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 opportunities 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 box. It seems that last year, but last Saturday DEF CON had drank every group that had ever been at the Alexes, except the British RAF. By Sunday we had duded the RAF and hold the record for most consumed. I think it was something like 2-3 months of normal sales done in a weekend. So be cool to the hotels. 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 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 channel. Those with a Ham license, we will be on CCH 1 and 2 (ask a goon for the freq.) I hope to have the video tapes made in time for the late night TV special. It wasn't done when I wrote this at 0245 after 4 cans of coffee, 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 picking around, but remember this 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 without 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 done now. 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-ssh web proxy, and a remaining. 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 disproportionate in the realm of Network IDS — with Host-based IDS lagging behind, only to see detect breaches after the incident.

This state of affairs often frustrates 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 saint of hopeful causes, the Saint Jude project is an IDS project that hopes to deliver a model and implementation able to stop a root compromised dead in its tracks, regardless of the exploit method.

Tim Lawless is a Systems Administrator with the University of Squatter Mississipp on the Sanrris 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 QFOD (formerly QOPA), 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 kids who think they are cracking over on you with their "sleazy" scans. But then something bad happens: your servers get hacked through your firewall, and that expensive IDS never utter a beep.
How did this happen? The root of the problem is that most commercial IDSs are little more than anti-spoofing tools and cannot detect unexpected behavior. This talk will show how to evade these IDSs using popular tools like Whois and fragrouter. It will also reveal the latest in additional secret techniques used by hackers.

Mr. Graham learned hacking as a toddler from his grandfather, a WWII codebreaker. His first IDS was written more than 10 years ago designed to catch Moris Codecopying. He is the author of several pending patents in the IDS field. He is the author of several high-profile security-related documents. (www.pearlstein.com/pub) and is a frequent speaker at conferences, IRL he is the co-founder, CTO, and chief architect at Network Inc.

Joni 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 Babylonian GCD algorithm and Euler's totient function and theorem. Complexity theory, fractality, and tractability will be explained. He will be discussing what a "hard" problem is (NP vs F) and algorithm runtime and Big-O notation with respect to graph. (He will also explain to show why picking the product of two large prime numbers isn't trivial. Then the RSA encryption algorithm 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, entanglement, and measurement. The potential 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 its ability to brute force anything in N^2 steps will hopefully be apparent. Since most conventional encryption will be shown to be insecure, a few quantum cryptography techniques will be covered: SRA, afterwards time permitting.

Joni Erickson was the product of a 6th grade science fair experiment in human genetics by little Steve. Geno on planet Veja? (His parents helped a little bit.) After the fair was over, Jon was told as slave short by the elementary school to the Orb Night intergalactic, casting and modeling agency. Due to his flashing good looks and human neck, John quickly found himself the poster boy for Zarla's exploitive 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 frosse do. He was sentenced to 160 years on the Prison Planet Earth. As it exits to Earth wasn't fixed enough, moments after landing, he was quickly carried away to Area 51 by the US Government. Only to be traded to a Japanese research group in exchange for some rare Pole cartoning by an agent named Jose Ronnicke. In Japan, the brilliant Dr. Keri Chronx and a low tech named Michelle began an experimental opiatesurgery procedure on Jon, hoping to teach him about human emotion. Something went horribly wrong, and when the anaesthetic wore off, Jon ended up in an empty operating room, with a giant hole in his skull. All the colors began to melt into his skin, and he panicked, plugging the hole with paper maché 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 entrepreneur. And he's sorry that he has to miles out to so many great adventures.

Ian Vickers, penetration tester at Intersec. IP-voodooping and sorting random connections with Linux 2.6.23.

