Welcome to DEF CON7.0! Because we are ina new hotel, please don't burn it down. Also if you have any questions, please feel free to contact the Goons(tm), who are your friends. Really. I wouldn't lie to you.

So, there will be a lot going on this year, and due to the size of the convention, there will be many things going on that we don't know about right now. It's up to you to make the most of it. We provide to venu, you provide the content. I won't bore you with a long intro, as most of this will end up on the floor in a few hours, so I'm providing the bare bones info here. - The Dark Tangent

Events Schedule

Friday	Big Area A	Area B	Area C	Area D
10:00-				Vendors open up
11:00-				Capture the Flag (CTF) Starts up
14:00-21:00				Hacker Death Match! First come, first served, sign up at the sign in area.
19:00-02:00		IRQ Conflict battle contest! Win prizes 'n stuph		
23:00-01:00			1st & 2nd round of Hacker Jeopardy	
Saturday				
12:00-05:00		Bands play on through the night!		
19:00-02:00				
19:30-21:00		IRQ Conflict battle contest! Win prizes 'n stuph		
21:00-23:00	The Black & White Ball		2600 will show a 10 minute clip from their movie	
23:50-01:11+			Third and Final Hacker Jeopardy rounds!	
Sunday				
16:00-		Capture the Flag prizes awarded		

Bands & DJs

Bands & DJs

Artist	Style	DJ or Band	Notes
DJ Crash	Industrial	DJ	Club Corrosion
DJ JerkFace	Industrial	DJ	Club Corrosion
DJ Delchi	Goth/Industrial	DJ	Fang Club Gotham
Jackalope	House	DJ	Colorado
CorruptData	Jungle	Band	Las Vegas, NV
Ripe	House	DJ	Chicago, IL
AJ Reznor	Industrial	DJ	Hells Kitchen
Thomas Ockens	House	DJ	Germany
Stevyn	Lounge/Techno	DJ	Iron Feather Journal
Garph	New Wave (?)	DJ	Bakersfield, CA
HiBias	Trance	DJ	All Passion
DJ Wonderbread	Phunky Breaks	DJ	LA, CA
The Public	80's	DJ	303
DJ Atari	Electronic	DJ	
DJ Medik	Electronic	DJ	
Max	Techno	DJ	LA, CA
Dis=co	House	DJ	Colorado
DJ Wedoe	House & Trance	DJ	LA, CA
Delinquent	House	DJ	All Passion
Jester47	Tekno	DJ	Seattle, WA
CheezeFish	Dance	DJ	Unknown
Ravnos	Jungle	DJ	Unknown
Orion	Industrial	DJ	LA, CA

AFIRM: IEC announces the first release in a series of papers on Adaptive Network Security and Proactive Computer Forensics. AFIRM & SANE provide an open and extensible foundation for comprehensive network security and creates an "Audit Friendly" environment. The first paper "Entitled XXYYZZ" will be released at Defcon VII in Las Vegas Nevada on July 9, 1999. Access to all AFIRM content available http://www.AFIRM.org. Pr0filer: HSK teams up with IEC to produce the first AFIRM certified product ever! Pr0filer is positioned to fulfill two very distinct goals. 1. To produce a publicly accessible enemy profiling database. 2. To refine the techniques for analyzing and rating said data. Project Pr0filer starts July 9, 1999 with the official kick-off at Defcon VII (http://www.defcon.org). A thirty-day open comment period will provide an opportunity for public comment and the creation of a base-line database. After thirty days public access to DB query will be available. Access to all Pr0filer content available at http://www.pr0filer.com.

EVENTS!

The Fourth Annual Black and White Ball - DJs spin music, and people dress up all spiffy. This is the third official year of this, which started all by itself back at DEF CON 3, when for some reason people started dressing up for no reason before going out on the town. A tradition is born! This year we'll take some pictures and have a voting booth for most crazy outfit, most swank, etc.

Hacker Death Match! - Always wanted to beat up some punk on the mailing list? You really hate the person who always argues with you? Who's tougher, Old Skool hackers or New Skool hackers? How about the Media vs. the Underground? Feds vs. Hackers? It is all possible now! We've rented giant inflatable sumo suits for you to do battle in. The first person to knock the other outside of the ring or down gets a point.. at the end of your match the person with the most points wins! Friday afternoon beware! Who is the master of the universe?

HACKER JEOPARDY: Winn Schwartau is back with Hacker Jeopardy!! The FIFTH year in the running! With his sexy sidekick, Vinsi Vana, and the ever present judge The Dark Tangent, get ready for a wild ride through hacker trivia, social and science questions. One year there was a question about a bird! (If you want to check out some questions, look at last years) This is how it works.. We supply the beer for the contestants, you supply the answers. The first round starts at 11pm on Friday and lasts until it is done. The second and secret rounds will happen Saturday at midnight and go through final jeopardy. If the host botches a question, he drinks. If contestants are cheating or sneaky, they drink. 6 teams will be picked at random and compete for the final round. There can be only one! [More rule clarifications soon]

Spot the Fed Contest - 6th ANNUAL SPOT THE FED CONTEST: The ever popular paranoia builder. Who IS that person next to you? "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

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 my attention and claim out loud you think you have spotted a fed. The people around at the time will then (I bet) start to discuss the possibility of whether or not a real fed has been spotted. Once enough people have decided that a fed has been spotted, and the Identified Fed (I.F.) has had a say, and informal vote takes place, and if enough people think it's a true fed, or fed wanna-be, or other nefarious style character, you win a "I spotted the fed!" shirt, and the I.F. gets an "I am the fed!" shirt.

