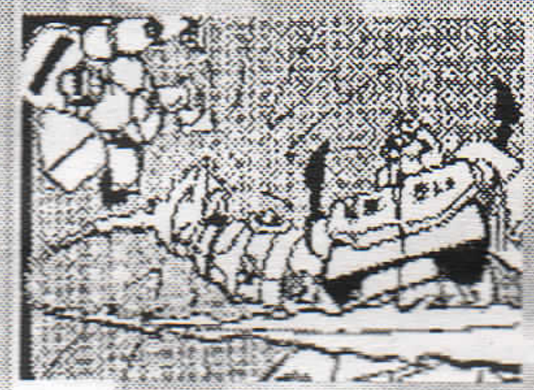
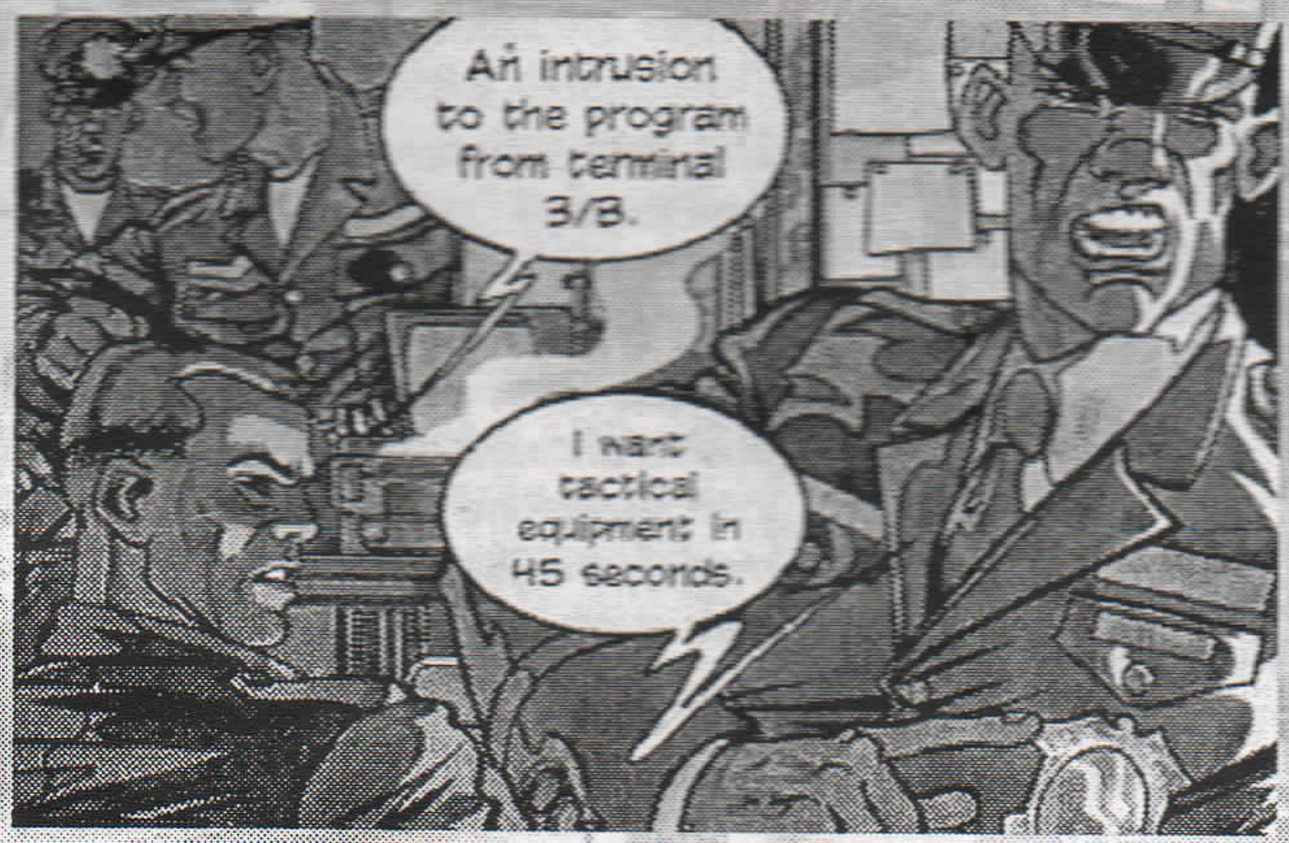
DEFCON 6.0



Welcome to DEF CON 6.0!

