DEFCON 8

Welcome to DEF CON 8.0. Or is it DC 2k? 2000? Whatever. You know the deal. It's another DEF CON, and that is all that matters.

From what I can gather this will be the largest DEF CON ever. I've tried to make a few changes this year. We will see what happens. We have another 9,000 square feet of space and another 125 rooms at the hotel (Which sold out in record time.) I've also tried to select more speakers on more interesting topics, and to tech-up the quality. Remember, the speakers all are doing this on their own time and dime. Please remember this when something goes wrong, or someone starts a few minutes late. We should also have some more A/V gear for people who are doing demonstrations. There should be plenty of opportunity to learn, and some great talks.

A couple of notes and then I'll get right into the list of speakers. First the dull stuff. Don't trash the hotel. They actually like us. Especially the people in the bar. It seems that last year, but Saturday DEF CON had out drank every group that had ever been at the Alexis, except the British RAF. By Sunday we had dusted the RAF and hold the record for most consumed. I think it was something like 2+ months of normal sales done in a weekend. So be cool to the hotel. Also be cool to the goons in red shirts. They volunteer to help out, and are putting up with a lot of crap to make sure the conference goes off OK. Other than that, don't do drugs in front of law enforcement. If you do something obvious we _have_ to do something about it, so be smart and discreet if you plan to do anything in your room.

OK, I hear there will be lots of parties. People will be handing out fliers for the various shin digs, if you are lucky you'll get to more than a few. For people with out a HAM license, hang out on the FRS radio channels, those with a HAM license, we will be on DOC 1 and 2 (ask a goon for the freq). I hope to have the video tapes made in time for the in hotel TV channel. It wasn't done when I wrote this at 02:45 after 4 cans of caffeine, but it should be included as separate print out at the show.

We plan to have big schedules printed out and up at various locations for last minute schedule changes. Please check them out for any last minute changes.

NOTE TO THE PRESS: Generally people are OK with you poking around, but remember this conference is for them. You are the spectator. Don't do anything to create bad vibes or an uncomfortable situation. I can tell you right now that asking someone what illegal stuff they have done in the past is a dumb question. I also know the live media love the people with green hair, but try to mix it up a bit. Here are the rules: Don't sweep a room with your video camera with out first letting people know. Backs of heads are OK, but no faces. You'll find this isn't a big deal. If you ignore this you will be kicked out. There is a press we will show you, and plenty of people will love to talk with you. Please check your facts!

OK, well that's pretty much it for me. It is so strange to be doing this two weeks in advance.. I'm used to doing it the night before. But if I want this thing to come out in color I have to get it to the printers tomorrow. I've got to make up for the last few years of crappy programs. I'm also printing a ton of these things. Look for new services from defcon.org in the next few months. We'll be putting on-line a secure voice chat bridge, a pseudo-anon web proxy, and a remailer. Also look for the speakers presentations on-line with their encoded talks. Thanks for attending my party!

- The Dark Tangent

Uber HaXors Speakers

Tim Lawless,
Saint Jude: Modeling, Detecting and Responding to Unauthorized Root Transitions.

The recent surge of interest in Security has been a boon for those developing IDS systems. Unfortunately,, the IDS advancements have been disproportional in the realm of Network IDS — with Host-based IDS lagging behind, only able to detect breaches after the incident.

This state of affairs offers administrators, faced with the looming threat of intruders gaining access to their systems via legitimate channels, little protection beyond hardening and continually patching their systems. An intruder need only find one hole, the administrator — all of them.

During this session, the Stain Jude project will be presented. Named after the patron saint of hopeless cases, the Saint Jude project is an IDS project that hopes to deliver a model and implementation able to stop a root compromise dead in its tracks, irregardless of the exploits method.

Tim Lawless is a Systems Administer with the University of Souther Mississippi on the Stennis Space Center Campus. After having spent many a night sleeping in the machine room after a security breach, he became REALLY interested in the topics of Computer Security and Information Warfare. He is also a member of the ACPO (formerly ACPM), working to remove child pornography from the Internet.

Robert Graham, CTO Network Ice.
Evading network-based intrusion detection systems.

You've just spent $10,000 on network IDS from a trustworthy company (obviously trustworthy because the vendor spends beaucoup $$$ on marketing). You are satisfied with the purchase because you're catching all these script-kiddies who think they areputting one over on you with their "stealth" scans. But then something bad happens: your servers get hacked through your
firewall, and that expensive IDS never utters a peep.

How did this happen? The root of the problem is that most commercial IDSs are little more than anti-script-kiddy tools and cannot detect ueberhackers. This talk will show how to evade these IDSs using popular tools like whisker and fragrouter. It will also reveal for the first time additional secret techniques used by ueberhackers.

Mr. Graham learned hacking as a toddler from his grandfather, a WW-II codebreaker. His first IDS was written more than 10 years ago designed to catch Morris-worm copycats. He is the author of several pending patents in the IDS field. He is the author of well-regarded security-related documents (www.robertgraham.com/pubs) and is a frequent speaker at conferences. IRL, he is the co-founder, CTO, and chief-architect at Network ICE.

Jon Erickson,
Number theory, complexity theory, cryptography, and quantum computing.

Mr. Erickson will talk about number theory, complexity theory, cryptography, and quantum computing. The basics of number theory pertinent to cryptography will be covered, including modular math, the Euclidian GCD algorithm and Euler's totient function and theorem. Complexity theory and tractability will be explained to give a feeling for what a 'hard' problem is (NP vs P) and algorithmic runtime and Big-O notation with respect of input size will be explained to show why factoring the product of two large prime numbers isn't trivial. Then the RSA encryption/decryption algorithms will be derived from scratch, using modular math, GCD, and Euler's totient function. A few factoring methods will be described, to emphasize the complexity involved in factoring the product of two large prime numbers. Then the basics of quantum computation will be explained; superposition, EPR state, decoherence, controlled NOT gates, and entanglement. The actual quantum mechanics will be skipped to focus on the algorithms. Peter Shor's quantum factoring algorithm will be explained and demonstrated, breaking RSA in two steps. Lov Grover's quantum search algorithm will be explained and it's ability to brute force anything in sqrt(N) steps will hopefully be apparent. Since most conventional encryption will be shown to be insecure, a few quantum encryption techniques will be covered. Q&A afterwards,time permitting.

Jon Erickson was the product of a 6th grade science fair experiment in human genetics by little Snirk Cojeno on planet Vega 7 (His parents helped a little bit). After the fair was over, Jon was sold as slave labor by the elementary school to the Orb Night intergalactic casting and modeling agency. Due to his dashing good looks and human neck, Jon quickly found himself the poster boy for Zarlak's explosive human restraint collars; his likeness plastered all over space billboards and magazines. The fame went to his head, and Jon soon attempted to join the unions, despite the strict regulations against human slaves working like the frees do. He was sentenced to 160 years on the Prison Planet Earth. As if exile to Earth wasn't bad enough, moments after landing, he was quickly carted away to Area 51 by the US Government, only to be traded to a Japanese research group in exchange for some rare Pokemon cards by an agent named Jose Ronnick. In Japan, the brilliant Dr. Kenji Cronos and a lab tech named michelle began an experimental open-brain surgery procedure on Jon, hoping to teach him about human emotion. Something went horribly wrong, and when the anasthetic wore off, Jon woke up in an empty operating room, with a giant hole his skull. All the colors began to taste like blue again, and he panicked, plugging the hole with paper mache and running into the streets to forage for himself. With 142 years left in his prison sentence, Jon began his own scientific research in the realms of cryptography, parallel algorithms and processing, artificial intelligence, and complexity theory, and has lived as a student, teacher, actor, director, writer, DJ, programmer, researcher, and entrepeneur. And he's sorry that she has to miss out on so many grand adventures...

Ian Vitek, penetration tester at Infosec.
IP-spoofing and source routing connections with Linux 2.0.X

The speech will discuss hacking firewalls and filtering routers by spoofing IP and MAC-addresses. Two different spoofing techniques will be presented. Ian will first talk about what to eavesdrop (with siphon, dsniff and tcpdump) and what kind of information one will need for these examples to work. Secondly Ian will show how to set up a working source route (full connection) with netcat through a filtering router. Then Ian will show how to set up the network on a Linux to be able to IP-spoof (with full connection) through a firewall if you sit on a untrusted network, U, between a trusted network, A, and the server, S. Both examples will be explained step by step.

Ian Vitek works as a full time penetration tester at Infosec, Sweden (The page is in swedish). He is right now researching within Media Access level security and LDAP security (which is a big unexplored hole). He also thinks that odems are underestimated hacker tools.

Bennett Haselton, peacefire.org
A protocol that uses steganography to circumvent network level censorship.