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: 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. Be stealth about it if you don't want people to spot you. Agents from foreign governments are welcome to trade too, but I gotta work on my mug collection and this is the fastest way.

Capture the Flag (CTF) contest - The question still remains, can anyone stand up to the power of Team SNI? The playing field is a 10bT ethernet segment with 3 groups on it.
1) The Bastard Operators from HELL(BOFH) - folks who want to be on the BOFH side have to either set up a bastion host, or a firewall with an unhardened host behind it. The hosts have to be running useful services & have user accounts. If you set up a host you should be able to point to it and say "that's a mailhost" or "warez site" or quake/Icecast server, etc. BOFHs win by running the coolest services and getting hacked the least.
2) The (L)USERS - Anybody who wants to should be able to walk up to an admin and ask them for an account on their host. What the admin gives you depends on the type of server they set up. The account should be enough to actually get mail from the mail server, play quake on the quake server, etc. Lusers can't win, they just get to use the servers.
3) The hackers. nuff said. - Hackers win by putting their team name or handle in a file in the root directory of any host on the network. To count, the file has to stay there long enough for a goon to verify it. Whatever hacker or team racks up the greatest number of hosts wins. (how can you tell the users from the hackers? If you figure that out, talk to me. I've got a job for you)
The rules:
1) No taking down the network or any host you didn't bring for more than 60 seconds. 2) no taking down a host you did bring for more than 5 minutes. 3) If your mail host doesn't run any mail protocol known to man we laugh at you, spit in your jolt & you don't win. 4) 10 points for style. Admins and hackers get prizes based on how stylish their host/hack is. Points will be taken away from you if you do stupid DOS attacks. (*clever* DOS attacks (if there is such a thing) could *win* you points) 5) No thuggery, summoning of elder gods/ Mickey Finns/ physical coercion.

Quake2/3 battle net - The irQconflict (http://collusion.org/conflict) will be in setting up for a Quake2/3 battle royal...so don't forget your gaming rig! The irQconflict is a unique experience, providing a gathering spot for gamers to compete for hundreds of dollars in prizes in a tournament setting unavailable to the average gamer geek sitting at home or gaming on his handi-hub with his 4 friends.

The Second annual "Who are you, any ways?" social engineering contest. The D.C. crew, after many hours of alcohol ingestion in our /dev/house headquarters, have formulated a plan that will measure the SE skillz of those brave enough to step to the challenge. Registration will be accepted in advance for individuals or teams, who will be given approximately 15 minutes to achieve a mission that will be provided 15 minutes before the clock starts. These missions will be executed via telephone, in a separate Telephone Booth, with audio piped out to the Con area. Our esteemed panel of judges (who prefer Purple Motherfuckers, for those inclined to bribery) will determine the DefCon 7.0 SE Stud/Studette based on ability to retrieve information, creativity, and overall style.

STREAMING AUDIO AND VIDEO: There will be various audio and video streams generated this year. Check the homepage http://www.defcon.org/ during the convention to select streams. RealMedia stream will be mirrored by the pirate-radio servers (http://www.pirate-radio.co.uk) in (at least): UK - Telehouse, INSNET USA -DEF CON Seattle

The Official DEFCON Shoot (3rd Annual!) is happening again. It's slated for Saturday morning at 8AM round up to go off to the shooting site. Be awake!
Live Band action - Currently the following acts are booked. Now, this is only the list of booked DJs/Bands..this IS NOT the set list, so don't get yer panties in a bind.

Speakers Speakers

Steven Alexander Firewalls: Trends and Problems. This talk will cover some of the new firewalling trends and how many of them are detrimental to security. The focus of this talk will be on how the discussed trends work and how they can be used by an attacker to defeat security, and how security problems can be avoided. The discussion will not cover specific products in order to allow anyone to apply the subject matter to their current configuration. Steven works for a small ISP, attends his local college as a math major and spends his free time studying cryptography.

Angus Bitter Fear and Loathing in Cyberspace: The art and science of enemy profiling. Quickly identifying your opponent, in any conflict, can mean the difference between success and failure. Knowing their capabilities, resources and limitations can provide the tactical advantage. The lack of this type of decision support is a serious deficiency in most information warrior's arsenals. Relying on single source intelligence is pure folly. Charlatans and carpetbaggers are salivating at the millions in government and corporate dollars earmarked for such a competitive advantage. Our discussion will provide a working definition for "profiling", how it is used and why it effects everyone! Angus Bitter is the founder and Grand Poopa of HSK.