The speech will discuss hacking firewalls and filtering routers by spoofing IP and MAC addresses. Two different spoofing techniques will be presented. Ian will talk about how to spoof an IP address (IP spoofing) and topdown what kind of information one will need for these examples to work. Second Ian will now how to set up a working source route (full connection) through a router. Then Ian will show how to set up the firewall on a Linux to be able to IP-spoof (with full connection) a firewall if you sit on a trusted network A, between a trusted network, A, and the service, B. Both examples will be explained step by step.

Ian Vickers works as a full time penetration tester at Intersec, Sweden. (This page is in ewdesh.) He is right now researching within Media Access level security and USB security (which is a big unexploited hole). He also thinks that odems are underestimated hacker tools.

Bennett Hatelson, peacefellow.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 unlocked 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 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 the fact that you're "using" a tool for circumventing the censors would often be enough to get you in trouble.

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

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 fail to meet these attacks.

Bennett Hatelson has been the coordinator of Peacefellow.org since its inception in 1998. Peacefellow opposes censorship that targets Internet users under 18, and maintains that privacy 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. Peacefellow 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 C and APIs. For those of you who already understand buffer overflows, this talk will be a refreshing discussion on technique. We will show how the injection method can't be discovered 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, viruses, and rootkits.

Phil King - 8-Bit Dodger: Microcontroller Hacking.

In days gone by, microprocessors didn't have units of bytes, at all, and names such as Commodore, Atari, and Apple (cigs Apple) ruled the land. Interped hackers of amazing skill and talent worked their magic with limited resources, producing code that was a thing...
an encrypted protocol would still be easy for eavesdroppers to detect, without breaking the encryption — just by noting how the data are being sent. Breaking the ciphers would often be enough to get you into trouble.

What we have designed is a protocol that uses steganography to circumvent network-level censorship, so that the protocol is unobservable to the censors. We explain in some detail the protocols to the problem — such as hiding information in a long, dynamically-generated URL that is sent in an “outside” reply, and hiding information in HTTP cookies or HTTP sessions. The idea is to embed information in the HTTP layer in a way that is difficult to detect.

This sounds simple, but the mathematics of using steganography to hide data is not easy. Our paper describes a new way to hide data in HTTP cookies or HTTP sessions.

Bennett Hasselton has been the founder of PGP.org since its inception in 1991. He created PGP, the first open-source public-key cryptography system, in 1991. He has won many awards for his work on cryptography, and is known for his work on steganography.

In this talk, we discuss how to work with the information in these protocols, and how to detect them. We explain the mathematics of using steganography to hide data in HTTP cookies or HTTP sessions.

Bennett Hasselton has been the founder of PGP.org since its inception in 1991. He created PGP, the first open-source public-key cryptography system, in 1991. He has won many awards for his work on cryptography, and is known for his work on steganography.

In this talk, we discuss how to work with the information in these protocols, and how to detect them. We explain the mathematics of using steganography to hide data in HTTP cookies or HTTP sessions.

Bennett Hasselton has been the founder of PGP.org since its inception in 1991. He created PGP, the first open-source public-key cryptography system, in 1991. He has won many awards for his work on cryptography, and is known for his work on steganography.

In this talk, we discuss how to work with the information in these protocols, and how to detect them. We explain the mathematics of using steganography to hide data in HTTP cookies or HTTP sessions.

Bennett Hasselton has been the founder of PGP.org since its inception in 1991. He created PGP, the first open-source public-key cryptography system, in 1991. He has won many awards for his work on cryptography, and is known for his work on steganography.

In this talk, we discuss how to work with the information in these protocols, and how to detect them. We explain the mathematics of using steganography to hide data in HTTP cookies or HTTP sessions.

Bennett Hasselton has been the founder of PGP.org since its inception in 1991. He created PGP, the first open-source public-key cryptography system, in 1991. He has won many awards for his work on cryptography, and is known for his work on steganography.

In this talk, we discuss how to work with the information in these protocols, and how to detect them. We explain the mathematics of using steganography to hide data in HTTP cookies or HTTP sessions.