Many trivial techniques are already available for circumventing firewalls and proxy servers that monitor or censor network traffic— for example, if your firewall blocks CNN, someone could set up an unblocked site outside the firewall where you can type "http://www.cnn.com/" into a form and retrieve the page contents. The problem with these "protocols" is that they make it easy to get caught, if the censors know what to look for — for example, a GET or POST form field containing "http://" is trivially easy to detect. Even an encrypted protocol would still be easy for censors to detect, without breaking the encryption — just thefact that you're *using* a tool for circumventing the censors would often be enough to get you in trouble.

What we have designed is a protocol that uses steganography to circumvent network-level censorship, so that the protocol is undetectable to censors. We explain why some naive solutions to the problem — such as hiding information in a long, dynamically-generated URL which is sent to an outside "friendly" site, or hiding information in cookies — are not steganographically secure. Our protocol hides information in "innocent-looking" text queries that pass through the censoring proxy undetected. The page contents are encrypted and embedded in more "innocent-looking" content that is sent back to the browser.

This sounds simple, but the mathematics of using steganography to make a protocol *undetectable* turn out to be infuriatingly complicated. Much of the talk will be devoted to attacks against the system that we didn't consider the first time around, and why more naive solutions may fall to these attacks.

Bennett Haselton has been the coordinator of Peacefire.org since its inception in 1996. Peacefire opposes censorship that targets Internet users under 18, and maintains that profanity and smut on the Internet are not, in fact, "dangerous" to anybody, as most lawmakers and blocking software companies have made them out to be. Peacefire publishes research into different Internet censorship programs and technologies, their shortcomings, possible misrepresentations by the companies selling them, and (most popular) how to get around them.

Greg Hoglund - Rootkit.com
Advanced Buffer Overflow Techniques.

This is a technical talk aimed at people who have already been exposed to buffer overflows and want to learn more. The talk assumes the audience has at least some knowledge of CPU's andProcesses. For those of you who already understand buffer overflows, this talk will be a refreshing discourse on technique. We will show how the injection method can be decoupled from the payload. We then explore the details and challenges of injecting code into a remote process. We will also explore the payload, the encoding methods, and how to dynamically load new functions. Lastly, we discuss the possible effects of a payload, including network worms, virus, and rootkits.

Phil King,
8-Bit Redux: Microcontroller Hacking.

In days gone by, microprocessors dealt in units of 8-bits at a time, and names such as Commodore, Atari, and Apple (as in "Apple][") ruled the land. Intrepid hackers of amazing skill and talent worked their magic with limited resources, producing code that was a thing

of beauty. The days of the widespread 8-bit desktop computer are past, but the 8-bit processor itself is not gone. It has gotten faster, added some peripherals and picked up some of the architectural features of it's larger later siblings, largely lost it's external memory, and gone into hiding as the ubiquitous microcontroller at the heart of embedded systems too numerous to count. Microcontrollers offer an excellent opportunity to recapture that spirit of the late 70's when 1K of code was a lot, while working with modern day technology. In this one hour talk, Phil King will describe how to set up a microcontroller development environment on a hacker budget and use it to learn and develop nifty 8-bit embedded system toys. The talk will be framed by descriptions of building an embedded keyboard sniffer with an Atmel AVR family microcontroller.

Phil King is a hardware design engineer with 8 years of experience in various Silicon Valley sardware and software jobs. He received his BSEE from Stanford University in 1992, and an MSEE with an emphasis in computer networking (also from Stanford) in 1998. He is currently preparing to teach EE-281, the Embedded system Design class, at Stanford University this fall.

Mythrandir,Software Evangelist and Visionary, Argus SystemsGroup, Inc.
Penetrating B1 Trusted Operating Systems.

If you have attended the Newbie B1 talk, or have previous experience with B1 systems then you will find this talk enlightening. Typically, B1 systems can only be penetrated due to misconfigurations. We will take a whirlwind tour of all of the areas to check for security is configurations and develop a methodology for attacking B1 Trusted Operating Systems. You are going to find B1 Trusted Operating Systems in increasing use, and you owe it to yourself to understand how to penetrate these systems and how to lock them down.

Evil Wrangler,
Building a Backdoor Binary (featuring SSH 2.0.13)

Adam Bresson,
Protection of info and device via encryption/decryption, Palm OS / hardware architecture, and the structure of a Palm application. Techniques for implementing security for information, accessing Palm system modes and understanding code will be covered.

Adam is a three year veteran of the Palm scene affiliated with PDAZone, PalmWarez and PalmOlive. I am dedicated to understanding the system and operational functions of the world's first usable PDA. I believe a Palm can do a hole lot more than just store numbers and appointments. My discussion will share my deep knowledge of this device.

ghandi,
Dot-Com Smashing: Buffer Overflows on the SPARC

The talk/demonstration is intended for audiences familiar with assembly language and/or stack-based buffer overflows on other architectures (most probably Intel).

The topics aren't really anything new, I would just like to present them with the focus on a different processor/paradigm thanIntel to better define the concepts in use. I will be covering SPARC assembly language on a fairly low level.

- Introduction to SPARC assembly - RISC, LOAD/STORE architecture - Register windows, Allocating space on the stack - SPARC subroutine calling conventions, How the code we're attacking will look - Leaf procedure optimization, How to write optimized assembly - Unix system calls from assembly language, Overview of traps - Hand assembling instructions, Conversion to hex, Testing hex-encoded instructions in C __asm__ blocks - Using GDB (Gnu Debugger) and ADB (Absolute Debugger), Disassembling compiled code, assembling instructions to hexadecimal (faster than by hand), Patching executables, Examining the stack of a running process, Altering the stack/return address - Hand-crafting shellcode, Basics, Basic shellcode, Intermediate shellcode, Advanced shellcode - Delivering the payload - Bonus topics (time permitting)

ghandi is a a Computer Science student beginning work on distributed, interactive environments (ala FreeNet or Stephenson's Metaverse) for an departmental honors project. I also work as a System Administrator at a web startup managing Sun clusters, FreeBSD servers, and Linux workstations.

syke, New Hack City.
opensource utilities and how to use them to test IDSes and firewalls.

This talk showcases free/opensource utilities and how to use them to test IDSes and firewalls. There have been a few talks on the common weaknesses of both kinds of products, but no practical means by which to test for said weaknesses. The point of the talk is to enable people to test vendor's claims (or their own products) themselves. This talk would be of interest to developers, security admins, product reviewers, and white/blackhat hackers. Knowledge of TCP/IP and programming are recommended.

I. What are firewalls/IDSes supposed to do? (expectations) a. stateful and non-stateful packet filters b. network-based and host-based IDSes

II. Common failings a. firewall 1. DoS 2. evasion b. IDS 1. DoS 2. evasion III. How do you test for this? a. Everyone's favorite: nmap 1. firewall exploits: filling up state table 2. IDS exploits: fragmentation, ACK/FIN scans b. The isic suite of utilities 1. firewall: options handling/frag DoS, packet leakage 2. IDS: IDSes that process options/state confused c. Sample programs included with libnet 1. firewall: boink, ping of death, etc d. whisker 1. IDS: evasion IV. Demonstration a. IDS: against libNIDS, IDS test cases above b. Firewalls: against netfilter, firewall test cases above.

syke is a member of New Hack City, a hacker collective based in San Francisco. He has 2 years of experience testing firewall and IDS products at a major vendor of security software.

Kent Radek,
Puzzlenet.net - Designing an anonymous network.

Mr. Radek began life as a satellite communications engineer, decided that sucked, and went to work on a computer science degree. After a few years (better not discussed), he began life over as a software engineer with a defense contractor. It took him five years to discover that also sucked, but in the meantime, he designed a pretty cool encryption system for military communications. Recently, he began his third incarnation as a Linux developer, who, in his spare time, decided to combine the best features of Gnutella, Freenet, and Publius in order to make the world a better place for people who enjoy privacy and free speech. His interest s(which are none of your business) include photography, running, cycling, SETI, penguins, and (unfortunately) DVDs. Sites to see: www.puzzlenet.net, www.radek.org, and www.grasshoppertakeover.com.

Chris Goggans, Security Design International
Kevin McPeake, Trust Factory
Wouter Aukema, Trust Factory
Patrick Guenther, Trust Factory
Lotus Notes/Domino Security

This session will cover security vulnerabilties and common misconfigurations in Lotus Notes and Domino servers. The presentation will contain exploit demonstrations and discuss work-arounds for the problems. This session will also announce the results of research into new vulnerabilties.

John S Flowers, Chief Scientist, Hiverworld, Inc.
Network IDS - Do not bend, fold, spindle or mutilate.

