Wrights had a problem with that. They solved the problem, and now people are willing to pay hundreds of dollars, stand in lines for hours, and get strip-searched, just for the privilege of riding on an airplane.

It sure is a good thing that the BMIAA[3] (Bicycle Manufacturers Industry Association of America) didn't try to pass a law to stop spare bicycle parts from being used in unauthorized ways.

All innovation is misapplication, and all refinement is reverse-engineering. An internal combustion engine can only work if it can blow up a carefully measured, well stirred mixture of fuel and air. The first time anyone got that to work properly, they stuck a perfume atomizer on a fuel hose. Today, we call it a carburetor, and it still isn't fundamentally different from a perfume atomizer.[4]

Fuel injection is a refinement. It is a more complex, but more controllable way to deliver that air/fuel mixture. Starting from the needed mixture already supplied by a carburetor, people worked out methods of getting that mixture at a finer level of control. Fuel injection was developed by reverse-engineering the carburetor. By studying the operation of the carburetor, researchers gained enormous understanding of the way liquids and solids mix, and developed more efficient and controllable ways to bring that about.

Fuel injection is a reverse-engineering of a hack.

It sure is a good thing the CMIAA[5] (Carburetor Manufacturing industry Association of America) didn't try to... You know where this is going.

It is common wisdom to say, "Use the right tool for the right job." But, what do you do when the right tool isn't available, or doesn't exist? And what if this tool here might do the job if it were twisted around like so... The truth is, common wisdom is often useless. Common wisdom held, up until about a hundred years ago, that tomatoes were poisonous.[6]

There are many who will tell you that is it not right to misuse anything. There are many others who will try to put you in jail for reverse engineering. Is this any way to run a civilization? Everyone seems to want new stuff. I'm sure even Jack Valenti and Michael Eisner want new stuff. Well this is how you get it: You allow (if not actively encourage) people to twist old stuff into new stuff. You convince the giants (who are often dim, and quick to anger) that it is a good thing for people to stand on their shoulders.

The fact is, intellectual property is not only a legal fiction, it is bad fiction. The plot gets lost and the dialog is not clear. The intention of intellectual property law, is to reward innovation by granting the innovator a temporary monopoly, allowing him a head start to make money on his innovation before the rest of the industry can close in. The key word is 'temporary' - in the sense of limited time, rather than in the sense of

the 60 year old Quonset huts that still house the math department at my old High School. It isn't supposed to be property, so much as a use permit. For patents and copyrights to be any stronger, or last any longer than the barest minimum necessary to fulfill their function, is a complete reversal of the whole point of IP law. That point is to encourage innovation for the good of the community, not to protect the right of a few obnoxious companies to get more obnoxious.

People getting filthy rich off their good ideas, does my heart good. People getting one extra dime by making innovation harder, makes me sick.

I'm writing this in the USA. The USA was once the biggest manufacturing power in the world. It isn't anymore. It used to be the big leader in natural resources, but that is starting to slip. We may still have more guns than anyone else, but that won't last forever. The one thing we produce on a 'world leader' scale, is innovation. We have the money to fund research, and the willingness to drop a tradition when it starts to mould. The stuff that is mass produced for the world by Japan, and Korea, and all the other manufacturing countries, is largely invented in the USA.

We, in the USA, will never maintain our lead in innovation if mindless greed makes us bite the hand that feeds us. Yet we are leading the way in software patents and anti-reverse-engineering legislation. We are passing laws against the things we need to survive. It's like holding your breath, trying to keep others from getting your oxygen. If we go down this stupid road far enough, we will end up like some of the more ancient countries of Europe, trying to earn a few crumbs pointing out to tourists how cool we used to be. We need all the hacking we can get. In the end, that's where all the money and the glory come from anyway.

There were people who were unhappy about Gutenberg reworking a wine press into a printing press. They were stupid people.[7] They wouldn't even be a footnote today, if it wasn't for Gutenberg and his movable type.

[1] From a letter to Robert Hooke, Feb 5, 1676

[2] The best book I've found on the Wrights was "Kill Devil Hill: Discovering The Secrets of the Wright Brothers"; Harry Combs (Houghton Mifflin 1979) The Wright brothers were very similar to modern hackers - totally lacking in formal education and thoroughly self taught, they brought a whole new mind set to the table.

