The Fifth HOPE Speakers List

Speakers, Talks, and Panels

Draft as of June 24, 2004. Please get updated information at the conference.

AS/400: Lifting the Veil of Obscurity
StankDawg
The AS/400 system from IBM is a powerful system that is in widespread use. Despite that, it is difficult to find information on it or learn about it from any school. A general overview of its design and the architecture of the OS will be presented. This will then be tied into fundamental computing knowledge to show where "interesting" data can be found and where possible weaknesses are in the system.
Saturday 1700, Area "B"

Automotive Networks
Nothingface
This presentation provides an introduction to the electronic networks present on late model automobiles. These networks will be described loosely following the OSI model of networking. Common uses of these networks will be presented and the privacy implications of some uses will be questioned. The presentation will conclude with an introduction to OpenOtto, a free software and hardware project implementing the network protocols previously described.
Friday 2100, Area "B"

Bloggers at the DNC
Brad Johnson
The Democratic National Convention has become a sclerotic, television-driven celebrity parade. This year bloggers — aka hacker journalists — are being invited onto the floor to shake things up. Can the Internet bring democracy back to the mother of all Democratic Party shindigs? The panel will talk about what is planned — from WiFi to video blogging — and how you can get involved, in Boston or remotely.
Friday 1800, Area "B"

Building Hacker Spaces
Binary, Count Zero, Freqout, Gweeds, Javaman, Mangala, Shardy
This is a panel discussion on how to build and maintain a hacker space, hosted by representatives of the Philadelphia Walnut Factory, the Hasty Pastry (Cambridge), New Hack City (San Francisco), PUSCII (Utrecht), ASCII (Amsterdam), the L0pht (Boston), and the Hacker Halfway House (Brooklyn). Experiences and tales will be shared.
Friday 2200, Area "A"

Building the Anti-Big Brother
Peter Wayner
This will be a talk on how databases can do useful work and serve society without storing any personal information. For the past several years, Peter has been exploring how banks, stores, and businesses everywhere can offer their customers personalized service without keeping personal data about them where it can be abused by nefarious insiders or malicious outsiders. Building these systems requires more of a change in attitude than a change in technology because all of the solutions use standard encryption tools as a foundation. Topics will include how to build these systems and when they can help make the world a safer, saner place.
Saturday 1100, Area "B"

Bypassing Corporate Restrictions from the Inside
barbwire
Working for an organization can be annoyingly restrictive. As they feel they need to cater to the lowest common denominator, you are subjected to web content filters, outgoing port restrictions, and firewalls. This panel attempts to provide an understanding of how these restrictions are usually implemented and how techniques such as tunneling can be your saving grace. It will also address potential security implications and measures that should be considered whenever you compromise your own company's infrastructure.
Saturday 2000, Area "B"

Cheshire's Rant Session
When the Cheshire Catalyst spoke about problems at his Directory Assistance job at H2K2, corrections that nobody could get done in over three years were miraculously being made within two weeks after getting back to work following the convention. Could telephone company agents have infiltrated the convention and reported back? What other Large Corporate Problems aren't corporate executives listening to? Write out your rant and be sure you can deliver it in 45 seconds (isn't that what the stopwatch mode on your digital watch is for?). When it's all over, any hyperlinks mentioned by ranting attendees will be available on the web, allowing the Agents of Normality to not only find out what you're ranting about, but have your own references to work from when they report back to their executives.
Sunday 1000, Area "A"

The CryptoPhone
Rop Gonggrijp, Barry Wels
Trying to keep government out of *everyone's* phone calls is a lost battle. What little legislation we had to protect us will be removed in the next few years and ignored until then. Storing the content of all phone calls forever is now affordable, even for smaller countries. Strong end-to-end cryptography on a massive scale is the only answer. But where are the phones? CryptoPhone makes a phone based on a commercially available PDA/phone that features an open protocol and published source code. And there's a free Windows client if you don't want to buy the phone! The talk will outline precisely how it works, what's next, and how you can help.
Friday 1800, Area "A"

Cult of the Dead Cow Hactivism Panel
Eric Grimm, Sharon Hom, Dr. James Mulvenon, Oxblood Ruffin, Nart Villeneuve
Over 40 years ago Marshall McLuhan declared that the Third World War would be an information war in which civilians and the military wouldn't be particularly distinguished. That vision has become a reality. Governments from China to Zimbabwe have strangled access to information critical of their regimes, often with the aid of American companies. And as quickly, resistance has sprung up to challenge that repression. Areas of opportunity are beginning to emerge as hackers, human rights activists, and the academic community begin to join forces. This panel will explore the phenomenon of state-sponsored censorship and grassroots resistance from the political, legal, technological, and human rights perspectives.
Saturday 1800, Area "A"

Digital Rights Management
Michael Sims
Digital Rights Management is quickly becoming pervasive in electronic devices of all sorts. This minimally-technical overview of DRM systems in use now and planned for the future will show you how and why your ability to make use of electronics is being reduced by corporate desires to increase profits and exercise control over their products. The emphasis here will be on DRM systems that have gotten little publicity. The DVD CSS system will be touched upon but most of the time will be spent describing systems for controlling television broadcasts, DRM built into CPUs and BIOS's, and other areas that haven't gotten nearly as much attention as CSS.
Saturday 1900, Area "B"