Dr. Byte IPv6: Who/What/When/Where/How/Why. The Internet Protocol has undergone substantial changes in past few years from version 4 (Classical IP) to version 6 (Next Generation IP). This presentation will overview who's using the new protocol, what the new protocol's features are, when it will become mainstream, where it's being deployed, how the transition from IPv4 to IPv6 is planned, and why we need a new fundamental protocol on the Internet. This speech will contain many technical details and will assume the knowledge of the basics of TCP/IP. Dr. Byte is a Ph.D. candidate in Computer Engineering and an instructor of Computer Engineering at a major university. He received his B.S. and M.S. in Computer Engineering in 1994 and 1997 respectively. For his M.S., he worked with a real time bit error rate simulator, and developed a next generation real time hardware system for bit error rate simulations. He has developed a 16 bit RISC microprocessor in VHDL in a Field Programmable Gate Array (FPGA) able to run compiled 'C' code. His research interests include developing a taxonomy of attacks and applying it to different network environments. He has co-authored 3 papers on IEEE 802.11 and IPv6.

Cyber How to use BSD to set up a firewall/gateway. This talk will cover the basics of using free software to setup a firewall/gateway machine. Basic concepts will be reviewed, and why certain things are important will be covered. Ideal setups as well as practical solutions will be discussed. Step by step instruction with examples will be given. Q/A will be done time permitting, slides will be availible online. Erik has done computer security for a number of years. He has added crypto layers to existing products, as well as designed and implemented the security authentication and authorization model for an internal account control system for a major US bank. He currently works as a consultant for KPMG LLP.

Cult of the Dead Cow BO2K! What will we be doing? R0xiN the HAU-aus, BlizaTch!!!@@!2121!!... But that goes with out saying. In addition to the rocking of the aforementioned house, we will also be releasing BO2k. We won't reveal our secrets of BO-Fu, but trust me when we tell you that it will make BackOrifice v1.0 look like LOGO for the TI99/4a. Founded in 1984, the Cult of the Dead Cow (cDc) is the oldest group still active in the computer underground, the only group (aside from a few tayniep1RaT3 gR0oPzZz) with a female group member; the only group to host its own annual HoHoCon hacker convention; and, with over 300 text files in circulation, the most prolific group. cDc is definitely cooler than the Legion of Doom (LoD), and more importantly, our T-shirts are more colorful. We also have stickers. Great, you may say, but have we ever disrupted communications on two continents by moving telecommunications satellites? Mhm. Hacked computing resources belonging to the three-letter agencies and the Pentagon? Yep. Altered environmental controls in local malls via modem? Done that. But unlike other hacker groups you've undoubtedly read about, we've never been caught. With qualifications like these, it's not surprising that over the past few years, the media has looked to us as the darling boy (and girl) torch-bearers of the DIY-cyber-hacker-underground movement. It's our unfortunate cross to bear. But as the whole of Generation X follows our lead into the new millennium, we feel it is our duty to our peers to maintain the struggle and "raise high our freak flag," as it were. On their behalf, we intend to dominate and subvert the media wherever possible. Information is a virus. And we intend to infect all of you.

Daremoe The Firewall Appliance: Friend or Foe? An introduction to appliance firewalls. What they are, how they work and what you can expect when you encounter them in the wild. These "new breed" firewalls are popping up everywhere, so be prepared when you meet them... Daremoe is the Alpha-Dog of the WolfPak, a "614 based group of security minded individuals". He is an independent computer security consultant withover ten years experience in e-commerce. He has just completed a comprehensive evaluation of appliance firewalls and

Dead Addict After working for The Man (TM) for several years, DA is finally working for the little guy - implementing worldwide financial systems for multinational banking corporations. He will speak on currency systems, credit systems and associations, SET technology, its message flow, crypto usage, implementation issues, and surrounding industry issues. He will alsobriefly discuss security issues with current e-commerce implementations.

Charles Faulkner Hacking Human Minds Human expertise is not found in the sum of explicit practices or algorithms. It's in the experience, mental models and heuristics of individuals. Invisible to current Knowledge Engineering, psychology and (most) linguistics, these 'rules of thumb' are available (can be hacked) through specific pragmatic, syntactic, and semantic 'fillers/handles' that can be detected, influenced, and transferred. Applications / instantiations to humans achieved. Computing and human/computer interface applications sought. Charles Faulkner is a hacker (modeler, in polite society) of human experience and expertise whose projects have included language acquisition, futures trading, metaphoric communication, and object oriented software testing.

Prof. Feedlebom Followup on Micropower Radio. Last DefCon, Prof. Feedlebom led a discussion on Micropower Radio that kinda glossed over a lot of the technical details. This year, he returns to discuss in more detail some of the things required to place a micropower station on the air. Will also include a short synopsis on the current state of Micropower Radio, including the effort to legalize it in the United States. Handouts from last year's session will be available for those who did not receive them in the mail (sorry).

Prof. Feedlebom has operated The Voice of Mercury and the Desert Crossing Radio broadcasts for the last five years. While he's taking the year off this year from the Big Broadcast, he has been responsible for strange radio emissions that have been heard in Los Angeles and Kern Counties on a variety of frequencies. He also acts as the chief engineer for Radio Invasion, a former micropower station now broadcasting through Real Audio.

Freaky Macintosh Security. From the Author of Freaks Macintosh Archives, Freak will be hosting a topic this year at the con about macintosh security, the programs out there and their flaws. Some new programs will be released for the macintosh platform to help secure your MacOS. And more programs will be released to Exploit your mac and many other platforms.