All modern Network Intrusion Detection Systems (NIDS) are succeptable to not only Ptacek and Newsham style attacks, but a variety of other problems that have not yet been addressed. This talk is meant to shed some light on why many NIDS today are referred to as "Network False-positive Recorders" and why current IDS technology cannot handle monitoring high speed network traffic. This discussion is meant to be a direct and straightforward analysis of why the current generation of NIDS will ultimately fail and how we can start taking proactive, not reactive steps in creating the future of intrusion detection technology. This discussion will also include examples of bypassing current intrusion detection systems and how the reation of a high speed, hybrid IDS will address many of the problems outlined in this talk.

Mr. Flowers is the founder of Hiverworld and reads the Core R&D team in creating the Ansible, Swarm and upcoming IDS product.
Prior to Hiverworld, Mr. Flowers was the chief architect of Inquisit's individualized news filtering service. He has also held positions as the chief security and Internet Architect at Utilicorp, chief architect of Neurosoft (later became Moviefone);
and architect of the interactive voice response system that was the prototype of Wildfire. In the early 1990's he worked as an engineer for Microsoft. John was also on the first team to ever win Capture the Flag at Defcon.

blanu-
Notes: This is an original presentation unrelated to the paper being presented in Berkeley. That paper was Freenet 101 + WhyWe're Anonymous. This presentation is Freenet 101 + Various Attacks on Freenet + Spiffy Animations I Made with Crayons and Photoshop.

jeru, New Hack City.
Advanced evasion of IDS buffer overflow detection.

This is a technical talk which assumes the audience understands x86 or SPARC assembly, and buffer overflow methodologies. It presents various stealth coding techniques that can be applied to preventing detection by most current generation IDSs.

The talk also includes a live demonstration of exploits written to evade IDS detection, source code of the examples included. A paper documenting the techniques, and sample code will be available from http://www.newhackcity.net after the presentation.

jeru is a member of New Hack City, a hacker collective based in an Francisco. He has worked in digital design, and embedded programming. He currently spends his time as part of an IDS development team, providing application level security assessment, and pickin' his fro.

Subterrain Security Group (SSG)
The Impact of Passive Network Mapping in Distributed Environments.

This new approach to information gathering is the latest in stealth target aquisition technology. This lecture will discuss dynamic routing protocol internals, network mapping methodology, vulnerability analysis techniques, and OS identification procedures. Come prepared for an in-depth compare / contrast session between active and passive network information gathering heuristics. We make informed target iquisition notoriously fun and difficult to detect. The portable tool to do this will be released on Sunday afternoon.

Subterrain Security Group releases solid, portable, and freely available open source tools for performing computer and network security related tasks.

Haxors Speakers

Gregory B. White, Ph.D.
The USAFA Cadet Hacking Case: What both sides should learn about computer forensics.

Basically I'll discuss the case that went to trial in the spring of 99. I was the Deputy Head of the Computer Science Department at the USAF Academy at the time and was asked by the cadet accused of "hacking" to help with his defense. I testified at the trial as an expert witness for the Defense. I sat at the Defense table throughout the trial serving as their "computer expert".

Basically the trial was a comedy of errors by the prosecution. law enforcement, and the cadet's attorneys alike. The cadet was involved in IRC but the law enforcement types and prosecution became convinced that he was the "hacker" (afterall, everybody KNOWS that IRC is nothing more than a place for hackers to trade information on how to break into computers — the actual sentiment expressed by the investigators). I had up to that point spent the majority of my time in the Air Force trying to protect systems and to catch those who broke into AF systems. This case really shook me as I saw the LE types latch onto the smallest of indicators and blow them into a full blown felony case (the cadet faced 15 years in Leavenworth had he been convicted of all counts). What I will cover in the talk is:

1) Background of the case 2) The "evidence" the prosecution thought they had 3) The many possible areas where clues might have been found had either side known where to look (or asked anybody who knew anything about it) 4) What lessons can be learned from this case. Those from the government and industry need to know where to look if they want to catch folks (and if they want to make sure they don't make fools of themselves) and those who might find themselves accused someday need to know how to help their attorneys find clues that could exonerate them.

Gregory B. White, Ph.D. Vice President, Professional Services. Gregory White joined SecureLogix in March 1999 as the Chief Technology Officer. Before joining SecureLogix, he was the Deputy Head of the Computer Science Department and an Associate Professor of Computer Science at the United States Air Force Academy in Colorado Springs, Colorado. While at the Academy, Dr. White was instrumental in the development of two courses on computer security and information warfare and in ensuring that security was taught throughout the computer science curriculum. During his two tours at the Academy, he authored a number of papers on security and information warfare and is a co-author for two textbooks on computer security.

Between his Air Force Academy assignments, Dr. White spent three years at Texas A&M University working on his Ph.D. in computer science. His dissertation topic was in the area of host- and network-based intrusion detection. Prior to his Academy assignments, Dr. White was a student at the Air Force's Advanced Communications-Computer Systems Staff Officer Course in Biloxi, Mississippi. He was awarded both the AFCEA and Webb awards for student leadership and academic excellence and was a Distinguished Graduate of the course. Before attending the course in Biloxi, Dr. White served as the Branch Chief of the Network SecurityBranch at the Cryptologic Support Center in San Antonio, Texas.His first assignment in the Air Force was as a systems analyst at the Strategic Air Command Headquarters in Omaha, Nebraska. Dr. White obtained his Ph.D. in Computer Science from Texas A&M University in 1995. He received his Masters in Computer Engineering from the Air Force Institute of Technology in 1986 and his Bachelors in Computer Science from Brigham Young University in 1980. He separated from the Air Force in 1999 and is currently serving in the Air Force Reserves at the Defense Information Systems Agency.

Ron Moritz, Senior Vice President and Chief Technical Officer at Symantec Corporation.
Proactive Defense Against Malicious Code.

Anti-virus software is an important part of a well-devised security policy, but reactive virus detection is not versatile enough for the demands that will be made on businesses engaged in e-commerce. The year 1999 began with the birth of the Happy 99 virus - a harbinger of things to come. Happy 99, plus Melissa, PrettyPark and the Explore.zip worm are all examples of third generation of malicious replicating code, designed to exploit the Internet for their rapid proliferation. A variant of Explore.zip, called MiniZip, managed to hide itself from antiviral utilities and spread at an amazing rate around the Internet at the end of 1999. Such programs, which launch new malicious code attacks, create "first strikes" against systems and networks. Allowing untrusted code to execute on the corporate network may not be suitable for your organization. But corporate security policies that block network executables adversely affect the evolution of the Internet, extranet, and intranet. While no security implementation is absolute, functionality is not achieved by disconnecting users from the network and preventing access to programs. Therefore, proactive defense against first-strike attacks is required today.

Almost all web sites today contain mobile code. Many of the powerful business (ecommerce) applications you need and use are written with mobile code. Consequently, net-enabled malicious software is likely to increase in prevalence and successful utilization. The factors accounting for such a prediction are the ease by which users are duped into double-clicking on malicious e-mail attachments and, the ease by which

the sources of those e-mails are automatically spoofed to seem to come from a boss or from an e-mail or instant message friend. Traditional pattern matching approaches are incomplete, out-of-date, and ineffective and were never designed in preventing a series of new generation attacks based on malicious mobile code and Trojan executables.

Ron Moritz is the Senior Vice President and Chief Technical Officer at Symantec Corporation where he serves as primarytechnology visionary. As a key member of the senior management team interfacing between sales, marketing, product management, and product development, Ron helps establish and maintain the company's technological standards and preserve the company's leadership role as a developer of advanced Internet security solutions. Ron was instrumental in the organization of Finjan's Java Security Alliance and established and chairs Finjan's Technical Advisory Board. He is currently chairing the Common Content Inspection API industry standards initiative. Ron is one of a select group of Certified Information Systems Security Professionals. He earned his M.S.E., M.B.A., and B.A. from Case Western Reserve University in Cleveland, Ohio.

D-Krypt,
Web Application Security
[No details available]

Dan Danknick, Team Delta Engineering.
Fighting Robots.

If you saw the BattleBots pay-per-view show on R/C fighting robots, you heard Dan giving technical commentary during the fights. He was hired to do this as a builder of six robots himself in the past five years, as well as having written for numerous magazines on this topic. To further broaden his claws into this sport he designs and sells electronic radio interfaces to the international market as well as the SFX industry in Hollywood.

Dan will bring a few working robots and explain their designs and how that fits into the various fighting styles developing within the sport. Time and interest permitting he would also like to discuss the developing security implications for popularized R/C robots and how they are shadowing the military construction of pocket-sized war machines. Lastly a giant box of parts and raw materials will be available for the audience to inspect and examine following the session.

David J. DiCenso, JD
The Citizen Hacker: Patriot or War Criminal?

