

向古亦向武

2003

WINNER'S

wallpaper and slogan contest winners



CIRCLE

WALLPAPER

Winner: Devildust

honorable mentions: Mindshadow & David Condrey

SLOGAN CONTEST

Winner: Emoticon

Plead the First

2nd place: A.S.T.Cell

216.231.63.34 36.10778N 115.15717W 20030801
ANY QUESTIONS?

3rd: Silent

Dont hack the best ! be the best!

Thank you all for submitting and participating!

WELCOME TO

DEF CON

Several things have changed since last year. We no longer have the roof tent for speaking. As a matter of fact, we don't have the roof at all. Somehow the Fire Marshall has decided that the roof is off limits to everyone, all the time. Not sure what the hotel did to deserve that one. Sounds severe to me.

So we have played games with the space, and you'll notice the Chill Out room has changed locations to make way for speaking in its old spot.

In this program you'll know pretty much everything we do about the show. If you have a question about an event or the network, just ask at our new Information Booth. It's right up front in the vendor area, so stop by and say hey. Speaking of new stuff, we have a new 24 hour movie channel, two FM low power radio channels, better wireless coverage, a WiFi shootout, a secret contest (You have to find the clues to learn how to compete), and an expanded speaker line up! The core events of DEF CON, Capture The Flag, and the Spot the Fed contest are back. Not to be missed is tenth year anniversary production of Hacker Jeopardy.

I wish I could tell you about all the parties and stuff hapening on the side, but even I don't know everything that is going on. That is how big the con has gotten! I would like to thank everyone for making the con a success, and I am psyched about how everything is lining up to make a great con!

A special thanks goes out to all those who made the convention possible. While maybe not complete, this is a pretty close call. A special thanks to Black Beetle who has done a great job with the DEF CON website, and is in the midst of planning an all new redesign for later this year!

We want to make the con a good time for everyone in the scene, so send us your feedback!

I don't mean stuff like "Are you ever going to do a DEF CON in Tempe?" I mean stuff like what speakers you liked or didn't. What contests ran well, and which ones sucked. We are constantly tuning the show, so without your feedback it's just me in my fantasy world guessing about it!



THAT VOODOO THAT YOU DO.

by Ming

I have always had a sort of love/hate relationship with the occult. On the one hand, there is a disdain for people who believe any old crap that comes shrouded in a little mystery. I think it is sad that people can't just put a little effort into finding out the amazingly cool way that things really work, and instead, make up a whole imaginary world of magic and superstition.


On the other hand, I am totally fascinated with it all. I am blown away by the intricate rules and explanations - the systems of magic and religion that make particle physics or colloid chemistry look like a recipe for chocolate cookies. I am amazed by the appeal of all this crap, not only to people who should know better, but often to people who DO know better.

So, imagine my surprise at opening my eyes one morning, and awaking with the shocking knowledge that I am not only completely immersed in the occult on a day-to-day basis, but I

am a High Priest/Witch/Warlock/Wizard/whatever of some powerful juju!

Of course, you all know what I'm talking about by now—the mystical occult world of networking and security. And you are probably thinking “Big deal, Ray Charles could see that.” And you would be right. But exactly how right?

The comparison of various professions to religion or magic (sorry folks, I just can't bring myself to spell magic with a 'k') is an old and obvious one. Doctors, lawyers, plumbers, and many others have been compared to priests and magicians as they cloak their rather mundane jobs in mystery and mumbo-jumbo jargon, and gather in exclusive professional societies. But in all cases, it is a metaphor. Sometimes more apt than others, but still a metaphor, and any metaphor taken too far will eventually break down.



In the networking world, the metaphor of the occult doesn't break down. It has gone from a glib similarity to a one-to-one correspondence. A powerful wizard conjures a daemon to accomplish a goal. A knowledgeable programmer writes a program (often called a daemon) to accomplish a goal. The only difference is that the programmer's daemon actually accomplishes real things in concrete, objective reality. A line printer daemon gets print jobs to the printer and real ink gets on real paper.

A magician creates a circle of protection using spells and runes and all manner of ceremonial crap, while a security consultant installs a firewall using access control lists and policies and all manner of ceremonial crap. A witch throws a curse—a hacker sends a syn flood. An astrologer creates a chart of heavenly forces to foretell the future, and a network analyst creates an oftentimes equally useless network utilization chart for the same reason.

A man who will laugh himself silly at the idea of funny hat clubs like the Masons or Shriners, will swell up with pride talking about his MCSE and his CISSP or some other certifications that really aren't that much different. Some certification programs are difficult and filled with esoteric nonsense that the practitioner will never use in his daily job, and some are ridiculously easy and pointless. All of them merely add to the voodoo aura in the eyes of the uninitiated.

The networking industry, just like the religions and magic of the past, lives on fear. These days, a router isn't that much more difficult to use than a microwave oven, and anyone who can read a manual can install one, but people insist on calling in a witchdoctor to set them up. "What if I do it wrong?" Actually nothing—until you get it right. But you won't hear that from the witchdoctor. Most of the computer security industry survives by selling fear to people who have nothing to secure, just as the village witch's stock-in-trade was protection spells and potions for people with no real enemies. It is no coincidence that most of the spam mail is about penis and breast enlargement or hair loss remedies and the like—the exact things people have always got from witches and wizards.

The Internet is the perfect drop-in-replacement for the occult. And it is easier to believe in, because you can grab a handful of CAT-5 cable or put an anarchy sticker on your cable modem if you like. The machinery is right there in the open rather than on an astral plane. But don't ever make the mistake of thinking that real physical gear wards off superstition.

Networking technology is fairly young—about 25 years old, and maybe 10 years of common use, and already it has gathered up all the worst trappings of the oldest occult systems. What will it be like 10 years from now? There has always been a natural limit on the influence of the occult, and that is that it doesn't do anything. You can chant and dance naked and wave toy swords around all day long,

and it won't really accomplish anything more than getting you all hot and bothered. But networks do real work, and more and more people depend on them. Even though the power that network professionals and hackers have is largely derived from the willing ignorance of the customers, it is still a power based on real stuff that actually functions. I think it could get ugly.

So what do we do about it? That is a tough question. The obvious answer is to yell the truth from the highest mountaintops, that it is all pretty mundane stuff and not very hard to deal with, but I don't think that would work. In about 1906 there was a religious con-man named Theodore White that took millions (in 1906 money) from people who wanted to believe his line of crap. After he was convicted of fraud, and was being led to prison, his followers gathered and waved signs and cheered him. When one of the guards said, "Why don't you give those poor boobs a break... tell them you're a fake." White said, "They wouldn't believe me." And he was probably right. People like their witchdoctors and many of them have been eagerly waiting for an excuse to believe in them again. Maybe all you can really do about it is put on your robes and amulets, and just go with it.

NOT THE NEWS!

Copyright 1993 IDG Communications, Inc.

InfoWorld

July 19, 1993

SECTION: NOTES FROM THE FIELD; Pg. 98

LENGTH: 615 words

HEADLINE: DoubleSpace may not scan your hardware, but DEF CON denizens do

BYLINE: Robert X. Cringely

BODY:

DEF CON I, last week in Las Vegas, was both the strangest and the best computer event I have attended in years. The hackers, crackers, and phone phreaks' convention was shut down for a while when security at the Sands Hotel didn't like people sleeping overnight in the meeting room. And several of the hackers present (median age 17) were shaken to find their Operation Sun Devil prosecutor sitting in the back of the room (she was one of the speakers). "I'm not here to bust you," she told the very interested crowd. "Just don't commit any felonies in front of me."

I'll have to try that line at Comdex.

DOUBLE TROUBLE

There were almost too many DEF CON highlights to relate, but one of my favorite moments was when a computer security guy from Sun Microsystems (name withheld to protect this guy from himself) gave a lecture on how to break into Unix systems. "After tracking more than a thousand break-ins at Sun," he said, "I am really tired of the same old techniques. Here are some new ideas..."

The kids at Microsoft are busily working to implement an old idea to improve DoubleSpace, the compression utility in DOS 6. DoubleSpace doesn't scan your hard disk for defects and so can write data onto bad blocks, ruining your whole day. Scanning for hardware defects will be in the next version.

On a similar theme, using the DOS 6 format on a freshly low-level-formatted drive can erase some bad sector/physical defect information. DOS 5 did this, too, but nobody noticed.

Not wanting to beat too hard on Microsoft, I still have to report that the folks at PC World last week received autodemio disks of MS Publisher and Word that were contaminated with the Forms virus.

SUBOPTIMAL

Viruses were a hot topic at DEF CON, especially when Mark Ludwig, author of the Little Black Book of Computer Viruses, threatened to release a virus that could be used to password-encrypt everything on everyone's hard disks. The idea here is not to encrypt without your permission (you could choose your own password or even decide not to encrypt), but rather to use the virus as a software distribution method. What a concept!

Lord knows that distributing software on floppies has problems, too. The install program for QEMM 7.0 asks for the serial number on the installation disk, except there is no serial number on the installation disk. Use the serial number from your invoice.

On the plus side, QEMM 7.0 seems to work well, though with some oddities. Remember, the following section refers to my machine, so your mileage may vary. The Stealth feature may work fine, but since it requires a page frame to operate, it didn't make sense for me to give up 64KB to a page frame just to gain 64KB of high RAM and lose 32-bit disk access in Windows. Running Optimize did free 12KB but cut Landmark performance on my 386/25 from 33 to 28: Forget that. Still, by throwing out the DOS-UP drivers, I got 642,256 bytes free, which beats HIMEM/EMM386.

After the episode with hotel security, a few disgruntled DEF CON attendees located the hotel's PBX barrier code, isolated the Sands VAX machine, and had the administrator's password ready to go. "Let us know if they give you a hard time, and we'll take care of it," the hackers told DEF CON organizers, who wisely backed off, fearing reprisals from Guido the Kneecapper.

Not even Cringe calls were completely secure. "Did you realize as soon as you got that cell call and got up to leave the room that four scanners clicked on and a coordinated effort was put forth to find your frequency?" asked Dark Tangent, the father of DEF CON. "Hope it wasn't a sensitive call."

GRAPHIC: Picture, no caption, FRED MACK

LANGUAGE: ENGLISH

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

Basically the contest goes like this: If you see some shady MIB (Men in Black) earphone penny loafer sunglass wearing Clint Eastwood to live and die in LA type lurking about, point him out. Just get Priest's attention (or that of a Goon(tm) who can radio him) and claim out loud you think you have spotted a fed. The people around at the time will then (I bet) start to discuss the possibility of whether or not a real fed has been spotted. Once enough people have decided that a fed has been spotted, and the Identified Fed (I.F.) has had a say, and informal vote takes place, and if enough people think it's a true fed, or fed wanna-be, or other nefarious style character, you win a "I spotted the fed!" shirt, and the I.F. gets an "I am the fed!" shirt. To qualify as a fed you should have some Law Enforcement powers (Badge / Gun) or be in the DoD in some role other than off duty soldier or Marine.

What we are getting as is there are too many people with military ID angling for a shirt, so civilian contractors are not even considered!

To space things out over the course of the show we only try to spot about 8 feds a day or

so. Because there are so many feds at DEF CON this year, the only feds that count are the kind that don't want to be identified.



it is legal to perform a body cavity search. Now that is cool. Be stealth about it if you don't want people to spot you. Agents from foreign governments are welcome to trade too. If I can't be found then Major Malfunction is my appointed Proxy.

Spot the Fed Contest

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

"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





Jason D just
back from
France...



from L-R:
blackwave,
ASTCELL,
KelviN...
where the h*ll
are they?



ck3k and twinvega... feeling old yet?

Around the World...

And the winner is...
Richard W, in Bogota, Colombia... pretty hard to beat out those M-16s.

Hackers have been showing up in fiction at least since William Gibson's seminal first novel *Neuromancer* was published in 1984, where he developed characters first sketched out in his 1982 short story "Burning Chrome." Before that, characters that can be identified as hackers appeared in John Brunner's novel *Shockwave Rider* in 1975, as well as Vernor Vinge's novella *True Names*, published in 1981. Computer hackers, by contrast, have been

to themselves and people like them (as developed by Steven Levy in his brilliant book *Hackers: Heroes of the Computer Revolution*), to being a term for a certain type of technological persona and/or computer criminal. Despite this, though, the hacker is a flexible figure without a fixed definition. This, of course, is common knowledge – not just for the people reading this but for the general public as well, the term 'hacker' having become in the media a

STREET LEVELS HACKERS in FICTION

"'The 'real' is now defined in terms of the media in which it moves.'"

– Neville Wakefield on postmodernism

"Since hackers are reluctant revolutionaries, the full implications of their utopia are not always apparent. So in order to see the direction that hacker ideology points toward, we have to turn to fiction."

– Jon-K Adams, from "Hacker Ideology (aka Hacking Freedom) in Recent Science Fiction Novels (1998

showing up in real life since the advent of the computer in the 1950s, (and probably before that.) Steven Levy traces the term back to 1958 or so at M.I.T., and it is also used in an eminently serious nonfiction book printed in 1976, *Crime by Computer*, by Donn. B. Parker. Interestingly, Parker, although he concentrates mostly on the type of computer crimes that were most prevalent at the time, usually embezzling from banking systems (including the round-down fraud that was portrayed twenty years later in the movie *Hackers*), uses the term 'hacker' only to refer to "systems hackers:" "expert perpetrators" that are usually "students so entranced and challenged with the campus computer systems that they forgo food, sleep, shaving, and haircuts." (Certainly, that stereotype has not persisted.)

The term "hacker" itself is loaded, then, with connotations and definitions that have evolved rapidly in the last twenty years – from being a term used primarily by people who were talented with electronics and math, inventive and creative to refer

catchall for computer crime whether creative or not. A little-explored question, however, is what role fiction – and slightly later, the movies – played and plays in determining how the public sees and defines hackers. Are the well-known stories that feature hackers – *Neuromancer*, *Snow Crash*, the stories in the now out-of-print collection *Hackers – realistic?* Are movies, like *Hackers*, *Sneakers*, *War Games*? Or rather, do these fictional sources have an influence on reality? Are the ways that people – the public, the media, politicians, lawmakers: in other words, the people that determine what is thought of as 'real' – see hackers unduly influenced by a handful of cyberpunk novels published from the mid-1980s to the mid-1990s? What are the differences between fictional portrayals of hackers (such as in the movie *Hackers*, or the novel *Snow Crash*) and "the real thing," like the people around you now, or the hacker movement of the 1980s that was popularized by Bruce Sterling in *The Hacker Crackdown*, or Kevin Mitnick (who Katie Hafner and John Markoff seem to be secretly terrified of in their bestselling 1991

book Cyberpunk), or more problematically, any of the hundreds of people who both created technology and “made it work” – like Steve Wozniak, most famously – such as Levy celebrates?

“Bobby was a cowboy. Bobby was a cracksman, a burglar, casing mankind’s extended electronic nervous system, rustling data and credit in the crowded matrix, monochrome nospaces where the only stars are dense concentrations of information” (“Burning Chrome” 3-4).

Neuromancer arguably didn’t set out to define computer hackers. However, in this, Gibson’s most famous novel as well as his first, we are introduced not only to the concept of cyberspace but also to Case, a console “cowboy” and the uncertain protagonist of the story. Case is, I believe, portrayed as a hacker (or perhaps what would later be known as a cracker); he is talented with computers, criminally involved with them, and young. “At twenty-two, he’d been a cowboy, a rustler, one of the best in the Sprawl.... He’d operated on an almost permanent adrenaline high, a byproduct of youth and proficiency.” Yet Case, like Bobby in “Burning Chrome,” “jacks in” quickly and gracefully with no show of the kind of time-intensive searching and system knowledge breaking security takes – hardly surprising, given that the internet was hardly a household word in 1984. Snow Crash, in contrast, published eight years later, gave us Hiro Protagonist, a more accurate and perpetually nervous character who loved motorcycles and knew how to program. Both Case and Hiro have an innate need to be in cyberspace, both qualify as postmodern subjects par excellence, both manipulate information in an environment where information is all-powerful, and both live in an urban dystopic world that is probably immediately

familiar to anyone who grew up in the 1980s and watched Blade Runner. Yet I believe that Stephenson in Snow Crash attempts a type of redefinition of the term hacker from meaning a figure like Case to in a way back to what it once was: from a narrow category and a (usually, by 1992) pejorative term to something that includes not just anyone who works with computers and programs in a creative way (from a programmer for the Feds, Y.T.’s mom, to Hiro himself) but also, for instance, neurolinguistic hackers, exemplified in the story by the ancient Sumerian god Enki.