Speakers' Speakers

Gh0st Phreaking and PBX tricks

Ian Goldberg ZeroKnowledge Network (zks.net) Using the Internet Pseudonymously. One Year Later Last year we told you about the plans for the Freedom network from Zero-Knowledge Systems: user-trivial, strong-crypto, pseudonymous use of the Internet. See how far we've gotten now. We will present the current status of the network, and discuss the challenges and obstacles we've encountered along the way.

Sarah Gordon Viruses on (and off) the Internet, Panel Session. Computer viruses are currently freely available on the Internet, as well as via various mailing lists. The recent Melissa virus incident has focused attention on some issues surrounding the public availability of viruses. The panel (representing virus writers, antivirus product developers, open source advocates and academics) will represent a wide range of views on topics such as: "Is it cool to make viruses available via the Internet? Is posting of viral source code to mailing lists as a 'necessary evil' which can force developers to improve products. Should virus writing itself be illegal?". We want to hear "your" views, too, so the session will end with Q&A interactive. Sarah Gordon graduated from Indiana University with special projects in both UNIX system security and ethical issues in technology. She currently works with the anti-virus science and technology R&D team at IBM Thomas J. Watson Research Center. Her current research projects include development of antivirus product certification standards, test criteria, and testing models. She has been featured in publications such as Forbes, IEEE Monitor, The Wall Street Journal, and WIRED, and is published regularly in publications such as Computers & Security, Network Security Advisor and Virus Bulletin. She has won several awards for her work in various aspects of computing technology, and volunteers in an advisory capacity to Virus Bulletin, The WildList Organization, and The European Institute for Computer Antivirus Research.

Jennifer Granick The Legalities and Practicalities of Searches and Interrogations. Jennifer Stisa Granick is a criminal defense attorney in San Francisco, California. She defends people charged with computer-related crimes, as well as other offenses. Jennifer has been published in Wired and the magazine for the National Association of Criminal Defense Lawyers.

Natasha Grigori ACPM Grand Announcement The Anti Child Pornography Militia will be making a showing at the 7th Annual DefCon Conference in Las Vegas, Nevada on July 9th - 11th. The ACPM will be actively recruiting individuals sympathetic to our cause and willing to take an active role in the battle to eliminate child pornography from the Internet. "We have big plans for DefCon", says Natasha Gregori, founder of the ACPM. "Not only will we be recruiting from a Hospitality Suite at the Convention,and seeking sponsors and allies; Plans are in the works for ACPM to make a presentation during the three day event, and be introduced by a major personality in the community." The Defcon Conference will also signify the commencement of operations for ACPM, after 5 months of preparation, organization, and amazing growth from its original one-woman cause. "I feel confident that the kick-off will be a success," Lawless, Director of ACPM Education, "from there, we will begin entering the political arena, lobbying for tougher enforcement against child pornography online, while assisting in any way possible with current enforcement." The Anti Child-Pornography Militia (ACPM) is an organization committed to removing child pornography from the Internet. Child Pornography is readily available on the Internet from Usenet, web sites, and chatchannels. These photographs of children, used to feed the grotesque sexual desires of pedophiles, contribute to the rising numbers in child sexual abuse cases world wide by emboldening and enticing potential perpetrators into committing acts of child abuse. The ACPM will be working to achieve its goal of Zero Child Pornography through legal, political, and legal technical means. The ACPM in no way promotes or condones illegal attacks against individuals or computers connected to the Internet.

Bennett Haselton The "Anti-Censorship Proxy" and technological circumvention of Internet censorship. Bennett Haselton has been publishing studies of Internet censorship software since 1996. His reports have been used as evidence in First Amendment court cases filed by the ACLU and People For the American Way, and he has been invited to speak on Internet censorship at Computers Freedom and Privacy 99, the American Library Association national conference, the ACLU of Ohio annual conference, InfoWarCon 99, and Spring Internet World 99. Peacefire's reports criticizing censorship software have been featured on CNN financial news, MTV Court TV, and MSNBC.

Christian Hedegaard-Schou What is opensource? This talk will focus on what opensource is, what it isn't, debunking some myths, showing some examples, and giving reasons why opensource is ready for the real world. This talk is primarily aimed at government and corporate IS/MIS/IT staff and managers, but anyone who's curious as to what this "open source" thing is they've heard so much about in the past months are encouraged to attend. Christian Hedegaard-Schou I is a private contractor and consultant who first embraced opensource about 5 years ago when he discovered linux and installed it over his DOS partition. He's never gone back. Since he first discovered linux he also played with FreeBSD and NetBSD on various architectures, and has been a proponent of Free software, GNU, and the newly defined "open source"

Kevin Higgins Nevada Attorney General Will do a brief thing on a topic near & dear to his heart then open the session to an "ask the prosecutor" Q & A so people with Burning Questions can ask about whatever interests them.