[3] I don't really think there's a real BMIAA, and even if there was, I would like to think it wouldn't be as ridiculous as some of the other *IAAs out there.

[4] Figuring out who did this is a toughy. The history of automotive design is a big list of people accusing each other of plagiarism. The most likely suspects for this particular tidbit are Charles Dureya, who made the first American car, and Dr. Wilhelm Maybach working with Gottlieb Daimler in Germany. (And don't get me started on Sigfried Marcus - his 'Atomizer' was a good idea, but totally unrelated to the modern carburetor)

[5] There probably isn't one of these either.

[6] Most thinking people never believed this, but thinking people are often outnumbered. In 1820, a tomato grower, Col. Robert Gibben Johnson, ate a whole basket of them in front of a crowd of 2000 people. His own doctor told him he would die. He didn't.

[7] Yes, even though Gutenberg was printing bibles, many in the Catholic Church were upset, mostly because of the money they were making off their scribes copying books by hand. Soon enough however, they embraced the printing press to such a degree that they were printing indulgences in press runs of up to 200,000 - prompting Martin Luther to nail things to churches, and opening up a whole new can of worms.

It starts, as usual, at 11PM on Friday night for two games where six teams (of up to three people each) fight it out, duke it out and drink it out with questions to our answers.

YOU KNOW THE GAME. Winners win great gifts from Dark Tangent and DefCon. Losers get to drink. All players drink (⇢ 21 Only). Hacker Jeopardy is rated Heavy-R, NC-17 and one year it was nearly X. You are warned.

WHO CAN PLAY? Most people play pretty lousy... but you can still try. Submit your teams (Three people max per team) at the sign up page in the registration area. We will pick teamsout of a hat before each Game. If your team is not there and ready we move on to another draw. One year a secret government group got so drunk, they didn't answer one question right. That was humiliating. For them.

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

WHEN: Friday night at 11PM. Rounds One and Two. Saturday night 11PM Round Three, and then the Final Round, where the winners from the first three Games compete. Last Year's winners can play in Final

vendors

The Following Products and/or Services have been approved for hacker consumption

ApacheCon
www.apachecon.com

BreakPoint Books
www.breakpointbooks.com

DallasCon Wireless Security
www.dallascon.com
contact@dallascon.com
DallasCon is the world's largest hacker conference devoted exclusively to wireless security.

Dis.org Crew

FightCo
shiftre@pacbell.net
We sell the hottest imported Kung Fu movies, uncut and unedited. See for yourself whose Fu is the best...

FMA
http://freaky.staticusers.net/ • freaky@staticusers.net

Gamma Gear

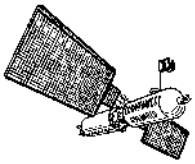
GeeKWearZ.com
www.GeeKWearZ.com
Tommy@GeeKWearz.com
GeekWearZ.com is a geek owned company that is looking out for the Geek. We develop products based upon the needs, usually the things that piss Geeks off, of Geeks. If you have ideas for custom shirtz or any other Geeky products let us know.

Greensector
www.greensector.com • info@greensector.com
Killer clothing & elite music.

Jinx Hackwear
http://www.Jinx.biz • jinx@jinx.biz
Swag for Hackers. Get the official Defcon Tshirts and merchandise here.

Legacy Studies
T-shirts featuring archaic computer systems.

Lockdown
www.lockdown.ws • administrator@lockdown.ws
Lockdown is a new hackers playground where security hacks can come to learn, practice, teach and try new stuff out. We will be hosting a root war at the end of the summer that includes a Windows 2000 Advanced Server as well as several Cisco Routers and a number of Linux boxes. Our partner site, hackerthreads.com has some great shirts and caps for sale too.



Loompanics Unlimited

www.loompanics.com • gia@loompanics.com
CYA - BBFL (Cover Your Ass - Buy Books From Loompanics)
Shoulda - Woulda - Coulda? - Turn the page - Turn to Loompanics for Inspiration

MECO

www.meco.org • ira@meco.org

Ninja Networks

www.ninjagear.net • www.ninjas.org
Ninja Networks is back again with NinjaGear, possibly the most popular and unique hacker swag available. We really take it to the limit putting stuff on shirts that your non-scene friends will never understand. Famous for our “Fuck Redhat” and “I am Jack’s Overwritten Stack Pointer” shirts, and our “My other machine is your linux box” stickers and others, our selection this year has more than doubled. Also, specifically for this year’s con, we’ve created a very limited edition (about 100) set of...well, you’ll have to come see. But they’ll probably sell out the first day (our best stuff did last year). We are also now the official sister company of Halibut Stuff, and we will be selling ALL of their gear that you know and love. Stop by the NinjaGear booth and check it out.