Both Neuromancer and Snow Crash sold well; in between their publication several less well known short stories came out featuring hackers and ethical hacking, such as “Blood Sisters” by Greg Egan. However, since then, aside from Stevenson’s other books and a handful of other novels, the fictional character of the hacker as complex figure and protagonist has faded along with cyberpunk itself, although hackers continue to be portrayed in the movies. But in between the two poles of these still-influential novels lies a certain definition of a hacker, someone who is similar in many ways to the ‘real thing’ but who is also ‘cooler’ and ultimately wields more informational power than has yet been demonstrated possible in real life, something that perhaps contributes to the public’s fear of hackers and the fear-mongering shown in both nonfiction and the legal realm.

“The figure of the hacker, at least since the movie WarGames, has been the source of a great deal of anxiety in contemporary culture.” – Douglas Thomas, Hacker Culture

Do fiction and reality help to shape each other, and do they, by their influence, in turn help to make each other more popular? As has been discussed at DefCon and elsewhere, laws concerning hacking

and related issues have in the last few years taken a decided turn for the worse. Movies have in this same period moved away from the mid-1990s phenomenon of portraying hackers as essentially innocent, righteous yet rebellious teenagers to a more “dark side” approach. And although the question of the degree of connection between these is unanswered, there is certainly a connection there, between public interest in hackers and their concurrent popular fictional portrayals. The life of Kevin Mitnick, for instance is instructive. He caught the public imagination so strongly – four books, two movies, and hundreds of articles later – that by himself he illustrates the ill-understood phenomenon that occurred between the mid 1980s to mid 1990s – a focus and romance with hackers not only in the news, conferences, legislation and bombastic nonfiction accounts but also in Hollywood movies and fiction. The idea of the hacker – not actual hacking itself, or even the actual hackers, but the idea – hacker as romantic outlaw hero, or as fear-engendering (and firewall selling) figure – sold and sold well in the popular media, and continues to both sell and be re-created to the present day. Perhaps when someone is presented as a hacker, that is, the public thinks about those tattered science fiction novels on the shelf, or, just maybe – Matrix 2. Now if only we all had the bodies and black vinyl to match.

For citations and a list of novels, stories and books featuring hackers, as well as nonfiction books about them, see: <http://www.brassrat.net/phoebelhackers.html>

DE XI Scavenger Hunt

the lowdown

Welcome Back to Defcon, and thanks for reading about the Scavenger Hunt. It's been a year and we're gearing up to once again catch Las Vegas with its pants down. The hunt will again be brought to you by the good folks of Utah, more specifically rootcompromise.org and 2600SLC. We had so much fun last year; we just knew we had to do it again.

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

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

stats

The stats will be back this year but with less glitches we assure you. The stats will be projected onto the wall of the Vendor Area in an attempt to drive more fierce competition. When we put the stats up Sunday at Defcon 10 there were two teams far in the lead and a few stragglers towards the bottom. We had someone walk by; notice the points it would take to get 3rd place, grab a list and go. He took 3rd and split the prizes amongst himself. So keep watching the wall, it might be easy for you to place.

Teams

On the Main Page of the hunt website there is a link that says "Teams". This is where you can feature your team after the con, to let others know you competed in the hunt. Send your team name and members handles to grifter@defcon.org to get your team posted here. We encourage you to send photos of team members too. They will also be posted.

Hunt Day

We will be collecting photos and video of items found and tasks completed for posterity. It'll be a nice way to remember the hunt, and you can laugh at all of the items from years past. Any time an item has the word "Proof" next to it means that the hunt staff will require a picture or video of the task or item being found or completed. You can also complete tasks in front of the Hunt Staff at the Scavenger Hunt table in the Vendor Area. This is also encouraged since it makes the vendor area a little more exciting and is a good time for the staff.

Now on to...

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 Staff 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 Scavenger Hunt Staff member about where to do it? Where applicable, an audio recording may suffice.
 4. rootcompromise.org and 2600SLC 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? Staff can create bonus items and their designated point values as they see fit although they must be approved by Grifter, dedhed, or kampf.
 6. The first team to find a listed or bonus item will receive the value of the item plus 5 additional points.
 7. Points may only be granted by a member of the Scavenger Hunt Staff. The Goons, while great guys/gals are not hunt staff and can not give you points for anything, at all, so forget it. Do not attempt to ask any Goons for points. There are three Goons that are Hunt Staff. Grifter, dedhed, and kampf. If anyone other than these three individuals says they can get you points for the hunt for something, you are going to look pretty silly trying to convince the Hunt Staff to give said points to you.
- Well, that should pretty much cover it. We hope to have a great hunt this year and hope to have some great teams competing. So head over to the Vendor Area and pick up a hunt list first thing Friday morning and get started. The hunt is a great way to enjoy Defcon and Las Vegas, and make some great memories as well. Hope you like what we've done, and hope to see you competing.

- Grifter

Scavenger Hunt

organized by 2600SLC and Rootcompromise.org

What is WarDriving?

by Chris Hurley, aka Roamer

In order to start WarDriving you first need to understand what it is...and what it isn't. According to Pete Shipley, the inventor of WarDriving, it is the search for and mapping of wireless Local Area Networks (LANs). The Church of WiFi's Blackwave clarifies this somewhat, stating that WarDriving is the benign act of locating and logging wireless access points (APs) while in motion. In short, WarDriving is the act of moving around a certain area, mapping the population of wireless access points, for statistical purposes and to raise awareness of the security problems associated with these types of networks. WarDriving is NOT connecting to or in any way utilizing the resources of any access point that is discovered without prior authorization of the owner. Lastly, for those with spell checkers, WarDriving is one word, not two; feel free to add it to your local spell checker.

Getting started

Before you decide to WarDrive it would be advisable to check out online resources such as <http://forums.netstumbler.com> and <http://kismetwireless.net/forum.php> to see what issues other WarDrivers are facing. This will allow you to determine if this is something you are interested in pursuing. If it is, you will need to get some equipment.

Equipment

There are a couple of different configurations that can be used in order to WarDrive: the laptop configuration and the handheld configuration. The laptop configuration requires a laptop computer and a PCMCIA wireless card (or a USB Client – which is generally a PCMCIA->USB Adapter for that card). The other requirement is a portable Global Positioning System (GPS) unit capable of National Marine Electronics Association (NMEA) output with data cable to interface with your laptop. Optionally, to be most effective you will need an external antenna, a pigtail (generally an antenna adapter from the antenna to the card – i.e. N-type Connector to MC) to connect the antenna to your card (some cards support more than one external antenna at any one time).

The handheld configuration requires a handheld computer (i.e. HP iPAQ), the appropriate sleeve (CF or PCMCIA) and a wireless card with the matching form factor (CF or PCMCIA). To improve results you will also need an external antenna, a pigtail to connect the antenna to your card, and a GPS capable of

NMEA output with data cable to interface with your laptop. You may also need a null modem cable in order to connect the serial interface on the GPS cable to your handheld input cable. The cost of an effective WarDriving setup can run from a few hundred dollars well into the thousands.

Antennae

Generally WarDrivers use a directional, or yagi, antenna or an omni directional, or omni, antenna. Depending on what you want to accomplish, you will need to determine which type best suits your purposes. A yagi is often best suited for when the location of the access point is known and the antenna can be trained on it. An omni is generally better for driving and detecting access points in all directions.

Software

There are several different wireless scanning programs. Some are freeware others are commercial products. A pretty extensive list can be found at <http://www.networkintrusion.co.uk/wireless.htm>. The most popular are Netstumbler (Windows) and Kismet (Linux). Netstumbler uses an active scanning method where it sends out a beacon request and any AP that is configured to do so will respond with to this beacon request. Kismet uses a passive scanning technique where the wireless card is placed in promiscuous (or monitor) mode and identifies any APs that are generating any traffic within range of the wireless card. This means that Kismet will detect APs that are "cloaked."

Wireless Cards

Before purchasing a wireless card you should determine the software and configuration you plan to use. Netstumbler offers the easiest configuration for cards based on the hermes chipset (i.e. Orinoco cards). Some Prism2 based cards (i.e. Linksys) will also work with Netstumbler (using NDIS, generally on Windows XP). A complete list of supported cards is provided in the Netstumbler README file included with the Netstumbler download (<http://www.netstumbler.com/download.php>).

Kismet works with both Prism2 and Hermes based cards, however most Linux distributions require kernel and driver patch modifications and recompiles in order for Hermes based cards to enter monitor mode as required by Kismet.

A complete listing of cards supported by Kismet can be found at <http://www.kismetwireless.net/documentation.shtml>.

Mapping

Most WarDrivers like to generate maps that depict the location of the access points they have discovered. Windows users commonly utilize Microsoft MapPoint 2002 and Stumbverter (<http://www.sonar-security.net>) created by Mother. MapPoint is a commercial product that costs about \$200.00 (available from <http://www.microsoft.com>). GPSTMap for Linux is a freeware product that accomplishes similar results. Additionally, there are online mapservers that allow WarDrivers to upload their data and generate maps online. Two of the more widely used are WiGLE (<http://www.wigle.net>) and Wi-Fi Maps (<http://www.wifimaps.com>).

Legality

According to the FBI, "it's not illegal to scan, but once a theft of service, denial of service, or theft of information occurs, then it becomes a federal violation through 18USC 1030. The FBI does not have a website with this type of information. You either need to pose the question to us or a cyber crime attorney (or our US attorney's office)"

Enjoy

WarDriving can be a fun and exciting hobby. There are several online communities devoted to WarDriving. The Netstumbler and Kismet forums provide the opportunity to interact online with other WarDrivers and exchange ideas. The WorldWide WarDrive (<http://www.worldwidewardrive.org>) gives WarDrivers an opportunity to coordinate WarDrives and meet in their local areas. Additionally, there are multiple Wireless User Groups around that world where ideas and experiences can be exchanged.



GENERAL

The DefCon 11 WarDriving Contest will be a tournament style contest this year.

Teams:

- There will be a maximum of 12 teams, each with a maximum of 5 members.
- Assuming there are enough people that want to participate, all teams will be full; i.e. no teams of 1, no teams of 3 etc.
- Teams are responsible for providing their own equipment.

TIMELINE

Friday • August 1st 2003

- 1000 - CHECK-IN (VENDOR AREA)
- 1200 - CHECK-IN is closed
- 1400 - The first round; Each team has two hours to drive.
- 1800 - posting of teams that have advanced to the final round

Saturday • August 2nd 2003

- 1200 - The final round drive will begin

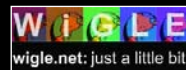
RULES

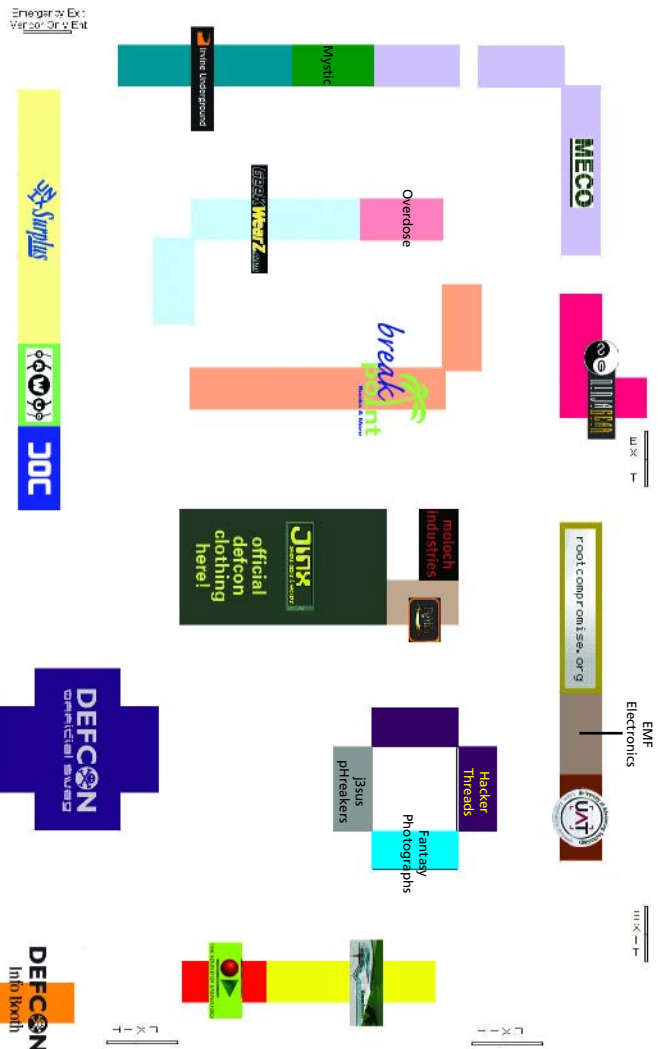
See the website <http://www.worldwidewardrive.org> for complete information or speak with the staff in the vendor area.

DefCon 11 WarDriving Contest Staff Members

- Chris: Lord of the Wasteland
- blackwave: Destroyer of all that is stupid.
- FReCKLeS: Great Sister of the FreckleHood.
- FAWCR: Crowd Control & General Master of the Beat Down.
- Russ: Overall logistical master and Sr. Staff Liaison.
- c0nv3r9: Mastah of Scoring
- Pete Shipley: Media Relations Guru

sponsors





**Bay Area Wireless Users Group
(BAWUG)**

www.bawug.org

Breakpoint Books

www.breakpointbooks.com

DefCon Swag

www.defcon.org

Dis.Org Crew

www.dis.org

EMF Electronics

Fantasy Photographs

www.fantasypictures.com

Fight Co

www.fightco.com

GeekWearz

www.geekwearz.com

Hacker Threads

Irvine Underground

www.irvineunderground.org

Jesus phreakers

jinx HackWear

www.jinxhackwear.com

MECO

www.meco.org

Mystic

Ninja Networks

www.ninjabgear.net • www.ninjas.org

Overdose

Root Compromise

www.rootcompromise.org

Greensector

www.greensector.com

Sound of Knowledge

www.tsok.net

tommEE Pickles

www.moloch.org

University of Advancing Technology

<http://www.uat.edu/>

Unix Surplus

www.unixsurplus.com

THE OFFICIAL DEFCON COFFEE WARS

"i cAn qUiT AnytImE I wAnt!"

It's that time of year again!

Attention: The fourth annual Coffee Wars will be on Friday, August 1st, at approximately 1000. I say approximately, because we don't start until the staff have fulfilled their own coffee intake requirements. This is for your own safety. Under-cafeinated judges = maimed contestants.

Time to renew the time-honored hobby of teeth-grinding, hypertension and general caffeinated insanity. As luck would have it, it's also getting very close to the next Defcon. And with Defcon comes The Defcon Coffee Wars!

We are now in our Fourth hyper-caffeinated year and we are now an Official Defcon Event. (Thanks to DT and crew for bestowing upon us this great honor. Check's in the mail. Love ya, babe. Mean it.)

Anyway, now's the time when you have an All-Inclusive Divine Excuse to

unashamedly mingle with your own kind without having to shroud your activities under the shadow of the Evil Corporate Coffee Empire! Yes, now we caffeine fiends can gather without shame!

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

You think you got what it takes? Then we'll take what you got! Bring your best beans and put 'em up for judgment by our over-qualified, over-caffeinated, (and over-rated) Coffee Wars judges and contestant panel! We keep hearing that someone else's beans are the best. Now it's time to prove it bean-to-bean!



All are welcome (unless we really, really don't like you). Bring your best java. You may bring a maximum of two entries. There are no guarantees we will get to both, but we probably will. Just make sure you note which one you want tested up first.

We (and by we I mean the Brewing Nazi, Shrdlu), will cook up your coffee, and all who enter are welcome to rate the brew. A form will be provided for each coffee, with several categories. Each category will be a 1-10 scale, with 10 being the Holy God Of Java, and 1 being Starbucks. Scores are averaged (high and low thrown out, traditionally 5 judging sheet minimum are required for a winning coffee to be considered).