We have lasted 6 years! Un-believable. I never planned for DEF CON to last this long, but it just sort of happens. This year we have a few firsts. A working net connection or two (cross your fingers), two tracks of speaking on Sunday, more demonstrations, events and contests and hopefully the most people in attendance ever. I have worked hard, and so have others, to bring you this event. As usual the Staff Goons(tm) in red shirts are there to help you, or hurt you, depending on how you behave. Please take care of the hotel. They have been very very cool to us, so far the nicest hotel to work with to date. NOTE: There are many spontaneous events happening this year, I have tried to put as many as possible in the schedule section, but better stay on your toes to catch them all. With that said it's on to the fun and information! - dtangent@defcon.org

As you can see this is the shiortest program ever (Well, except maybe last year, because people seem to thro them away. So I am attempting to tell you the schedule and what events are happening. I'll let the rest be up to you. See you at the show!



Events & Contests

BLACK & WHITE BALL

Saturday evening 19:30-21:30 in the speaking hall:

New Rule: No one allowed into the Black & White hall with out sressing up one way or the other. You can always hang out in the main hall if you don't like it!

I have learned from last year, and have refined the Black & White ball for this year. For the last two years at DEF CON there has been a sort of unspoken Saturday night dress up event. People have worn everything from party dresses and Tuxedoes to AJ's ultra pimp Swank outfit with tiger print kilt. Wear your cool stuff Saturday night, be it gothic, PVC vinyl, or Yakuza looking black MIBs. No prizes, just your chance to be the uber-bustah pimp.

Live DJ action, a cash bar and some cooling out to be had by all.

THE L0PHT'S TCP/IP DRINKING GAME

If you don't know the rules, you'll figure 'em out.

CAPTURE THE FLAG (CTF) Part 3

Sure 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 defcon, 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.

NET CONNECTION AND TOPOLOGY
DSL, T-1, ISDN backup and dialup!#@

NetNevada is kind enough to help us out this year, spearheading the first xDSL connection in Nevada just for us. Planned speed is 768Kb syncronus. If everything suceeds we may have a second network connection. The network connection will require 10BaseT to get on, and the gateway and static IPs will be available at the NOC (In the front area near sign in) We plan on having Intrusion Detection Defeating talks and demonstration. The connection is up, we have a class 'c', and will be giving out address space on a first come, first served basis. there also should be aT-1 connection up by the time you read this. If those fail we have an ISDN as backup. For once, we're covered! check http://www.defcon.org for updates!

STREAMING AUDIO AND VIDEO

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

6th ANNUAL SPOT THE FED CONTEST

(These rules haven't changed in years, so if you know them by heart, just skip this section)

The ever popular paranoia builder. Who IS that person next to you?

"Like a paranoid version of pin the tail on the donkey, the favorite sport at this gathering of computer hackers and phone phreaks seems to be hunting down real and imagined telephone security and Federal and local law enforcement authorities who the attendees are certain are tracking their every move.. .. Of course, they may be right." - John Markhoff, NYT

Basically the contest goes like this: If you see some shady

ers & Speakers &

Jennifer Grannick - Attorney at Law - A review of several major computer crime cases from the past year or two. [At this point, I'm thinking 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 not to 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

Peter Shipley - An overview of a 2 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 2 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 a Senior Manager with KPMG in San Francisco with 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 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

Speakers &Speak

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 PhD 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.

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 QTVRtechnology; VP of Engineering for Nebucon, Inc., a startup developing secure Internet services for small businesses; and contracts mechanical design services bicostally.

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

Prof. Feedlebom - 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. Kind-of a how-to, kind-of a demo, kind-of a "let's make the FCC real nervous" kind a thing.

Prof. 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.

Dr. Byte - 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* overview of 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.

Ira Winkler, Author of Corporate Espionage - 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 you "really" want to challenge your abilities and stay out of jail, you won't want to miss this session. Otherwise go play with the other Tools Kiddies.

ers & Speakers &

Dan Veeneman, Writer & communications consultant. - 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 hand-held 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 worldwide 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.

Gregory Gilliss (of the DoC) - 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.

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.

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

Speakers & Speak

level smartcard commands. If you know how to use a 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.