Jericho Fakes Walk Among Us. The recent explosion of the security industry has found itself littered with newcomers, all 'experts' in the field. Unfortunately, many of these 'experts' are nothing more than self proclaimed windbags that are no more qualified to help you with security than your local 6 year old. How do these charlatans manage to find work? Why are they accepted? More important, how do you distinguish legitimate security professionals from the fakes? These are valid concerns in today's security community. Answers to follow? Jericho is a security consultant (read: not an expert) working almost full time these days. His travel has taken him to standard corporate networks, to consulting for wacky spooks that everyone fears. On top of run-of-the-mill consulting, he has participated in network analysis via penetration testing, computer forensics and more. He hates crowds. :)
James Jorasch "Hacking Las Vegas." If you missed it lasst year, don't miss it this year. Excellent.

Phillip J. Loranger, Office of the Secretary of the Army, Office of the Director, Information Systems Command, Control, Communications and Computers (ODISC4), Information Assurance Program Management Office The ethics/morality/practicality/patriotism of hacking

Robert Lupo Introduction to computer Viruses. This class covers how different virus work and how to defend agent them, including: Boot Sector Virus, File infecters, Multi partite, Macro, and Fakes in the world.

Steve Mann Inventor of the so-called "wearable computer" Steve Mann, inventor of the so-called "wearable computer" (WearComp) and of the EyeTap video camera and reality mediator (WearCam), is currently a faculty member at University of Toronto, Department of Electrical and Computer Engineering. Dr. Mann has been working on his WearComp invention for more than 20 years, dating back to his high school days in the 1970s. He brought his inventions and ideas to the Massachusetts Institute of Technology in 1991, founding, what was to later become the MIT Wearable Computing Project. He also built the world's first covert fully functional WearComp

with display and camera concealed in ordinary eyeglasses in 1995, for the creation of his award winning documentary ShootingBack. He received his PhD degree from MIT in 1997 in the new field he had initiated. He is also the inventor of the chirplet transform, a new mathematical framework for signal processing. Mann was both the founder and the Publications Chair of the first IEEE International Symposium on Wearable Computing (ISWC97). Mann has chaired the first Special Issue on Wearable Computing in Personal Technologies Journal, and has given numerous Keynote Addresses on the subject, including the Keynote at the first International Conference on Wearable Computing, the Keynote at the Virtual Reality conference, and the Keynote at the McLuhan Conference on Culture and Technology, on the subject of Privacy Issues and Wearable Computers. He can be reached via e-mail at mann@eecg.toronto.edu.

Michael J. Martinez Hackers and the Media: A Love-Hate Thing. For hackers, contact with the media is both exciting and frustrating. Everybody loves to grab that 15 minutes of fame and set the record straight, but the media has this annoying habit of getting things wrong, at least from a hacker's point of view. Mainstream reporters feel the same way — hacking is cool, sexy, and guarantees readership. But hackers are so evasive, way too full of themselves, and then there's this godawful technology to try to understand. How can reporters and hackers work together, or at least understand each other? Michael J. Martinez reports on technology for ABCNEWS.com. In addition to covering more mainstream issues, Martinez has written about hacker culture, the VX community, the Pentagon's "cyberwar" problems, and the melissa virus. His articles have been featured on Slashdot and the Hacker News Network.

John Q. Newman Speaking on "Topic One" and Topic Two" For privacy purposes Mr. Newman's biography is not listed here. He is a recognized expert in the field of privacy and protection of personal information. He has been a DefCon presenter in the past and shared interesting information related to credit report interpretation and personal anonymity.

Michael Peros Privacy Electronics - Detecting wiretaps This year I would like to speak about how to identify body wires, recorders and government informants. Also I have verified from a very reliable source that President Clinton passed a wiretap bill through executive order of the White House allowing the Federal Government to Wiretap and intercept electronic oral communication without a warrant. This came into law as of January of 1999. He did not have to go in front of the congress to bring this into law.

Deanna Peugeot Embedded systems hacking. Embedded systems can often go where the average hacker cannot. They don't reside on the server to be detected by a vigilant sysop, nor do they need the dedicated resources of a computer. But no one in the hacking community seems to be taking advantage of this arena. This will cover the possible uses for a custom embedded system and how to go about creating it.

Kevin Poulsen The Legalities and Practicalities of Searches and Interrogations. You all know who Kevin Poulsen is. If you don't, please go learn.

Brian Ristuccia The "Anti-Censorship Proxy" and technological circumvention of Internet censorship. Brian Ristuccia's Anti-Censorship Proxy (ACP) is a tool for circumventing network-level Internet censorship. It combines functionality of older software such as PGP, Anonymizer, and steganography software, enabling Internet users to bypass firewalls and proxy servers without detection. ACP can be used to circumvent firewalls used by China and Saudi Arabia to block criticism of their governments, or to bypass software used in American schools to censor pages about contraception, animal rights, and many non-Christian religions. These countries and institutions are likely to crack down on the use of such software, provoking an "arms race" between ACP developers and their opponents. (The use of strong encryption in ACP may even conflict with some countries' import/export regulations.) This talk will describe the ACP and look at some of the directions that such an "arms race" might take, as well as describing real-world implementations of network-level censorship (in China, Serbia, the Middle East, as well as many U.S. schools), what kind of content is censored, and how the ACP could be used to bypass these restrictions. More information at http://ians.978.org or http://www.peacefire.org/bypass/Proxy/

Rooster Insecurities in Networking Devices Routers and switches. These devices make up the core of what is networking. Devastatingly important, this infrastructure is key to a properly working environment. Amazingly, many administrators don't know the weaknesses and holes that are being exposed to the Internet. This talk will discuss the most common security issues in routers and switches, how they can be exploited, what a person gains from this, and how to prevent people from gaining access to your network equipment. Rooster has extensive knowledge of systems and networking. His experience includes all manner of networking and systems including: ATM, BGP, Gigabit Ethernet, FDDI, etc. Rooster is currently a network engineer at a fortune 500 company where he maintains the Internet connectivity.