The scoring fields....

- Aroma
- Flavor
- Strength
- Bang for your Buck
- Overall

Bang for your Buck is described as the following (the others should be self explanatory): Each entry shall have its price per pound listed, and as such, the masses shall determine if this coffee is indeed worth its price tag.

Other than that, there's not much to it. Enjoy yourselves, get wired, and may the best brew win.

Failing that, may the highest bribe to the judges win.

And of course, what Coffee Wars is complete without the consequences of your rule-breaking?

Rules, Things That Piss Us Off, and Jay's Firearms Collection
Golden Rule of the Coffee Wars: No decaf. No flavored coffee. No exceptions.

Offense: What you have brought that we don't like.

Punishment: What Jay and his guns will do to you.

Offense	Punishment
Store Brand Coffee	Lose one kneecap.
Flavored Coffee	Lose two kneecaps.
Starbucks	Lose both kneecaps, come back after injuries have healed. Lose both knees again.
Decaf	Please leave contact info for next of kin.
Flavored Decaf	Please leave home addresses for all known relatives.

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

DEFCON RADIO

Tune in to 93.7FM

0000 - 0100
0100 - 0200
0200 - 0300
0300 - 0400
0400 - 0500
0500 - 0600
0600 - 0700
0700 - 0800
0800 - 0900
0900 - 1000
1000 - 1100
1100 - 1200
1200 - 1300
1300 - 1400
1400 - 1500
1500 - 1600
1600 - 1700
1700 - 1800
1800 - 1900
1900 - 2000
2000 - 2100
2100 - 2200
2200 - 2300
2300 - 0000

Off Air

Can Hackers
Dance?

Phreak Fest

Black & White Ball
DJ's or DMZ DJ
content

Morning Reggae & Trance

Hippies gotta Hack Greatful Dead ...

Tear down the
(fire) Wall Pink
Floyd Finale

Big Iron Rock

Core Dump Listener Requests

Off Air

Not all
Hackers are
Goth

Phreak Fest

Black & White
Ball DJ's or DMZ
DJ content

<http://defcon.dmzs.com/>

Watch the web site for information on listening & participating with DCR
while @ the con or look for DMZ or any of the DMZS crew to get your comments or thoughts broadcast!

HACKER GENERATIONS

by
Richard Thieme



Richard Thieme
(rthieme@thiemeworks.com)
speaks writes and consults about
life on the edge, creativity and
innovation, and the
human dimensions
of technology.

First, the meaning of hacker.

The word originally meant an inventive type, someone creative and unconventional, usually involved in a technical feat of legerdemain, a person who saw doors where others saw walls or built bridges that others thought were planks on which to walk into shark-filled seas. Hackers were alive with the spirit of Loki or Coyote or the Trickster, moving with stealth across boundaries, often spurning conventional ways of thinking and behaving. Hackers see deeply into the arbitrariness of structures, how form and content are assembled in subjective and often random ways and therefore how they can be defeated or subverted. They see atoms where others see a seeming solid, and they know that atoms are approximations of energies, abstractions, mathematical constructions. At the top level, they see the skull behind the grin, the unspoken or unacknowledged but shared assumptions of a fallible humanity. That's why, as in Zen monasteries, where mountains are mountains and then they are not mountains and then they are mountains again, hacker lofts are filled with bursts of loud spontaneous laughter.

Then the playful creative things they did in the protected space of their mainframe heaven, a playfulness fueled by the passion to know, to solve puzzles, outwit adversaries, never be bested or excluded by arbitrary fences, never be rendered powerless, those actions began to be designated acts of criminal intent.. That happened when the space inside the mainframes was extended through distributed networks and ported to the rest of the world

where things are assumed to be what they seem. A psychic space designed to be open, more or less, for trusted communities to inhabit, became a general platform of communication and commerce and security became a concern and an add-on. Legal distinctions which seemed to have been obliterated by new technologies and a romantic fanciful view of cyberspace à la Perry Barlow were reformulated for the new not-so-much cyberspace as cyborgspace where everyone was coming to live. Technologies are first astonishing, then grafted onto prior technologies, then integrated so deeply they are constitutive of new ways of seeing and acting, which is when they become invisible.

A small group, a subset of real hackers, mobile crews who merely entered and looked around or pilfered unsecured information, became the definition the media and then everybody else used for the word "hacker." A hacker became a criminal, usually defined as a burglar or vandal, and the marks of hacking were the same as breaking and entering, spray painting graffiti on web site walls rather than brick, stealing passwords or credit card numbers.

At first real hackers tried to take back the word but once a word is lost, the war is lost. "Hacker" now means for most people a garden variety of online miscreant and words suggested as substitutes like technophile just don't have the same juice.

So let's use the word hacker here to mean what we know we mean because no one has invented a better word. We don't mean script kiddies, vandals, or petty thieves. We mean men and women who do original creative work and play at the tip of the bell curve, not in the hump, we mean the best and brightest who cobble together new images of possibility and

announce them to the world. Original thinkers. Meme makers. Artists of pixels and empty spaces.

Second, the meaning of "hacker generations."

In a speech at the end of his two terms as president, Dwight Eisenhower coined the phrase "military-industrial complex" to warn of the consequences of a growing seamless collusion between the state and the private sector. He warned of a changing approach to scientific research which in effect meant that military and government contracts were let to universities and corporations, redefining not only the direction of research but what was thinkable or respectable in the scientific world. At the same time, a "closed world" as Paul N. Edwards phrased it in his book of the same name, was evolving, an enclosed psychic landscape formed by our increasingly symbiotic interaction with the symbol-manipulating and identity-altering space of distributed computing, a space that emerged after World War II and came to dominate military and then societal thinking.

Eisenhower and Edwards were in a way describing the same event, the emergence of a massive state-centric collaboration that redefined our psychic landscape. After half a century Eisenhower is more obviously speaking of the military-industrial-educational-entertainment-and-media establishment that is the water in which we swim, a tangled inescapable mesh of collusion and self-interest that defines our global economic and political landscape.

The movie calls it The Matrix. The Matrix issues from the fusion of cyborg space and the economic and political engines that drive it, a simulated world in which the management of perception is the

cornerstone of war-and-peace (in the Matrix, war is peace and peace is war, as Orwell foretold). The battlespace is as perhaps it always has been the mind of society but the digital world has raised the game to a higher level. The game is multidimensional, multi-valent, played in string space. The manipulation of symbols through electronic means, a process which began with speech and writing and was then engineered through tools of literacy and printing is the currency of the closed world of our CyborgSpace and the military-industrial engines that power it.

This Matrix then was created through the forties, fifties, sixties, and seventies, often invisible to the hackers who lived in and breathed it. The "hackers" noticed by the panoptic eye of the media and elevated to niche celebrity status were and always have been creatures of the Matrix. The generations before them were military, government, corporate and think-tank people who built the machinery and its webbed spaces.

So I mean by the First Generation of Hackers, this much later generation of hackers that emerged in the eighties and nineties when the internet became an event and they were designated the First Hacker Generation, the ones who invented Def Con and all its spin-offs, who identified with garage-level hacking instead of the work of prior generations that made it possible.

Marshall McLuhan saw clearly the nature and consequences of electronic media but it was not television, his favorite example, so much as the internet that provided illustrations for his text. Only when the Internet had evolved in the military-industrial complex and moved through

incarnations like Arpanet and Milnet into the public spaces of our society did people began to understand what he was saying.

Young people who became conscious as the Internet became public discovered a Big Toy of extraordinary proportions. The growing availability of cheap ubiquitous home computers became their platform and when they were plugged into one another, the machines and their cyborg riders fused. They co-created the dot com boom and the public net, and made necessary the "security space" perceived as essential today to a functional society. All day and all night like Bedouin they roamed the network where they would, hidden by sand dunes that changed shape and size overnight in the desert winds. That generation of hackers inhabited Def Con in the "good old days," the early nineties, and the other cons. They shaped the perception as well as the reality of the public Internet as their many antecedents at MIT, NSA, DOD and all the other three-letter agencies co-created the Matrix.

So I mean by the First Generation of Hackers that extended or distributed network of passionate obsessive and daring young coders who gave as much as they got, invented new ways of sending text, images, sounds, and looked for wormholes that let them cross through the non-space of the network and bypass conventional routes. They constituted an online meritocracy in which they bootstrapped themselves into surrogate families and learned together by trial and error, becoming a model of self-directed corporate networked learning. They created a large-scale interactive system, self-regulating and self-organizing, flexible, adaptive,

and unpredictable, the very essence of a cybernetic system.

Then the Second Generation came along. They had not co-created the network so much as found it around them as they became conscious. Just a few years younger, they inherited the network created by their "elders." The network was assumed and socialized them to how they should think and act. Video games were there when they learned how to play. Web sites instead of bulletin boards with everything they needed to know were everywhere. The way a prior generation was surrounded by books or television and became readers and somnambulist watchers, the Second Generation was immersed in the network and became surfers. But unlike the First Generation which knew their own edges more keenly, the net made them cyborgs without anyone noticing. They were assimilated. They were the first children of the Matrix.

In a reversal of the way children learned from parents, the Second Generation taught their parents to come online which they did but with a different agenda. Their elders came to the net as a platform for business, a means of making profits, creating economies of scale, and expanding into a global market. Both inhabited a simulated world characterized by porous or disappearing boundaries and if they still spoke of a "digital frontier," evoking the romantic myths of the EFF and the like, that frontier was much more myth than fact, as much a creation of the dream weavers at CFP as "the old west" was a creation of paintings, dime novels and movies.

They were not only fish in the water of the Matrix, however, they were goldfish in a bowl. That

environment to which I have alluded, the military-industrial complex in which the internet evolved in the first place, had long since built concentric circles of observation or surveillance that enclosed them around. Anonymizers promising anonymity were created by the ones who wanted to know their names. Hacker handles and multiple nymms hid not only hackers but those who tracked them. The extent of this panoptic world was hidden by denial and design. Most on it and in it didn't know it. Most believed the symbols they manipulated as if they were the things they represented, as if their tracks really vanished when they erased traces in logs or blurred the means of documentation. They thought they were watchers but in fact were also watched. The Eye that figures so prominently in Blade Runner was always open, a panoptic eye. The system could not be self-regulating if it were not aware of itself, after all. The net is not a dumb machine, it is sentient and aware because it is fused bone-on-steel with its cyborg riders and their sensory and cognitive extensions.

Cognitive dissonance grew as the Second Generation spawned the Third. The ambiguities of living in simulated worlds, the morphing of multiple personas or identities, meant that no one was ever sure who was who. Dissolving boundaries around individuals and organizational structures alike ("The internet? C'est moi!") meant that identity based on loyalty, glue born of belonging to a larger community and the basis of mutual trust, could not be presumed.

It's all about knowing where the nexus is, what transpires there at the connections. The inner circles may be impossible to penetrate but in order to

recruit people into them, there must be a conversation and that conversation is the nexus, the distorted space into which one is unknowingly invited and often subsequently disappears. Colleges, universities, businesses, associations are discovered to be Potemkin villages behind which the real whispered dialogue takes place. The closed and so-called open worlds interpenetrate one another to such a degree that the nexus is difficult to discern. History ends and numerous histories take their place, each formed of an arbitrary association and integration of data classified or secret at multiple levels and turned into truths, half-truths, and outright lies.

Diffie-Hellman's public key cryptography, for example, was a triumph of ingenious thinking, putting together bits of data, figuring it out, all outside the system, but Whit Diffie was abashed when he learned that years earlier (1969) James Ellis inside the "closed world" of British intelligence had already been there and done that. The public world of hackers often reinvents what has been discovered years earlier inside the closed world of compartmentalized research behind walls they can not so easily penetrate. (People really can keep secrets and do.) PGP was – well, do you really think that PGP was news to the closed world?

In other words, the Second Generation of Hackers, socialized to a networked world, also began to discover another world or many other worlds that included and transcended what was publicly known. There have always been secrets but there have not always been huge whole secret WORLDS whose citizens live with a different history entirely but that's what we have built since the

Second World War. That's the metaphor at the heart of the Matrix and that's why it resonates with the Third Generation. A surprising discovery for the Second Generation as it matured is the basis for high-level hacking for the Third.

The Third Generation of Hackers knows it was socialized to a world co-created by its legendary brethren as well as numerous nameless men and women. They know that we inhabit multiple thought-worlds with different histories, histories dependent on which particular bits of data can be bought on the black market for truth and integrated into Bigger Pictures. The Third Generation knows there is NO one Big Picture, there are only bigger or smaller pictures depending on the pieces one assembles. Assembling those pieces, finding them, connecting them, then standing back to see what they say – that is the essence of Third Generation hacking. That is the task demanded by the Matrix which is otherwise our prison, where inmates and guards are indistinguishable from each other because we are so proud of what we have built that we refuse to let one another escape.

That challenge demands that real Third Generation hackers be expert at every level of the fractal that connects all the levels of the network. It includes the most granular examination of how electrons are turned into bits and bytes, how percepts as well as concepts are framed and transported in network-centric warfare/peacefare, how all the layers link to one another, which distinctions between them matter and which don't. How the seemingly topmost application layer is not the end but the beginning of the real challenge, where the significance and symbolic meaning of the

manufactured images and ideas that constitute the cyborg network create a trans-planetary hive mind. That's where the game is played today by the masters of the unseen, where those ideas and images become the means of moving the herd, percept turned into concept, people thinking they actually think when what has in fact already been thought for them has moved on all those layers into their unconscious constructions of reality.

Hacking means knowing how to find data in the Black Market for truth, knowing what to do with it once it is found, knowing how to cobble things together to build a Big Picture. The puzzle to be solved is reality itself, the nature of the Matrix, how it all relates. So unless you're hacking the Mind of God, unless you're hacking the mind of society itself, you aren't really hacking at all. Rather than designing arteries through which the oil or blood of a cyborg society flows, you are the dye in those arteries, all unknowing that you function like a marker or a bug or a beeper or a gleam of revealing light. You become a means of control, a symptom rather than a cure.

The Third Generation of Hackers grew up in a simulated world, a designer society of electronic communication, but sees through the fictions and the myths. Real hackers discover in their fear and trembling the courage and the means to move through zones of annihilation in which everything we believe to be true is called into question in order to reconstitute both what is known and our knowing Self on the higher side of self-transformation. Real hackers know that the higher calling is to hack the Truth in a society built on designer lies and then – the most subtle, most

difficult part – manage their egos and that bigger picture with stealth and finesse in the endless ambiguity and complexity of their lives.

The brave new world of the past is now everyday life. Everybody knows that identities can be stolen which means if they think that they know they can be invented. What was given to spies by the state as a sanction for breaking laws is now given to real hackers by technologies that make spies of us all.

Psychological operations and information warfare are controls in the management of perception taking place at all levels of society, from the obvious distortions in the world of politics to the obvious distortions of balance sheets and earnings reports in the world of economics. Entertainment, too, the best vehicle for propaganda according to Joseph Goebbels, includes not only obvious propaganda but movies like the Matrix that serve as sophisticated controls, creating a subset of people who think they know and thereby become more docile. Thanks for that one, SN.

The only free speech tolerated is that which does not genuinely threaten the self-interest of the oligarchic powers that be. The only insight acceptable to those powers is insight framed as entertainment or an opposition that can be managed and manipulated.

Hackers know they don't know what's real and know they can only build provisional models as they move in stealthy trusted groups of a few. They must assume that if they matter, they are known which takes the game immediately to another level.

So the Matrix like any good cybernetic system is self-regulating, builds controls, has multiple levels of complexity masking partial truth as Truth. Of what

else could life consist in a cyborg world? All over the world, in low-earth orbit, soon on the moon and the asteroid belt, this game is played with real money. It is no joke. The surrender of so many former rights – habeas corpus, the right to a trial, the freedom from torture during interrogation, freedom of movement without “papers” in one's own country – has changed the playing field forever, changed the game.

Third Generation Hacking means accepting nothing at face value, learning to counter counter-threats with counter-counter-counter-moves. It means all means and ends are provisional and likely to transform themselves like alliances on the fly.

Third Generation Hacking is the ability to free the mind, to live vibrantly in a world without walls.