Distributed Password Cracking API
David "Bernz" Bernick
The low-cost of the modern PC, the proliferation of the Internet, and the speed of its underlying networks make parallel task-based computing very possible. We've seen massive networks like SETI demonstrate this. SETI is programmed for a simple task: Get a piece of data, process it at leisure, spit out results if any, get a new piece of data. This has been used already to do some brute-forcing of security tasks with systems like distributed.net. But that system is sophisticated and large and you can't make it do tasks like cracking crypt() passwords or websites or any variety of brute-forcing tasks. This talk is about an extensible framework and API for creating distributed password crackers. The framework is easy to use, easy to distribute, and easy to add different kinds of cracking to. The software will be released open-source during the conference.
Sunday 0900, Area "B"

Encryption Key Signing
Seth Hardy
It's a surprising fact that a large number of attendees at this very conference, even those who call themselves hackers and/or security professionals, probably don't use any sort of encryption — or don't use it properly. One reason may be because people think nobody else uses it. So until it has a stronger presence, it won't be as widespread as it really should be. In order to help fight this, Seth will be hosting a key signing session. There will be a rundown of why people should be using strong crypto, how the web of trust works, and moderation to public verification of identity and key fingerprints. ***If you want in on this, send your public key to `shardy@aculei.net` so that he can prepare a keyring ahead of time to make things more convenient — or visit him in the NOC in area "4."***
Sunday 1700, Area "B"

Everything You Ever Wanted to Know About Spying, 9-11, and Why We Continue to Screw Up
Robert Steele
Two 30 minute PowerPoint slide shows will be presented, followed by as much discussion as desired. The first, "9-11, U.S. Intelligence, and the Real World," will discuss the specifics of how we failed and why we will continue to fail. The second, "The Failure of 20th Century Intelligence," will discuss the specifics of how American intelligence has blown it in collection, in processing, in analysis, in leadership, and in mindset. If desired, for those who last into the night, other briefs will be available, including "New Rules for the New Craft of Intelligence" and "The Literature of Intelligence: Why People Hate Us and Why We Don't Get It."
Saturday 2200, Area "A"

The Fifth HOPE Closing Ceremonies
Another one of our traditions is to gather everyone together in one room and bid farewell until next time while summarizing some of the highlights of the last three days. This is also where we give away various prizes to audience members. If you're one of those people who booked your return trip for Sunday afternoon, you'd best get on the phone and change those plans. The weekend ends Monday morning, after all!
Sunday 1900, Area "A"

Friday Keynote: Kevin Mitnick
Friday 1600, Area "A"

Frustrating OS Fingerprinting with Morph
Kathy Wang
Sun Tzu once stated "Know your enemy and know yourself, and in a hundred battles you will never be defeated." By denying outsiders information about our systems and software, we make it more difficult to mount successful attacks. There are a wealth of options for OS-fingerprinting today, evolving from basic TCP-flag mangling tools such as Queso, through the ICMP quirk-detection of the original Xprobe and the packet timing analysis of RING, to today's suite of multiple techniques employed by nmap. The ultimate advantage in the OS-detection game lies with the defender, however, as it is they who control what packets are sent in response. Morph is a BSD-licensed remote OS detection spoofing tool. It is portable and configurable, and will frustrate current state-of-the-art OS fingerprinting. This presentation will discuss the current techniques used for OS fingerprinting and how to frustrate them. There will be a live demo, and Morph v0.2 will be released with this talk.
Sunday 1600, Area "B"

Hack Nano
Jim "Cipz"
This is a continuation of Jim's presentation at H2K2 on hacking nanotechnology. This year there will be more on developing simulation software, thinking of new ideas, and investigating current discoveries. All of these are theory and thought driven. There will be a demonstration of some experiments and a discussion on the realities of nano hacking and why it's an important area of exploration.
Friday 2000, Area "B"

Hacker Radio
Sl1pm0de
Hacker radio is a growing phenomenon throughout the world. Hackers are discussing the current issues faced in today's technological world over the airwaves and through the net. There are all sorts of hacker issues being discussed via hacker radio including the DMCA or software patents in the European Union that seriously limit innovation and allow for others to have too much control over something you purchased in your home. By having this discussion in a radio format, those outside the hacker community have the opportunity to hear it and learn. The evolution of hacker radio from the early days of spreading information via bulletin board systems, websites, forums, and mailing lists to today's online audio streams will be explored. There will also be a discussion of hardware and open source software methods for setting up your own show and getting your own opinions and ideas out there for all to hear. Current examples of hacker radio will be featured.
Saturday 2100, Area "B"