Bennett Hasselton has been the founder of PGP.org since its inception in 1991. He created PGP, the first open-source public-key cryptography system, in 1991. He has won many awards for his work on cryptography, and is known for his work on steganography.

In this talk, we discuss how to work with the information in these protocols, and how to detect them. We explain the mathematics of using steganography to hide data in HTTP cookies or HTTP sessions.

Bennett Hasselton has been the founder of PGP.org since its inception in 1991. He created PGP, the first open-source public-key cryptography system, in 1991. He has won many awards for his work on cryptography, and is known for his work on steganography.
Mr. Flowers is the founder of Hivewire and reads the Core R&D team in creating the Ambis, Swarm and upcoming IDS product. Prior to Hivewire, Mr. Flowers was the chief architect of The Inquirer's individualized news filtering service. He has also held positions as the chief security and Internet Architect at Utopiap, chief architect of Neurossoft (later become Movitron), and architect of the Interactive voice response system that was the prototype of WinTalk 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.

Haxors Speakers

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

Basically I'll discuss the case that went to trial in the spring of 97. 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 defenses. I served as 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 attorney alike. The cadet was involved in IRC but the law enforcement types and prosecution... basically convinced that he was the "hacker" (after all, everybody KNOWS that IRC is nothing more than a place for hackers to trade information on how to break into computers - the usual sentiment expressed by the investigators). It had up to that point, kept my information. To the AF's surprise, I was able to identify a silent connection that could be tracked back to the AF's systems. The case was dropped as a result of this evidence that was given in court.

1) Background of the case
2) The "evidence" the prosecution thought they had.
3) The many possible areas where clues might have been found that would suggest where the attackers were coming from.
4) What lessons can be learned from this case.
5) How the government and technology industry need to know where to look for the information they want to track.

I have to reiterate that the cadet's attorney was able to help the cadet by seeing the evidence of the case that was found in court.

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 more than 20 course 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 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 Computer Systems Staff Office-Center in Bolling, 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 Bolling, Dr. White served as the Branch Chief of the Network Security Branch 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 Reserve at the Defense Information Systems Agency.
Between his Air Force Academy assignments, Dr. White spent three years at Texas A&M University working on his Ph.D. in computer science. Dr. White's 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 Bodo, Mississippi. He was the only person in the class to achieve both the Academic and Military awards for student leadership and academic excellence and was a Distinguished Graduate of the course. Before attending the course in Bodo, Dr. White served as the Branch Chief of the Network Security Branch at the Cryptologic Support Center in San Antonio, Texas. His first Air Force assignment was to the National Security Agency as an 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 1990. He returned from the Air Force in 1989 and is currently serving in the Air Force Reserve at the Defense Information Systems Agency.

Ron Moritz, Senior Vice President and Chief Technical Officer at Symantec Corporation, where he serves as leading technology visionary. As a key member of the executive leadership team, he is responsible for the development of products and services that transform the relationship between security and business. Ron was one of the first executives to recognize the importance of security and compliance as business drivers and to develop strategies that are designed to protect the company's leadership role in the high-impact web security industry. He holds 20 patents and has made 40 speeches at industry conferences. He is also an active member of the board of directors of the Information Security & Privacy Organization.

Mr. Ikoj, Windows 2000 security.

Ivan Goldberg, Zero Knowledge Systems, and Jeff Goff, Director of Enterprise System Services at the University of Texas at Austin, have created a new version of their popular product, SecureDCC, which is designed to protect the University's mainframe and UNIX computer systems. The new version includes the following features:

- Increased performance by up to 50%.
- Enhanced security features, including improved encryption algorithms.
- Compatibility with all versions of UNIX and mainframe operating systems.
- Support for remote access and virtual private networks.

The product is currently available for download from the University's web site.