When might international computer hacking become an Act of War? Some within the hacker community have felt that international hacking wasn't being done right by the DoD - it could be done much more effectively and efficiently if left to the experts - civilian hackers. This position is interesting, but is it appropriate? What ARE the international implications of electronic network information operations which target foreign actors or states? How far can an operator go before his acts become an "act of war"? What type of retaliation by a target country is permitted under international law and custom? What are the rules? Whose rules apply? In a world where hacker groups are so bold as to declar war upon a nuclear-capable major world power, and countries take military action against non-state actors geographically located in a non-hostile state, these thorny issues attain paramount importance. This presentation explores these issues in an effort to help shed light upon this "dark secret" of international relations.

David J. DiCenso, JD - Director, Training Services at SecureLogix Corporation. Before coming to SecureLogix, Mr DiCenso was an Associate Professor of Law at the United States Air Force Academy in Colorado Springs, Colorado. While at the Air Force Academy, Mr. DiCenso taught CyberLaw, Computer Law and Policy, as well as traditional general law topics. He was also an occasional guest speaker in the Acadmey's Information Warfare course. Mr. DiCenso's article on information warfare has been published in the Airpower Journal, and he has submitted an article on Information Operations for publication in another profesional journal this Fall. Mr. DiCenso became an attorney in 1988, and served as a JAG in the USAF for over a decade. He joined SecureLogix Corporation in the Summer of 1999.

Jason Scott,
Texfiles.com: Oneyear later.

Jason Scott gave you an overview of the many amazing things that happened in the BBS world of the 1980's at the last DEFCON. This time, he talks both about some pieces of history that he forgot to mention, and a wide selection of the most interesting events to happen to textfiles.com in the last year.

Hear about the legal threats, the newspaper articles, the links to the Trenchcoat Mafia(!), just how many times textfiles.com has come close to being declared illegal, and why history is so important and yet hated by hackers.

Jason will also pull out some nuggets of history about The Works BBS, which was at one point the largest textfiles-only BBS in his bedroom. Specifically, the truth will finally be revealed about the once-dreaded "L00ZER-B-G0NE" button.

A quarter million visitors and going strong, textfiles.com has expanded into not only a historical collection but a group of essays about all manner of cultural aspects about BBSes, and where they've brought people today. There is also a new companion site, scene.textfiles.com, run by one "mogel", which covers the newest of the new of the textfiles "scene", which is still as active as ever.

Mr. Mojo,
Windows 2000 security.
[No more information available]

Ian Goldberg, Zero-Knowledge Systems
"Using the Internet Pseudonymously III: It's Alive!"

The Freedom Network from Zero-Knowledge Systems allows users to maintain their privacy while on the Internet (WWW, email, IRC, etc.) by giving them cryptographically-protected pseudonyms ("nyms"). Not even Zero-Knowledge knows the identities behind the nyms (hence the name).

Freedom has been up, running, and available for download since December. In this session, I will talk about the privacy-enhancing technology behind Freedom, what we've learned in deploying it to the world, and how various other groups have reacted.

Ian Goldberg is Chief Scientist and Head Cypherpunk of Zero-Knowledge Systems, a Canadian company producing Internet privacy software for consumers. He is simultaneously completing his PhD from UC Berkeley in the field of Computer Security and Privacy. Ian has in the past been known to find security holes in Netscape's SSL implementation, to break cryptographic algorithms used in GSM cell phones, and to throw a lot of parties.

Ender of the GhettoHackers
Demonstration and presentation of the Autonomous Nodes that Batz and Caezar presented in concept at BlackHat Singapore.

I am working in conjunction with them on this project and plan on a lengthy on site demonstration of the nodes' functions and AI. It's purpose mainly to demostrate that the theory of these nodes is highly functional in both network research, for exploitation and protection.

To give you a quick surmise. A small LAN will be setup. NodeH (node hacker) will be inserted and printed documents of the timing and actions that NodeH will take, will be passed out to the crowd. The node will perform actions and an oversight of it's AI will be presented to the crowd describing the reasons and purposes behind it's decisions.

Automated exploitation with an attack tree backbone (Bruce Shniers idea from DR Dobb's Journal) are some of the main features. I have currently a 13 page overview which I am working on with Caezar. I have already begun development, the first run being MS compatible, with a Linux port possibly before DefCon.

Ender is an embedded system software coder and tester for 4+ years. He has coded in solutions engineering group for customers world wide, he specializes in C and x86 assembly. Interests include Prime Number Theory, Cryptonalysis, DSPs, Music, and Ruling the World. Motto: Be good, be bad, just

be good at it.

Phillip J. Loranger, GS-14, Director of Army Biometrics
The Army Biometrics program.
[No more information available]

Simple Nomad, NMRC
A how-to regarding network mapping that covers some interesting techniques not commonly used.

noise,
Anonymous Remailers: The importance of widely-available anonymityin an age of Big Brother.

From the golden days of the Penet pseudononymous remailer, to Janet Reno's call to squelch Internet anonymity, anonymous remailers have played a vital and oft-hated role in making the 'Net safe from Big Brother.

People regularly use anonymous remailers to avoid spam, to speak their minds without fear (of peers, family, employers, or governments), and to stay out of search engine indices. Like nearly any other technology, anonymous remailers can also be used by "criminals" to do "criminal" things. Under this guise, the government wishes to outlaw or severely restrict access to anonymous remailers.

Remailers are not difficult to use. They're not prohibitively difficult to run, either.

"The only way the public remailer network will sSoftware Evangelist and Visionary, Argus SystemsGroup, Inc. survive, is if more people start setting up remailers. Even if all the current remailers never get shutdown by the Powers That Be [TM], people do tend to move, change lifestyles, pass on, lose their jobs or lose the time to run a remailer. Remailers go away. Change is the constant in life. We need more remops if the system is to survive." — Shinn Remailer Operator.

History, current status, and known attacks on Type I/II remailers will be the focus of the talk.

noise holds a BS in CS from some university and will be attending her second year of law school this fall. she runs the noisebox anonymous remailer, helps the Electronic Frontier Foundation, and delights in holding heated debates with bureaucrats. noise thinks the world would be a better place (tm) if it had more cypherpunk lawyers.

Bruce Schneier, CTO, Counterpane Internet Security, Inc.
The Internet and the Death of Security.

Building a secure system requires a lot more than just stringing together a bunch of security buzzwords. Most systems are insecure, not because of any one problem but because of failures in the desig process. Engineers misuse secure primitives, introduce security flaws in the implementation, build bad user interfaces, don't allow for errors or failures, and generally fail to design systems that counter the actual threats. Traditional engineering is about making things work; security engineering is about programming Satan's computer: a malicious system that does exactly the wrong thing at exactly the right time.

The problem with bad security is that it looks just like good security. In this talk Bruce will discuss the failure of security on the Internet: the failure of testing, the futility of building security that relies on the average user, and the problems of securing modern complex systems. Security is not a product; it's a process. Strategies that leverage process are our only hope for a secure digital future.

Internationally renowned security technologist and author Bruce Schneier is both a Founder and the Chief Technical Officer of Counterpane Internet Security, Inc. He established the Company with Tom Rowley to address the critical need for increased levels of security services. Schneier is responsible for maintaining the Company's technical lead in world class information security technology and its practical and effective implementation. Schneier's successful tenure leading Counterpane Systems make him uniquely qualified to shape the direction of the company's research endeavors, as well as to act as a spokesperson to the business community on e-commerce issues and solutions.

While president of Counterpane Systems, Schneier designed and analyzed hardware and software cryptographic systems, advised sophisticated clients on products and markets, and taught technical as well as business courses related to the field of cryptography. Concerns as diverse as Microsoft, the National Security Agency, Citibank, and the White House staff have all relied upon Schneier's unique expertise. In addition, Schneier designed the Blowfish algorithm, which remains unbroken after eight years of cryptanalysis. And Schneier's Twofish is among a small number of algorithms currently being considered by the National Institute of Standards and Technology for the advanced encryption standard (AES) to replace the current data encryption standard (DES).

Schneier is the author of five books including Applied Cryptography, the seminal work in its field. Now in its second edition, Applied Cryptography has sold over 110,000 copies worldwide and has been translated into three languages. He has presented papers at many international conferences, and he is a frequent writer, contributing editor, and lecturer on the topics of cryptography, computer security, and privacy. Schneier served on the board of directors of the International Association for Cryptologic Research, is an Advisory Board member for the Electronic Privacy Information Center, and was on the board of directors of the Voter's Telecom Watch.

John Q. Newman, Author.
Fake id by mail and modem.
and
10 steps you can take to protect your privacy.

I will cover topics such as the legal rules regarding fake id, when and where it can be safely used, how to determine if an internet seller of fake id is a scammer or legit, and finally the federal governments new interest in fake id. The id shop, the place I recommended last year, was raided by the secret service 3 months ago, and I will also talk about this case. If you remember, the owner was at last years convention making and seling id.