Craig H. Rowland How to be aware of security problems on your network. A critical component of network security is being aware of what is occurring on your systems so you can spot security problems before they become a big headache. The Abacus Project is a suite of free security tools that allows administrators to monitor critical aspects of system operations on a variety of Unix hosts to help increase their awareness. The core components of the project attempt to address the more common indicators of an attack such as: 1) Strange messages in audit files indicating errors or invalid input that indicate security problems 2) Port probes that are a pre-cursor to attack and compromise 3) Compromised user accounts and suspicious user activity. The three currently released tools address the above issues using generic techniques that work on a number systems. These tools are: Logcheck, Portsentry, and HostSentry. This talk will detail why it is important to watch your systems closely for problems and how these and other free security tools can help bolster your site security using a variety of simple techniques. Craig is a security software developer and consultant currently working for Cisco Systems Inc. His area of focus falls into network attack tool programming and intrusion detection systems. He is the author of several free security tools on the Internet and maintains the Psionic Software website to distribute security tools, papers, and advice.
Gail Thackeray Maricopa County Prosecutor, AZ Will do a brief presentation on a topic near & dear to her heart then open the session to an "ask the prosecutor" Q & A so people with Burning Questions can ask about whatever interests them.

Jason Scott TEXTFILES, G-PHILES, AND LOG FILES: Remembering the 1980's Through ASCII In the 1980's, life started to move online, bringing with it all the wonder, terror, and breadth of human nature. Most markedly, an entire generation of teenagers turned their energies and efforts onto this growing culture and turned the world of Bulletin Board Systems into a combination street corner and clubhouse, sharing their knowledge, lying and bragging into infamy, and creating a shared experience that lasts in their hearts and minds to this day as they become the foundation of the Internet Society. While the unique forces that combined to make BBSes the experience they were have since shifted and formed other cultures in the years since, a feel for the 1980's can be found in the Textfiles (also known as g-files or 'philes') that nearly every self-respecting BBS traded, offered, or created as a matter of gaining notoriety (and more importantly, callers) in a sea of similar voices. In these textfiles, readers can reminisce or learn anew about what the BBS experience meant to those who lived through it, and easy parallels can be drawn to the 'scenes' that are now thriving online today. This talk will attempt to give historical perspective and narrative to the BBS 'scene' of

Speakers Speakers

today. This talk will attempt to give historical perspective and narrative to the BBS 'scene' of the 1980's, presented by a user who was around for a good portion of it and took notes. Expect shouted refutations from the audience and eerily familiar battles waged across the message boards to live again. Jason Scott (Formerly The Slipped Disk) has been an observer and participant in the world of BBSs since about 1982, cutting his teeth on Boards such as OSUNY, Sherwood Forest II and III, Milliways/Outland, The Dark Side of The Moon AE-BBS, as well as hundreds of others. His experience in BBS culture of the 80's ranges from Compuserve and The Source to Deversi-dials, AE Lines and anything else that gave a carrier when you called it. He is best known as the SysOp of The Works BBS, a textfile-only board that he ran from 1985-1988 before switching to SysOp-At-Large from 1989 to the present. Realizing an entire generation's shared lore was being diluted and lost, he has started the site www.textfiles.com, dedicated to preserving all things ASCII from the 1980's. This web site is slowly killing him.

Winn Schwartau HERF Guns, EMP Bombs and Weapons of Mass Disruption (UnClassified) At DefCon III, Winn Schwartau talked about High Energy Radio Frequency Guns, Electromagnetic Pulse Bombs and assorted nefarious weapons. Trouble is, the government doesn't admit to a thing. However, through constant research, he has found more than the government would like. The August issue of Popular Science, due out on or about July 15 will feature Schwartau's article on these emerging devices – but you will get an early peek at DefCon 7 on Saturday afternoon. Russian HERF and EMP devices for sale world wide. Some are even on the Internet! Terrorist level weapons made in a garage for less than $600 and put out an E field in excess of 1MV/meter. A video of real HERF at work. Be ready with your questions and Schwartau, as usual, will have answers

Peter Shipley Intro to TCP/IP exploits.

Simple Nomad Overview of activities at the Nomad Mobile Research Centre. Simple Nomad will give an overview of activities at the Nomad Mobile Research Centre, provide status on several projects, and give a detailed overview of NMRC's latest Netware hacking tool, Pandora. The new version of Pandora sports a "point, click, and attack" GUI interface, and works against Novell Netware versions 4.x and 5.x. Simple Nomad is the author of several FAQs on hacking, including "The Hack FAQ" which is a combined FAQ covering Netware, NT, Unix, and web technologies. The Nomad Mobile Research Centre is a non-profit organization dedicated to independent computer security research, with a focus on corporate-deployed commercial file servers.