The Freedom Network from ZeroKnowledge Systems, CyberGhost, and Jeff Goff, Director of Enterprise System Services at the University of Texas at Austin, have created a new version of their popular product, SecureDCC, which is designed to protect the University's mainframe and UNIX computer systems. The new version includes the following features:

- Increased performance by up to 50%.
- Enhanced security features, including improved encryption algorithms.
- Compatibility with all versions of UNIX and mainframe operating systems.
- Support for remote access and virtual private networks.

The product is currently available for download from the University's web site.
Engineers misplace 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 facility 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 technology and author Bruce Schneier is both a founder and the Chief Technical Officer of Counterpane Internet Security, Inc. He established the company with Tom Romeo 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 makes 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 all security issues and solutions.

White president of Counterpane Systems, Schneier designed and analyzied hardware and software cryptologic systems, advised sophisticated clients on products and markets, and taught technical as well as business courses related to the field of cryptography. Concerned as a citizen, Microsoft, the National Security Agency, Gibbani, 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 Tookey 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, his seminal work in this 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 author, 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 Security Information Center, and was on the board of directors of the Voter's Telecomputing Monitor.

John Q. Newman, Author, Fake ID by mail and in person, and 10 steps you can take to protect your privacy.

I will cover topics such as the legal issues regarding fake ID, where and when it can be safely used, how to determine if an Internet seller of fake ID is a scammer or legit, and finally the federal government's new interest in fake ID. The id shop, the place I recommended last year, was raided by the Secret Service 4 months ago, and I will stick with that here. If you remember, the owner was at last years convention making and selling id's.

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 give at the conference circuit in the next few months. 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 only high hackers met in face-time for the first time to Def Con 5 when thousands crept into a hotel for a hacking "event". Richard Thieme has been called a "shrewd observer of hacker attitudes and behaviors" and sometimes he is. You are the judge. In this talk he reviews "very subjectively" the 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 more. He takes on the truth - trash-truth and outright lies that we exchange as currency in this looking-glass world.

Thieme's predictions at DefCon W.I. - Hacking as Practice for TransPlanetary Life in the 21st Century. How will 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 hacking in your heart.

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

He is "a figure head 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 CYBERPATH.

He has spoken for OmniTech; Strong Capital Management; System Planning Corporation (SPC); UOP; Atlantic Energy; Firstar Bank; MAPICS; Influential Technology Group; Navy Federal Credit Union; Arthur Andersen; the Conference of State Legislatures; the Societe for Technical Communication; Association for Information Management and Research; the PDR, the
Engineers secure secure primitives, introduce security flaws in the implementation, build bad user interfaces, allow for errors or failures and generally fail to design systems that counter the actual threats. Traditional engineering is about patching holes, and the non-engineer obsession 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 future.

Internationally renowned security technologist and author Bruce Schneier is both a Founder and Chief Technical Officer at Counterpane Internet Security, Inc. He does not discuss in this talk Bruce will discuss the failure of security on the Internet, the failure of testing the quality that can be trusted in such a complex environment, and the need to understand the business and technical aspects of security.

Richard Thiemeyer, Social Engineer at DefCon: Games Hackers Play

DefCon has changed dramatically from DefCon 1 - when sixty real hackers met in face to face for the first time to DefCon 8 when thousands crowd into a hotel. Richard Thiemeyer has been involved in the process. Richard Thiemeyer has been a "shrewd observer of hacker attitudes and behaviors" and sometimes he "bores the listener." In this talk he reviews "subjectively" the ways hackers are invented, perceived, and manipulate in the many rings of DefCon. It's all here - the headaches, the good times, and the pain and new, innovative ideas. The problems are in the people who are "located" in the hacking class window.

Thiemeyer's predictions at DefCon 8 as "hacking as practice for TransPlanetary life in the 21st Century" have all come to pass. But what's next? How to open the door for yourself in the Next Big Thing, dependent on your hacking generation and the degree of real insecurity in your heart.