My second talk will be called"10 steps you can take to protect your privacy". This will be the dry run for a presentation I will take on the lecture circuit when my big new book from random house comes out on privacy. This talk will give straightforward steps everyone can take to drop out and stay out of big brother's databases.

Richard Thieme,
Social Engineering at Def Con: Games Hackers Play.

DefCon has changed dramatically from Def Con 1 - when sixty real hackers met in face-time for the first time to Def Con 8 when thousands crowd into a hotel for a hacking "event scene." Richard Thieme has been called a "shrewd observer of hacker attitudes and behaviors" and sometimes he is. You be the judge. In this talk he reviews *very subjectively* the way truth is invented, perception managed, and media manipulated in the many rings of Def Con. It's all here - the familiar icons of good and evil, enemies of the people, Feds in disguise, happy and unhappy hackers, and his take on the truths, half-truths and outright lies that we exchange as currency in this looking-glass world.

Thieme's predictions at DefCon IV in "Hacking as Practice for TransPlanetary Life in the 21st Century" have all come to pass. But what's next? Hear how to position yourself for the Next Big Thing, depending on your hacking generation and the degree of real larceny in your heart.

Richard Thieme is a writer and professional speaker focused on "life on the edge," in particular the human dimensions of technology and work.

He is "a father figure for online culture," according to the (London) Sunday Telegraph and "one of the most creative minds of the digital generation" according to the editors of CTHEORY.

He has spoken for OmniTech; Strong Capital Management; System Planning Corporation (SPC); UOP; Alliant Energy; Firstar Bank; MAPICS; Influent Technology Group; Navy Federal Credit Union; Arthur Andersen; the Conference of State Legislatures; the Society for Technical Communication; Association for Information Management and Research; the FBI; the

Black Hat Briefings, Def Cons IV, V, and VI; PumpCon, Xmas Con, RootFest and RubiCon. He writes for Information Security, Village Voice, Forbes Digital, Wired, South Africa Computer Magazine, CTHEORY, and LAN Magazine.

Eric Sinrod, partner, Duane, Morris & Heckscher LLP.
Bill Reilly, Student
Federal Computer Fraud and Abuse Act .

We are going to discuss the Federal Computer Fraud and Abuse Act and look at how various hacking, virus and denial of service attacks trigger different sections of the Act. We will also discuss how intent and status affect levels of criminal liability. We will further discuss recent Congressional proposals to the amend the Computer Fraud and Abuse Act. Finally, we will look at international efforts to harmonize cyber-crimes laws.

Bill Reilly is a law student at the University of San Francisco, who has a focus in E-commerce legal issues. Prior to law school, Mr. Reilly spent 8 years in Denmark and Sweden working with different Danish and American Internet-related firms, where he was recently acknowledged as a "Dot Com Pioneer of Denmark" by a Danish newspaper. Mr. Reilly also has a Master's degree in International Management with a specialization in International Finance and a Journalism degree from the University of Southern California. Mr. Reilly was a co-author of a recently published article in the Santa Clara Computer and High Technology Law Journal entitled Cyber-crimes: A Practical Approach to the Application of Federal Computer Crime Laws. Also, Mr. Reilly is a co-author for the upcoming release of Intellectual Property and Unfair Competition in Cyberspace a comprehensive Internet Law Treatise to be published by Commercial Clearinghouse (CCH) in 2000. Mr. Reilly has recently written an article entitled "Hacking to Hard Time: Federal Anti-Hacking Laws and the Hacker soon to be published in the Journal of Internet Law and contributed to a legal e-commerce text book International E-commerce Law and Application. Mr. Reilly is a senior staff member of the U.S.F. Law Review, board member of the USF Intellectual Property Law Association, research assistant to Prof. J. Thomas McCarthy, and web master for several law school and other commercial web sites.

Eric J. Sinrod is a partner in the San Francisco office of Duane, Morris & Heckscher LLP. Mr. Sinrod¢s practice has covered a number of important Internet, technology, intellectual property, information, communications, commercial and insurance coverage issues. He has represented domestic and international clients in major class actions and where hundreds of millions of dollars have been at stake. He also has handled numerous matters for smaller companies and individuals. Mr. Sinrod has had significant trial and appellate experience, including cases before the United States Supreme Court. Mr. Sinrod has been quoted or his work has been profiled in Time Magazine, the National Law Journal, Cyber Esq. Magazine, Business Insurance Magazine, the ABA Journal, the California Lawyer and a number of other publications.

Mr. Sinrod is an adjunct professor of law and has published many law review and other journal articles. He is a frequent speaker on Internet, information and communications issues. He is an advisor to the Cyberspace Law Seminar at Hastings College of the Law and teaches an Information Law Seminar at Golden Gate University School of Law. Mr. Sinrod is on the Editorial Board of the Journal of Internet Law, is a member of the ABA Internet Industry Committee, and is a member of the Executive Committee of the Law Practice Management & Technology Section of the State Bar of California. He is the author of a treatise entitled *Intellectual Property and Unfair Competition in Cyberspace,* to be published soon by CCH, Inc. He writes a weekly Cyberlaw column for the online version of Upside Magazine, entitled *Upside Counsel,* and he is a regular guest speaker covering Internet legal issues for Live Online News.

Sarah Gordon,
Virus Writers: The End of The Innocence.

Earlier research has empirically demonstrated the cyclic nature of virus writing activity: As virus writers age out, new virus writers take their places; enhanced connectivity amplifies the existing problem and various technical factors result in new types of virus writers surfacing and the cycles repeat. However, a new variable has recently been introduced into the cycle: legal intervention. The virus writing community now has experienced visits by concerned law enforcement; there have been arrests and sentencings. New laws are being enacted, and acted upon. Thus, the virus writing scene is no longer a casual game of kids on local BBS.

What has been the impact (perceptually and operationally) of these visits, arrests, and most importantly, the (yet to be imposed) sentencing of David Smith. In other words, as the virus problem gets more and more attention, where are we actually going in terms of shaping acceptable behavior in our virtual communities and what, if any, impact are these legal interventions having on the impact of viruses impacting users ?

In order to produce a scientifically meaningful answer to this question, this pre and post-test study examines pre-sentencing opinions of the impact of the visits/arrests/sentencing and compares these findings with those from post-sentencing opinions. Opinions are interesting and must be considered, as we know the opinions of today shape how people behave in the future.

However, we are also concerned with immediate impact. To this end, impact will be examined in terms of viruses found both ItW and on the WWW, as a function of time with parameters being pre/post sentencing. In particular, we are interested in any discontinuity noted in the graph of viruses both ItW and on the WWW, and in online references to legal concerns.

The conclusions will obviously depend on the actual results, but there appear to be essentially one of two scenarios: i. The pre and post tests studies will demonstrate significant differences. Thus, proponents of tough police follow-up of virus writers will have some hard evidence that this actually has a financial value, as well as a societal impact.

ii. The pre and post test studies will demonstrate no appreciable difference. This means that we need to re-evaluate the worth of pursuing virus writers as a useful way of curbing the problem and evaluate the wisdom of spending large amounts of public funding to pursue this avenue of defense.

Lee Johnston, Senior System Analysis with Computer & Network Associates (CNA)
Demonstration of software that allows the construction of an enterprise network (complete with servers) inside a single computer.

Based on RedHat Linux, users can accurately simulate an enterprise network populated with real servers and workstations on a SINGLE COMPUTER (the system literally runs several real networked operating systems simultaneously inside one computer). It also runs multiple firewalls, gateways, routers, VPNs, or any other network device. Security experts (or hackers) can create a virtual network, populate it with Windows systems and then attack them with the latest exploits. In addition, all packet traffic can be (sniffed) sent to a file or displayed in real time. This provides security experts with detailed information about the nuts and bolts exchanges between networked computers. Thus, software-programming flaws can be identified and exploited. In addition, the system is a outstanding platform to create and test the most twisted of viruses. The kicker is you can build a virus, instantly infect a networked os, and then rapidly see the results. If it doesn't work correctly, within seconds you can restore the infected windows os to a virgin state, modify the virus, and try it again.

A California native, Lee Johnston is a Senior System Analysis with Computer & Network Associates (CNA). He holds a bachelor's degree in Management Information Systems from the State University of New York. He has over 12 years of experience in computer security. Prior to his move to CNA Lee was a System Administrator for the Air Force in Biloxi, Mississippi. On behalf of the Air Force, he authored several articles and textbooks on military networks and security. Currently, he leads the CNA's network security development team.

Aaron Grothe,
Tunneling and Firewalls.

A Firewall is the first line of defense for almost every LAN connected to the Internet. Using a Firewall many

System Administrators restrict privileges to services they do not want to allow access to such as telnet and ftp. Using tunneling software, people can re-enable those services by establishing virtual data paths through allowed protocols such as http.