Hackers and the Law
Dr. D. Kall Loper, Ph.D., Annalee Newitz, Policy Analyst, Electronic Frontier Foundation, Wendy Seltzer, Staff Attorney, Electronic Frontier Foundation
This panel will cover current legal crises around privacy, free speech, and intellectual property, with a special focus on the concerns of hackers. Presenters will discuss the laws which protect (or don't protect) your right to anonymous free speech online, your right to reverse-engineer, and your ability to make fair use of your digital media. They will also discuss the USA-PATRIOT Act and the ways this sweeping set of laws changed the nature of investigation and the rules governing wiretapping online.
Saturday 1700, Area "A"

Hackers in Modern Imperialist America vs. Barbarians in the Holy Roman Empire
Christopher Davis
In the time the Roman Empire controlled most of western civilization, the barbarians were known as enemies to society — savages that lived in the frontiers of the empire that resisted control by the Romans. Today, as the United States moves forward with an imperialist foreign policy, a new enemy has emerged that is resisting the system from the outskirts of the socially accepted: the hackers.
Saturday 1000, Area "B"

Hacking CDMA PRLs
The Prophet
CDMA is the dominant mobile phone technology in North America and is operated by Alltel, Sprint, US Cellular, Verizon, and many other carriers. On CDMA handsets, roaming is controlled via a configuration file called the PRL. In this talk, you will learn how to unload PRLs from CDMA handsets, how to disassemble them, and how they can be hacked. This talk isn't about making free phone calls or doing anything illegal, but you will learn how to determine what you're *really* buying when your carrier promises "nationwide service."
Sunday 1300, Area "B"

Hacking More of the Invisible World
Bernie S., Barry "The Key" Wels
An update on the H2K2 panel focusing on HF, VHF, UHF, and microwave signals. You will learn what's out there and how to intercept it. There will also be a discussion on TSCM (Technical Surveillance Counter Measures), the art of evading electronic surveillance, and a presentation of selected intercepts and equipment demonstrations.
Friday 1200, Area "B"

Hacking National Intelligence: Power to the People
Robert Steele
Do you want to live in a nation where decision makers lie, cheat, and steal? Where national intelligence is so secret that you are not allowed to know a) the truth, b) that national intelligence (spies) are ignorant about the real world, and c) that what policy makers tell the people (e.g. about reasons to go to war in Iraq) has nothing to do with reality? Imagine instead an America in which public intelligence supersedes secret intelligence and elitist corruption is displaced by an informed democracy in which consensus conferences at every level assure that "We the People" all serve the public interest. That is "The OSINT Story." Come hear the story and discuss how we are going to run the world as we achieve open spectrum, open source software, and open source intelligence.
Friday 1000, Area "A"

Hacking the Grid
Greg Newby, Porkchop
One of the biggest projects in computing for big science and enterprises these day is computational grids. Grid computing is at the heart of marketing plans from Oracle, IBM, Sun, and other big companies. For them, "grid" is mostly a buzzword that describes various ways of tying computers together. A more specific use of "grid" is found in big science, however. The national TeraGrid, based on the National Science Foundation's Middleware Initiative (NMI), uses the Globus toolkit and a variety of other packages to run some of the world's largest supercomputers. It's also used to tie many smaller computers and clusters together in the academic and business worlds. Can this "big iron" be hacked? This talk will examine real and potential weaknesses in Globus and other elements of NMI, as well as the promise and reality of end-to-end security for Grid-enabled computers.
Saturday 1500, Area "B"

Hardware Bus Security in Embedded Systems
Dan Matthews
Surprisingly, every individual comes into contact with over 100 embedded computer systems every day. A great many exist in our homes without our realizing it and many more operate the commonplace items in the world around us. An "embedded system" is a self contained miniaturized "computer system" (CPU, memory, I/O) that is dedicated to performing a single type of operation. They are now common in households through HVAC (Heat Ventilation and Air Conditioning), stoves, refrigerators, televisions, video players, set-top boxes, lawn sprinkler systems, and many other items. They are in the world around us controlling our street lighting, door openers, intruder alert systems, product theft security, speed cameras, and much more. The concept of security for these buses is traditionally very low because the designer has always been able to depend on physical security of an enclosed box. However, as more of the "boxes" are connected together more external buses and networks come into being and more opportunities for access and malfunction, whether through poor design, unforeseen circumstances, or foul play, become possible. This is a discussion of the progression of design from self-contained systems to more complex ones with internal buses and finally external standard buses. There will be an explanation of what an embedded system is and examples of complex embedded networks. Their security, and hence *your* security, is at risk in many cases, much of it due to "security through obscurity."
Saturday 1800, Area "B"

Homeland Security And You: Harry Potter Meets Reality
Marc Tobias
A study of how conference participants can use their expertise to assist private industry and government in assessing vulnerability. Marc will present his ideas for a National Security College to train young adults in many topics: crypto, lockpicking, encryption, etc. He will outline the technical subjects that would need to be taught so students could assist in protecting private sector and government from cyber and physical attack. Also, a look at some of the potential conflicts students might have in such an environment, including attitudes on intellectual property and its protection.
Saturday 2100, Area "A"