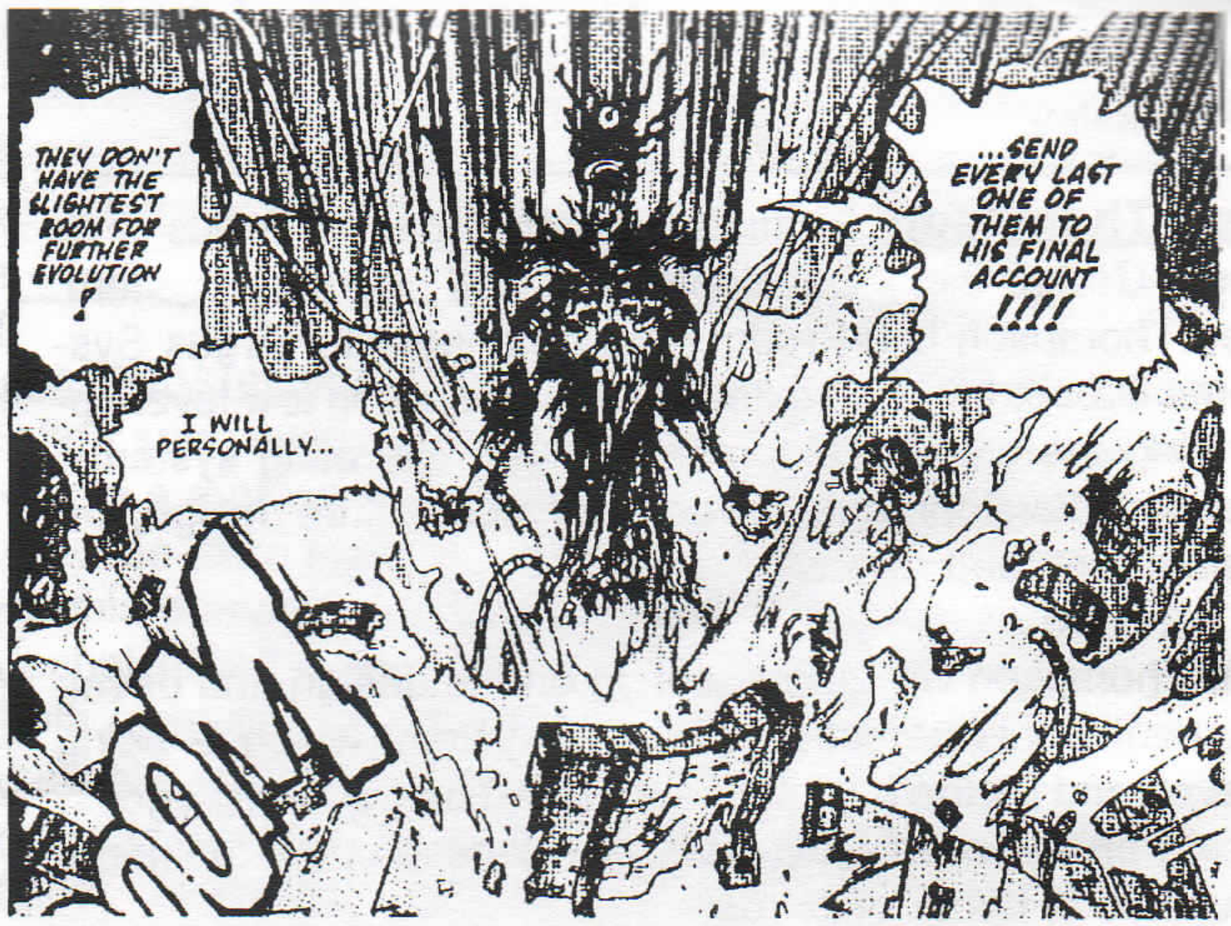
Marc Briceno is the Director of the Smartcard Developer Association <http://www.scard.org>, the only vendor-independent smartcard industry association. The SDA's member base is comprised of smartcard and security experts in Europe, Asia, the Americas, and Australia. The SDA distributes universal smartcard 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 at several major universities.

Richard Thieme, Thiemeworks, Inc. - The More Things Change The More They Don't: Soft Destruction and the Ancient Wisdom of Hacking. What works? What does it take to be an expert? To know how to see desirable goal states just before they become visible? Instead of hoping the doors you blow open have something inside besides a smiling Fed? DefCon has everything you need, right here right now, if you know how to use it. The ancient wisdom lives here but you have to know what it looks like. Hacking is the serious exploration of complex systems. It's not about using somebody else's tools or the latest equipment. Hacking is about knowing how to know how to hack. This talk gives you meta-rules, not rules. It's the truth about why the ancient wisdom of real hacking still applies.