The talk will provide an overview of how tunneling may be used, how to combat it, and when to use it. There will be a demonstration of how tunneling works using the httptunnel http://www.nocrew.org/software/httptunnel.html software.

Aaron Grothe is a System Administrator for a small startup based in Omaha, Nebraska.

Newbie Speakers

Wyatt,
Radio hacking.

Thomas Munn,
Need for home-based firewalls.

V1ru5, ConXion, Network Security Administrator.
Virus talk: This will be an introduction to computer viruses.

Covering Boot sector, File infector, Multi-Parti, Polymorphic, Macro, Trojan, and Script viruses. We will talk about how they infect, types of damage, and repairing.

Lock picking Talk: This talk will cover different kinds of locks, and hand cuffs. And how there opened!

Robert Lupo aka "V1RU5" has several certifications in the security field, including CCSA, CCSE. He Currently works as a Network Security Administrator. He is known for his lock picking, Virus, and Social Engineering skills. MCSE, CCSA, CCSE and SeaGate NerveCenter Certified.

Xs,
LDAP
[No more information available]

Mr. Nasty,
Using tools to obtain recon on NT networks.

I have worked in the field of Computer Security for the past 7 years. I test systems throughout the US for various vulnerabilities and report to management how these vulnerabilities can be lessened. No one listens!

Jennifer Granick, Attorney at Law
Brian Fin, Attorney atLaw
The law and hacking.

A panel of a criminal, civil attorneys and a federal prosicuter to talk, debate and answer questions. While in some situation there my be no law against something that does not mean you can be sued in civil court or charged on "related" charges.

Mike Scher, Anthropologist, Attorney, Policy Analyst.
What is DNS and alt roots? What are alternate roots and why does Internet suck.

Recently, the overlaping space among DNS, the design of browsers and search engines, international, national, and local trademark interests andlaw, have come to a head. A sprawling organization dubbed ICANN has taken over what used to be a task that sat squarely on one man's shoulders. The tensions are largely the result of ignorant (and purposeful) confusions of the purposes and functions of the various Internet name and resource locating systems. In this talk, we will discuss what a DNS root fundamentally IS, and the factors that keep a unified name service root in place despite many pressures to decentralize DNS root services. We'll then look at the ways in which decentralized or alternate roots could be (and have been) implemented, and their implications for trademark and software politics and design.

Mike Scher is an attorney and network security consultant working on both the policy and technology fronts. He has designed private DNS roots and TLD systems for international Fortune 500 companies, and worked with public alternative DNS root projects. Most recently, Mr. Scher has become infrastructure technology and policy manager for a fast-growing start up company in Chiago.

DDT,
PGP: What Pgp and crypo is and how to use (and not use) it.

sinster,
Energy Weapons
[No more information available]

Thomas Munn,
How to make a linux firewall with IP-chains.
[No more information available]

Freaky, staticusers.net and Freaks Mackintosh Archives.
Security and hacking of the MacOS and details of OSX.

Freaky will be presenting his second speech this year. Last year he covered the basics of macintosh security and answered questions. This year he will be going over security / hacking of the MacOS and details of OSX and the security it offers. Macintosh Security is a topic not well known, so he is willing to take questions early to cover in the topic.

Pyr0, Network Administrator - The r00t Cellar.com
FAQ the Kiddies

Every year the attendance at Defcon grows. It was apparent this last year that many of the Kiddies (W@r3z d00d5, Script Kiddies, and lamers) had come with the intention of learning something. Problem is upon arrival these groups think that the only way they will be able to benefit from Defcon is if they "PROVE THEMSELF" to everybody they come across. By the end of Day 1 they have successfully burned any bridge they had the chance of building. This speech will give newbies some of the info needed to get on "the right track". Some of the highlights are:

Dangers of being a script kiddie, Learning vs. Compiling, What your local library has to offer "Follow the rainbow booked road," "Hacking without going to jail," "Shutting your mouth and opening your ears," There will be many URL's and book titles given so please bring a pen and paper.

Daremoe,
System Profiling: Target Analysis or How Crackers Find You.

This presentation will walk through profiling and target selection from an attack point of view. I will demonstrate techniques, commands and tools used to remotely identify systems, services and possible vulnerabilities for exploit. The presentation should teach newbie hackers how to identify potential targets while explaining to system administrators how their systems are targeted for attack.

Natasha Gregori, President ACPO.
Hacktivits to Activists - Making the Transition.

In 1999 The ACPM was formed with the goal of removing child pornography on the Internet via any means possible. After an initial announcement on HNN, and recruitment at DefCon 7, we began the daunting task of shutting down Child Porn Sites.

Initially successfully, we found that the sites we took down would come back up after a few days or weeks. Not only would they return, but it became increasingly more difficult to take them down. We were not effectively removing sites, just making them stronger. A Change in tactics was necessary, and so the transformation to ACPO began.

The transformation into a "legit" activist group from our beginnings in the H/P/A community did not occur without its own pains. Some felt we were becoming "soft" on child pornography and left. Others joined, not deterred by our history. We have come to form strong bonds with law enforcement internationally, and have had success at identifying both those that traffic and receive child pornography.

Recent articles in apbnews.com, cbsnews.com, and wired.com have focused on ethical "hacker" groups fighting child porn have featured ACPO and Condemned.org, who is currently in the process of "going legit".

In my Talk I (and possibly Rloxy of condemned.org) will present the problems which convinced us that hacktivism was not the appropriate path, the transition process into an activist group, and the benefits the transition has has brought us.

Jim McCoy,
Majo Nation: Building a next generation distributed data service.

Jim McCoy is a long-time cypherpunk and who decided long ago that cypherpunks may talk about writing code but it takes Evil Geniuses to really get the job done. After helping Steve Jackson build Illuminati Online using the money from the secret service raid he was convinced that the best way to bootstrap a start-up was to antagonize the government, since then he has learned that there are easier ways...

Arthur L. Money, Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD (C3I))
Meet the FED Panel

Arthur L. Money was sworn in as Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD (C3I)) on October 5, 1999. Mr. Money served as the Senior Civilian Official, Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) and Chief Information Officer of the Department of Defense from February 20, 1998 to October 4, 1999.

He served as Assistant Secretary of the Air Force for Acquisition from January 1996 to May 1999. He was President of ESL Inc., a subsidiary of TRW, before it was consolidated with TRW's Avionics and Surveillance Group, and Vice President and Deputy General Manager for the TRW Avionics and Surveillance Group. The group is internationally recognized for airborne electronic systems and technologies, including reconnaissance and intelligence systems and advanced integrated avionics.

Mr. Money has more than 35 years of management and engineering experience with the defense electronics and intelligence industry in the design and development of intelligence collection analysis capabilities and airborne tactical reconnaissance systems.

Shane O., Project Manager for the Bluebird Project at OpenNMS.org
Overview of SNMP and other management technologies.

The network and systems management marketplace has been dominated by the "frameworks" that provide minimum functionality at a maximum price, whileover 70% of their deployments are considered failures. Fortunately, the open source tools are evolving and beginning to provide scalablealternatives to these 800-pound gorillas. This presentation will provide an overview of SNMP and other management technologies, a survey of the current state of open source tools, and a discussion on OpenNMS' Bluebird Project,the emerging open source alternative for scalable network and systems management deployments.

Shane O'Donnell is Project Manager for the Bluebird Project at OpenNMS.org, where he is part project manager, architect, and evangelist. Shane has an Master's degree in Computer Science from Illinois State University, and has worked as a consultant and architect for some of the largest network management installations in the world. His free time is spent with his wife and two sons, hacking Linux, and writing annoying Perl scripts.

Events

The Fifth 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.

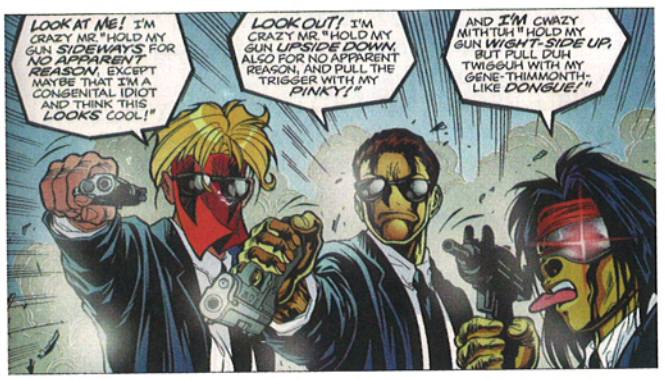
Hacker Jeopardy:
Winn Schwartau is back with Hacker Jeopardy!! The Sixth year in the running! With his sexy sidekick, Vinal Vana, and the ever present judge The Dark Tangent, get ready for a wild ride through hacker trivia, social and science questions. One year there was even a question about a bird! (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 clairifications soon]

Spot the Fed Contest:
7th 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 hckers 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.
The way this works in reality is that we can give out 1/3 of our shirts per day to space them out over the weekend. If you spot a FED (Generally considered someone with arrest authority and a badge) find Priest (Talk to a Goon in a red shirt) and tell him. If he hasn't been spotted, and isn't an already publicly known FED, you may me a winner.