OpenBSD

Overdose

Root Compromise

http://www.rootcompromise.org • grifter@rootcompromise.org
Back for another year in the Vendor area, Grifter is returning with a new eye catching design. Often mistaken for the Official Defcon shirt. Grifters’ shirts are have many colors but remain true to the cold hacker look. You can go to the website for information on ordering a shirt if you don’t get a chance to get one at the con. These shirts sell out fast. There is no doubt that you’ll be seeing this design worn by many throughout the con weekend.

Sound of Knowledge

http://www.tsok.net/
Contact us for audio and video of past and present Defcon and Black Hat talks.

UnixSurplus-Bodoman

http://www.unixsurplus.com • unixsurplus@unixsurplus.com
Specializing in outfitting Geeks with cool hardware at rock bottom prices. Check us out if you ever need any Sun, SGI or Networking gear. Call us if you need Rack mount X86 servers. 408-752-0455

4 designs... collect them all!

All your wireless are belong to us.

Announcing the 1st Annual DefCon WarDriving Contest

Netstumbler.com is proud to support the DefCon 10 WarDrive.

NETSTUMBLER.COM

The Rules:

- WarDriving teams will consist of up to four members.
- Teams are responsible for providing their own equipment
- Participants must register with Chris in the Vendor Area on Friday between 10 AM and 6 PM.
- If you don't have a full team, DefCon staff will assign you to a team on Friday so you can still participate.
- Wardrive Roll Call will take place on Saturday at 12:30 (Location to be announced)
- ALL team members must be present for Roll Call.
- The WarDrive will take place on Saturday from 1 PM until 3 PM.
- All federal, state and local laws (to include traffic laws) must be obeyed.
- At the conclusion of the WarDrive, each team will submit their data to the contest judges in wi-scan/wl-scan format
- The location (latitude and longitude) of a qualifying AP must be submitted

Scoring:

Each team will be scored by the following criteria:

1 point for each Access Point (AP) found
2 additional points for an AP that has a default SSID and WEP disabled
5 Additional points for an AP that no other team finds

Team with the most points wins.

We are proud to announce that the judging will be performed by the inventor of WarDriving, Pete Shipley!

The Prize:

- There can be only one (team that is).
- The winning team will be awarded the prize.
- The prize will be announced, but it is good.
- Additional prizes have been provided by Netstumbler.com, BSDatwork.com, and Shadow Incorporated.

Special thanks to Blackwave, EMP, and Pete Shipley for their support on the WarDriving contest.

Hacking Chinatown

By Richard Thieme
1997
rthieme@thiemeworks.com
www.thiemeworks.com

"Forget it, Jake. It's Chinatown."

Those are the last words of the movie "Chinatown," just before the police lieutenant shouts orders to the crowd to clear the streets so the body of an innocent woman, murdered by the Los Angeles police, can be removed.

"Chinatown," with Jack Nicholson as Jake Gittes, is a fine film: it defines an era (the thirties in the United States) and a genre— film noir— that is a unique way to frame reality.

"Film noir" is a vision of a world corrupt to the core in which nevertheless it is still possible, as author Raymond Chandler said of the heroes of the best detective novels, to be "a man of honor. Down these mean streets a man must go who is not himself mean, who is neither tarnished nor afraid."

"Chinatown" also defines life in the virtual world— that consensual hallucination we have come to call "cyberspace." The virtual world is a simulation of the "real world." The "real world" too is a symbolic construction, a set of nested structures that— as we peel them away in the course of our lives—reveals more and more complexity and ambiguity.

The real world IS Chinatown, and computer hackers— properly understood— know this better than anyone.

There are several themes in "Chinatown."

(1) People in power are in seamless collusion. They take care of one another. They don't always play fair. And sooner or later, we discover that "we" are "they."

A veteran police detective told me this about people in power.

"There's one thing they all fear— politicians, industrialists, corporate executives— and that's exposure. They simply do not want anyone to look too closely or shine too bright a light on their activities."

