DEF CON VI Convention Announcement

July 31 - August 2, 1998

The Plaza Hotel and Casino

Las Vegas, Nevada

LAST UPDATED: 18 JUNE 1998

ABSTRACT:

It's time to brave Las Vegas again for DEF CON! This is an initial announcement and invitation to DEF CON VI, a convention for overlooked elements of the computer culture such as Hackers, Phreaks, Hammies, Virii Coders, Programmers, Crackers, Cyberpunk Wannabees, Civil Liberties Groups, CypherPunks, Futurists, and Artists.

What DEF CON is known for is the open discussion of all ideas, the free environment to make new contacts and the lack of ego. More people have made great friends at DEF CON over the years, and it is also known for letting the "Suits" (Government / Corporate) mix with everyone and get an idea of what the scene is all about. The media makes an appearance every year and we try to educate them as to what is really going on. It has turned into the place to be if you are at all interested in the computer underground.

COSTS: $40.00 at the door

CONFERENCE HOME PAGE: http://www.defcon.org

CONFERENCE E-MAIL: info@defcon.org

PAST SPEAKERS:

Over the years DEF CON has had many notable speakers including:

- **Yobie Benjamin** (*Cambridge Technology Partners*)
- **Dan Farmer** (*Earth Link*)
- **Dr. Hobbit** (*avian.org*)
- **Eric Hughes** (*Cypherpunks*)
- **Dr. Mudge** (*L0pht*)
- **Winn Schwartau** (*Infowar.com*)
- **Bruce Schneier** (*Counterpane Systems*)
- **Jim Settle** (*ex-FBI*)
- **Robert Steele** (*ex-CIA*)
- **Gail Thackeray** (*Deputy Attorney, Phoenix*)
- **Ira Winkler** (*ISCA*)
- **Phil Zimmerman** (*PGP Inc.*)

CURRENT SPEAKERS:

Jennifer Stisa Granick, Attorney at Law - ***A review of several major computer crime cases from the past year or two***, perhaps Salgado, Kashpureff and one other. This review will describe the hack (in relatively non-technical terms), what laws applied to criminalize the hack, how the hacker got caught, the prosecution that ensued, and the result of that prosecution. Through these case studies, audience members should be able learn what they should not do, and why.

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

Bruce Schneier, Author of Applied Cryptography - *Tradecraft on Public Networks*. Dead drops, semaphores, cut outs, telltales...the tools of spying. In a world of continuous communications and ubiquitous eavesdropping, is there any hope for covert communications? Learn about some old tricks of the trade, and some new ones.

Bruce Schneier is president of Counterpane Systems, the author of Applied Cryptography, and the inventor the Blowfish algorithm. He serves on the board of the International Association for Cryptologic Research and the Electronic Privacy Information Center. He is a contributing editor to Dr. Dobb's Journal, and a frequent writer and lecturer on cryptography.

Ian Goldberg, ISAAC Research Group, UC Berkeley - ***Cryptanalysis of the GSM Identification Algorithm.*** About 80 million digital cell phones worldwide implement the Global System for Mobile communications (GSM) protocols. Recently it was announced that COMP128, the cryptographic algorithm that protects the "identity key" in the majority of these phones, was extremely weak, thus allowing GSM phones to be "cloned". In this talk, we will examine how COMP128 is used in the GSM protocol, describe the algorithm itself, and demonstrate how to break it. We will also discuss the implications this result has for the security of of the voice privacy features of GSM.

Ian Goldberg is a Graduate Student Researcher and founding member of the Internet Security, Applications, Authentication and Cryptography (ISAAC) research group at UC Berkeley. His research areas include cryptography, security, privacy systems, and digital cash.

Peter Shipley - ***An overview of a two year effort in massive multi-modem wardialing.*** Security problems occur when obvious security problems are overlooked. One commonly overlooked problem is alternative access methods to a corporate Intranet from an external machine. Many if not most companies are overlooking their secondary vulnerabilities surrounding alternate methods of network access. Mr. Shipley will present research covering an overview of a two-year effort in massive multi-modem wardialing. His findings will include some personal observations and the results obtained from scanning the San Francisco bay area. When Mr. Shipley started this project he noted that there were no published research references to wardialing or documented statistical results of the types of equipment and computer networks commonly found on the POTS (Plain old telephone system) network. Mr. Shipley decided to change that through his research.