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


Eric Simms, partner, Diana, Morris & Hockecker LLP; Bill Reilly, Student

Federal Computer Fraud and Abuse Act

We are going to discuss the Federal Computer Fraud and Abuse Act and its enforcement with the United States' Attorney's Office. We will discuss the history and nature of the Act and its impact on law enforcement. We will also discuss the enforcement of the Computer Fraud and Abuse Act. Finally we will look at recent criminal cases in which the Computer Fraud and Abuse Act was found.

Bill Reilly is a student at the University of San Francisco, who has a focus in business and legal issues. Before law school, Bill Reilly spent 8 years in the Department of Justice, working with the Department of Commerce and the Federal Trade Commission, and recently acknowledged as a "Computer Crime Expert" by the University of San Francisco. Bill Reilly also has been noted as a "shrewd observer of hacker attitudes and behaviors" and sometimes he "bores the listener." In this talk he reviews "subjectively" the ways hackers are invented, perceived, and manipulate in the many rings of DefCon. It's all here - the headaches, the good times, and the pain and new, innovative ideas. The problems are in the people who are "located" in the hacking class window.

Thiemeyer's predictions at DefCon 8 as "hacking as practice for TransPlanetary life in the 21st Century" have all come to pass. But what's next? How to open the door for yourself in the Next Big Thing, dependent on your hacking generation and the degree of real insecurity in your heart.

Richard Thiemeyer is a writer and professional speaker focused "on a lifetime," in particular the human dimensions of technology and work.
Newbie Speakers

Wyatt, Black hacking.

Thomas Munn, Need for home-based intranets.

Virus, Worms, Network Security Administrator. This talk will be an introduction to computer viruses.

Covering Boot sector, File Infected Multi-Part, Poly-Boot, Malware, Trojan, and Script viruses. We will talk about how they infect, their types of damage, and repairing.

Lock picking Talk. This talk will cover different kinds of locks, and handouts. And how were opened?

Robert Lupo says "VIRUS" has several certifications in the security field, including CCNA, CCSE. He currently works as a Network Security Administrator. He is known for his lock picking, virus, and Social Engineering, MCSE, CCA, CSCE, and Security.

Certified:

TX 

CDP [No more information available]

Mr. Nasty:

Using tools to perform heist 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 Grimack, Attorney at Law.

Brian, Attorney at Law. The law and hacking.

A panel of criminal civil attorneys and a federal prosecutor to talk, debate and answer questions. While in some situations they may not be against something that does not mean you can be sued in civil court or charged with a related charge.

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

Recently, the overwhelming space among DNS, the design of browsers and search engines, international, national, and local trademark review, and have come to a head. A pending resolution published in ICANN has taken on a level of use as a task that sat squarely on one man's shoulders. The tension is largely the result of interest and purposeful conclusions of the purpose and functions of the various Internet and resource locating systems. In this talk, we will discuss what a DNS root is, fundamental to this 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 implemented, and their implications for trademark and software policies and design.

Mike Scher is an attorney and network security consultant working in both the policy and technology domains. He has designed private DNS roots and TLD systems for international Fortune 500 companies, and worked with public-private alternative DNS root projects. Most recently, Mr. Scher has become the architecture lead for a fast-growing startup company in Charlotte.

DOT: POP: What Pop and corps is and how to use (and not use) it.

sinned.

Energy Weapons: [No more information available]

Thomas Munn,

How to make a virus with TP property.

[No more information available]

Freaky, stalker.s.net and Freaks Mechanics 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 and 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.

Pymo, Network Administrator - The 100 Cellar.com FAQ the Kiddles.

Every year the attendance at Defcon grows. It was apparent last year that many of the Kiddles

(With dr. d00s, Script Kiddies, and lamen) had come with the intention of learning something. A problem is upon arrival these groups think that the only way they will be able to benefit from Defcon is if they "ROVE THEMSELVES" 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 newbie some of the info needed to pass the 'right track'. Some of the highlights are:

- Danger of being a script kiddie, learning and complicity. What your local library has to offer. "Hacking without going to jail. Shutting your mouth and opening your ears. There will be many URLs and book titles given up peeling a join and paper.