Do not be deceived by uniforms, theirs or ours, or language that serves as uniforms, or behaviors. There is no theirs or ours, no us or them. There are only moments of awareness at the nexus where fiction myth and fact touch, there are only moments of convergence. But if it is all on behalf of the Truth it is Hacking. Then it can not fail because the effort defines what it means to be human in a cyborg world. Hackers are aware of the paradox, the irony and the impossibility of the mission as well as the necessity nevertheless of pursuing it, despite everything. That is, after all, why they're hackers.

Thanks to Simple Nomad, David Aitel, Sol Tzvi, Fred Cohen, Jaya Baloo, and many others for the ongoing conversations that helped me frame this article.

THE 3RD ANNUAL VERY UNOFFICIAL DEFCON JUMP

The third annual
DefCon Band of Renegades Skydive
is scheduled for Friday, August 1st, 2003,
at 0900

www.djump.com



thursday

0000 - 0030
0100 - 0130
0130 - 0200
0200 - 0230
0230 - 0300
0300 - 0330
0330 - 0400
0400 - 0430
0430 - 0500
0500 - 0530
0600 - 0630
0630 - 0700
0700 - 0730
0730 - 0800
0800 - 0830
0830 - 0900
0900 - 0930
0930 - 1000
1000 - 1030
1030 - 1100
1100 - 1130
1130 - 1200
1200 - 1230
1230 - 1300
1300 - 1330
1330 - 1400
1400 - 1430
1430 - 1500
1500 - 1530
1530 - 1600
1600 - 1630
1630 - 1700
1700 - 1730
1730 - 1800
1800 - 1830
1830 - 1900
1900 - 1930
1930 - 2000
2000 - 2030
2030 - 2100
2100 - 2130
2130 - 2200
2200 - 2230
2230 - 2300
2300 - 2330

tune in
via
channel 29

friday

saturday

sunday

Akira

Ninja Scroll

Ghost in the Shell

Fight Club

Blade Runner

Iron Monkey

The Lawnmower Man

Blade

Ronin

The Killer

The Saint

Heat

Pump Up the Volume

The Fifth Element

Way of the Gun

Replacement Killers

Sneakers

Aliens

Office Space

Three Days
of the Condor

Tron

The Bourne Identity

Hackers

Dark City

Swordfish

Antitrust

Enemy of the State

Run Lola Run

Minority Report

Ocean's Eleven

Hard Boiled

Cube

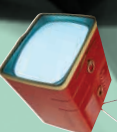
The Matrix

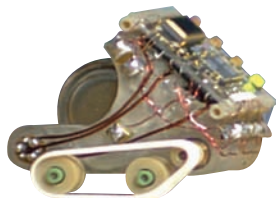
Johnny Mnemonic

War Games

Westworld

organized by 2600SLC
and
RootCompromise.org





Over the past several years, we've tried to bring the technology closer and closer to the attendees of Defcon. As part of this effort, we're initiating the first annual DefCon Robot Rally for Defcon 12. This contest is being announced now in the hopes that as many attendees will participate as possible.

More information will be forthcoming before the end of the year, but to get you started, below are some general guidelines. This contest will only be really cool if everyone starts from scratch when building their bots, so that's a rule. No pre-fab robot kits, please. We'll try to get representation from one of the cool TV robot shows and maybe we can talk them into bringing some of their creations. If you have questions, keep an eye on the DefCon website.

Def Con proudly announces the first annual

Def Con Robot Rally!

1 What are the rules?

There are no rules yet. More information will be posted on the Defcon website at <http://www.defcon.org> as they become available.

2 Who can participate?

At this point, we expect that anyone can participate as long as they have created an original robot of some sort.

3 What are the categories of competition?

Again, the details have not been totally laid out yet, but we expect to see categories similar to the ones listed here: "Overall Coolest Robot", "Best Covert Robot", "Winner of the Insectoid Obstacle Course", "Best Design", etc.

4 Will this be similar to the "Battle Bots" or "Robot Wars" seen on TV?

No. We're not out to exponentially increase the chaos at Defcon. No spinning blades, flame throwers, or rocket launchers allowed.

5 When will more information be available?

We hope to have the official information updated on the web site by the end of 2003.

6 Can we work in teams?

Sure. Teams should consist of no more than 5 individuals. Teams can adopt their own name, identity, etc. Teams might want to focus on a particular category of robot so they have a better chance of dominating the competition.



DEFCON 11 - Lockpick Contest

```
LPCONS$ ./pick -s deadbolt
--include /usr/pickmaster/residential.script

...PickMaster v.4.1/2.03 Started
...Detected lock - kwikset
...Pick Completed (00:00:39)

LPCONS$ █
```

(<http://www.d0718.org>)

The DEFCON 11 Lockpick Contest will be held in three elimination rounds consisting of multiple 6-contestant heats over two days.

FRIDAY • VENDOR AREA

1000 -1 200 - check in; 1500 round one

SATURDAY • VENDOR AREA

1000 - round two

1600 - round three; bonus round

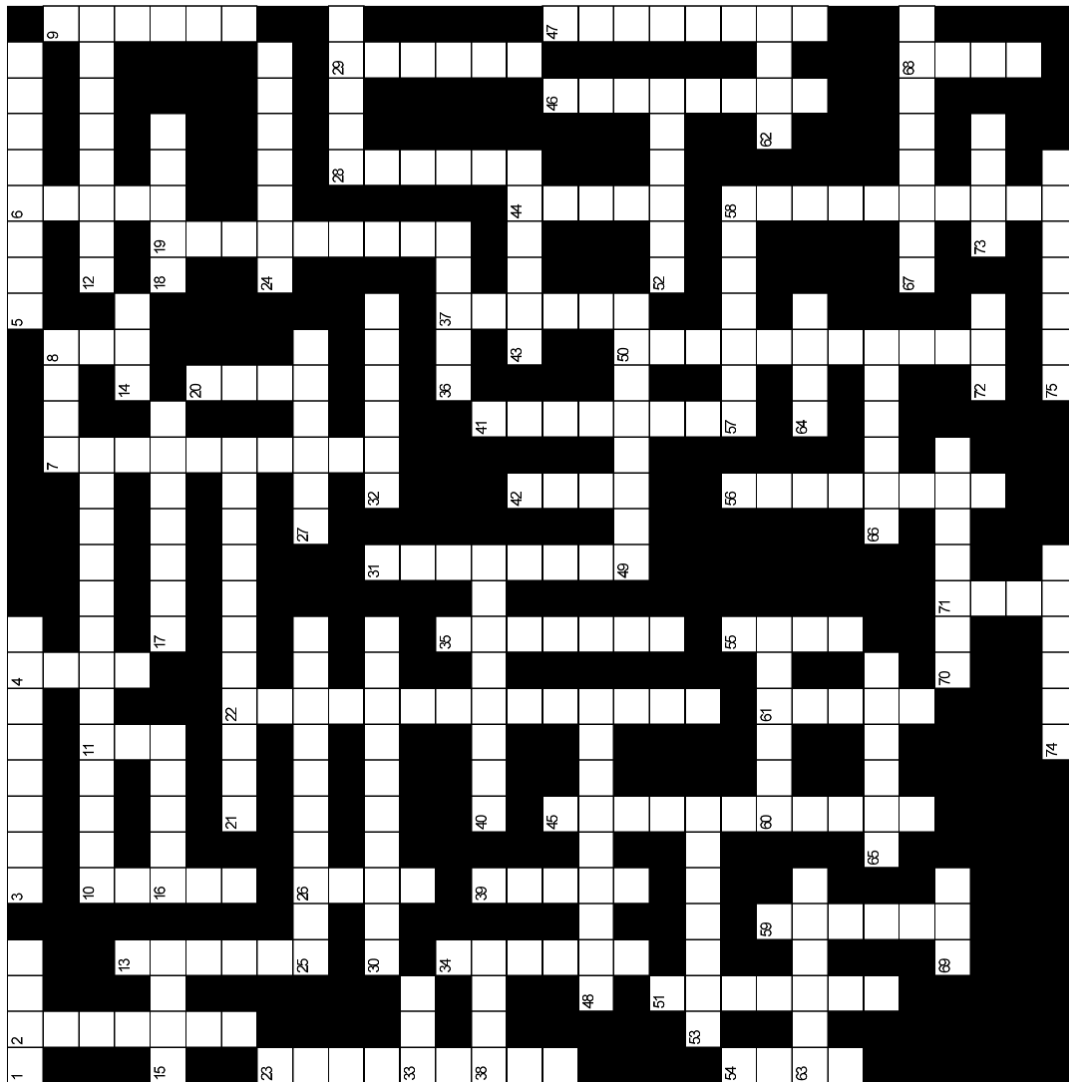
- There will be a maximum of 72 individual contestants for round one, dropping to 36 in round two, 12 for round three, and the top three individuals will compete in the final round to crown the DCLPSF.
- Individuals are responsible for providing their own equipment, no loaners will be available from the contest staff. *Note: Irvine Underground will be on site to supply tools for purchase for those whom do not bring their own or simply want to add to their collection.*
- This contest is free to all.
- There will be available lock boards for people to practice on at the booth while the contest is not in process, or for anyone wanting to learn about lockpicking!
- We invite all experienced individuals to strut their stuff and help others.



Those who can
FEEL a pin drop

complete details can be found at:
<http://www.worldwidewardrive.org/dclp/DCLP.html>

sponsored by



crossword puzzle by sleestak

ACROSS

- 1 unidirectional antenna used for freqs above 10 mhz
- 3 geometric arrangement of a network or system
- 5 popular WEP password sniffer
- 7 Geneva lab where HTTP was born
- 10 science of hiding information in another medium
- 12 Redford hacking movie
- 14 won't open the pod bay doors
- 15 DOD branch that underwrote the beginnings of the Internet
- 16 possible most Orwellian name for a gov. agency yet...
Information Awareness
- 17 Texas radio conglomerate with more than 1200 radio stations. Clear _____
- 18 first airline to implement passenger prescreening program called CAPPS II
- 21 reading all data from the network, regardless of who it's addressed to
- 24 first hacker to appear on "America's Most Wanted"
- 25 term for the rules of the usenet road
- 27 first word in the acronym bash
- 28 file-sharing giant some call the "new napster"
- 30 Redford phreaking movie.. Three days of the _____
- 32 Apple's wildly successful online music service
- 33 often called Big Blue
- 36 sequence of eight bits
- 38 most popular brand of PVR
- 40 how Winnie the Pooh might catch hackers
- 43 last name of the head of the FCC
- 48 Arab news network recently hacked by a Los Angeles man
- 49 tom cruise's last name in Minority Report
- 52 penned "the Origin of Species"
- 53 Scott Adam's cubicle-bound Everyman
- 57 1,000,000,000 bits□
- 60 wrote the "Hacker Manifesto"
- 62 another name for the abominable snowman
- 63 female AI courier in Heinlein novel
- 64 i "invented" the internet
- 65 precedes and describes the main file
- 66 unit of data that is routed between an origin and a destination
- 67 popular encryption algorithm created in 1993
- 69 standard unit of electrical resistance
- 70 person who fears or loathes technology
- 72 protocol often used between gateway hosts on the Internet
- 73 most recent online "safety" act, targets libraries
- 74 code name for OS 10.2
- 75 venerable video editing software package for the amiga

DOWN

- 2 name for virii that are resistant to analysis
- 4 to understand, in an old-school way
- 6 interactive user interface with an operating system
- 7 to own a domain name someone richer than you wants
- 8 said to claim there is "no such agency"
- 9 newsgroups live here
- 10 dan farmer's scary sounding network analysis tool
- 11 VA company that bought Time-Warner
- 13 last name of the professor in WarGames
- 19 Russian software company recently acquitted of DMCA charge
- 20 diagram type for displaying set intersections
- 22 summer movie starring NMAP
- 23 behavior-based analysis is also called□
- 26 divides each cellular channel into three time slots
- 28 essential center of a computer operating system
- 29 author of I, Robot □
- 31 Internet file sharing utility that sounds like food
- 34 search engine so powerful it's now a verb
- 35 the name of the con in all those "help me recover my millions" emails. _____ prisoner
- 37 hailing from troy
- 39 achieved blog celebrity for his Baghdad-based site "dear raed" .. _____ Pax
- 41 current singing attorney general
- 42 one electronic state change per second
- 44 light amplification by stimulated emission of radiation
- 45 popular wardriving app
- 46 creator of
- 47 keanu's other cyberspace movie... Johnny _____
- 50 virus that copies its code onto host files is called an _____ infector
- 51 first hacker to be named one of the FBI's most wanted
- 54 nickname for wireless networks
- 55 tool for specifying and handling the incidence of regular expressions
- 56 two competitor recently forced to drop its "commercial skip" feature
- 58 full name of TTL - although it should be the name of a soap opera
- 59 Intel programmer currently being held as "material witness"
- 61 number of Laws of Robotics
- 68 Pork shoulder and ham, mostly
- 71 recent act that prohibits most copying and reverse engineering□

Where's Leeto?

Follow the clues, solve the mystery.

<http://www.findleeto.com>



DEFCON groups

Current DC Groups:

DC207 • Auburn, MAINE

"Con", con@lostboxen.net

DC719 • Colorado Springs, CO

"McGruffD", mcgruffd@dc719.org

DC802 • SLC, UT

"Grifter", grifter@defcon.org

DC210 • San Antonio, TX

"Octalpussey", dc210@octalpussey.net

DC503 • Portland, OR

"telco88", junk@pdx-tech.com

With Defcon 0b we introduce an old concept to a new generation of hackers; The DC Group. For the folks that have been around a while, they'll remember when most hacker meetings were actually cool and you could learn something technical if you went to a meeting. This year Defcon jumps head first into foray with Defcon Groups (DC Groups)

DC Groups are starting all around the country! Listed below are the beta groups. Defcon would like to thank the founders of the new groups for all of their hard work and input. We invite you to attend a DC group meeting in your area and if your city isn't listed, START ONE! Got ideas? Share them!

"What does it mean to have a DC Group in my city?" The DC Group function is a cooperative environment where each member contributes somehow. They get together once a month and mull over a particular technical topic (no politics or 'save the planet' crap here). Hanging out to meet fellow hackers is recommended, but not required

(some of you won't even get along with your own mom). Presentations given at the meetings should be put on the website for other groups to use as inspiration for their own groups. Each DC Group has an alias in the defcon.org DNS server that points to their own group website. The DC Group page will be available on defcon.org shortly.

"There's no group in my area, how do I start one?" Send an email to dcgroups@defcon.org and we'll get you the information you need to know to get started.

"What's required?" A place to meet - park, library, mall food court, etc. A point of contact (POC) for the group - someone who doesn't mind keeping things focused. A website - not required, but it helps to give your group visibility and allows other groups to look at the talks your groups has had. Technical talks - let's face it, every hacker wants to be more technical. Members - that's mostly up to you. We'll list you on the site, but only you have direct access to the tech heads in your area.

For more information email dcgroups@defcon.org.
And watch for the DCG website, coming soon to a browser near you.

DEF CON @ The Movies

Day 1 • Friday Night:

#1 Random movies, Animations, and Audio

Building on the success of last year, check out a random selection of flash, .mpg and .mp3 shorts. From "Beer Good, Napster Bad!", some Animatrix, Troops, to Apples 1984 introduction of the Macintosh computer and everything in between.

#2 Shaolin Soccer

Voted best movie of 2001 in China. An absolute must see if you are into the whole kung-fu scene. If you wanted to know where the quote on defcon.org "Team evil is not so wonderful" came from, it is this movie. I don't want to give it away, but when you see the final scenes of the movie you will be blown away.

#3 Spy Games

While it's not Three Days of the Condor, it is still an great movie with Robert Redford. While on his last day of work at the CIA some trouble crops up with a past agent he used to manage. He uses all of his skills to manipulate the players in the Agency while planning for his retirement. Add Brad Pitt as a sniper and you can see where this is going. While there is no hacking going on, it is a great glimps into the mindset

Day 2 • Saturday Night:

#1 Equilibrium

Think of Farenheight 451 + A Brave New World + 1984 + THX1138 + a little gun-fu adds up to a thought provoking movie with some killer action scenes. If you missed its short run in the theatres, now is your chance to check it out.