Capture the Flag (CTF) contest:
Time to dust off those sniffers and shine those 'sploits, because CTF is back with a vengeance. This year many of the rules and goals have changed to refocus participants on the fun involved, as well as make the event more relevant to a real world hacking situation. So pay attention to the changes, this will be on the final exam.
The Players: 1) *The Bastard Operators from HELL (BOFH)* - The people 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 and have user accounts. If you set up a host you should be able to point to it and say "that's a mail host" or "warez site" or a Shoutcast server, etcetera.
Registration of Servers will be required to obtain an IP address. Be prepared to provide the Judges a hard copy of the configuration of the machine. (Box, OS,

Patches, Services running & bound ports.) Persons found to be connecting unregistered servers will not be allowed to join the competition. Please remember to to label your box with your name and contact info, as this will speed things up considerably.
Judging will be based on the number and type of services and whether the host is compromised. So the more services the better, just make sure you lock 'em down.
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 - 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 designated Judge to verify it. Whatever hacker or team racks up the greatest number of hosts wins. Additional points will be awarded for speed and efficiency. Hack fast, Hack



well.
The Rules:
1) Everyone must register as a participant in order to obtain an IP address. If you're wondering if this means you, then it does.
2) No hacking from any network segments other than the designated one. There will be no tolerance for those taking down the DEF CON network.
3) No taking down the CTF network or any host you didn't bring for more than 60 seconds. 4) No taking down a host you did bring for more than 5 minutes. That's just dirty pool.
5) Physically accessing any server after it is put into operation will result in a disqualification for that person. Administration may only be performed via the LAN.
6) 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.
7) 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.
8) No thuggery, summoning of elder gods/ Mickey Finns/ physical coercion.
9) Obey the Goons, they exist for your protection.

Streaming Audio and Video:
DEF CON and Pirate Radio UK will be streaming the conference both live and post processed. This will depend on how many cameras are set up. Feeds will be available using Real Player, and MP3 (audio only). Links to the content will be off the main www.defcon.org page. If you have a Real Server with a splitter licence, or an Icecast or Shoutcast server and would like to contribute bandwidth for the event, contact Major Malfunction.

Live Band action:
We have enough space that an area just for live bands and DJs is set up. See the Band / DJ schedule to see who and when.

The 4th Official DEFCON Shoot:
The DC Shoot is happening again. It's slated for Saturday morning at 8AM round up to go off to the shooting site. Please visit the web site linked above for complete information on safety requirements, responsibilities, and what to bring. Be awake!

The DEF CON network: The network this year will be in several segments. Internet Connection: The line is still TBD, however, we will have a high bandwidth line (T1 or DSL) with a class-C of IP space (staticly assigned by DefCon Staff).
Network Structure: We'll wire the general con space & hallways for 10/100 ethernet. You will need to bring your own NIC cards; if you forget ethernet cable, the NOC will have cable available (inexpensively :)
Wireless: We will be providing IEEE-802.11 public access to the Network. You will need to bring your own wireless network cards to connect to the network. (DefCon NOC staff will NOT provide 802.11 PC-Cards or PCI cards). We're going to try to get the pool, bar, and lobby areas within network range (nothing like hacking wirelessly by the pool with a beer!). The 802.11 network will be DSSS, not FH. Freq. Hopping (FH) is old & slow (1-2Mb). DSSS allows 11Mb+. We'll be using equipment implementing the 11Mb DSSS 802.11b standard.

Iron Feather Journal Presents: The best of the commodore 64 cracker screens.
A 90 minute video with audio featuring the top computer graphix of the crackers intro screens put on warez from the 1980's in the commodore scene. Produced by Towne Club.

DEF CON is pleased to announce **"DEF CON goes to the Movies".**
In our first annual presentation, we will be screening the popular 1998 action-thriller movie "Enemy of the State", written by our guest host, David Marconi and starring Will Smith and Gene Hackman among others. The audience is invited to discuss the movie and some of the scenes with the writer.
Enemy of the State
The murder of a congressman is caught on tape and Robert Dean (Will Smith) has it. He has to save his family career and life all in 2 hours! Although the plot twists aren't always surprising they are convincing. Gene Hackman plays the role of the paranoid informant wonderfully but Will Smith can't help being funny no matter how hard he tries. Tony Scott shows the action from surveillance camera and telephoto angles giving an edgy feeling throughout the picture. Most of the chases are on foot keeping car chases are kept to a minimum. The story moves along at a good speed making it a good action movie with a solid plot.
David Marconi is a Hollywood writer and Director. He has worked the film scene in TV as well as movies since the early 80's. His credits include Enemy of the State, The Harvest, Rumble Fish, and The Sky's No Limit. He has worked with major studios like 20th Century Fox, Disney, Warner Brothers, Dreamworks, Paramount, and Columbia TriStar.
Mr. Marconi has written and been involved with over 10 screen scripts including Mission Impossible II, WWIII.com, and an untitled Chris Rock thriller coming out next year.

Iron Feather Presents: Best of C-64 cracker screens.
A 90 minute video with audio featuring the top computer graphix of the crackers intro screens put on warez from the 1980's in the commodore scene. Produced by Towne Club.

Un-Official Events

These events are usually planned and done by other groups, such as last years Cult of the Dead Cow announcement. If you want your party, band, group, etc. announcement or activity listed here just email events, and we'll list it.

The First Annual Coffee Wars:
Seeing how Java is a good Thingtm, the attendees of DEF CON have come up with Coffee Wars. The idea is to bring your favorie roast beans, and we'll grind 'em up Friday morning and have a good start to the Con, and a chance to compare yours to many other types of coffee. I can tell you right now, Uban and Sanka will loose the war. So will Maxwell House. Location and time to be announced soon.

First Annual CD Exchange:
In the spirit of USENIX tape exchange DEF CON will have this year it's own cd exchange and burn table.

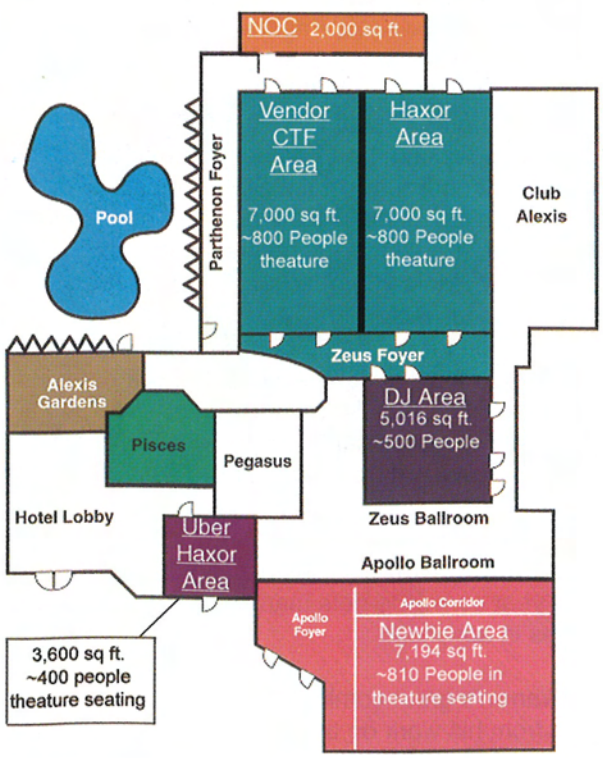
Just bring a CD full of Open Source, Freeware, Shareware to the table and exchange with someone else CD. Also we'll have some cd burners if you want to get a custom cd or linux distro made. Run by Cloaked. Co-sponsored by www.linuxiso.org, who are supplying the isos for all major linux distros including PPC and Sparc.

The Fifth Annual Black and White Ball:

DJs spin music, and people dress up all spiffy. This is the Fifth 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. Held in the DJ area there should be a mobile bar so you don't have to walk too far for drinks. We will tryfor a more strict dress code. IE: If you don't make an attempt to dress funky you don't get in. We'll see if this works.

Hacker Jeopardy:
Winn Schwartau is back with Hacker Jeopardy!! The Sixth year in the running! With his sexy sidekick, Vinal 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 even 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! Submit your team of up to three people at the NOC for the drawings before each round starts!

Hotel Map:
Food is in Pegasus or Alexis Gardens



Event area schedule.