Mr. Shipley is an independent consultant in the San Francisco Bay Area with nearly thirteen years experience in the Computer Security field. Mr. Shipley is one of the few individuals who is well known and respected in the professional world as well as the underground and hacker community. He has extensive experience in system and network security as well as programming and project design. Past and current clients include TRW, DHL, Claris, USPS, Wells Fargo, and KPMG. In the past Mr. Shipley has designed Intranet banking applications for Wells Fargo, Firewall design and testing for and, WWW server configuration and design for DHL. Mr. Shipley's specialties are third party penetration testing and firewall review, computer risk assessment, and security training. Mr. Shipley also performs post intrusion analysis as well as expert witness testimony. Mr. Shipley is currently concentrating his efforts on completing several research projects.

Lorenzo Valeri - *Why are we talking about Information Warfare?* Lorenzo will try to assess the reasons of the growing fame of information warfare subject. The world is changing but not that much. He will speak at continuity and changes in information warfare in relation to military and strategic thinking. Most of the ideas developed in relation to information warfare have been thought at the beginning of this century. Moreover, there is the problem of intelligence requirements for performing information warfare. The main argument of his speech can be that what has changed is the TIME and SPEED factors but not the strategic and military thinking behind.

Mr. Valeri is a researcher in the information warfare programme of the International Centre for Security Analysis, which is part of the Department of War Studies, King's College London. He is also a Ph.D. candidate at the Department of War Studies at King's College. His research interests are information security policies, the impact of the Internet and other online services on military and strategic thinking and, in general, non-military threats to national and international security and stability.

Se7en - *Hacking the Travel Industry*. Learn the techniques of social engineering skills from one of the best in the profession. For example, learn how one could get permanently upgraded to First Class flying status, be upgraded to a luxury hotel suite, get admitted to airport V.I.P. lounges, get their luggage from baggage claim before anyone else does, be provided with limousines and bodyguards, and much, much more.

David Gessel (Super Dave, of the DoC) - *Copyright vs. Freedom of Speech*. As policy and the economics of a world-wide economy force us to attempt an information based economy, the manufactured concept of Intellectual Property becomes paramount. Our preeminent corporations have shifted from GM and Ford to Disney and Microsoft; our government struggles to develop and globally enforce laws to protect the profitability of IP. These laws are intrinsically at odds with the free and unfettered exchange of ideas which is central to the validity of democracy. But IP law is built on a weak legal and moral foundation, and it is far from clear that an IP based economy is viable.

David Gessel spent his childhood hammering steel in front of a coal-fired forge as a blacksmith's apprentice for seven years. He then went to MIT to get a degree in physics where he focused on robotics and precision engineering. Switching coasts, David joined Apple's Advanced Technology Group and worked on various things including pen-based computers, LCD technology, and digital cameras. After ATG, David worked at Interval Research Corp, researching rapid design/prototyping technologies for mechanical systems. David is now CTO of Spinner, Inc., a startup developing QTVR technology; VP of Engineering for Nebucon, Inc., a startup developing secure Internet services for small businesses; and contracts mechanical design services bicostally.

Professor Feedlebom and Technopagan – *Micropower Radio Stations*. If you have ever been slightly interested in operating your own micropower radio station, this is it. Why to, How to, and how to not get caught. Will also discuss the potential of legal micropower radio in the future.

Professor Feedlebom and Technopagan have operated The Voice of Mercury and the Desert Crossing Radio broadcasts for the last four years. They are also responsible for strange radio emissions that have been heard in the Los Angeles area on 104.7 MHz.