“There’s no knowledge so sweet as that

I grew up in Chicago, Illinois, known for its political machine and cash-on-the-counter way of doing business. I earned money for my education working with the powerful Daley political machine. In exchange for patronage jobs— supervising playgrounds, hauling garbage— I worked with a precinct captain and alderman. My job was to do what I was told.

I paid attention to how people behaved in the real world. I learned that nothing is simple, that people act instinctively out of self-interest, and that nobody competes in the arena of real life with clean hands.

I remember sitting in a restaurant in a seedy neighborhood in Chicago, listening to a conversation in the next booth. Two dubious characters were upset that a mutual friend faced a long prison term. They looked and sounded different than the “respectable” people with whom I had grown up in an affluent part of town.

As I grew up, however, I learned how my friends’ fathers really made money. Many of their activities were disclosed in the newspaper. They distributed pornography before it was legal, manufactured and sold illegal gambling equipment, distributed vending machines and juke boxes to bars that had to take them or face the consequences. I learned that a real estate tycoon had been a bootlegger during prohibition, and the brother of the man in the penthouse upstairs had died in Miami Beach in a hail of bullets.

For me, it was an awakening: I saw that the members of the power structures in the city— business, government, the religious hierarchy, and the syndicate or mafia— were indistinguishable, a partnership that of necessity included everyone who wanted to do business. Conscious or unconscious, collusion was the price of the ticket that got you into the stadium; whether players on the field or spectators in the stands, wewere all players, one way or another.

Chicago is Chinatown, and Chinatown is the world. There is no moral high ground. We all wear masks, but under that mask is ... Chinatown.

(2) You never really know what’s going on in Chinatown.

The police in Chinatown, according to Jake Gittes, were told to do “as little as possible” because things that happened on the street were the visible consequences of strings pulled behind the scenes. If you looked too often behind the curtain— as Gittes did— you were taught a painful lesson.

We often don’t understand what we’re looking at on the Internet. As one hacker recently emailed in response to someone’s fears of a virus that did not and could not exist, “No information on the World Wide Web is any good unless you can either verify it yourself or it’s backed up by an authority you trust.”

The same is true in life.

Disinformation in the virtual world is an art. After an article I wrote for an English magazine about detective work on the Internet appeared, I received a call from a global PR firm in London. They asked if I wanted to conduct “brand defense” for them on the World Wide Web.

What is brand defense?

If one of our clients is attacked, they explained, their Internet squad goes into action. “Sleepers” (spies inserted into a community and told to wait until they receive orders) in usenet groups and listservs create distractions, invent controversies; web sites (on both sides of the question) go into high gear, using splashy graphics and clever text to distort the conversation. Persons working for the client pretend to be disinterested so they can spread propaganda.

It reminded me of the time my Democratic Party precinct captain asked if I wanted to be a precinct captain.

Are you retiring? I asked.

Of course not! he laughed. You’d be the Republican precinct captain.

Then we’d have all our bases covered.

The illusions of cyberspace are seductive. Every keystroke leaves a luminous track in the melting snow that can be seen with the equivalent of night vision goggles.

Hacking means tracking— and counter-tracking— and covering your tracks— in the virtual world. Hacking means knowing how to follow the flow of electrons to its source and understand on every level of abstraction— from source code to switches and routers to high level words and images— what is really happening.

Hackers are unwilling to do as little as possible. Hackers are need-to-know machines driven by a passion to connect disparate data into meaningful patterns. Hackers are the online detectives of the virtual world.

You don’t get to be a hacker overnight.

The devil is in the details. Real hackers get good by endless trial and error, failing into success again and again. Thomas Alva Edison, inventor of the electric light, invented a hundred filaments that didn’t work before he found one that did. He knew that every failure eliminated a possibility and brought him closer to his goal.

Listen to “Rogue Agent” set someone straight on an Internet mailing list:

which you've discovered on your own."

"You want to create hackers? Don't tell them how to do this or that. Show them how to discover it for themselves. Those who have the innate drive will dive in and learn by trial and error. Those who don't, comfortable to stay within the bounds of their safe little lives, fall by the wayside.

"There's no knowledge so sweet as that which you've discovered on your own."

In Chinatown, an unsavory character tries to stop Jake Gittes from prying by cutting his nose. He reminds Gittes that "curiosity killed the cat."