How the Great Firewall Works
Bill Xia
China currently puts in the most effort to censor information on the Internet. Bill was first involved in freenet-china and started DynaWeb in 2002. He has developed a thorough understanding of China's Internet censorship technology ranging from IP blocking to DNS hijacking etc. Various techniques have been implemented to get around them. There will be an explanation of a censorship algorithm never before publicly released as well as a live demo on how it works. Time permitting, an analysis of how the Chinese government uses information control on its people will also be presented.
Friday 1300, Area "B"

How The Net Worked
The Fifth HOPE network has been in the planning stages for many months. Did it hold together? How was it built? What worked and what didn't? An open discussion from members of the network crew on what it's like to do something on this scale, some of the hurdles that were faced, ways in which the technology has evolved, and how we can do things differently for future gatherings.
Sunday 1800, Area "A"

How To Break Anonymity Networks
Nick Mathewson
Today's anonymous communication software (such as Mixmaster, Mixminion, Nymservers, JAP, Tor, Anonymizer, etc.) allows people to communicate while concealing their identities from each other and from external attackers. But no deployed system is strong enough to protect every pattern of user behavior against a sufficiently resourceful adversary, and many of them fall to far simpler attacks. In this talk, Nick will discuss working attacks against today's anonymity networks, drawing from past technical and social attacks on deployed networks and from recent academic research in traffic analysis, stylometry, and mix-net design. He will present defenses to these attacks when such defenses are known to exist.
Saturday 2300, Area "B"

How To Send Encrypted Email
Joshua Teitelbaum
One day you wake up and you have the sinking feeling that someone may be reading your e-mail correspondence. Your only recourse is to encrypt or hide your sensitive communications. This is a look at one web-based solution — CryptoMail — and how it deals with the problem of simplifying encrypted e-mail while maintaining a high level of confidentiality. A detailed analysis of the CryptoMail session establishment, message encryption, and data store model will be presented. Furthermore, a demonstration of the working system will be given and attendees may create accounts, ask questions, or comment on the system.
Saturday 0900, Area "B"

How to Talk to the Press
Stephen Cass
Whether you're an activist planning a campaign, a hacker caught in a legal squabble, or just a bystander buttonholed on the street, dealing with journalists can be an essential part of ensuring that your views are heard. *IEEE Spectrum Magazine* associate editor Stephen Cass talks about how you can improve your chances of getting a fair hearing. Topics include understanding what journalists want, interviewee tips, and how to get the attention of news organizations.
Saturday 1600, Area "B"

Incentive Structures: Mechanisms of Control
Jason Kroll
Where do incentive structures come from? How do political elites use incentives to make us die for them? How do market elites use incentives to control politicians and co-opt the media? How can we stop them from doing the same to computing and communications technology? Why does mankind have to be led through the desert for 40 years every time technology advances? How are cultural and religious values like computer code and the institutions they create analogous to programs? How are markets like the AIs in *The Matrix?* When mechanisms of control get out of control, we have to ask who really coded Agent Smith and how can we retain control of technology before it comes to that?
Saturday 1400, Area "B"

An Introduction to Dissembler
Jon Erickson
A presentation of a tool called dissembler, which can be used to generate printable ASCII polymorphic bytecode from any existing piece of x86 bytecode. The technique used will be explained and the tool will be demonstrated to exploit various sample programs. Q&A session afterwards.
Saturday 1330, Area "B"

Indymedia 2004
How are hundreds of independent journalists from around the country going to work together to cover the Democratic and Republican National Conventions? From networks to working groups, from distributed communications such as text message networks and leaflets, and from ftp video transfers to people hawking newspapers on street corners, this session will examine all the tools of organization and distribution that will make these large scale collaborations possible. Find out how IMCs everywhere have challenged the monopolies of mass media and how this summer in particular will be one of the most active ever for independent media.
Sunday 1200, Area "B"

The Kismet Story
Dragorn
Hear the tale of how the widely acclaimed wireless network detector, sniffer, and intrusion detection system came to be from its creator. This talk will also focus on how Kismet's development has been shaped by other security tools and users, along with predictions on where it's likely to go in the future. Also included will be a look at the current state of open wireless drivers and the impact security tools are having on the use of wireless networks.
Saturday 1600, Area "A"

Lockpicking
Matt Blaze, Marc Tobias, Barry "The Key" Wels
Lockpicking is becoming popular as a sport/hobby among hackers throughout the world. In a special two-hour session the joy of lockpicking will be explained and demonstrated, from basic techniques to the state of the art. A whole range of new tools and tricks will be covered. Many stories will be told including that of Matt discovering a vulnerability in MasterKey systems as well as the members of Toool (The Open Organization of Lockpickers — `http://www.toool.nl`) discovering a severe vulnerability in a European lock. This forced a major European lock manufacturer to shut down the factory for a few days and collect a lot of locks from shops.
In addition to this panel, a lockpicking workshop will be ongoing throughout the conference. And at the end of it all, a lockpicking championship will take place.
Saturday 1100, Area "A"