Ira Winkler, Author of Corporate Espionage - *Tasks that Require Real Skills and Abilities* - As I have often said, most hackers display skills that can be picked up by a monkey in a few hours. Hacking is mindless the way the clear majority of hackers seem to be practicing it. In this presentation, you will learn tasks that require real technical skills and abilities. Not only will this provide you with more of a challenge, it will provide you with real marketable skills. If one "really" wants to challenge one's abilities and stay out of jail, you won't want to miss this session. Otherwise go play with the other "Tools Kiddies".

Dr. Byte – *Security of Wireless Technology*. Dr. Byte will give a technical presentation on the security of wireless technology. Included in this talk include overviews of:

- wireless networks, protocols, systems, and access mediums such as AMPS, GSM, FDMA, TDMA, CDMA, CDPD, 802.11, Mobile-IP, and Ad-Hoc Networks
- current IP security technology (IPSEC) in IPv4 and IPv6
- areas of research and exploration of security in wireless technologies.

Dr. Byte is a Ph.D. candidate in Computer Engineering and an instructor of Computer Engineering at a major university. He received his B.S. and M.S. in Computer Engineering in 1994 and 1997 respectively. For his M.S., he worked with a real time bit error rate simulator, and developed a next generation real time hardware system for bit error rate simulations. He has developed a 16 bit RISC microprocessor in VHDL in a Field Programmable Gate Array (FPGA) able to run compiled 'C' code. His research interests include security over wireless networks, in particular ad-hoc networks using IPv6. He has co-authored 3 papers on IEEE 802.11 and IPv6.

Dan Veeneman, Writer & communications consultant. – *LEO Systems, Iridium, and a Satellite Hacking Update* - Several low earth orbiting satellite systems are already in orbit, and commercial service is just around the corner. Global wireless voice and data services will be available from handheld terminals. Dan Veeneman will bring us up to date on existing and future systems and answer questions from the audience.

Dan Veeneman has served in various management and technical positions in the computer industry since 1980. He has developed financial programs for the banking, investment and real estate industries, as well as software for a variety of companies including A.C. Nielsen, McDonalds, Reuters and Baxter-Travenol. Dan has installed and supported many local and wide area networks, including a nation-wide data delivery network. He also has experience supporting Internet connectivity, including Motorola's world-wide Network Information Center. Dan has provided data security and encryption services for a number of government and civilian clients, encompassing video and data delivered over telephone, satellite and the Internet. He also edits a quarterly newsletter concerning cryptography. Dan holds an engineering degree from Northwestern University. Dan also writes a monthly column for Monitoring Times magazine called PCS Front Line.

Trask - *Hacking the Big Iron - Security Issues in Large Unix Environments.* I will be using the Sun Ultra Enterprise 10000 and IBM SP/2 as examples of how some of the newer, bigger unix systems (which are increasingly being used for jobs previously performed by mainframes) present some interesting challenges in the area of system security. As you may know, the Ultra Enterprise 10000 is a SMP system that can be configured with up to 64 processors, which may then be partitioned into a maximum of 8 independent partitions. The SP/2, on the other hand, is an MPP architecture that can be configured with up to 64 8-way SMP nodes. These two architectures are different in almost every way, however both are extremely fast, and both have some security concerns not present in more traditional UNIX systems. What I have found is that the security problems are surprisingly similar between the two types of machines.

By failing to consider all aspects of security when implementing the system management tools provided with these computers, the vendors are selling million-dollar-plus products that are less secure than typical end-user workstations. I contend that as UNIX offerings start providing mainframe class computing power, they need to also look towards providing mainframe class security.

Trask dropped out of high school about a month prior to graduation. After working at Wendy's, Wal-Mart and Texaco for a few months each, he decided that he would rather be a Unix sysadmin. He lives in 602 with his beautiful fiancé (mgd) and is currently employed by American Express, where he gets to play with all sorts of expensive toys.