Daremore, System Profiling: Target, Analysis, and How Crackers Find You.

This presentation will walk through profiling and target selection with a live scan at the start of the presentation. I will demonstrate techniques and tools used to remotely identify systems, services, and vulnerabilities. The presentation should teach newbie hackers how to identify potential targets while explaining how system administrators know their systems are targeted for attack.

Nasatka Gregor, President ACPO.

Hacktivists vs. Activists - Making the Transition.

In 1999 the ACPO formed the goal of removing child pornography on the Internet via any means possible. After an initial announcement, RMR, and recruitment at Defcon 7, we began the daunting task of shutting down Child Peril Sites. Initially successful, we found that the sites we took down would come back up after a few days or weeks. Not only did 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 HiP/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 newspapers, on-line, and radio have focused on ethical "hackers" groups fighting child porn have featured ACPO and Condemnation, who is currently in the process of going legit.)

We're on the front page, on-line, and in print. The community is growing, and we are making a difference.
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 all roots? What are alternate roots and why does internet work?

Recently, the overlapping spaces among DNS, the design of browsers and search engines, electrical networks, and local trademarks interest an alive, have come to a head. A growing organization dubbed the "DNS Interoperability Roundtable" (DIR), that has a high-level meeting quarterly on one man’s shoulders. The tensions are, the result of any (and potentially) confusions of the purpose and functions of the various Internet service and resource localizing systems. In this talk, we 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 will 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 in both the policy and technology fronts. He has designed private DNS roots and TLD systems for international Fortune 500 companies, and worked as a policy public defender. DNS is not something he has ever done recently. Mr. Scher has also become infrastructure technology and policy managing for a fast-growing start-up company in Chicago.

Dawn
What this small is and how to use it (and not use it).

silent,

Energy, Weapons
No more information available.

Thomas Mullen
How to make a little friend with $5,000.

word information available.

Fresky, stavola.net and Fresk Muskrat

Security and hacking of the MACOS and Debian of OS.

Fresky will be presenting his second speech this year. Last year he covered the basics of machine security and answered questions. This year he will be going over security hacking of the MacOS and Debian of OS. And and ask what it offers. His topic not well known, so he is willing to take questions early to cover the topic.

Pyro, Network Administrator - The 98th Cellar.com

FAG the Kids

Every year the attendance at Detcon grows. It was apparent this last year that many of the Kiddles

(WOZs, d0WS, Script Kiddies, and lammers) had come with the intention of learning something. Problem is you are not in the appropriate path, there is no transition process into an activist group, and the benefits the transition has brought us.

Jim McCoy, Major 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 a very service based model he was convinced that the best way to bootstrap a start-up was to antagonize the government, since then he has learned there are easier ways.

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

Arthur L. Money was sworn in as Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASC) on October 5, 1990. Mr. Money served as the Senior Civilian Office, Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence and Chief Information Officer of the Department of Defense from February 26, 1990 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 telecommunications 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 maximum functionality at a maximum price, whereby 70% of their deployments are considered failures. Fortunately, the open source tools are evolving and becoming available to those 800-pound gorillas. This presentation will provide an overview of SNMP and other management technologies.

In my talk (and possibly Roxy of conditionedorg will present the problems which convinced us that having a transition process into an activist group, and the benefits the transition has brought us.

Jim McCoy, Major 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 a very service based model he was convinced that the best way to bootstrap a start-up was to antagonize the government, since then he has learned there are easier ways.