Making Use of the Subliminal Channel in DSA
Seth Hardy
This talk will focus on one reason why it's extremely important to verify the trustworthiness of your encryption programs. A number of papers about a subliminal channel in the Digital Signature Algorithm (DSA) used by the United States Digital Signature Standard were published more than ten years ago. This channel allows for undetectable communication via digital signatures. The subliminal channel is generally viewed as a method of legitimate but hidden communication, but it can also be used for leaking secret information (such as keys) in an undetectable way to anyone who knows what to look for. This presentation will show how this subliminal channel works and demonstrate — using a patched version of the GNU Privacy Guard — how to use it for both benign and malicious reasons: legitimate communication using the subliminal channel, and leaking secret keys with each signature.
Saturday 2000, Area "A"

Media Intervention via Social and Technical Hacking
Nathan Martin, Tyler Nordgren
The Carbon Defense League (CDL) and Conglomco are two tactical media arts collectives engaged in both technical and social hacking processes. Their first collaboration with each other was a website that facilitated barcode relabeling for "user defined pricing." The site was live at re-code.com before it was shut down by pressure from Wal-Mart, Kellogg's, Price Chopper, and the FBI. CDL and Conglomco will present details of their past and present projects (including peoplesjeans.com) and discuss alternative tactics for media intervention.
Sunday 1700, Area "A"

Mischief and Mayhem at the RNC
ShapeShifter
Back in 2000 at H2K, Bernie S. and ShapeShifter led a discussion on secrets of the major political conventions in the United States. Not long afterwards, ShapeShifter was arrested on the streets of Philadelphia on suspicion of being a"ringleader" of dissent. In the end, he won his case against the city and all charges were dismissed. Like Bernie, his interests weren't squashed because of unjust prosecution. That's why this panel will focus on the 2004 Republican National Convention taking place across the street from the Hotel Pennsylvania in late August. The panel will detail how cops spy on people, their methods of surveillance, and how they often abuse authority. You will learn how to infiltrate organizations like the RNC, how to look for and find security holes, and how mischief and mayhem is achieved. There will also be details on a unique scavenger hunt. **Friday 1900, Area "B"**

Non-Lethal Technology
Gonzo
Technology is neutral. The patterns to which it is submitted are what determines if it can be used for betterment or detriment. This panel will go into that. As we all know, technology has greatly helped mankind. But what about technology that has been altered so that it can be used for non-lethal means? Imagine a bomb that can be dropped that won't kill anyone but will kill any technological related hardware. How about a blast from a sound wave, or a radio wave that can do physical damage to the body? These and other topics will be discussed, as will the technology behind it, and sinister applications.
Sunday 1500, Area "B"

"Off The Hook" Special Broadcast
As part of the *2600* 20th anniversary and the HOPE tenth anniversary, we're putting on a special two hour edition of our weekly WBAI radio show live from the conference. We did a show like this once before at Beyond HOPE in 1997 and it was great fun. We'll have all kinds of special guests who will visit the stage and we'll have plenty of audience participation. The show will be transmitted over WBAI 99.5 FM in New York City throughout the entire tri-state region as well as throughout the Internet.
Friday 2000, Area "A"

Packet Purgatory — Twist Your Packets Before You Set Them Free
Todd MacDermid
Ever wondered what it would be like to have your own custom IP stack readily programmable? Ever wanted to be able to use stock clients connecting to stock servers, but still be able to tweak the underlying connection? Have you ever wished you could poke at individual packet bits within a real connection without having to patch your kernel? Packet Purgatory is a library that allows userland programs to do all of the above portably. This talk will highlight the development of Packet Purgatory, how to use it, and ideas for future tools. Also included in the talk will be a discussion of two example tools that have been constructed on Packet Purgatory: Stegtunnel, a tool to hide covert channels in TCP/IP connections and LSRTunnel, which spoofs connections using loose source routing.
Sunday 1400, Area "B"

Phreaking In The Early Days
Captain Crunch and his friend The Cheshire Catalyst will tell some "war stories" from the early days of phone phreaking. They'll explain what the Blue Box did, how it was used, and some of their "adventures" in using them. And kids, don't try this at home!
Saturday 1000, Area "A"

Phone Losers of America
The PLA was created in 1994 as a general hacker/phreaker group. They eventually started *PLA Magazine* which in its lifetime released 46 issues (the most recent being a few months ago). The PLA has done many things over the years, including pulling pranks, operating numerous voice bridges, running their own forums (`http://cal.phonelosers.org`), etc. This panel will involve a discussion of the history of the PLA, what they are up to now, and the future. There will also be some videos and sound files presented along with a few "how-to" presentations.
Friday 2300, Area "B"

Pirate Radio: Running a Station and Staying on the Air
b9punk, Monk
A guide to the setup and operation of a pirate radio station and how to stay on the air when the federal government wants you off. Monk, founder of KBFR and ongoing benevolent dictator of the group (now over 40 DJs broadcasting 24/7), will moderate this panel on how to beat the authorities at their own game. Discussion will include types of technologies used to stay a step ahead of the FCC (and some that have failed) as well as more general information on how to set up and run a successful pirate radio operation.
Friday 2300, Area "A"