Panel Discussion - Securing Distributed Systems. *Members include Brian Martin, Gale Katz, Ira Winkler, Route, Ejovi Nuwere, Mudge, Alhambra, and Anthony Eufemio.*

Morgan Wright - *The best social engineers understand behavioral analysis, and how to use it.* The police have been using it for years to obtain confessions from homicides to simple misdemeanors. Have you ever wondered why someone would confess to homicide when they know they will go to prison for the rest of their life? Why is non-verbal behavior more accurate than verbal behavior? How do proxemics affect an interview? How do you obtain information from someone unwilling to give it to you? The art of interview and interrogation relies more on understanding human behavior than on cliché techniques from your favorite cop shows. A sole source study of the Reid Technique of Interview/Interrogation funded by the NSA revealed that a properly trained interviewer, analyzing both verbal and non-verbal behavior, and supplied with the case facts, can correctly assess truthful or deceptive behavior 96% of the time. Find out how these techniques are used to SE the opposition, regardless of which side of the fence you're on.

Morgan Wright is a former law enforcement officer with 15 years experience. He is court qualified as an expert in computer crime, and interview and interrogation. He is a regular instructor for the International Association of Computer Investigative Specialists (www.cops.org) in the areas of computer crime. He has also taught interview/interrogation techniques nationally for Reid and Associates (www.reid.com) to the FBI, Secret Service, NSA, and many state and local agencies. Part of his training has included extensive work in the area of criminal personality profiling and behavioral analysis interviews. He works in the private sector conducting internet investigations for software piracy, copyright and trademark infringement, economic and corporate espionage investigations, and with intellectual property law firms in the area of electronic discovery. In addition he has conducted over 200 undercover internet investigations, and has been asked to provide training to the FBI and RCMP on undercover internet investigative techniques.

Richard Thieme, Thiemeworks, Inc.

Richard Thieme is a business consultant, writer, and professional speaker focused on the human dimension of technology and the work place. His creative use of the Internet to reach global markets has earned accolades around the world. "Thieme knows whereof he speaks," wrote the Honolulu Advertiser. He is "a prominent American techno-philosopher" according to LAN Magazine (Australia), "a keen observer of hacker attitudes and behaviors" according to Le Monde (Paris), "one of the most creative minds of the digital generation" according to the editors of Digital Delirium, and "an online pundit of hacker culture" according to the L A Times.

Thieme's articles are published around the world and translated into German, Chinese, Japanese and Indonesian. His weekly column, "Islands in the Clickstream," is published by the Business Times of Singapore, Convergence (Toronto), and South Africa Computer Magazine as well as distributed to subscribers in 52 countries. Recent clients include: Arthur Andersen; Strong Capital Management; System Planning Corporation; UOP; Wisconsin Power and Light; Firstar Bank; Northwestern Mutual Life Insurance Co.; W. H. Brady Company; Allstate Insurance; Intelligent Marketing; and the FBI.

Gregory Gilliss (of the DoC) - TBA

Gregory survived growing up in New York City where he learned how to program computers using punch cards and paper tape. After graduating from Clemson University with a Computer Science degree, he developed an extensive consulting business. Greg currently is VP of Software Development at Energy Interactive of Berkeley.

Jeff Thompson, Product Area Manager for Argus Systems Group, Inc. - *Developing a 32 bit operating system.* Jeff Thompson is a Product Area Manager for Argus Systems Group, Inc. with extensive experience in low level operating systems development, trusted operating systems, network development, and security architecture design, development, and reviews.

Mr. Thompson will be presenting on the design and development of his personal operating system, which is being developed for the hacker community. The OS, while egotistically being called JeffOS, will be released under the name GuildOS in honor of its roots.

Marc Briceno, Director of the Smartcard Developer Association – *Smartcard Hacking for Beginners.* Smartcards are a marvelous tool for the security software developer. Their small form factor and tamper resistant, though not tamper proof, packaging allows for numerous applications, such as secure key storage and encryption. Unfortunately, many software developers still consider smartcards difficult to work with. No doubt largely due to the fact that vendors have so far failed to provide sufficient information and development tools.