David Sobel General Counsel to the Electronic Privacy Information Center - "Internet Anonymity Under Assault: The 'John Doe' Lawsuits". Several recent court cases around the country highlight an increasingly popular litigation tactic: the use of civil discovery to unmask the identities of anonymous Internet posters. In the last few months, a growing number of corporations have issued subpoenas to Internet service providers (ISPs) and operators of online message boards seeking to identify and locate individuals who posted material that the companies, for one reason or another, find objectionable. A spokesman for Lycos recently told Salon Magazine that the firm receives subpoenas on "pretty close to a regular basis." The underlying allegations in these cases include defamation, misappropriation of trade secrets and securities law violations. Many observers worry, however, that the legal tactic can easily be used to intimidate potential critics into silence and destroy the anonymity that has contributed to the Internet's explosive growth. David Sobel will discuss these cases and efforts to protect online anonymity. David Sobel is General Counsel to the Electronic Privacy Information Center in Washington, DC, where he has litigated numerous cases under the Freedom of Information Act (FOIA) seeking the disclosure of government information on cryptography and privacy policy. Among his cases are those involving Operation Sun Devil, the Clipper Chip, the FBI's Digital Telephony wiretap proposal and the Secret Service's Pentagon City 2600 raid. David served on the Association for Computing Machinery's Special Panel on Cryptography Policy, which produced the report "Codes, Keys, and Conflicts: Issues in U.S. Crypto Policy." David also served as co-counsel in ACLU v. Reno, the successful constitutional challenge to the Communications Decency Act decided by the U.S.Supreme Court in 1997. He has been profiled as a "Newsmaker" by CNET's NEWS.COM for his work on Internet liberties issues. David has a longstanding interest in national security and civil liberties issues and has written and lectured on these issues frequently since 1981. He was formerly counsel to the National Security Archive, and his FOIA clients have included Coretta Scott King, former Ambassador Kenneth Rush, the Nation magazine and ABC News.

Peter Stephenson Principle consultant of the Intrusion Management and Forensics Group (IMF). Introduction to Cyber Forensic Analysis This session will address the techniques used to investigate network-based intrusions, especially those originating from the public Internet. Emphasis will be on techniques that provide an acceptable chain of evidence for use by law enforcement or in anticipation of civil litigation. We will cover back-tracing, forensic

Peter Stephenson Principle consultant of the Intrusion Management and Forensics Group (IMF). Introduction to Cyber Forensic Analysis This session will address the techniques used to investigate network-based intrusions, especially those originating from the public Internet. Emphasis will be on techniques that provide an acceptable chain of evidence for use by law enforcement or in anticipation of civil litigation. We will cover back-tracing, forensic tools, end-to-end tracing and evidence collection and preservation as well as the forensic use of RMON2-based tools for documenting the path of an attack. Peter Stephenson is a well-known writer, consultant and lecturer with an international reputation in large scale computer networks and information protection. He has lectured extensively on network planning, implementation, technology and security. He has written or co-authored 14 books (including foreign language translations) and several hundred articles in major national and international trade publications. He is the principle consultant for InfoSEC Technologies division of Sanda International Corp. Mr. Stephenson has participated in investigations of computer system intrusions, Internet misuse and abuse and has performed forensic analysis of computer disk drives as well as backtracing analysis of intrusions coming from the Internet. He has used forensic techniques to recover lost data from computer disk drives. Stephenson is a member of the Information Systems Audit and Control Association (ISACA), the Information Systems Security Association (ISSA) and the High Technology Crime Investigation Association (HTCIA). He provides volunteer assistance on request to the Michigan State Police and other law enforcement agencies.

Tom from because-we-can.com. Security problems associated with client-side scripting in popular web-based services. This info will also be appearing in Wired magazine around the same time as Defcon so it's good timing, and extends the 'shorts' in Business Week (may 17, p8) and NY Times (thurs of same week).

V1RU5 Lock Picking explored 14 years as a professional magician, V1rus will assist on the Lock picking class and will talk about Hand cuffs, and how to improve picks

Vic Vandal Hacking Oracle 101 so you've hacked your way into your "test" O/S. What are you going to do now? All the really fun data is stored in a database, probably an Oracle database. This talk will discuss some of the gory details of Oracle security and insecurity. Vic Vandal is a certified information security professional. He has been providing enterprise-level security design and implementation for U.S.government and military entities for the past 10 years. He currently works for a major consulting firm as a Senior Information Security Engineer. His areas of expertise are; O/S security, database security, network security, application security, firewalls, encryption, VPN's, and digital signatures.

Jonathan Wignall Extra Border Hacking - How a company can be hacked without the hacker ever picking on that companies machine. Companies may defend themselves from hacking

Speakers Speakers

attacks from the internet by using firewalls and other defences, but what about their defences beyond their site's boundary? Can attacks here cause damage? or enable an intruder to break into their sites? This presentation will outline what tricks can happen on the internet and how you can defend yourself outside your normal area of control, without resorting to illegal measures. An experienced college lecturer despite being under Thirty years of age. Is well used to public speaking and his research interest is in the field of Internet Security. Head of programme for higher education courses in Computer Networking at St Helens college, he is also actively tring to establish similar courses on Information Security.