Preserving Digital History — A Quick and Dirty Guide
Jason Scott
Knowledge doesn't move forward without history and while there have been many steps to capture the stories, lore, and data of different aspects of computer cultures, a lot of the same mistakes are made over and over. In a fast-paced talk, Jason Scott of textfiles.com busts out some ideas, tools, and mindsets towards halting the loss, bringing the stories back, and making something to build upon instead of throw away. Along the way, expect a few bucketloads of trivia and memories to sauce up the proceedings.
Sunday 1100, Area "B"

Privacy — Not What It Used To Be
Steve Rambam
Steve has been at every one of our conferences and each time he's outdone himself with tales and demonstrations on how much data is stored on each and every last one of us. We all hear the news reports about how government and industry want to expand their databases and share all kinds of information. We hear how people try to protect their privacy and how various organizations attempt to quash the legislation that would broaden these databases. But what we don't hear is how much of our info is already out there and how much of it is being shared between law enforcement, private industry, and many more. Steve will share some of his vast knowledge on the subject and leave you feeling terrified and helpless. And as a special treat, a selected "victim" will learn firsthand just how much personal data can be uncovered on them.
Saturday 1500, Area "A"

Prometheus Radio Project
Dharma Dailey, Josh Marcus, Hannah Sassaman, Pete Tridish
The Prometheus Radio Project started with radio pirates fighting for local groups to be able to run community radio stations. But over the years, Prometheus has sued the FCC to stop media consolidation, built stations in places like Guatemala and Colombia, and experimented with using off the shelf wireless technologies to do for hundreds of dollars what commercial stations spend tens of thousands to do. This panel will help bring you up to date on the political debates in Washington about low power FM, reforming the spectrum for wireless broadband access, and the grassroots organizing that can be done to reshape the media. A picture show of community radio barn raisings and stations that Prometheus has worked on around the world will be included.
Friday 1500, Area "A"

Propaganda in Art and Media
b9punk, Mike Castleman, Frederic Guimont, Lazlow
We see propaganda around us every day, some of it a lot more obvious than others. This panel will show you how to find it and how to make some of your own. Whether it's something like Frederic's comic book adaptation of George Orwell's 1984 or Mike's "Students For an Orwellian Society" website, you too can have fun with manipulation of the masses. Lazlow will reveal from the inside how mainstream media strives for control of the masses while b9punk will explain how much of her propaganda art creations came to be displayed at this conference.
Saturday 1200, Area "B"

Retaliation With Honeypots
Laurent Oudot
Most of the time a honeypot is considered to be a security resource whose value lies in being probed, attacked, or compromised. The purpose of this talk is to explain how honeypots might be deployed not only to use passive defense technologies, but also active defense ones. As a specific example, think about what might happen the day honeypots are able to automatically strike back at an aggressor or a worm! Different technical possibilities offered to honeypots on the cyberwarfare field will be explored, such as playing with or even hacking back an usual aggressor (scanner, worm, exploit, client of a trojan, etc.), improving traceback capabilities to find the real source of an attack, etc. This will open up all kinds of legal implications which will also be discussed.
Sunday 1000, Area "B"

Retrocomputing
Richard Cheshire, Sam Nitzberg, Steve Wozniak
The focus of the Retrocomputing panel will be computing technologies from the 1980s and even earlier. Experiences involving the Altair 8800, the Apple II, and other great machines, their software, and operating systems will be discussed.
Sunday 1200, Area "A"

Saturday Keynote: Steve Wozniak
Saturday 1300, Area "A"

Secure Instant Messaging
Phar
A look at the evolution of secure instant messaging and how AOL tried to shake off open source and non-vanilla clients by altering the AIM (oscar) protocol. The open source community adapted and readapted until AOL finally gave up. Phar, who has written the first secure messaging clients for Unix and Windows (BLAIM and Impasse), will discuss other IM issues, such as the buyout of ICQ by AOL and the subsequent change (and deterioration) of its protocol.
Sunday 1800, Area "B"

Security, Liberties, and Trade-offs in the War on Terrorism
Bruce Schneier
Since 9/11, we have the Patriot Act, tighter screening at airports, a proposed national ID card system, a color-coded national alert system, irradiated mail, and a Department of Homeland Security. But do all of these things really make usany less vulnerable to another terrorist attack? Security expert Bruce Schneier evaluates the systems that we have in place post-9/11, revealing which of them actually work and which ones are simply "security theater." Learn why most security measures don't work and never will, why bad security is worse than noneat all, and why strong security means learning how to fail well. Most of all, learn how you can take charge of your own security - personal, family, corporate, and national.
Friday 1200, Area "A"

Security Through Automated Binary Analysis
Dildog, Weld Pond
Automated binary analysis techniques have become sufficiently advanced so that having the source to software is no longer a prerequisite for finding security flaws. The binary is equivalent to the source. And a patch is equivalent to a detailed description of a security flaw. This talk will cover the implications of the latest binary analysis technology and give an overview of some of the technology available.
Friday 1100, Area "A"