We will introduce SCARD, a free, cross-platform smartcard development, analysis, and integration tool. No longer does the smartcard-curious individual have to learn obscure low level smartcard commands. If you know how to use UNIX shell or Windows NT, you can use smartcards. There will be a demonstration of several cryptographic, electronic cash, and GSM cards. The audience is encouraged to submit any smartcards in their possession for analysis.

Marc Briceno is the Director of the Smartcard Developer Association <http://www.scard.org>, the only vendor-independent smartcard industry association. The SDA's member base is comprised of smartcard and security experts in Europe, Asia, the Americas, and Australia. The SDA distributes universal smartcard analysis and integration tools to software developers worldwide.

Mr. Briceno coordinated the efforts leading to the discovery and break of COMP128 <http://www.scard.org/press/19980413-01/>, the GSM digital cellular telephony authentication cipher. Mr. Briceno is a senior advisor on digital telephony issues to an international development effort engaged in designing low cost phone encryption devices and a consultant to memory chip forensic data analysis teams at several major universities.

SCHEDULE OF EVENTS:

FRIDAY July 31st:

Network Setup, Sign in, and Informal PGP Keysigning at the "PGP table"

10:00 Doors open, sign in starts
16:00 Capture the Flag III starts
22:00 Hacker Jeopardy Starts.

SATURDAY August 1st:

Speeches, Capture the Flag, TCP/IP Security Panel Session, and other special events to be announced.

10:00 – 10:50 **Richard Theime** - *TBA*
11:00 – 11:50 **Bruce Schneier** – *Trade craft on Public Networks*
12:00 – 12:50 **Ian Goldberg** – *Cryptanalysis of the GSM Identification Algorithm*
13:00 – 13:50 **Jennifer Grannick** – *Review of Several Major Computer Crime Cases from the Past Year*
14:00 – 14:50 **Lorenzo Valeri** – *Why are we talking about Information Warfare?*
15:00 – 15:50 **Ira Winkler** – *Tasks that Require Real Skills and Talents*
16:00 – 16:50 **John Q. Neumann** – *TBA*
17:00 – 17:50 **Winn Schwartau** – *Introducing the Time Based Security Model and ApplyingMilitary Strategies to the Network and Infrastructural Securities (AKA Humbug)*
19:30 – 21:30 **Black and White Ball** *(Social Event)*
22:00 - 23:59 **Final rounds of Hacker Jeopardy**.

SUNDAY August 2nd:

Speeches, Wrapping up Capture the Flag and Award giveaways

Track A 10:00 - 10:50 **Dan Veeneman -** *LEO systems, Iridium, and a satellite hacking update.*
Track B 10:00 - 10:50 **Jeff Thompson -** *Developing a 32 bit operating system.*

Track A 11:00 - 11:50 **Dr. Byte -** *Technical presentation on The security of wireless technology.*
Track B 11:00 - 11:50 **Morgan Wright -** *The best social engineers understand behavioral analysis and how to use it.*

Track A 12:00 - 12:50 **Peter Shipley -** *An overview of a 2 year effort in massive multi-modem wardialing.*
Track B 12:00 - 12:50 **Prof. Feedlebom -** *Operating your own micro power radio station.*

Track A 13:00 - 13:50 **Se7en -** *Hacking the Travel Industry.*
Track B 13:00 - 13:50 **Trask -** *Hacking the Big Iron, Security Issues in Large UNIX Environments.*

Track A 14:00 - 14:50 **Panel Discussion - *Securing Distributed Systems.***
Track B 14:00 - 14:50 **Gregory Gilliss -** *TBA*

Track A 15:00 - 15:50 **Super Dave, of the DoC** - *Copyright vs. Freedom of Speech.*
Track B 15:00 - 15:50 **Marc Briceno –** *Smartcard Hacking for Beginners.*

16:00 Awards for Capture the Flag

TECHNICAL EVENTS AND DEMONSTRATIONS:

Capture the Flag (CTF) III:

Sure Carolyn Meinel stole the idea, but **Capture the Flag** started here. Going on the third year, the rules have changed once again to reflect the reality of letting everyone attack a network at once.