Time	CTF / Vendor Area	Haxor Area
Friday	**Friday**	**Friday**
10:00 - 10:50	CTF Setup	Coffee Wars
11:00 - 11:50	CTF Starts	
12:00 - 12:50	CD Exchange	
16:00 - 16:50	Registration moved from Uber area.	
19:00 - 21:50		DEF CON goes to the movies.
23:00 - 23:50		Hacker Jeopardy: Round One
Saturday	**Saturday**	**Saturday**
07:00	Meet in front for DEF CON Shoot	
19:00 - 19:50		Iron Feather Presents: Best of C-64 cracker screens
20:00 - 22:50	Black & White ball in DJ Area.	
23:00 - 00:50		Hacker Jeopardy Final Rounds!
Sunday	**Sunday**	**Sunday**
16:00 - 16:50	CTF Ends - Prizes Awarded	
18:00 - 18:50	Convention	Closes!

Time	DJ / Band	DJ / Artist	Style
Friday	**Friday**	**Friday**	**Friday**
17:00 - 18:00	Band	Fenris	Death Metal
18:00 -19:00	DJ	DJ Phear	Industrial
19:00 - 20:00	DJ	Christian	Industrial / EBM
20:00 - 21:00	DJ	RazourBlade	Industrial / Goth
21:00 - 22:00	DJ	Shadowvex	Industrial / Dark Trance
22:00 - 23:00	Band	Chainsaws 'n Children	Industrial Thrash Metal
23:00 - 00:00	DJ	DJ Delchi	Industrial / Goth
Saturday	**Saturday**	**Saturday**	**Saturday**
00:00 - 02:00	DJ	Orion	Industrial / Electronic
02:00 - 03:00	DJ	DJ Jerkface	Industrial / EBM
12:00 - 13:00	DJ	Stevyn	Unknown
13:00 - 14:00	DJ	Pepse	Happy Hardcore
14:00 - 15:00	DJ	Polymorph	Hard House
15:00 - 16:00	DJ	Thomas Ockens	Who Knows
16:00 - 17:00	DJ	Iceman	Electronic
17:00 - 18:00	DJ	Wonderbread (?)	Phunky Beats
18:00 - 19:00	DJ	TDA	Progressive Trance
19:00 - 20:00	DJ	Atari	Electronic
20:00 - 21:00	DJ	Medik	Electronic
21:00 - 22:00	Band	Corrupt Data	Electronic
22:00 - 23:00	DJ	Jackalope	Hard Techno
23:00 - 00:00	DJ	HiBias	Progressive Trance
00:00 - 01:00	DJ	Felix K	Trance
01:00 - 02:00	DJ	Ripe	Chicago House
02:00 - 03:00	DJ	DJ Iceberg	Trance
03:00 - 04:00	DJ	Zziks	Electronic

Time	Newbie	Haxor	Uber Haxor
Friday	**Friday**	**Friday**	**Friday**
11:00 - 11:50		**Arthur Money** - Met the FED panel.	
13:00 - 13:50		**Eric Sinrod** - Federal Computer Fraud and Abuse Act.	
14:00 - 14:50		**noise** - Anonymous Remailers.	
15:00 - 15:00		**Dan Danknick** - Fighting Robots.	
16:00 - 16:50		**Jennifer Granick** - The law and hacking.	
17:00 - 17:50		**John Q. Newman** - 10 steps you can take to protect your privacy.	**syke** - opensource utilities & how to test IDS & firewalls.
18:00 - 18:50		**Jason Scott** - textfiles.com: One year later.	**jeru** - Advanced evasion of IDS buffer overflow detection.
Saturday	**Sunday**	**Saturday**	**Sunday**
10:00 - 10:50	**Wyatt** - Radio hacking.	**Gregory B. White** - The USAFA Cadet hacking case.	**Tim Lawless** - Responding to unauthorized root transitions.
11:00 - 11:50	**Thomas Munn** - Need for home based firewalls.	**Ron Moritz** - Proactive defense against malicious code.	**Robert Graham** - Evading network IDS.
12:00 - 12:50	**Xs** - LDAP	**D-Krypt** - Web application security.	**Jon Erickson** - Cryptography & quantum computing.
13:00 - 13:50	**V1ru5** - More lock picking.	**Bruce Schneier** -	**Ian Vitek** - Configuring Linux 2.0.* for IP-spoofing & source routing.
14:00 - 14:50	**Mr. Nasty** - Using tools to obtain recon on NT networks.	Cult of the Dead Cow -	**Bennett Haselton** - Using stego to circumvent censorship.
15:00 - 15:50	Legal Panel Discussion -	**David J. DiCenso** - The Citizen Hacker: Patriot or War criminal?	**Greg Hoglund** - Advanced buffer overflow techniques.
16:00 - 16:50	**Mike Scher** - What is DNS?	**Ian Goldberg** - Using the net Pseudonymously III: It's Alive!	**ghandi** - Dot-Com Smashing: Buffer overflows on the SPARC.
17:00 - 17:50	**DDT** - What PGP & Crypto is, how to use, & not use, it.	**John Q. Newman** - Fake ID by mail & modem.	**Mythrandir** - Penetrating B1 Trusted OS.
18:00 - 18:50	**sinster** - Energy weapons.	**Ender** - Demo of the Autonomous Nodes.	**Evil Wrangler** - Building a backdoor binary
19:00 - 19:50	**Jim McCoy** - Building the mojo nation.	**Aaron Grothe** - Tunneling & firewalls.	**Chris Goggans** - Lotus Domino vulnerabilities.

Time	Newbie	Haxor	Uber Haxor
Sunday	**Sunday**	**Sunday**	**Sunday**
10:00 - 10:50	**Freaky** - Mackintosh security.	**Mr. Mojo** - Windows 2000 security.	**Adam Bresson** - Palm data protection.
11:00 - 11:50	**Pyr0** - FAQ the kiddies.	**Philip J. Loranger** - Army biometrics.	**Phil King** - 8-bit redux: Microcontroller Hacking.
12:00 - 12:50	**Thomas Munn** - How to make a linux firewall with IP-chains.	**Simple Nomad** - A how to on network mapping.	**John Flowers** - Network IDS: Do not bend, fold, or mutilate.
13:00 - 13:50	**V1ru5** - Updated computer virus class.	**Richard Thieme** - SE at DC: Games Hackers Play.	**blanu** - Freenet.
14:00 - 14:50	**Daremoe** - Target analysis or How Crackers Find You.	**Sarah Gordon** - Virus Writers: The end of innocence.	**Kent Radek** - Designing an anonymous network.
15:00 - 15:50	**Natasha Grigori** - Hacktivits to activists, making a transition.	**Lee Johnston** - Software to construct entire networks inside a computer.	**Subterrain Security Group** - The impact of passive network mapping.
16:00 - 16:50	**Shane O'Donnell** - Overview of network management, SNMP		
17:00 -	Prizes, Clean up, see you next year!		

A Special Thanks To:

DEF CON 8.0 could not have been possible without the help of the following people: Zac, Xylorg, Noid, Major Malfunction, Ping, Lockheed, Tina, Swift Grigs, Artimage, Bink, Bad Kitty, Metal Head, Crusader, The Bisop, Dead Addict, Megsusa, Evil Pete, Dr. Kool, Russ, Uncle IRA, Josh, Ming of Mung, Dr. Nick 2000, Priest, The People, Petty Larceny, Flea, Evil, Rooster, Queeg, Pescador, Sqweak, Warflower, Teklord, Shatter, Fiery, Bink, Kuzubic, Cyber, All the DJs who put in their time to spin tunes for everyone, The NOC staff for getting the CTF and network going, Arthur Money for speaking, Iron Feather Journal for the videos, David Marconi for his work on Enemy of the State, Christian Hedegaard-Schou for planning the DC Shoot, All the people who helped to organize car caravans to get to DEF CO including the Death Race2k.org 2000 group by boogah, Moloch.org, zoltan, The Bay Area Caravan 2.0 (BAC2.0), bonq and the whole San Diego Caravan, Lord Almus for the 801 Caravan, tdargon for the Sattle Caravan, suidzero of the I-70 Def-convoy. I also want to thank all of the zines that have helped to promote DEF CON including Anti-Social magazine, The Iron Feather Journal, phrack, and many more I can't remember. Thanks to all the websites and links people have put up. With out this support, DEF CON would not be possible!

Happy wedding vow renewal for AbbyNrml & Ghstwrtr. Happy wedding to Evil Wench & ???. Every year someone gets married at DEF CON, at least I knew about these ones in advance!

Please go and read Adam Warren's great comics. I've lifted some of the great Kung-Fu backgrounds from his work on the Gen-13 bootleg series. The cover robot is from a Phil Foglio & Freff's comic from 1982.