Richard Windmann The Defcon Proxy Server Richard Windmann will give an overview of the Defcon Proxy Server - what it is, how it came to be, and how to access and use it. Don't want your boss to know where you're surfing to on his dime? Would you like to anonymously view your artwork after the fact? If this is you, don't miss this informational talk. It will cover new features and access policies. Richard Windmann started out in life as a BBS operator in 1989. After setting up Unix boxes to provide Usenet and Email via UUCP for his customers, he gave out shell accounts on the same machines - and after cleaning up that mess, he was a Security Expert! He also authored the first Windows based email application and roaming code for American Mobile Satellite Corporation and the Trimble C/GPS transceiver, and was head of Network Security for Telegroup, Inc. Richard currently works for International Network Services, where he is a Network security Engineer, and has a bunch of certifications that start with "C".

Ira Winkler The myths associated with hiring hackers. While Ira Winkler is not an advocate of hiring your off the street hacker, he has come to the opinion that many of them are more useful than people who call themselves security professionals. He believes that compounding the problems are bureaucrats who don't understand the problem, and try to form solutions without thinking. For example, the Critical Infrastructure Assurance Office (CIAO), formed by a Presidential Directive to help protect the Critical Infrastructure, was considering a plan to recruit a group of teenagers who they would guide through their college careers to be the Info Warriors of the future. Ira talks about the myths associated with hiring hackers and security professionals, as well as the problems with the efforts to supposedly protect the Infrastructure. An "Are you Clueless?" test for "Security professionals" is given. Also recommendations to excel in the corporate world are given for hackers who are really skilled.

THANKS!

Thanks go out to many poeple. Zac, Xylorg, The People, Dr. Kool, Uncle Ira, Noid, Booga, Lori, Sleestak, Swift, Waz, Nihl, Artimage, Tina, Jeff, Major Malfunction, Lockheed!, Dead Addict, Texorcist, the DJs, Bands, and to all the hard working staff Goons (tm). With out these people and the speakersthis conference would not be possible!

You know the schedule will change. Make the notes here!

The Speaking Schedule

Friday July 9th	Newbie Area A	Area B	Big Area C
15:00-15:50		Simple Nomad:Hacking Novell Netware	Kevin Poulson & Jennifer Granick: Issues in Interrogrations
16:00-16:50	Gh0st: Phreaking and PBX tricks	Darence: The Firewall: Friend or Foe?	Gail Thackeray & Kevin Higgins - Nevada Attorney General : Legal Q&A
17:00-17:50	Mojo: Hacking Windows registers & File shares	Vic Vandal: Hacking Oracle 101	James Jorasch: Hacking Las Vegas!
18:00-18:50	Radio Guy:	Room Closed for Band Set-Up	Meet the Fed Panel
19:00-19:50	Peter Stephenson: Cyber Forensics	Bands Start	Angus Bitter: Fear and Loathing ins Cyberspace The art and science of enemy profiling
Saturday July 10th			
10:00-10:50	Cyber: How to use BSD to set up a firewall / gateway	Rooster: Insecurities in networking devices	Philip Loranger: The ethics, morality, practicality, and patriotism of hacking
11:00-11:50	Punkis: Introduction to TCP/IP	Dead Addict: SET Technology	Michael Martinez:
12:00-12:50	Peter Shipley: Intro to TCP/IP expolits	Room closed for Band Setup	Ira Winkler: The myths of hiring hackers
13:00-13:50	M0dify: Introduction to radio scanning	Bands Start	Sarah Gordon: Viruses on (and off) the Internet. Panel Discussion
14:00-14:50	Room Closed		Cult of the Dead Cow: Back Orifice 2000 (BO2k) is Announced!
15:00-15:50	Robert Lupo: Introduction to Viruses		John Q. Newman: Talk #1
16:00-16:50	Freaky: Macintosh Security		Dr. Byte: IPv6: Who, What, When, How, Why?
17:00-17:50	Cyber: What are public keys?		Winn Schwartau: HERF guns, EMP bombs and weapons of mass disruption (Unclassified)
18:00-18:50	Craig H. Rowland: How to be aware of security problems on your network		DEF CON 7.0 "Who Are You, Anyways?"

Sunday July 11th			
10:00-10:50	Richard Windmann: The DEF CON Proxy Server, and future direction of that technology	Ian Goldberg: Zero Knowledge Networks, One year later!	Tom: Security problems associated with client-side scripting
11:00-11:50	Jonathan Wignall: Extra Border Hacking	V1RU5: Lock picking demo	Jason Scott: Textfiles, G-Files and Log Files Remembering the 1980's through ASCII
12:00-12:50	A.J. Reznor: How to use BO2K	Professor Feedlebom: Follow up on Micropower Radio Broadcasting	Bruce Schneier: Crypto Year in Review
13:00-13:50		Sameer Parekh: "Crypto Tales"	Security Experts Panel: Year Two
14:00-14:50		Steven Alexander: Firewalls: Trends and Problems	Jericho: Fakes walk among us
15:00-15:50		Christian Hedegaard-Schou: Open source	Deanna Peugeot: Embedded systems hacking
16:00-16:50		Charles Faulkner: Hacking human minds	David Sobel: Internet Anonymity under assault: The 'John Doe' Lawsuits