This year the capture the flag network is looking to borrow any working computers that are strange, historic, goofy looking or somehow deserve to be hacked. If you're willing to bring a machine to DEF CON, have it hacked, and either bring or give it away, mail ctf@defcon.org. All the donated machines will be put on an Ethernet network, which will have 3-5 gateway machines (in parallel) separating it from the hacking network. When the contest ends, the gateway machines will be unplugged. Whichever hacker or team has the most machines with their pgp public key in the machine's root directory wins. This year there will be a $2 dollar entrance fee, which will get you a copy of the small print rules and an IP address on the hacking network. There will be a $250 prize for the first machine hacked, and the team which hacks the most machines. Last year the winner won $500 for winning in both categories. A third category may be introduced.

The network connection and topology will have T-1 availability. Bring your own hubs, cables, etc. if you want to jump on it. The network will be switched into several segments. More information will be provided as it becomes available.

TCP/IP Security Panel Session:

A panel of security experts will host a question and answer session on security in the TCP/IP suite.

Social Engineering Demonstration:

Who Are You, Anyway? Administered by hacker Reverend Krusty.

SOCIAL EVENTS:

"Hacker" Jeopardy:

Friday and Saturday evening 22:00 to Midnight. Played like the real game, but with many more computer questions.

Black & White Ball

Saturday evening 19:30-20:00 in the speaking hall:

No one allowed into the Black & White hall with out dressing up one way or the other. Live DJ action, a cash bar and some cooling out to be had by all.

TRAVEL INFORMATION:

CONFERENCE HOTEL:

We have a block of rooms, but it is first come, first served. Rooms get released about one month before the convention. The room rates are quite good this year. When reserving a room, reference the "Network Security Solutions" conference.

Jackie Gaughan's Plaza Hotel
Number One Main Street in the Old Downtown Las Vegas Reservations
Phone Number: 1-800-634-6575

There are four room sizes available. Friday and Saturday night the rates are:

- $50.00 Single/double room
- $60.00 One room king-sized bed
- $100.00 - Suite with one bedroom: one king or two queen-sized beds (sleeps up to four)
- $150.00 - Suite with two bedrooms: one king, two queens, and a pullout sofa (sleeps up to eight)

OTHER ATTRACTIONS IN LAS VEGAS:

Listings of other hotels in Las Vegas

http://www.intermind.net/im/hotel.html
http://vegasdaily.com/HotelCasinos/HotelAndCasinos/CasinoList.html

Radio Scanner frequency list by Clay Irving for Nevada.

http://www.panix.com/userdirs/clay/scanning/frequencies/states/nv/

Las Vegas Night Life

http://www.best.com/~lvnv/lvnight.htm#Brewers

MISCELLANEOUS CONVENTION INFORMATION:

WWW Site: http://www.defcon.org/defcon-6-pre.html

Convention updates, hotel contact information, room rates, updated speaker lists, and archives from previous conventions are housed here. Past speakers, topics, and stuff for sale is featured. A growing section of links to other places of interest and current events also exists.

Mailing List

Send email to majordomo@merde.dis.org and in the body of the message include the following on a separate line.

subscribe dc-stuff

dc-stuff is related to general conversation, planning rides and rooms, etc. Be warned! When the convention time is near the list starts to generate quite a bit of traffic.

Vendors / Sponsors / Research:

- If you are interested in selling something (shirts, books, computers, etc.) and want to get a table contact **dtangent@defcon.org** for costs.
- If you have some pet research project and you want to have the participants fill out anonymous questioners please contact me for the best way to do this.
- If you want to sponsor any event or part of DEF CON VI in return for favorable mentions please contact me.
- This year Index Publishing Group, The London Pirate Radio show Interface, and Some Caffeinated Drink Company are currently sponsoring events and atmosphere.

Streaming Audio and Video:

There will be various audio and video streams generated this year. Check the homepage http://www.defcon.org/ during the convention to select streams. Radio servers will mirror the RealMedia streams

Interested in Speaking or Helping?

If you are interested in speaking or demonstrating something please contact me (dtangent@defcon.org).