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

Arthur L. Money was sworn in as Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASC) on October 5, 1990. Mr. Money served as the Senior Civilian Office, Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence and Chief Information Officer of the Department of Defense from February 26, 1990 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 telecommunications 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 maximum functionality at a maximum price, whereby 70% of their deployments are considered failures. Fortunately, the open source tools are evolving and becoming available to those 800-pound gorillas. This presentation will provide an overview of SNMP and other management technologies.
Patches, Services running & bound ports. Persons found to be connecting unregistered servers will not be allowed to join the competition. Please remember 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 (IJ) 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. Users can't win; they just get to use the servers.

3) The Hackers - Hackers win by putting their team name or handle in the 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 radius 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 Films' 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 on the main www.defcon.org page. If you have a Real Server with a splitter license, or an Iocessor or Rocketcast server and would like to contribute bandwidth to the event, contact Major Malfunction.

Live Band action:
We have enough space that an area just for live bands and DJ's 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 T1, however, we will have a high bandwidth line (T1 or DSL) with a class-C of IP space (statically 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 ( inexpen-

sively)

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 PG-Cards or PCI cards). We're going to try
to let the pool, ber, 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 implement-
ing 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 graphic of the crackers intro screens put on
ewave from the 80'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 Thing, the attendees of DEF CON have come up with Coffee Wars. The idea is to bring your favorite roast beans, and we'll grind 'em up Friday morning and have a good stroll to the Con, and a chance to compare yours to many other types of coffee. I can tell you right now, Urban and Sanka will
curse 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's own cd exchange and burn table.
Streaming Audio and Video: DEF CON and Pirate Radio UK will be streaming the conference 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 localhost or Showcast 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 9th round up to go out to the shooting site. Please visit the web site linked above for complete information on safety requirements, responsibilities, and what to bring. Be aware!

The DEF CON network:
The network this year will be in several segments. Internet Connection: The line is still T10, however, we will have a high bandwidth line (T1 or DSL) with a class-C of IP space (statically assigned by DEFCON Staff). Network Structure: We’re wiring the general conference & hallways for 10/100 ethernet. You will need to bring your own NIC cards; if you forget ethernet cables, the NOC will have cables available.

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 trying to get the pool bar, and lobby areas within network range (nothing like hacking wireless by the pool with a beer!). The 802.11 network will be DSSS, not FH. Freq. Hopping (FH) is old & slow (1-2Mbps). DSSS allows 11Mbps. We’ll be using equipment implementing the 11Mm IEEE 802.11 standard.

Iron Feather Journal Presents: The best of the comodore 64 crack screens.
A 90 minute video with audio featuring the top computer graphics of the crack screens into screens put on from the 1980s in the conference room. 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 announced event. If you want your party band, group, etc. announcement or activity listed here just email events, and we’ll list.

The First Annual Coffee Wars:
Seeing how Java is a good thing, the attendees of DEF CON have come up with Coffee Wars. The idea is to bring your favorite roast beans, and we’ll grind ‘em up Friday morning and have a good start to the Con, and a chance to compare to many other types of coffee. I can tell you right now, Urban and Sanka will lose 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’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 old burners if you want to get a custom cd or linux distro made. Run by Clawd, Co-sponsored by www.linuxiso.org, who are supplying the iso’s for all major linux distros including PPC and SPC.

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 sceptical, most original. Held in the DJ area there should be a mobile bar so you don’t have to walk too far for drinks. We will try 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 it works.

Hacker Jeopardy: When Schwarzenegger is back with Hacker Jeopardy!!! The Sixth day in the running! With his sexy sleeclothes, Vinal Vasa, and the ever present judge The Dark. The Blacklist, get ready for a wild ride through hacker trivia, social and science questions. One year there was even a question about a bird! We want to work 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 talks a question, he drinks. If contestants are creating or sneaking they drink. It teams will be picked at random and compete for the final round. There can be only one! Submit your teams of up to three people at the NOC for the drawings before each round starts!

Event area schedule.