Security Through Diversity
Javaman
Establishing a diversity of operating systems and software on the Internet is now being viewed as essential to global information security. This talk will explore how individual systems and large networks can improve their tolerance to massive attack through this principle. Copies of obscure OS's will be handed out for good questions. Interpretive dance may or may not be involved.
Friday 1400, Area "B"

Slaying the Corporate Litigation Dragon: Emerging the Victor in an Intellectual Property Cybersuit
Atom Smasher
Have you ever wanted to tackle a corporate giant and live to tell about it? Meet web warrior Atom Smasher, whose lifelong fascination with law proved an invaluable commodity the day he found himself in the cross-hairs of some Fortune 500 big guns. In this lively discussion he'll recount his personal odyssey with the "men and women in black" whose federal lawsuit attempted to pull the plug on his whistle-blowing site. Learn how he responded to a cease and desist letter, what he did when served with a lawsuit, and how he triumphed in his legal battle.
Friday 1500, Area "B"

Social Engineering
Emmanuel Goldstein, Kevin Mitnick
This has always been one of the more popular panels since we started it at the first HOPE in 1994. And this year, for the very first time, Kevin will be at the conference to be part of the festivities. He authored a book on the science of social engineering entitled *The Art of Deception* which was an eye-opener to many in the corporate world. Emmanuel has been confusing people on the telephone for many years and derives great pleasure out of getting total strangers to give him information he has no right to possess. In addition to a discussion of methods and stories, be prepared for some live demonstrations over the phone. Suggestions for good targets are always welcome.
Sunday 1600, Area "A"

Sunday Keynote: Jello Biafra
Sunday 1400, Area "A"

Tactical Media and the New Paranoia
Mike Bananno, John Henry
The Institute for Applied Autonomy (IAA), The Yes Men, and the Critical Art Ensemble (CAE) are activist collectives that use unconventional means to deliver their message. The IAA is an anonymous collective of artists, hackers, and radical engineers who have produced projects such as high speed graffiti-writing robots and map-based websites that help people avoid surveillance cameras. The Yes Men have gained international notoriety for their use of extreme social engineering in order to impersonate World Trade Organization officials at conferences, on the web, and on television. A feature length film documenting their antics will be released by United Artists in August. The Critical Art Ensemble is a collective that explores the intersections between art, technology, radical politics and critical theory. Their books including *Electronic Civil Disobedience* and *The Molecular Invasion* have been translated into 18 languages and are used in universities the world over. Recently the FBI has accused the group of bio-terrorism. Due to the ongoing investigation, members of CAE are unable to speak publicly on these issues. However, members of IAA and The Yes Men will describe the events of the case and discuss it as it relates to investigations of hackers.
Sunday 1100, Area "A"

Technology in Romania
Catalin Acio
An overview of the ten year period in Romania from 1989 to 1999 and the challenges involving access to technology, the perception of IT in the formerly communist country, and issues of freedom of speech and information. Ninety percent of all access to the Internet is still done via timed dial-up connections which makes connectivity much harder for programmers, researchers, and the average citizen. Learn about the differences in technical cultures and what is being done to level the playing field.
Friday 1700, Area "B"

Ten Years of Practical Anonymity
Len Sassaman
Strong anonymity systems have been available for public access on the Internet for the last decade. During this time the Internet landscape has changed considerably, while the body of knowledge in the field of anonymity research has deepened greatly. This talk will review the history of anonymity systems, describe the methods by which modern anonymity systems protect their users, explore the classes of attacks which exist against anonymity systems, and give examples of practical anonymity systems which can be freely and easily used by the public at large. Emphasis will be placed on e-mail anonymity and the long-lived anonymous e-mail software Mixmaster and the associated remailer network, though other forms of Internet access anonymization will be included for discussion.
Saturday 2200, Area "B"

Terrorism and Hackers
Greg Newby
This presentation will put forth a full range of activities in which hackers can apply their skills to achieve goals related to "the systematic use of violence to create a general climate of fear in a population and thereby to bring about a particular political objective" (britannica.com). This range includes many specific ways for hackers to combat terrorism, methods to fight terrorist tendencies of your country, and how hackers might actually participate in terrorism. Despite being demonized by corporate media and the subject of many recent laws, most hackers, like most people of all types, are not terrorists. What can we do to protect against hackers being misperceived as threats and terrorists?
Friday 2200, Area "B"

Today's Modern Network Killing Robot
Viki Navratilova
This is an overview of the new generation of DDoS tools. Back in the day, a couple of large pings could take down lots of machines. When those techniques stopped being effective means of taking down networks, people started writing DDoS programs. These programs required a little bit of manual work to install, but were effective at taking down large networks for a while. This generation of DDoS tools was made famous in the media for victimizing famous websites for hours at a time. Soon people learned to control the damage done by these tools, and so a new generation of DDoS tools was born: Ones that could infect thousands of machines automatically to create large botnets and hide their communications in order to evade detection better than their predecessors. These botnets are now the most effective DDoS tools in popular use today. This talk will go over the more popular botnets, such as gtbot and sdbot, and talk about how they work and some ways to spot them on your network. There will be a demonstration of an irc botnet in action.
Friday 1000, Area "B"