#2 Avalon

A movie by Mamoru Oshii. Be warned this movie has subtitles, so if you don't know how to read, focus on the pretty pictures. From the back of the DVD: "In a future world, young people are increasingly becoming addicted to an illegal (and potentially deadly) battle simulation game called Avalon. While slow moving at times, you can see an influence of Tron, The 13th Floor and the Matrix in the story line. Since you wern't likely to ever see it, I thought I'd put it in the line up.

10th Anniversary

HACKER Jeopardy

Last year thousands of DefCon-ers hooted and cheered as Vanna Vinyl, Beer Betty and the HJ competitors drank their way through tough questions, meaningless trivia and nearly x-rated pictures.

One team of women, the “RRRRRs”, bet their clothing on the final round... You had to be there to see what happened... and then when Vanna and Betty decided to... well... you gotta come to see whassup.

Well, for DC11, and HJ10, we are going to continue the tradition that started in DC2. Winn went to Jeff at DC1 and said, “This is boring. Why don’t you liven this thing up?”

Jeff said, “OK. What do you want?”

Winn replied, “Oh, why not something like Hacker Jeopardy:” (I was dancing!)

Jeff: “So do it.”

And that’s how it got started, and Capture the Flag got started the same way a couple of years later.

So much for history.

It starts, as usual, at 10PM on Friday night for two games where the teams (of up to three people each) fight it out, duke it out and drink it out with questions to our answers.

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 to dtangent@defcon.org and we’ll pick you out of a hat before each Game. 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, August 1, 2003: 2200. Rounds One and Two.

Saturday, August 2, 2003: 2200 Round Three, and then the Final Round, where the winners from the first three Games compete.

Last Year’s winners can play in Final Round as Team #4, if they choose.

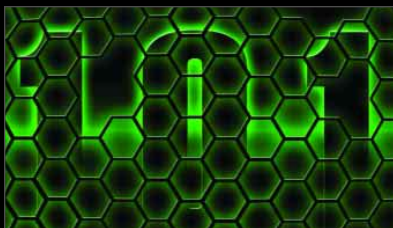
WHAT YOU CAN WIN:

Members of the winning team will each win a coveted DEF CON leather jacket.

THE CAST:

host: Winn
emcee: stealth
score keeper: G Mark
beautiful babe: Vinyl Vanna
supporting babe: Beer Betty

Day 1
Friday
August 1



zeus



tent



apollo

11:00 - 11:50

A Conversation with Phil Zimmermann
Phil Zimmerman

Deploying DNSSEC, part 1
Paul Wouters

Bluetooth
Bruce Potter

12:00 - 12:50

After Napster
Leia Amidon, Omar Ahmed, David McLeod, Harry Regan

Deploying DNSSEC, part 2
Paul Wouters

Advanced Network Recon Techniques
Fyodor

13:00 - 13:50

Interface Design of Hacking Tools
Greg Conti

At Risk! Privacy
Lenard Kleinrock and Sally Richards

Online Corporate Intelligence
Michael Schrenk

14:00 - 14:50

PDA Insecurity
Bryan Glancey

Mimicry
Mystic

Watching the Watchers
Johnny Long

15:00 - 15:50

Satellite TV Technology
OldSkool5

The Luna Correspondence Protocol
Chung's Donut Shop

Hacking From the Palm of Your Hand
Paul Clip

16:00 - 16:50

Credit Card Networks 101
Robert Imhoff-Dousharm

Behind the Remailers
Len Sassaman, Peter Palfrader, noise, Michael Shinn, Ryan Lackey

Revolutionizing OS Fingerprinting
Ofir Arkin

17:00 - 17:50

Beat the Casinos At Their Own Game
ParanoidAndroid

Government IP_TAPPING
Jaya Baloo

What Your Networks RTT Says About Itself
Tony (aka Xam) Kapela

18:00 - 18:50

Punishing Collaborators Redux
Bill Scannell

Increasing The Security of Your Election
Daniel C. Silverstein & Damon McCormick

The WorldWide WarDrive
Chris Hurley (aka Roamer)

19:00 - 19:50

Abusing 802.11
Abaddon, Dragorn, Anton Rager, Joshua Wright & h1kari

Aura
Cat Okita

Information Leakage— You posted what?
Joe Klein, CISSP



Saturday
August 2
1900 - 0400
Apollo

organized
by 23.org

DJ	Style	Time
The Minibosses	Punk	2000
DJ Pepse	Trance	2100
Corrupt Data	Electronic IDM	2200
Jackalope ov Orbis**	Techno	2300
Catharsis	Techno/Indust	0000
DJ Jerkface	Industrial	0100
Idiot Stare	Industrial	0200
Krisz Klink	Psy Trance	0300
Prophei	Psy Trance	0400

Dress Code
Rubber, Leather, Vinyl, Fetish Glam,
Kinky, Drag, Cyber Erotic, Uniforms,
Victorian, Tuxedo, Costumes...
absolutely No Jeans or Street Clothes!
No exceptions!!!

Day 2
Saturday
August 2



zeus



tent



apollo

11:00 - 11:50

Toward a Criminal Law for Cyberspace
Susan W. Brenner

Putting The Tea Back Into CyberTerrorism
Sensepost

The Future Frontiers of Hacking
Roberto Preatoni (akaSy\$64738)

12:00 - 12:50

Criminal Copyright Infringement & Warez
Trading, Eric Goldman

The UPS (Undetectable Packet Sniffer)
Spyde~1, AutoNIN & Mystic

Theft of Service Attacks
Robert Sheehy

13:00 - 13:50

The Story of EFFI
Mikko Valimaki & Ville Oksanen

Opensource Kernel Auditing & Exploitation
Silvio Cesare

Streaming Media Theft and Protection
tommEE pickles

14:00 - 14:50

Hacker Generations
Richard Thieme

Airsnarf
Beetle & Bruce Potter

Internet Radio Politics
Brian Hurley & Ann Gabriel

15:00 - 15:50

The Internet's Private Cops
Wendy Seltzer

Embedded Reverse Engineering
Seth Fogie

Hack Any Website
Gregoire Gentil

16:00 - 16:50

What to Know About Post 9/11 Legal Changes
Cindy Cohn

Stack Black Ops
Dan Kaminsky

Microsoft: Flaw Left Millions At Risk
Muhammad Faisal Rauf Danka (aka) MFRD

17:00 - 17:50

Free Your Mind: The NMRC Info/Warez
NMRC

Why Anomaly Based Intrusion Detection
Systems Are A Hackers Best Friend, Icer

_vti_fpxploitation
Matthew Shannon

18:00 - 18:50

NMRC: Simple Nomad, Inertia, Jrandom, Weasel, Cyberiad,
Sioda an Cailleach, HellNBak

More Embedded Systems
FX

closed

19:00 - 19:50

Adversary Characterization & Scoring Systems
Tom Parker, Dave Farrell, Marcus H. Sachs and Toby Miller

Manyonymity
Adam Bresson

closed

Day 3
Sunday
August 3



zeus



tent



apollo

11:00 - 11:50

HTTP IDS Evasions Revisited
Daniel Roelker

Hacking the Invisible Network
Michael Sutton & Pedram Amini

Dumpster Diving
Grifter

12:00 - 12:50

Metamorphic Viruses
Sean O'Toole

Locking Down Mac OS X
Jay Beale

OSI Layer 1 Security
Michael D. Glasser

13:00 - 13:50

Network Worms
Jonathan Wignall

Self-Abuse For Smarter Log Monitoring
Mick Bauer

Social Engineering Fundamentals
Criticalmass, Rob (Phantasm) and Matt (404)

14:00 - 14:50

Malicious Code & Wireless Networks
Brett Neilson

Introducing nmrcOS
Inertia

Technical Security Countermeasures
Jeffrey Prusan

15:00 - 15:50

Today's Modern Network Killing Robot
Viki Navratilova

Intrusion Prevention Techniques on
Windows and Unix, Rich Murphey

HavenCo
Ryan Lackey

16:00 - 16:50

Awards Ceremony
Hosted by the Dark Tangent

NoteEx
Your convention, recapped

Inspired by the South By Southwest Notes Exchange your pals at VP Labs have decided to throw together one of their own. Quite simply, the DEFCON Notes Exchange exists so con attendees can swap and compare notes on talks in a central area. Drink too much the night before and miss a talk? Debating between two different speeches on two separate tracks? Check the notes exchange to see what

other folks had to say about the talk you missed. Happen to take notes on something? Chip in. We operate on the zen like 7-11 policy of "Got a penny? Leave a penny. Need a penny? Take a penny." except until we get the Amazon micro payment tip jar up we'll just take your notes. Pay a visit to DC Notes Exchange at <http://defcon.noteex.com> during or after the convention.



Wireless technology is becoming more and more prevalent, and many people have experimented with transmitting wi-fi over large distances. The Guinness World Book of Records distance for a wi-fi link is 310 kilometers, and was set by the Swedish company Alvarion. Amateurs have been making antennas out of everything from Pringles cans to Primestar dishes, and getting amazing results. Sound interesting? Read on!

CONTEST GOAL: To see who can achieve the greatest wi-fi/802.11b connect distance.

EVENT STAFF: Dave Moore, Michele Moore, Anna Moore, Stefan Morris, Other volunteers

EVENT DETAILS: The contest will be open to Defcon attendees who agree to the contest rules. Contestants must register with and be accepted by contest staff in order to participate.

The contest begins Friday at 1200, August 1. Contestants should meet with staff in the lobby of the Alexis Park Hotel. Look for the Wi-Fi Shootout sign. At the meeting, contestants can register, and we can coordinate to see if anyone needs a ride to the contest location.

There will be two transmission log times, one on Friday, and one on Saturday. Contestants must log their transmission distance entries with contest staff. Contestants may log transmission distances at both log times, or at only one of the log times. The log times are:

- Friday, August 1, following the 1200 meeting in the hotel lobby;
- Saturday, August 2, following the 1200 meeting in the hotel lobby.

COMPETITION CATEGORIES

1. Stock/unmodified, with commercially made omnidirectional wi-fi antenna
2. Stock/unmodified, with commercially made directional wi-fi antenna
3. Homemade omnidirectional antenna
4. Homemade directional antenna
5. Enhanced power, (omni or directional) commercially made
6. Enhanced power, (omni or directional) homemade

Visit the Defcon Info Booth or
<http://home.earthlink.net/~wifi-shootout>
for detailed information.

h a r d a t w o r k

official defcon
bbs / party calendar

<https://bbs.defcon.org/>

or <http://bbs.defcon.org> and
<https://cal.defcon.org/> or <http://cal.defcon.org>

the purpose of this server is to replace the large piece of butcher paper that normally serves as the defcon bbs. feel free to list your parties on here as well as any other information you would like to share with other defcon attendees.

Abusing 802.11 - Weaknesses in Wireless LAN's

Abaddon, AirJack author
 Dragorn, Kismet author
 Anton Rager

Joshua Wright, SANS speaker, WLAN IDS researcher
 h1kari, BSD-Airtools author

Panel will discuss network detection, protocol-level vulnerabilities in all the 802.11 families, new techniques for defeating WEP, vulnerabilities in WPA/802.11i, and detecting attacks against 802.11 networks. Other topics will be driven by questions from the audience.

[PANEL] After Napster: The Inevitable Ascent of Peer-to-Peer Networks, LiveHives, Smart Mobs and Massive Subscription File-Sharing Services

Panel Lead: Leia Amidon, Partner / Principal Security Technologist SunStorm Security Group; Former Principal, Security Technologies, Napster, Inc.

Panel Members:

Omar Ahmed, CEO, Madscientest Foundation;
 Former VP of Operations, Napster, Inc.

David McLeod, Tension Structure Films, Director,
 "LiveHives: theBuzz @ theBarricades"

Harry Regan, CEO, SunStorm Security Group;
 Security Infrastructure Consultant, Napster, Inc.

From Napster to the current emerging techno-social phenomena of livehives and smart mobs, the evolution of peer-to-peer networks is exhibiting an exponential profligacy both in use and popularity, and actually influencing the evolution of human social interaction on both a local and a global scale.

Beginning with Napster, the popular Internet file sharing software created in 1999 by Shawn Fanning, arguably a revolution has taken place. Napster was at the forefront of the one of the most important electronic debates of the 20th century's fin-de-siecle: DMCA and various attendant copyright debates.

However, the perhaps the most important role that Napster played was as a "proof of concept" on a grand scale (98 million globally at it's peak) of the power of peer-to-peer communications.

Wireless data communication devices have screamed onto the networking scene in and may be poised to revolutionize social intercourse. Blogger journals can instantly upload text, audio, and video to their weblogs from the scene of breaking news events. With conventional cellular telephones tactical organization of crowds, "smart mobs," can be coordinated in political actions.. The newest breed of communication technologies can document in real-time documentation of an event without the need to rely on traditional media reports.

In "proof of concept" exercises, recent anti-war protests have utilized "livehive" and "smart mob" technologies to out flank police actions and effectively shut down city centers and targeted economic targets. "After Napster" will follow the evolution of peer-to-peer networks and their evolution as social communities of affording a new level of global awareness and action.

Revolutionizing Operating System Fingerprinting

Ofir Arkin, Founder, Sys-Security Group
 Xprobe is an active operating system fingerprinting tool, which was officially released two years ago at the Blackhat briefings USA 2001. The first version of the tool was a proof of concept for the methods introduced in the "ICMP Usage in Scanning" project, which I have conducted. Two years after, and several versions later (mainly Xprobe2 v0.1 release), this talk would examine several issues with operating system fingerprinting we (Fyodor Yarochkin and myself) have encountered during the development of Xprobe and Xprobe2.

Mainly the talk will explain why traditional operating system fingerprinting methods suffer from a number of caveats, and how these issues directly affects the results

different operating system fingerprinting tools relying on these methods produce (these issues will be explained along with different examples).

During the talk I will introduce several advancements in the field of operating system fingerprinting. The methods introduced greatly enhance the accuracy of operating system fingerprinting. Several new ways to gather information about a host OS will be uncovered along with ways to overcome many of the current issues of active operating system fingerprinting methods.

During the talk examples will be given, and the audience will be encouraged to participate in a discussion.

A paper release, and a new version of Xprobe2 will accommodate the talk.

Government IP_TAPPING: Vendors & Techniques

Jaya Baloo

Self-Abuse For Smarter Log Monitoring

Mick Bauer, Information Security Consultant,
 Upstream Solutions

Your Unix-based webserver has logs, and you know you should be keeping an eye on them. But what should you be looking for? Would you recognize an attack even if you saw one? What sort of automated log-watchers are available, and what if you need to tell *those* what to look for?



art by mindshadow

Attacking your own system while scanning its logs is a quick way to learn what anomalous log activity looks like. Plus, it's a fun excuse to run Nessus, nmap, and whisker against someone who won't call the cops on you (i.e., yourself). In my presentation I'll demonstrate this sort of productive self-abuse, using the aforementioned tools plus less-glamorous but equally useful commands like telnet and wget. My groovy two-laptop demos will show both attacks and logged messages simultaneously, adding to the overall excitement.

In addition to all that, I'll discuss how to fine-tune the mechanisms that control logging, and how to use automated log-watchers such as swatch (which needs to be told what to look for) and logwatch (which doesn't necessarily).

The presentation will culminate in a challenging game of "You Be the K1d10t," in which Def Con attendees will be welcomed to take their best shot at my wireless-connected laptop, while the audience & I watch the log messages that result (or don't). Anybody who roots my box, or causes a really entertaining log message, will receive a piece of the donated junk arrayed on the stage for that purpose. (But if my box gets DoSed beyond salvage, I'll just ask some trivia questions and call it a day, so please play nice!)

This will be a fairly technical presentation. Attendees should have a working knowledge of the Unix variant of their choice (my demo systems both run Linux), but my presentation should be comprehensible to most Unix newbies, while still being useful to intermediate and maybe even advanced users (hey, everybody knows different stuff).

Locking Down Mac OS X

Jay Beale

Apple's OS X operating system combines BSD Unix with easy-to-use Mac operating system components. This has produced an operating system that natively runs Microsoft Office, is friendly as can be finding you people with which to chat and exchange fileshares with, and yet still runs a command line! Needless to

say, it could probably use some lockdown before you want to take it to Def Con, or even to the airport, with the wireless card plugged in.