Time   CTF / Vendor Area   Haxor Area
Friday  Friday  Friday
1800-1900 CTF Setup  Coffee Wars
1900-2100 CTF Starts  CD Exchange
2100-2300 Registration moved from upper area
2000-2300 DEF CON Goes to the movies
2300-2400 Hacker Jeopardy, Round One
Saturday  Saturday  Saturday
0700 Meet in front of DEF CON Shoot
1900-2100 Iron Feather Presents: Best of C64 crack screens
2000-2200 Black & White ball in DJ Area.
2300-000 Hacker Jeopardy Final Rounds
Sunday  Sunday  Sunday
1600-1800 CTF Finals - Prizes Awarded
1900-1900 Convention Close!
<table>
<thead>
<tr>
<th>Time</th>
<th>Haxor</th>
<th>Newbie</th>
<th>Uber Haxor</th>
<th>Time</th>
<th>Haxor</th>
<th>Newbie</th>
<th>Uber Haxor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Friday</td>
<td>Friday</td>
<td>Friday</td>
<td>Friday</td>
<td>Sunday</td>
<td>Sunday</td>
<td>Sunday</td>
<td>Sunday</td>
</tr>
<tr>
<td>14:00 - 14:30</td>
<td>Jason Scott - HVhax.org - One of those PMSL.</td>
<td>Neurotic - Open Source Ventures.</td>
<td>Mark - A special thanks to:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:00 - 15:30</td>
<td>John D. Newman - 10 steps you can take to protect your privacy.</td>
<td>John D. Newman - 10 steps you can take to protect your privacy.</td>
<td>Mark - A special thanks to:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16:00 - 16:30</td>
<td>John D. Newman - 10 steps you can take to protect your privacy.</td>
<td>John D. Newman - 10 steps you can take to protect your privacy.</td>
<td>Mark - A special thanks to:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17:00 - 17:30</td>
<td>John D. Newman - 10 steps you can take to protect your privacy.</td>
<td>John D. Newman - 10 steps you can take to protect your privacy.</td>
<td>Mark - A special thanks to:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18:00 - 18:30</td>
<td>John D. Newman - 10 steps you can take to protect your privacy.</td>
<td>John D. Newman - 10 steps you can take to protect your privacy.</td>
<td>Mark - A special thanks to:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Saturday**

**Sunday**

**A Special Thanks To:**

DEF CON 8.0 could not have been possible without the help of the following people: Zsc, Xylo, Nof, Mud, Mullafunktion, Ping, Lockheer, Tina, Swift Gray, Antimon, Bink, Bad Kitty, Meathead, Crusader, The Biscuit, Dead Artist, Megabyte, Evil Pete, Dr. Koo, Russ, Uncle IRA, Josh, Ming of Mung, Dr. Nick 2000, Priest, The People, Petey Lanway, Flea, Evil Rooster, Queeg, Persuader, Slowoak, Waflower, Teldor, Shatter, Fiery, Bink, Kuzbide, Cyber, All The Guys who put in their time to spin tunes for everyone, The NCSC for getting the CFT and network going, Arthur Money for speaking, Iron Feather Journal for the videos, David MacFarlan for his work on Enemy of The State, Christian Haggard Schel for planning the DC Shoot. All the people who helped to organize end users to get to DEF CO including the Death Track2.org 2000 group by bogmah, Molech.org, Zollan, The Bay Area Caravan 2.0 (BA22.0), and the whole San Diego Caravan, Lord Almas for the 801 Caravan, Irgadon for the Seattle Caravan, the creators of the 1-70 Def-convey. I also want to thank all of the zones thatoto to promote DEF CON (including Anon-Seci magazine), Iron, Feather Journal, phrack, and many more. I can't remember. Thank you to all the websites and links people have put up. With out this support, DEF CON could not be possible.

Happy wedding aka renewal for AbbyKorni & Ghastly. Happy wedding to Evil Wench & Prv. Every year someone gets married at DEF CON, at least I know about those 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 & Frey comic from 1982.