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.



Thanks!

Thanks to:
NetNevada for helping out on the net connection, Noid for gooning, Lockheed for network, Evil Pete for hosting the dc-stuff mailing list and bringing some beer, Metalhead (The Original Goon[tm]) for Nambadges, Ninja Cut Master Ray-K for name badges, Cancer Omega for the "defcon 6.0" logo on the front of the program, and Joe630 for last minute emergency layout rescue!@#

All th people who put up ride sharing pages and created events for this years show: William Knows Spot the Screen writer contest, Rev. Krustys SE contest, Noid for organizing the DJs, Bing for the lights, Major Malfunction for the audio and video streaming, The People for the Capture the Flag contest. Zac for organiznig the reg crew including: Susan, DA, Megsusa, Ray K, Metal Head, Bing, Video Man, The Dark Knight, and as yet unknown people. I am sure I am forgetting people that deserve recognition, and I will put an updated list online after the convention. As you can see it is a group effort. The convention is what you make of it, and lots of people have worked hard, so make sure you enjoy it!

Emmanuel Goldstein is going to do a Kevin Mitnick update

Notes. I have nothing to put here right now.

Oh! The Holly Cow Brewery has decided to give us a special! Buy one one, get one free! So check out the Cow!

Lock picking demonstration

by Gurney Halleck and *Hobbit*

Bring your tools, and prepare to learn the basics of how locs work, and how to defeat them. Hobbit slaved over a grinder for days building a lock chopped in half to demonstrate pin tumblers, so it looks to be good.

The Events Schedule

FRIDAY July 31st:

10:00 - The conference doors open!
12:00 - DJs start to kick in with live music.
Game networks start getting set up.
14:00 - Capture the Flag network starts up. People will also be dropping IDS systems, firewalls, weird machines, etc. into this network to see what happens.

18:00 - 18:45 Lockpicking demonstration in the main speaking hall by Gurney Halleck.
18:55 - 19:55 Mystery speaker in the main speaking hall. Emmanuel goldstein will give us a Kevin Mitnick situation update.
20:00 - 21:30 The "Who are you anyway?" Social engineering contest. In the speaking hall.
22:00 - 23:59 First Round of Hacker Jeopardy in the main speaking hall.

SATURDAY August 1st:

Speeches, people selling stuff, Capture the Flag, The DEF CON shoot, other special events to be announced. There will be one track of speaking for the larger interest more general topics.

10:00 - 10:50 Richard Thieme - The More Things Change The More They Don't:Soft Destruction and the Ancient Wisdom of Hacking.
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 - A review of several major computer crime cases from the past year or two.
14:00 - 14:50 Lorenzo Valeri - Why are we talking about Information Warfare?
15:00 - 15:50 Ira Winkler, Tasks that require real technical skills and abilities.
16:00 - 16:50 The Cult of the Dead Cow - Introducing Back Orfice for NT.
16:00 - 16:50 John Q. Newman - The lastest in paper tripping, false identity, and how to REALLY not be found.
17:00 - 17:50 Winn Schwartau - Introducing the Time Based Security model and applying military strategies to network and infra structural securities. A/K/A Humbug.
18:00 - 18:30 Austin Hill and Ian Goldberg - Explaining the concepts behind ZKS's anonymous network cloud, Q&A session.
18:40 - 19:40 John Q. Newman - The lastest in paper tripping, false identity, and how to REALLY not be found.
19:30 - 21:00 The Black and White Ball in the speaking area with live DJ action.
21:00 - 21:30 The TCP/IP Drinking Game in the main speaking hall.
22:00 - 23:59 Final Rounds of Hacker Jeopardy in the main speaking hall.

SUNDAY August 2nd:

Wrapping up Capture the Flag, award giveaways, demonstrations to be announced There will be two tracks of speaking for more focused discussion of more technical topics.

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 Marc Briceno - Smartcard Hacking for Beginners.

Track A 15:00 - 15:50 Super Dave, of the DoC - Copyright vs. Freedom of Speech.
Track B 15:00 - 15:50 Gregory Gilliss -