Isn't it ironic that curiosity, the defining characteristic of an intelligent organism exploring its environment, has been prohibited by folk wisdom everywhere?

The endless curiosity of hackers is regulated by a higher code that may not even have a name but which defines the human spirit at its best. The Hacker's Code is an affirmation of life itself, life that wants to know, and grow, and extend itself throughout the "space" of the universe. The hackers' refusal to accept conventional wisdom and boundaries is a way to align his energies with the life-giving passion of heretics everywhere. And these days, that's what needed to survive.

Robert Galvin, the patriarch of Motorola, maker of cell-phones and semi-conductors, says that "every significant decision that changes the direction of a company is a minority decision. Whatever is the intuitive presumption— where everyone agrees, "Yeah, that's right"— will almost surely be wrong."

Motorola succeeded by fostering an environment in which creativity thrives. The company has institutionalized an openness to heresy because they know that wisdom is always arriving at the edge of things, on the horizons of our lives, and when it first shows up— like a comet on the distant edges of the solar system -- it is faint and seen by only a few.

But those few know where to look.

Allen Hynek, an astronomer connected with the U. S. Air Force investigation of UFOs, was struck by the "strangeness" of UFO reports, the cognitive dissonance that characterizes experiences that don't fit our orthodox belief systems. He pointed out that all the old photographic plates in astronomical observatories had images of Pluto on them, but until Clyde Tombaugh discovered Pluto and said where it was, no one saw it because they didn't know where to look.

The best computer consultants live on the creative edge of things. They are path-finders, guides for those whom have always lived at the orthodox center but who find today that the center is constantly shifting, mandating that they learn new behaviors, new skills in order to be effective. In order to live on the edge.

The edge is the new center. The center of a web is wherever we are.

When I looked out over the audience at DefCon IV, the hackers' convention, I saw an assembly of the most brilliant and most unusual people I had ever seen in one room. It was exhilarating. We all felt as if we had come home. There in that room for a few hours or a few days, we did not have to explain anything. We knew who we were and what drove us in our different ways to want to connect the dots of data into meaningful patterns.

We know we build on quicksand, but building is too much fun to give up. We know we leave tracks, but going is so much more energizing than staying home. We know that curiosity can get your nose slit, but then we'll invent new ways to smell.

Computer programmers write software applications that are doomed to be as obsolete as wire recordings. The infrastructures built by our engineers are equally doomed. Whether a virtual world of digital bits or a physical world of concrete and steel, our civilization is a Big Toy that we build and use up at the same time. The fun of the game is to know that it is a game, and winning is identical with our willingness to play.

To say that when we engage with one another in cyberspace we are "Hacking Chinatown" is a way to say that asking questions is more important than finding answers. We do not expect to find final answers. But the questions must be asked. We refuse to do as little as possible because we want to KNOW.

Asking questions is how human beings create opportunities for dignity and self-transcendence; asking questions is how we are preparing ourselves to leave this island earth and enter into a trans-galactic web of life more diverse and alien than anything we have encountered.

Asking questions that uncover the truth is our way of refusing to consent to illusions and delusions, our way of insisting that we can do it better if we stay up later, collaborate with each other in networks with no names, and lose ourselves in the quest for knowledge and self-mastery.

This is how proud, lonely men and women, illuminated in the darkness by their glowing monitors, become heroes in their own dramas as they wander the twisting streets of cyberspace and their own lives.

Even in Chinatown, Jake. Even in Chinatown.

If you plan on using and hand held transceiver this year, here are some basic guidelines passed on from Evil Pete:

"You may want to add a note about not using HAM freqs unless you have HAM ticket (license). While in years past we (goons, attendees, etc.) have used "DOC 2" 147.8MHz and other HAM channels without problems, in the last year or so the FCC has started actually enforcing the rules and tracking violations. They have "busted" more people in the last 18 months then in the previous 10 years. Considering all the RF Jamming at DEF CON it is only a matter of time.

You may want to use a channel from the "Unlicensed Bands" such as CB, FRS, V-Link (Family Radio) and MUR (Multi-Use Radio Service) frequencies. Any modified Dual Band can cover any of these except for CB)."