The speaker has ported Bastille Linux to OS X and learned a thing or two about locking down OS X in the process. This talk will demonstrate lockdown, showing you how to harden the OS X operating system against future attack.

Airsnarf— Why 802.11b Hotspots Ain't So Hot

Beetle, The Shmoo Group

Bruce Potter, The Shmoo Group

As wireless hotspots continue to pop up around the country, the opportunity to take advantage of the weakest point of this new networking fad becomes greater. What weak point is that? Why, the user, of course. Why sniff traffic, or crack WEP, or spoof MACs, when you can simply ASK for and easily receive usernames and passwords? Members of the Shmoo Group discuss how wireless miscreants can garner corporate or hotspot credentials the easy way: rogue access points.

Additionally, a new utility will be provided to make rogue AP setups a cinch—with a twist. Little to no wireless knowledge is needed to understand how simple it is to never again pay for wireless hotspot access.

Toward a Criminal Law for Cyberspace

Susan W. Brenner, NCR Distinguished Professor of Law and Technology, University of Dayton School of Law

The traditional model of law enforcement was shaped by certain assumptions about criminal activity. These assumptions derive from characteristics of real-world crime, i.e., that victim and offender must be in physical proximity, that crime is limited in scale, that physical evidence will be found at a crime scene and that crime falls into identifiable patterns. These assumptions gave rise to a hierarchically-organized model which operates on the premise that crime is localized, i.e., occurs within a specific geographical area encompassed by a single set of national laws. The traditional model, in effect,

assumes the primacy of nation-states as law enforcers.

Neither these assumptions nor the premise that crime is localized apply to cybercrime; cybercrime makes nation-states irrelevant. It evades the assumptions that shaped the traditional model and, in so doing, creates significant challenges for law enforcement. It is therefore necessary to devise a new approach for dealing with cybercrime, one that takes into account the distinctive characteristics of technologically-mediated crime.

Such an approach is evolving in the cybercrime task forces established pursuant to a mandate contained in the USA PATRIOT Act. Whereas the old model emphasized law enforcement's reacting to completed crime, this approach emphasizes collaboration between potential victims and law enforcement in an effort to prevent cybercrime. It also emphasizes lateral, networking arrangements in which law enforcement personnel often function more as consultants than as sole investigators. Clearly, a lateral, collaborative approach is a more advantageous strategy for dealing with cybercrime.

The problem is that individuals also need to be involved if this approach is to be effective. Currently, corporations and other entities are more likely to understand the need and have the resources to partner with law enforcement in an effort to implement cybersecurity. This is not generally true of individuals, but it may be possible to use new principles of criminal liability – modified rules of criminal law and imported, modified civil law rules – to create incentives for individuals to participate in such an approach.

Manyonymity: PHP Distributed Encryption

Adam Bresson, adambresson.com

Manyonymity is an advanced, self-programmed PHP Distributed Encryption web application under the GNU GPL. Manyonymity premieres at DEFCON 11 in conjunction with a self-developed, new theory of encryption: geometric transformation. Manyonymity is a customizable, easily-

maintained PHP Distributed Encryption web application including verified installation, maintenance and a powerful user interface. Manyonymity allows anyone to run their own GNU GPL encryption and fingerprinting server. We'll discuss general encryption, the functionality of Manyonymity, demonstrate a sample implementation and discuss future development. Manyonymity, it's who you don't know.

Opensource Kernel Auditing and Exploitation

Silvio Cesare

For a period of up to 3 months in 2002, a part-time manual security audit of the operating system kernels in Linux, FreeBSD, OpenBSD, and NetBSD was conducted.

The aims of audit were to examine the available source code, under the presumption of language implementation bugs. Thus classic programming bugs, prevalent in the implementation language [C], exemplified in integer overflows, type casting, incorrect input validation and buffer overflows etc were expected. The initial introduction to auditing examined easily accessible entry points into the kernel including the file system and the device layer. This continued to an increased coverage and scope of auditing. From this work, identification of conjectured prevalent bug classes was possible. These results are in favour of the initial expectations; that bugs would be that in line of classical language bugs.

The results of this audit are surprising; a large [more than naively expected] number of vulnerabilities were discovered. A technical summary of these vulnerabilities will be treated in detail. Bug classes and [conjectured] less secure specific subsystems in the kernel will be identified. These conjectures support the the research of Dawson Engler's work in automated bug discovery in application to open-source kernel auditing.

Vulnerabilities after bug categorisation, are applied in the treatment of exploitation. The results are again surprising; exploitation sometimes being trivial, and primarily being highly reliable. The assumptions of exploitation difficulty, is

conjectured to be a false belief due to lack of any serious focus on kernel auditing prior to this paper. This conjecture is supported by in-line documentation of kernel sources indicative of immediate security flaws.

Attack vectors are identified as a generalisation of bug classes. Risk management is touched upon to reduce the scope of attack, but is not the primary purpose of this paper.

Discussion is finally that of vendor contact, and the associated politics of vulnerabilities. First hand reports of acknowledgement times, problem resolution times and public dissemination policies are presented in candid. The author may be biased at this point, but it appears that in during this audit period, open-source holds up to the promise of security concern and responsibility in its community. Problem acknowledgement in at least one of the the cases presented is perhaps the fastest in documented history (less than three minutes).

The majority of the vulnerabilities discovered during the audit, were resolved and patched in co-operation with the open-source developers and community responsible for each respective operating system. A very large thanks must go to Alan Cox, Solar Designer and later followed by Dave Miller who made enormous efforts to continually resolve all issues uncovered.

The Luna Correspondence Protocol

Chung's Donut Shop

Keith Hoerling, Software Designer & Donut Dipper

Dorian Andreatte, Chief Hacking Officer & Donut Sprinkler

Mark Wilkerson, Conceptual Developer & Dough Roller Supreme

Chung San, Master Donut Sen Sei

The Luna Correspondence Protocol is an anonymous finitely improbable data dispersal and stealth security nexus. Elaborated, Luna is a protocol designed to ensure traffic travelling across the internet can't be snooped by prying eyes. Luna is the greatest and best attempt--to date--at purely

anonymous and secure data transmission by commingling various techniques involving encryption, data relaying and mathematics--absolutely not security by obscurity.

By attending our presentation, the viewer will learn of our comprehensive first-class research conducted in the fields of wide data dispersal, data security and anonymity. The attentive listner will receive free donuts (Chung's special recipe).

No esoteric knowledge is required of the listener, only a grasp of networking, as our talk is straight-forward. Data coding and math theory (discrete math) will be discussed, so appropriate knowledge is a plus, but definitely not required.

Hacking from the Palm of Your Hand

Paul Clip, Managing Security Architect, @stake

Palm handhelds have become almost ubiquitous and very cheap, every month sees the announcement of yet another flavor with new and improved functions. Yet, how effective are Palms as a hacking platform?

This presentation will cover some of the existing security tools on PalmOS before focusing on the release of a new TCP-based scanner running on PalmOS capable of net recon, banner grabbing, and web vulnerability scanning. Design criteria and implementation details will be discussed, as well as a demonstration of the tool in action. The scanner will be available for download at DEFCON.

What Hackers Need to Know about Post 9/11 Legal Changes

Cindy Cohn, Legal Director, Electronic Frontier Foundation

The Bush Administration's relentless assault on freedom and privacy online and offline hit the ground running with the Patriot Act in the immediate aftermath of 9/11, but hasn't slowed since then. While the terrorist acts had absolutely no relationship to computer hacking, hackers were a clear target in the Patriot Act and subsequent developments. The changes in the legal landscape are vast and wide, but anyone interested in

d c o b s p e a k e r s a n d t o p i c s

computer security research, whether professionally or as a hobby, should have a basic understanding of the new world order. EFF was one of the broad coalition of groups that fought the Patriot Act—its analysis comes up first in a Google search on the law—and continues its work opposing all of its ugly brothers, sisters, cousins and stepchildren. The talk will focus on the portions of these laws and programs that affect hackers of all hat colors, including:

- Changes in the Computer Fraud and Abuse Act
- The expanded definitions of “terrorist” and “material assistance to terrorists” and what they may mean for toolmakers
- All your logs are belong to us - the reduced provisions for subpoenas to ISPs and others who have information about you
- What reduced judicial oversight, fewer checks and balances and more sharing among various cops means in practice
- What Patriot II/DSEA holds in store
- TIA, CAPPs II and other acronyms you should know about
- How can you legally to better protect yourself and others.

Interface Design of Hacking Tools

Greg Conti, Assistant Professor of Computer Science, United States Military Academy

Publicly available computer security tools are often great works of technological expertise. A great deal of effort goes into the technical implementation, often at the expense of the user interface and overall user experience. Designed for all levels of expertise, this talk explores common user interface design techniques that will put a usable front end on computer security tools. A variety of tools will be examined and critiqued to illustrate and reinforce these techniques. Attendees will leave with an increased understanding of user interface and

user experience design that they can apply to their own development projects to make them more effective.

Social Engineering Fundamentals

Criticalmass, Textbox Networks

Rob, aka Phantasm

Matt, aka 404

This presentation will tell you about how social engineering and its fundamentals come into play with an attack on a network, person or company. It will inform people on how to prevent these attacks and how to tell if a person is being attacked

Microsoft: Flaw Left Millions At Risk

Muhammad Faisal Rauf Danka, aka MFRD, Director IT Security Services, Bay Systems Consulting Pakistan, an offshore division of Bay Systems Consulting, Inc, USA

Microsoft® .NET Passport is a Web-based service designed to make signing in to Web sites fast and easy. .NET Passport enables participating sites to authenticate a user with a single set of sign-in credentials, eliminating the need for users to remember numerous passwords and sign-in names.

Microsoft Passport has over 200 million accounts performing more than 3.5 billion authentications each month. .NET Passport participating sites include NASDAQ, McAfee, Expedia.com, eBay, Cannon, Groove, Starbucks, MSN® Hotmail, MSN Messenger, and many more, Theoretically, that would set the maximum fine at \$2.2 trillion by FTC (Federal Trade Commission).

Due to Microsoft's Hotmail and Passport .NET account's flaw discovered by the speaker Passport / .NET accounts were exposed vulnerable to having their password reset by a remote attacker because of lack of input validation for a secondary email address.

The presentation will cover the various aspects of discovering such a flaw, including:

- Microsoft's incident response

- Media's response
- FTC and Microsoft (Past and Present)
- Microsoft's efforts to re-build the reputation
- Microsoft's vulnerability to its trustworthy computing marketing campaign
- Microsoft's official statement regarding the flaw

More Embedded Systems

FX, Phenoelit

The talk focuses on more embedded systems - this time, looking into the mobile world of GSM as well. How can the infrastructures and protocols in the Internet enabled GSM world be used for attacks? This session will give you an introduction to the concepts of WAP and GPRS. Equipped with this knowledge, some interesting applications of these protocols will be presented. Of course, it also covers some funny things you can do with (against) mobile phones. The second part will show you the latest advancements in Cisco IOS exploitation. While Phenoelit showed you last year that it can be done, we will go on and show you this year that it can be done better, more reliable and more elegant.

Embedded Reverse Engineering: Cracking Mobile Binaries

Seth Fogie, Aircanner Corporation

The embedded mobile market is headed for a day of reckoning when it will become the target of virus/trojan writers. To prepare for this, security experts must understand reverse-engineering fundamentals, as they apply to the pocket PC device, so they can research, investigate and understand the impact of malware and how to prevent it from spreading.

Unfortunately, when it comes to understanding malware for the PPC environment, there is little guidance. The only exception to this is ironically found in the backyard of some people who would write the destructive code. What we are talking about is the reverse-engineering of software protection schemes.

As a result, this talk will focus on the security protection schemes built into PocketPC software, and how these protections are circumvented. Using the same tricks, tools, and techniques that crackers use to bypass anti-piracy schemes, we will demonstrate first hand how these programs are cracked using a simple 'crackme' serial validation program as an example. We will start with a discussion on the hardware environment and reverse-engineering fundamentals to provide a background and foundation for the core of the talk; a step-by-step demonstration on how to crack a real program.

Advanced Network Reconnaissance Techniques

Fyodor, Insecure.Org
Fyodor will present real-life examples of common network and firewall configurations, then demonstrate practical techniques for exploring and mapping those networks. He will cover IDS evasion, "phantom ports", advanced ping sweeps, firewall circumvention, DNS hackery, IPv6, and more using his free Nmap scanner and many other Open Source tools.

Hack Any Website

Gregoire Gentil, CTO, Twingo Systems
This session will learn how you can hack any website whatever its protection. The most basic and simple attack against a website is to change the content of one of its pages. When trying to attack a website, one first thinks to attack the web server. But attacking the client could be easier and more powerful. This is what you will see during this session. In one hour, you will understand how to take the full control of Internet Explorer 4.x and above and modify on-the-fly the content of any HTML page before it is rendered.

PDA Insecurity

Bryan Glancey, VP of R & D, Mobile Armor.
Palmtops are going in power and popularity. How is the security on these devices and what can be easily bypassed. We will look at the HP 5455, the pinnacle of Palmtop security and

see how easily it's biometric security can be overcome. We will also cover basic security holes present in all palmtops - regardless of model.

OSI Layer 1 Security

Michael D. Glasser
In today's corporate environment electronic physical security is a serious business. Every corporation has some form of access control and/or CCTV system in place. There are only three really important questions to ask about it. Does it do what it's designed to do? Was it designed to do what it needs to do?
WHO'S RESPONSIBLE AT THE END OF THE DAY?

This presentation will:

- Give in depth explanation of the different technologies used in Access Control & CCTV today.
- Give an overview of general system designs.
- Give the most common security flaws that are existing today.

Criminal Copyright Infringement & Warez Trading

Eric Goldman, Assistant Professor of Law,
Marquette University Law School in Milwaukee, WI
This talk will discuss criminal copyright infringement and how it applies to warez trading. We will discuss what is legal and what isn't, who has been prosecuted, why they were prosecuted and what happened to them, and why the law is bad policy. You should expect to leave the talk more knowledgeable about what activities are criminal and how great or small the risks are.

Dumpster Diving: One man's trash...

Grifter
There are few things that yield more information about an individual or organization than their very own trash. This simple fact can be both fun and frightening depending upon which side of the fence you're on. Practiced by hackers for countless years, the act of Dumpster Diving has been an

essential tool in the hackers toolkit; and an often overlooked area of an organizations security policies.

This speech will cover but not be limited to:

- Who are Dumpster Divers? What it is, and why they do it.
- What to wear and take with you when Dumpster Diving.
- Basic Rules to follow to stay safe and within the law.
- What to do if approached by the authorities.
- Areas to dive and not to dive.
- Interesting and Humorous Anecdotes.
- Ethics.
- Protecting your privacy or the privacy of your organization.

Internet Radio Politics: A Tale of Betrayal & Hope

Brian Hurley, Owner / DJ, Detroit Industrial
Underground, Spokeperson for Webcaster Alliance
Ann Gabriel, Owner, Gabriel Media & President of Webcaster Alliance

A summary of the current legal state of internet radio. How the RIAA, a group of popular commercial webcasters, and Congress conspired to betray smaller webcasters, in an attempt to eliminate the majority of stations broadcasting on the internet. We will compare the philosophies of those who see internet radio as just another mass medium to be controlled and consolidated into as few stations as possible, and those who want to maintain a large number of stations with a rich variety of programming, and how these groups are fighting to influence the public, Congress, and the media. We'll close with a look at the future of internet radio, and outline the Webcaster Alliance's strategy to break the RIAA's hold over this new medium.

The WorldWide WarDrive: The Myths, The

Misconceptions, The Truth, The Future

Chirs Hurley, aka Roamer

The WorldWide WarDrive is an effort by security professionals and hobbyists to generate awareness of the need by individual users and companies to secure their access points. The goal of the WorldWide WarDrive (or WWWD) is to provide a statistical analysis of the many access points that are currently deployed.

Roamer will discuss the origin of the project, many of the difficulties the project has run into with the press and "other entities", the truth behind the goals of the project and the direction the project is moving in the future. Also, the full statistical analysis and results of the Third WorldWide WarDrive will be revealed for the first time.



art by david condrey

Why Anomaly Based Intrusion Detection Systems Are A Hackers Best Friend

Icer

The security market is booming. New types of tools are emerging all the time with promises of being able to protect networks better than the last generation. The newest trend is anomaly based intrusion detection systems. These systems claim the ability to detect new types of attacks before comprable signature based systems while being able to scale to higher network speeds. Are these claims true? Will these systems be the silver bullet to protect the clueless? Are these tools any better than the other script kiddie prevention tools? This talk will answer these questions and more.

Credit Card Networks 101: What They Are, and How to Secure Them

Robert Imhoff-Dousharm

Credit card networks have grown into a viable and necessary asset in large transaction based businesses. Are these networks protected? Are there formal security measures to protect these packets from external, and internal threats? Most network administrators, controllers (CFO) and CIO's are not even aware of credit card's flow or existence on a network. Further some over protect their switched network, disabling these systems from working correctly. One needs to have knowledge of these networks, know the possible exploits, and how to secure them.

Introducing nmrcOS

Inertia

nmrcOS provides a secure environment for the modern hacker-type to call home, which would help protect the privacy and security of the users of the system. In addition, it provides a portable working environment for the hacker on the go—easy loading on simple hardware, no-nonsense command-line for uber control, yet usable by most people out of the box.

Discussion will focus on the history of the project and current design choices. Details on how to develop for the system will also be presented. Presentation includes demonstration of installation and configuration.

Stack Black Ops: New Concepts for Network Manipulation

Dan Kaminsky, Senior Security Consultant, Avaya, Inc.

What can your network do? You might be surprised. Layer by layer, this talk will examine previously undocumented and unrealized potential within modern data networks. We will discuss aspects of the newest versions of scanrand, a very high speed port scanner, and the rest of the Paketto Keiretsu. Interesting new techniques will also be discussed, including:

Bandwidth Brokering - a technique that allows market-based load balancing across administrative boundaries using existing TCP protocols

DHCP-less Bootstrapping - a sub-optimal but effective strategy for bootstrapping network access for hosts that cannot directly acquire a DHCP lease

State Reconstruction - a design model that allows stateless network scanners (such as scanrand) to acquire deep knowledge about scanned hosts

Multihomed Node Detection - a simple set of techniques that expose firewalled hosts with alternate paths to an unfirewalled network link.

Generic ActiveX Encapsulation - a step-by-step methodology for safely launching arbitrary win32 tools (such as putty or a Cygwin OpenSSH environment) from a web page

We will also be discussing significant advances in data visualization, made necessary by the sometimes daunting amount of raw information these sorts of tools can expose one to.

Fashionably Late - What Your Networks RTT Says About Itself

Tony (aka Xam) Kapela

In this session, we will explore network fingerprinting through the use of high-frequency active probes to determine the network's delay. We will also discuss how signal analysis techniques on those delay measurements can be employed to characterize a network's performance and configuration. Using examples from a real-world enterprise network, various layer-1 and layer-2 features will be exposed including: a router or switch's queuing behavior, evidence of unrelated cross-traffic, and the presence of a configured monitoring or "span" port, perhaps indicating the presence of an eavesdropper.

Information Leakage... You posted what?!

Joe Klein, CISSP

If information is power, they why are so many organizations willing to give away this power? Are they are not aware of the risk to their network by posting network diagrams on the Internet? Or to staff, by posting the CEO's home addresses, wife and kids names on their website? Or to the organizations financial wellbeing by leave their financial transactions zipped on their company ftp server?

The focus of this presentation will show the ways organizations release information both intentionally and non-intentionally.

At Risk! Privacy: Homeland's Rights To Take It Away And The Hacker As A Hero To Restore Privacy Via Code To Protect The Every Day User

Lenard Kleinrock, Co-founder of the Internet

Sally Richards, Author, Privacy Advocate

Leonard Kleinrock, co-creator of the Internet and Sally, author and privacy advocate, talk about the past present and future of privacy and civil rights and how they pertain to the next wave of technology -- keeping your data safe from both government agencies and commercial entities leveraging your info for Big

Brother and commercial uses? Will this next level of technology to block Big Brother be illegal and the technologists developing it be jailed for some government infringement of national security? Where will the code heroes of tomorrow come from? And how will they be able to leverage their code into commerce?

HavenCo: What Really Happened

Ryan Lackey

HavenCo, an attempt at creating an offshore data haven, was launched in 2000 by a small team of cypherpunks and pro-liberty idealists.

During 2002, the Sealand Government decided they were uncomfortable with their legal and PR exposure due to HavenCo, particularly in the post-DMCA and post-911 world, and regulated, then took over the remains of the business, forcing the remaining founders out. While HavenCo continues to serve a small number of customers, it no longer is a data haven, and has exposed the ultimate flaw in relying on a single physical location in one's quest for privacy.

Watching the Watchers: Target Exploitation via Public Search Engines

Johnny Long, Johnny.ihackstuff.com

In today's world of all-knowing, all-seeing search engines, it should come as no surprise that very sensitive information lies in the deep recesses of big search engines' data banks.

What may come as a surprise, however, is just how much of a search engine's collected data exposes security flaws and vulnerabilities about the crawled sites. In some cases, even after a security hole is fixed, a search engine may cache data about that vulnerability, providing information about other avenues of attack. This process of "watching the watchers" is not theoretical. It happens, and it happens daily.

This session demonstrates the technique of crawling one of the most popular search engines for security vulnerabilities on one or many targets simultaneously.

Sample information will be extracted about various friendly targets without sending any data or packets to the intended targets, leaving those targets completely unawares.

A database of hundreds of vulnerabilities (and growing) will be uncovered and presented to the participants, as well as an automated tool which can be used to scan search engines for vulnerabilities on participant's hosts and networks.

A little-known research page has been started with working examples of this technique applied to one popular public search engine.

This presentation (especially when presented in conjunction with a live internet feed) is not only informative and eye-opening, but both refreshingly fun and amazing to watch. Most participants will have a great deal of familiarity with the search engines presented and will be delighted (and rightfully concerned) to see them operating in a manner they were not designed for. Solutions for remedying and controlling this amusing (yet very serious) vulnerability will also be discussed.

Intrusion Prevention Techniques on Windows and Unix

Rich Murphey, Chief Scientist, White Oak Labs

What exactly is intrusion prevention and why the heck should we care? This talk surveys some of the common features of Intrusion Prevention systems, largely constrained by architectural layering of Windows and Unix kernels We then look at a case study of intrusion prevention and discuss how it differs from IDS, Firewall, AV, and others.

Mimicry

Mystic

Mimicry is the ability to survive by mimicking your surroundings. In 1996 a book named Disappearing Cryptography by Peter Wayner was published and with it proof of concept code called the mimic functions that allow for encrypted data to be hidden in innocent looking text. This allows for encrypted data to be passed through networks

d c o b s p e a k e r s a n d t o p i c s

undetected by filters looking for anything out of the ordinary. This talk will include an introduction to how the mimic functions do what they do and will also be an introduction to a tool called ircMimic that uses the mimic functions to hide data in an IRC conversation.

Today's Modern Network Killing Robot

Viki Navratilova, Network Security Officer, University of Chicago

Today's Modern Network Killing Robot will give an overview on the new generation of DDOS tools. Back in the day, a couple of large pings could take down lots of machines. When those techniques stopped being effective means of taking down networks, people started writing DDOS programs. These programs required a little bit of manual work to install, but were effective at taking down large networks for a while. This generation of DDOS tools were made famous in the media by DDOS'ing famous websites for hours at a time. Soon people learned to control the damage done by these tools, and so a new generation of DDOS tools were born: Ones that could infect thousands of machines automatically to create large botnets, and hide their communications in order to evade detection better than their predecessors.

These botnets are now the most effective DDOS tools in popular use today. This talk will go over the more popular botnets, such as gtbot and sdbot, and talk about how they work and some ways to spot them on your network.

There will be a demonstration of an irc botnet in action.

Malicious Code & Wireless Networks

Brett Neilson

With over 55,000 viruses circling the globe it is no wonder we are so paranoid about protection, but are we being paranoid enough? A new threat stands to potentially disrupt systems worldwide and cause hundreds of millions in damage.

In this presentation we will discuss current wireless trends and some of the vulnerabilities they bring. In addition we

will also discuss some potential wireless threats and explore some reasons why malicious code could spread within a wireless system.

[PANEL] Free Your Mind: The NMRC Info/Warez

NMRC members: Simple Nomad, Inertia, jrandom, Weasel, Cyberiad, Sioda an Cailleach, HellNbak

New years bring new threats. Laws such as the DMCA, PATRIOT and DSEA are threatening hackers to the core. But instead of lecturing on what the underground could be doing to counter, NMRC will lead by example and present what they have been working on for the past year. New tools, new techniques, new information, and a new operating system! All open source, all full disclosure, all with security and privacy in mind.

Aura: A Peer To Peer Reputation System

Cat Okita

Aura is a peer-to-peer reputation system designed to create localized reputation information linked to specific users and/or systems. It can also function as a carrier of information in the form of 'recommendations'. Current research in trust metrics and reputation systems will be briefly covered, and implementation and design challenges will be discussed in greater depth.

Satellite TV Technology: How It Works and What You Can Do With Different Dishes

OldSkoolS

Ever wondered what that big 10' dish in your neighbor's back yard is good for? Pondered what signals you could pick up other than subscription TV on your small dish? Let OldSkoolS walk you through the wonderful world of satellite technology.

He will quickly bring you up to speed on what the difference is between C and Ku Band, and what the different protection systems used in today's satellite communications. Tips on procuring used and new hardware will be given as well as a few legal tips. A live demonstration of hardware and

software will be shown (If a view of the southern sky is provided for the satellite dish). No background knowledge of satellite TV technology or systems is needed.

Metamorphic Viruses

Sean O'Toole

This talk will cover the components and theory behind metamorphic engines. Also, how they create a better stealth method for viruses since it will cause the body of the virus to completely change in appearance while still containing the same functionality. This method of virus writing has gained much attention since this century, compared to it's earlier day, which include the '98 Win95/Regswap and others whose techniques have now developed into what we know as Metamorphism today.

Beat the Casinos At Their Own Game

ParanoidAndroid

Tired of having casinos take your money? Did you know that it is possible to be a long-term winner in some casino games? This presentation will cover the basic information that you need to learn about card counting, sports betting and other casino games where you can gain an advantage. The presentation will also cover casino surveillance and how to avoid detection. There will also be discussion on casino comps and other ways to take money from the casinos.

Adversary Characterization and Scoring Systems

Dave Farrell, Founder, CyberAdversary.com,

The Cyber Adversary Research Center

Toby Miller, www.ratingthehacker.net

Tom Parker, Director of Research,

Pentest Limited (UK)

Marcus H. Sachs, Cyber Program Director,
Department Of Homeland Security; National
Cyber Security Division

Cyber adversary characterization is a topic which was conceived by the panel members along side other members of the

computer security and intelligence communities in an attempt to provide an accurate way to build profiles of cyber adversaries, much like the way in which criminal psychologists profile more traditional criminals.

The characterization metrics conceived attempt provide a characterization of both theoretical adversaries, classing them based on statistics harvested from the wild and an accurate way of characterizing an adversary at an incident response level by studying the methodologies used during the attack.

The panel will begin with an introduction to the topic, followed by in depth discussion regarding the various characterization metrics and their applications; toward the end, we will be taking questions from the floor.

Streaming Media Theft and Protection

tommEE pickles, psycho clown, Moloch Industries,
<http://moloch.org>

tommEE pickles presents an 101 type approach to streaming media. He will talk about sites that host streaming media, how to leech the media off of them and how to also protect site that host streaming media.

Bluetooth – The Future of Wardriving

Bruce Potter

By some estimates, there are more Bluetooth radios deployed than 802.11 radios. However, Bluetooth as largely been ignored by the security community. Over the next several years, this will change dramatically as Bluetooth security tools catch up with 802.11 security tools. Bluetooth devices tend to be always-on machines that generally contain and transmit highly personalized information. Due to limitations of the platforms and interfaces that utilize Bluetooth, many developers chose to avoid implementing security mechanisms. This combination of private information and lowered security makes Bluetooth a likely candidate for attacks targeted at an individual... or simply an interesting protocol to keep voyeurs happy.

This talk will cover the basics of the Bluetooth protocol and its security mechanisms. I will discuss attacks that may be carried out against Bluetooth enabled PANs. I will compare Bluetooth and 802.11, especially from a discovery and interception point of view. Finally, I will present The Shmoo Group's new Bluetooth wardriving utility.

The Future Frontiers of Hacking— UMTS Mobile Phone Platform Web Intrusions: the Best Indicator of the Vulnerable Status of the Internet

Roberto Preatoni (aka Sy564738), Founder, zone-h.org

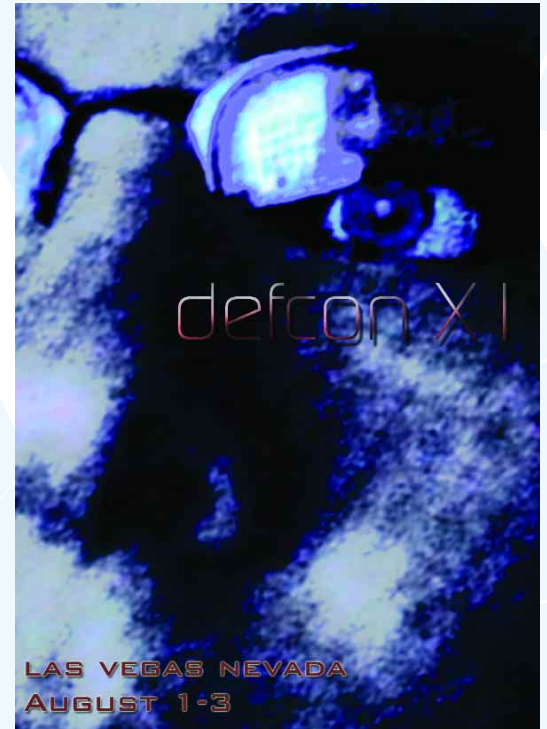
- The introduction of the UMTS mobile telephone protocol will be the last frontier for hackers. How will they act? What vulnerable points will be exploited?
- How the UMTS technology will pose a threat to our everyday lives leading to complete loss of privacy.
- Web defacements and Internet scams.,A sharp overview on trends and techniques used by web intruders.
- Linux or Windows? Internet security myths. Zone-H, the Internet thermometer.
- Internet scams are the best indicator of the vulnerable status of the average Internet users.

Technical Security Countermeasures: The Real Story Behind Sweeping for Eavesdropping Devices

Jeffrey Prusan, President, Corporate Defense Strategies Inc.

As a corporate security advisor, former investigator, and TSCM technician, we will dispel the myths behing bugging and wiretapping. We will separate what tappers can and can not do (everything you see in the movies is not always true!!). What companies can do that will realistically protect themselves from

eavesdropper and thereby help to protect their network, proprietary information, and intellectual property. We will explain and demonstrate the sophisticated electronic tools used by a professional sweep team, and describe what happens during the sweep process. We will demonstrate how phones are tapped in homes(analog phones), small businesses (KSU telephones systems), and larger companies (PBX systems). We will show how corporate spies attempt to infiltrate company telephone systems and ultimately compromise your network



d c o b s p e a k e r s a n d t o p i c s

infra-structure. We show how anything purchased to detect eavesdropping from a “spy shop” will only waste your money and give you a false sense of security. We lay out the planning and execution of a successful sweep, and explain how to protect your company from threats in the future.

HTTP IDS Evasions Revisited

Daniel Roelker, Security Researcher & Software Developer, Sourcefire, Inc

HTTP IDS evasions have been prevalent ever since the release of RFP's whisker. But what's been happening since? This presentation addresses the advancement in HTTP IDS evasions since whisker. Some of the specific topics covered will be:

The evolution of protocol-based IDS and signature-based IDS in regards to HTTP evasions. What's the same and what's different?

Latest and greatest obfuscations in URL Encoding (what the IDS vendors don't know). We'll go into the various types of URL encodings, how the different types of Unicode encoding really work, and new encoding types and combinations that confuse IDS HTTP decoders.

Evasions using HTTP/1.1 protocol characteristics, in the spirit of Bob Graham's Sidestep program.