FRS Freqs (In the 462-467Mhz Range) will have better building penetration, MIRs will work better long distances see http://www.dis.org/radio/freq/unlic.html if you want a table of freq to include:

Happy Channels: 14 Channels (FRS) maximum of .5watt .250 step

1	462.5625
2	462.5875
3	462.6125
4	462.6375
5	462.6625
6	462.6875
7	462.7125
8	467.5625
9	467.5875
10	467.6125
11	467.6375
12	467.6625
13	467.6875
14	467.7125

V-Link Channels (19) Channels

1	916.8750
2	915.8625
3	915.0000
4	914.0875
5	913.3375
6	912.0000
7	910.9125
8	910.2375
9	909.3375
10	908.5000
11	907.6625
12	907.0000
13	906.3375
14	905.6625
15	904.5000
16	904.0000
17	903.4875
18	903.0000
19	902.5000

MURs 2 Watts Max (5) Channels

1	151.820
2	151.880
3	151.940
4	154.570
5	154.600

notes

The Very UN-Official Defcon Jump

www.dcjump.com

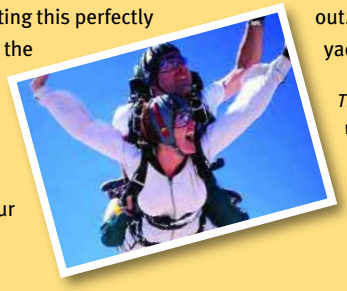
The 2nd Very Un-Official DefCon Jump is scheduled to begin the first Tuesday of Black Hat and will continue with at least one jump per day until the Monday just after the close of DefCon X. The Monday event is exclusively for the DEFCON GOONS and the EVENT STAFF. Go to the GOON ZONE link and read all about it.

Participants in The 2nd DefCon Jump must meet us promptly at 11AM. We will be meeting outside by the front doors of the Alexis.

You will be responsible for all your own costs, but transportation will be provided. This activity is not cheap, bring cash or valid plastic. You need to be at least 18 years old and be able to pass the Jump-Masters physical exam.

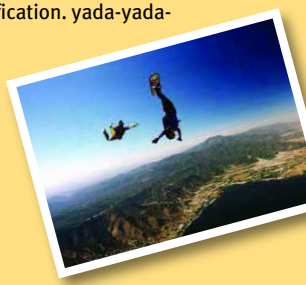
If you plan on participating in this JUMP you must E-MAIL me (vann@dcjump.com). The Jump-Master needs to know in advance how many people are going to show up so he can arrange for the planes and the instructors.

For all beginners, this JUMP is a Tandem Sky Dive from a perfectly functional aeroplane. You will be exiting this perfectly functional aeroplane at roughly 3 miles above the safety of terra firma and you will be plummeting in free-fall at roughly 120mph to 140mph. If you have already Sky Dived then you know the score. This is a life endangering event. If you participate, you do this act at your own risk of injury and/or death. If this is your first time you will be expected to to attend a short instruction class and sign off on a legal form.



The DZ we are using welcomes all FUN JUMPERS! You will need to bring your own equipment, they don't loan or rent stuff out. Bring proof of your certification. yada-yada-yada...right?

This JUMP is not affiliated with DEFCON or the DEFCON organization. This JUMP is not sanctioned by DEFCON or by the DEFCON ORGANIZATION.



CYBERETHICAL SURFIVOR *the game*

Ethics. CyberEthics. Kids. Hackers. And what about those Parents, huh?

Corporations... and let's not forget Government, too!

Ethics is that gray area between Legal and Illegal...and maybe your personal or corporate ethics are different that his or hers, or of someone from a different country or culture. Yet, we all need to live in the same "Space".

And that's the whole point of "CyberEthical Surfivor."

CyberEthical Surfivor is an Interactive Game that pits 18 brave souls on two teams against each other. The object of the Game is to be...duh... the last one standing: A true Surfivor.

How you get there is half the fun, but Da Judge and Da Time Keeper and the D'Audience will be heavily involved in who become the Surfivor!

Think:

- Originality, Creativity, Positivity and Sticking to Time
- Evolve and Develop a Consistent CyberEthical Profile and Persona That Your Team Mates, Opponents and Audience Will Support Throughout the Game.
- Strategy? Compete with your team? Want winners or losers on your side? The other side? What does the audience want?

AUDIENCE PEOPLE:
You get to play, too, by second guessing and challenging the contestants on stage. You can pick and choose who stays and who goes. Who is the most or least ethical... in your humble opinion?