The following source code will be released to demonstrate and automate the various URL encoding methods and HTTP/1.1 protocol evasions tactics:

- Source code for automatically generating URL IDS evasions using the tactics discussed in the presentation.
- Source code for generating Unicode codepoint values on target IIS machines for further fun with URL obfuscation and evasion.
- Source code that profiles web servers for what types of evasions do and do not work against them -- hopefully this can be released.

[PANEL] Behind the Remailers: The Operators and Developers of Anonymity Services

Panel Lead: Len Sassaman

Panel members:

Peter Palfrader
noise

Michael Shinn

Ryan Lackey

Anonymity and privacy are cherished rights of Internet users. This panel brings together some of the key figures behind the Type II remailer network in operation today. Intended to be an audience-directed presentation, these panelists are prepared to answer all of your remailer related questions, from topics concerning remailer software development, usage, legal implications, social aspects, and personal experiences.

Online Corporate Intelligence

Michael Schrenk

A rapidly growing number of businesses use webbots and spiders to collect corporate intelligence about their competitors. This session will explore: the types of information companies gather about each other, where they get it and what they do with it. We'll also discuss: privacy concerns, methods for writing stealthy webbots, and various related opportunities for the community.

The Internet's Private Cops: Defending Your Rights Against Corporate Vigilantes

Wendy Seltzer, Staff Attorney, Electronic Frontier Foundation

It is not only governments that are engaged in surveillance of Internet activity. Increasingly, private actors, including corporations asserting intellectual property interests, are being given the power to police the network and demand user identities, in the name of enforcing their private interests. Even when the law does not give them the authority, some have been overzealous in sending legal threats claiming such rights.

This presentation will examine the legal claims (such as DMCA, copyright, trespass) frequently raised by private parties, your rights in response, and ways to protect yourselves from these threats, including via the Chilling Effects website.

Putting The Tea Back Into CyberTerrorism

Sensepost

Many talks these days revolve around cyber terrorism and cyber warfare. Some experts suggest such attacks could be effective - others say that targetted country-wide cyberterrorism is just for the movies...or a Tom Clancy book. In this talk we look at very practical examples of possible approaches to Internet driven Cyber Warfare/Terrorism. The talk will include an online demo of a framework designed to perform closely focussed country-wide cyber attacks.

_vti_fpxploitation

Matthew Shannon

With over 32,000 Frontpage enabled web servers currently on the Internet, it's easy to take it for granted. However, Microsoft Frontpage is one of the least documented and most misunderstood web authoring systems available.

In this presentation we will seek to close that gap, and expose the inner working of the Frontpage and Frontpage Server Extensions protocol. We'll show the hidden flags and undocumented options within the session data, many of which are unavailable even to Microsoft Frontpage users!

Plus we will debut new open source tools geared directly toward taking advantage of the Frontpage systems, including a Perl-Gtk Frontpage vulnerability scanner.

Our presentation will cover the following areas:

- Frontpage: An Initial Perspective “Breaking down the overall system, providing an overall process view.
- Frontpage: Decoding the System “Explaining the authentication system, the protocol spec, command sequence, and undocumented options
- Frontpage: Knocking on the door “Debut custom

tools built to specifically manipulate the authentication system and provide an open source Frontpage vulnerability scanner.

- Frontpage: What to do when your there"Provide a basic understanding of Microsoft's Active Server Pages Visual Basic language, and provide example hacker tools developed in ASP.
- Frontpage: Holding down the fort"Give those supporting frontpage the much needed information to help better secure their enterprise.

Theft of Service Attacks

Robert Sheehy, Zendtech.com

This talk will focus on the security holes prevalent in many subscription based service products such as Internet dial-up service, web hosting, software purchases, and satellite television. Specifically the talk will focus on various billing system attacks, application attacks, increasing account privileges to gain unauthorized or extended access to subscription content, and bypassing account restrictions; It will be demonstrated how these attacks are performed, and how to detect and react to them.

Increasing The Security Of Your Election By Fixing It

Daniel C. Silverstein

Damon McCormick

In response to the problems that plagued the last United States presidential election, many communities plan to replace existing paper ballot machines with electronic voting systems. Unfortunately, the new systems open up a Pandora's box of security issues that traditional paper ballots do not face. It is difficult to understand the issues because there is a serious lack of data describing the real world performance of these systems. This problem is compounded by the fact that the major commercial vendors' products are closed, proprietary systems

protected as trade secrets. Ignorance of the unique security concerns raised by electronic voting could leave US State and Federal elections open to unprecedented levels of fraud.

This past April, a new online election system was used at the University of California at Berkeley. We present this system as a case study, which sheds much needed light on electronic voting security. We describe the workings of this system, and discuss the findings of our security analysis. Additionally, we crafted a man-in-the-middle attack that exploits a flaw inherent in the system architecture. Our talk provides a detailed technical explanation of the attack.

Finally, we discuss the implications of the case study. We will show that many of our conclusions apply to the major commercial systems, in spite of tangible differences with the case study system. We will answer questions from the audience, and offer constructive ways to address some of the concerns we raise.

This talk is suitable for attendees of all technical levels. For a thorough understanding of our man-in-the-middle attack, we suggest that you have some programming experience and familiarity with DNS and NAT.

The UPS (Undetectable Packet Sniffer)

Spyde~1, Tri-Valley Security Group

AutoNiN

Mystic

Presentation of the UPS - the Undetectable Packet Sniffer: a Hostile packet sniffer posing as an Uninterruptible Power Supply. Complete HOW-TO: Hardware configuration, Software configuration, integration into a non-functional UPS, installation and use. Proof of concept project by the Tri-Valley Security Group (TVSG).

Hacking the Invisible Network: The Risks and Vulnerabilities Associated with Wireless Hotspots

Michael Sutton, Director of Product Development, iDEFENSE

Pedram Amini, Security Engineer, iDEFENSE

Wireless hotspots are emerging as an effective means of providing on-demand Internet access for users with 802.11x enabled devices. The networks typically exist in places frequented by business travelers, such as hotels, airports or in locations with persistent clientele such as coffee shops. The technology provides an efficient and cost effective way for companies to deliver Internet access to their customers and also offers an alternate revenue source, as many networks are "pay for play".

Most users are enticed by the convenience of these networks, but are unaware of the security risks that they present. Companies have historically implemented security by building an impenetrable fortress around network assets. This system is flawed. It does nothing to protect the multitude of portable devices such as laptops and PDAs that are frequently used outside of this fortress. Hotspots are shared networks that broadcast traffic. By design, hotspots do not implement encryption schemes such as WEP, which provides a target rich environment for malicious attackers. Unencrypted network traffic can be intercepted and traditional remote attacks can be perpetrated on machines that are operating without protection from attack. This poses a significant risk for corporations as these devices commonly contain sensitive corporate data.

Research conducted on numerous hotspot implementations has revealed that most leave end users unnecessarily exposed to both local and remote attackers. Most networks also have weak access controls that leave business owners exposed to loss of revenue from various attack scenarios such as session hijacking, data tunneling and connection sharing.

d c o b s p e a k e r s a n d t o p i c s

- The presentation will address the following:
- The risks associated with using Hotspots
- Specific attack scenarios – identifying tools and techniques that were used
- The network design of specific hotspot implementations
- What users can do to protect themselves

Hacker Generations: From Building the Network to Using the Network to Being the Network

Richard ThiemeThiemeworks

It has all happened so fast.

Eleven years of Def Con define three identifiable generations of hackers. (Yes, that's an arbitrary distinction, but it's useful.)

The first generation helped build the network, the second learned how to use the network, and the third has become the network.

The management of perception in the mind of society is the battle in which we are now engaged. Online life is threaded through with deception and counter-deception, intelligence and counter-intelligence, but that's second nature to the latest generation of hackers. They understand that intuitively. They operate in small cells, manage their egos with discipline, and execute stealthy sophisticated operations with finesse.

The Story of EFFI: How We Started a Cyber-rights Group in Finland, Which Kicks Ass

Mikko Valimäki, Chairman, EFFI - Electronic Frontier Finland

Ville Oksanen, Vice Chairman, EFFI - Electronic Frontier Finland

We want to show you how just a couple of fellows can start a truly efficient cyber rights group at a regional level (state, country etc) and influence the encryption, privacy, fair use etc laws & change the public opinion. We did this in Finland in a year.

EFFI was founded in 2001 and now, in summer 2003, has some 300-400 paid members and counting. We got to the nation's main newspapers in spring 2002 and hit the radio and TV in fall 2002 and been since then regulars in the media. Our top achievement so far has been stopping EU Copyright Directive (Europe's DMCA) in Finland. We've also fundamentally changed the law on the freedom of speech and spamming (see <http://www.effi.org/> for details).

Next, we'll answer basic questions on how we get there. Who proposes these laws and how can even individual hackers and tech enthusiasts influence the legislative process? How did we build relationships to politicians? How did we get ourselves to TV regulars in Finland and changed the public opinion to our support? How can we extend our regional success to European level?

Finally we want to explain why the political, moral and legal issues are inherently global and why the hacker community should support action in every corner of the world. We get into details of US and European hacker-unfriendly politics and compare different options to support our common cause: influence parliamentary and democratic process vs. act independently & anonymously hacking the software of "evil corporations". Our approach is to act with names and do everything politically correct.

Network Worms, What Is Possible

Jonathan Wignall, Data & Network Security Council
Network worms have been around for almost as long as the computer networks they need to spread via, but it only with the advent of mass internet access that they have become commonplace. This presentation will outline what network worms are, and how they differ from a 'normal' computer virus. but in the main concentrate on what future worms could achieve.

The presentation will look forward to what we could see in both the near, and far future giving examples of what can be

developed. Web replication and other possible distribution methods will be discussed and you will learn why so few worms currently effectively achieve mass distribution.

No prior technical knowledge is required of the audience, and should be understandable by those with limited knowledge of computers, although greater knowledge will be a plus.

Deploying DNSSEC

Paul Wouters, in close collaboration with NLnetlabs, RIPE NCC and the FreeSwan Project

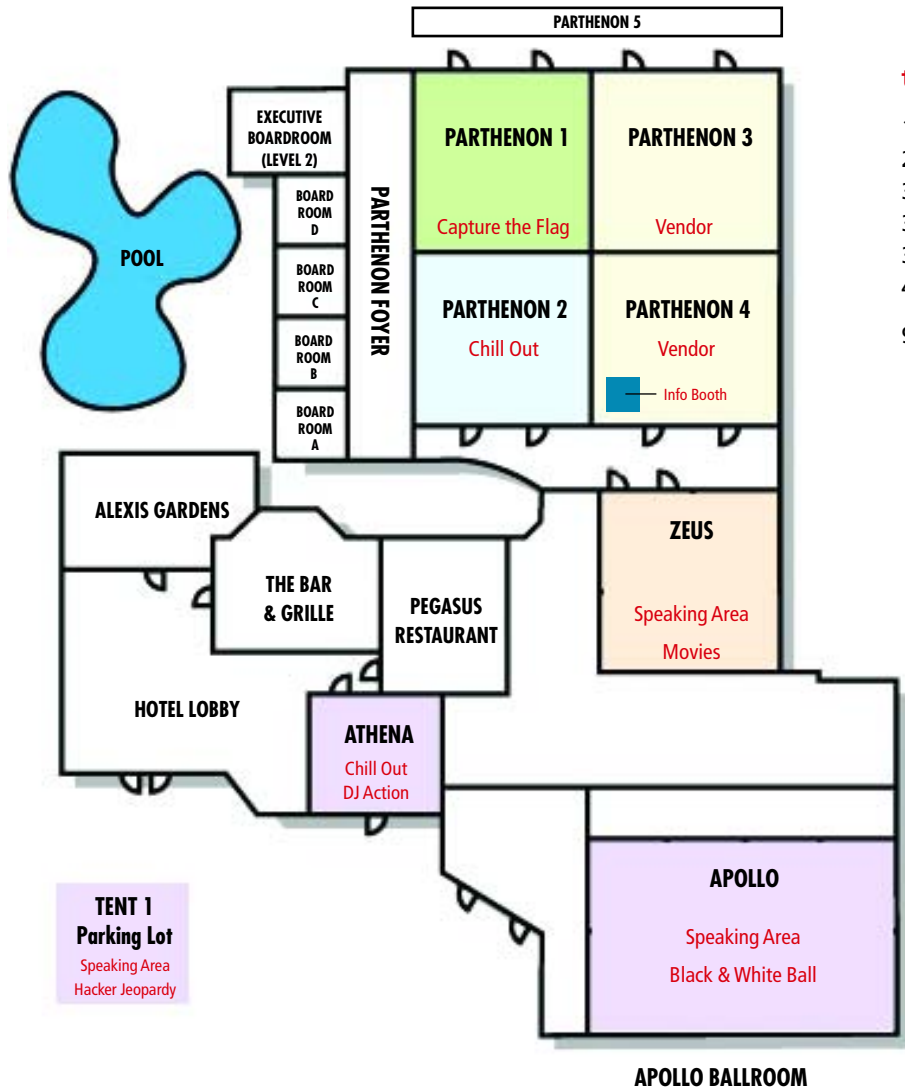
Although DNSSEC is still a moving target, it has matured enough for large scale experimenting. The first part of the presentation explains the new concepts in DNSSEC and the new record types introduced. Rudimentary knowledge of DNS is required.

The second part of the presentation is a step-by-step guide using Bind to secure an existing zone. Participants who wish to secure their own domain need to have the latest Bind9 snapshot and a copy of the zones they wish to secure.

The third part of the presentation will demonstrate the interaction between the Registrant and the Registrar. The Dutch SECREG system will be demonstrated for securing .nl domains at the ccTLD. The VeriSign experiment will also be shown on how to secure the generic TLD's. Time permitting, participants are invited to try and compromise the Speaker's secured zones.

A Conversation with Phil Zimmermann

Phil Zimmermann, creator, PGP



tune in to the con

- 16 Tent Speaking Channel
- 29 Movie Channel
- 32 Athena Speaking Channel
- 33 Zeus Speaking Channel
- 35 CTF Channel
- 42 Josh's Enigma Channel (Truly random noise :-)

93.7FM DC radio hosted by DMZ

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



art by Yodaboy
www.yodaboys.com

DMZ

Thanks to, in no particular order for they are all worthy of mucho props:

SH0UT0UT SH0UT0UT

Major Malfunction, Zac, Ping, Noid, Lockheed, Black Beetle, DJ CM0S, Tina, Cal, Bro, McNabstra, Cat Okita, Sleestak, B.K., Agent X, TechnoWeenie, Gonzo, Josh, Everyone on the DC Forums, Skrooyoo, Spun0ut, CHS, Priest, Bink, Evil, Roamer, Xylorg, Heather G, Flea, Justabill, Pescador, Queeg, Teklord, Cyber, Stealth, Ming of Mongo, Grifter, Monk, LRC, Xam, RussR, Zain, Shatter, Caezar, DevinC, JayA, Kampf, Kruger, The People, Artimage, Anti-Bill, Nulltone / Grifter / Blackwave / Simon for the DEFCON Forums, Humperdink, The Ghetto Hacker staff who ran CTF, Chris, 23.org for general support, Moloch.org, LA2600, the ISN and BugTraQ mailing lists, dedhed, Arclight, World Wide War Drive crew, Jesse, Vandul, Timo, Scott Post, Mark W, Charel, The Alexis Park Staff, Winn for HJ, Dead Addict, Ghent, resonate, SD, Uncle Ira's Fun Farm O Death, the whole FreeBSD project, the OpenSSH and OpenSSL projects, D A/V Las Vegas (lighting support), Las Vegas Sound & Video, Dan Bernstein for QMail, Sidewinder, the JAP team for making web browsing more anonymous, all the people who sent in suggestions after reading my letter to the community, and anyone that took the time to create artwork, submit a slogan, organize a car caravan, maintain an archive of pictures, or generally help the underground scene and the con.

Note: After you have stumbled home, recovered from your hangover, patched all the vulnerabilities you have just learned about, restored your warez, and caught up with 3 squares and some sleep, please take some time and let us know what happened! Email us with evidence, links to anything con related, picture archives, stories, news articles, video, etc. We are trying to preserve our history and are looking for any and all things DEF CON.

Until next time,
The Dark Tangent