We'll have roving microphones so you can get your 2-cents in! Wouldn't want our contestants to feel they're getting off easy, would we? In fact, you can make their cyberethical lives a tad miserable, if you choose.

LOSERS:
There will be 17 losers, and they will all win something, just for playing. Nothing stupendous, but hey... you lost!

SIGN UP:
Anyone can play. Kids. Spooks, Spies, Hackers, Suits. No age limits (this is a PG/PG-13 Game).

Capture the Flag

CTF

Assemble a security consulting team now! HyperGlobalMegaCorp is offering excellent IT contracts! Qualified teams must be able to administer and secure ASCII/TCP/IP services and review and patch the corporate default installation for any vulnerabilities discovered since it was created.

Teams will be presented with the latest release of HGMC's official x86 based server software. The software interoperates with a large accounting system that determines which contractor is providing which services. If a host is completely operational at the end of each polling cycle, its current operator identification is requested. The contractor matching that identification is credited.

Business hours are Friday 11:00 to 23:00, Saturday 10:00 to 22:00 and Sunday 10:00 to 14:00.

Fine Print: This is a closed network that is not connected to the Internet, so bring all your tools. While not required, it might help your team to have someone with employable skills such as navigation, RF hacking, physical security, accounting, dumpster diving and phone phreaking. If you have to worry about it in your day job, you probably have to worry about it in CTF.

The Rules

- Be the team with the largest balance on the corporate books after 28 hours to win.
- Denial of service is strictly forbidden. Intentional acts will be punished.
- All patches to open-source software must be published.
- No physical coercion. This is still a game.
- If required, the folks running the contest may step in to take the place of the press, judicial system or stock market.
- The team leaders can hire whoever they want whenever they want, but the number of teams is fixed.

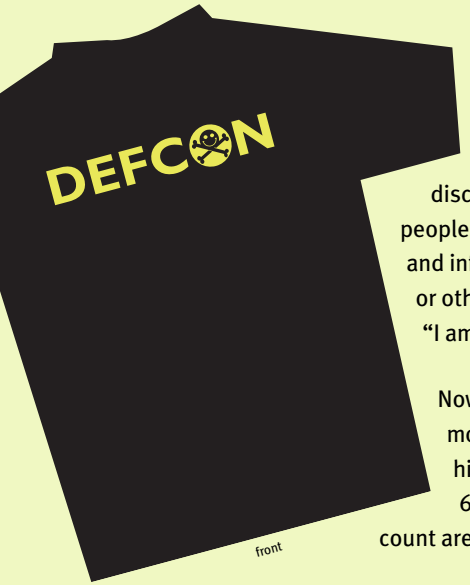
The contest is to maintain a given number of services, starting with an x86 operating system. As long as the scoreboard server sees that your services are up AND your server has your team's flag, you get points. If the server is down, you don't get points. If the server is up with somebody else's flag, they get the points. Polling is done pretty often. You can join whatever team will have you, but teams can't merge.

Yes, the CTF scoreboard is only going to running for 28 hours. There will be work for you to do between shifts if you want, or you can do the right thing & go see the rest of Defcon.

Team Name	Web Site	Team Color	Playing as
unix-monkey	unix-monkey.org	blue	Azul Security Systems
oxooffoo		green	Midori Consulting
Digital Revelation	www.digrev.org	orange	Orange Team Security
The Network Idiots		purple	Roxo Ultra Research Labs
CRMO		red	The Rouge Group
Immunix	immunix.org	white	Weiss Labs Gmbh
ChaosComputerCoderZ	cccz.tronicum.org	yellow	Amarelo Industries

8th Annual SPOT THE FED Contest:

The ever popular paranoia builder. Who **IS** that person next to you? Same Rules, Different year!



front

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 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.

Now Priest has had a leg operation, so is confined to a wheelchair while healing this month. Just look for the big guy in the Hawaiian shirt and the kid with a PRC-77 pushing him around. To space things out over the course of the show we only try to spot about 6 feds a day. 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.

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

– John Markhoff, NYT

back

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.

CYBERSCOPE NEWSLETTER

All of DEF CON ? almost fit in a Bug.

DEFCON

The Ultimate Brain Freeze.

Cool.

www.myntz.com

MYNTZ! is a registered tradmark of Vitech America. All rights reserved. Copyright Vitech America 2002.