Urban Exploring: Hacking the Physical World
John and Laura Leita
Urban exploring is the art of going places off limits to most and unseen by many. Explorers are brave souls who often dredge through great dangers for their art. Often they research and document historic abandoned places to accompany pictures and video taken on the locations of sites with enormous history. Otherwise they are simply in search of a beautiful view. John and Laura will talk about the different locations of interest to urban explorers, such as abandoned asylums, steam tunnels, rooftops, abandoned rail spurs, former used industrial sites, and deserted gold coast estates. From there they will go into how this art is best performed and various associated issues. Topics will include how to find urban exploration sites, how to go about exploring and documenting them, UE photography and video, computer assisted exploring, and research techniques to learn about a site. A Video CD presentation will be shown to illustrate urban exploring and show some cool places.
Sunday 1300, Area "A"

When Corporations Attack
Acidus, Virgil Griffith, Dan Morgan, Wendy Seltzer
We all know the wrath that major corporations are capable of unleashing when the actions of hackers and other individuals anger them. This panel will focus on two of these cases. Dan was the publisher of *Satellite Watch News,* a publication that focused on the technical workings of the satellite industry. DirecTV (owned by General Motors) managed to completely shut down the newsletter and take nearly all of his possessions. Acidus and Virgil did research into the Blackboard college ID card system (used at universities everywhere) and they uncovered all kinds of interesting facts. This was to be presented at the Interz0ne conference in Atlanta in 2003. Blackboard filed an injunction that not only kept that from happening but has prevented the two from discussing specifics about Blackboard to this day. In addition to these three panelists, a representative of the EFF will be on hand to talk about the legal aspects of these frightening cases.
Friday 1400, Area "A"

Where'd All That Spam Come From?
John Draper
A study of the mechanisms spammers use to flood your mailbox along with what some of the work and research of SpamCrunchers have uncovered. Topics of this talk will include spam bots, spam trojans, some of the sneaky methods spammers use, how they get around filters, why none of this stuff really works anyway, and what *you* can do to significantly cut down on spam.
Friday 1100, Area "B"

Wireless and WiFi: The Good, the Bad, and the Ugly
Dragorn, IrishMASMS, Mike Lynn, Porkchop
A panel to discuss wireless networking: the basics of 802.11 and current products, along with stories of wardriving and a look at network security. Find out why you should care about your network's security even if you don't think anyone else would take an interest in your traffic. Questions and comments from the audience will be solicited.
Friday 1300, Area "A"

The Fifth HOPE Speakers List

Speaker Biographies

Acidus has lectured for the past two years at the PhreakNic and Interz0ne conferences in the Southeast, and has been published numerous times in *2600*. Topics have ranged from circumventing lockdown software, building a magstripe authenticating Coke machine, hacking the PC heart of ATMs, XM Radio infrastructure concerns, and various hardware projects. He is currently doing grant research on embedded systems at a well known engineering university.

Catalin Acio was raised in Galati, Romania, the fifth biggest city of the country (population 400,000). In 1995 he graduated magna cum laude from CFR High School with a major in computer programming. He attended Dunarea de Jos University, one of Romania's top educational institutions, and studied electromechanical and computer science until he left the country in 1999. He has worked as a database programmer and network admin for two small Romanian software development companies.

Atom Smasher is a self-taught hacker with over 20 years of experience. He is the author of several open source applications, and regularly writes and teaches classes about computer security for activists. Atom earns an honest living designing custom solutions for web-based applications. His unique approach enables him to accomplish tasks often deemed "impossible" by others.

b9punk is a designer and pretentious artist at large (`http://www.jennifergergen.com`) who managed to get mixed up in a few *bad* crowds, including pirate radio, the coordination of the Hacker Halfway House, and "fascism for the fashion." She is a veteran of KBFR pirate radio. During her tenure, in addition to hosting a show, she was instrumental in growing the stations' participants and music archive. Most notably, she survived a visit from the FCC. She loves the FCC. She is also largely responsible for the "propaganda" look and theme of this grand event. She's not sorry, and she'll do it again.

Mike Bananno is a member of The Yes Men (`http://www.theyesmen.org`), a group that has impersonated World Trade Organization officials at international trade conferences the world over. At times they have given keynote addresses as the WTO to international trade attorneys, textile representatives, accountants, university students, and the entire audience of *CNBC Marketwrap* just to name a few.

barbwire has been working in the IT industry in Australia for the past ten years. With roles ranging from infrastructure design and support to application development, he has a broad scope of knowledge. He has been specializing in Internet technologies over the last five years with a strong focus in knowledge management and security.

David "bernz" Bernick has been active in Boston's *2600* scene for many years. Currently Bernz is the Senior Engineer at Legal Computer Solutions, a company that provides a secure document repository center for large (1,000,000 pieces of evidence) legal cases (criminal and civil). Part of the work also includes sometimes cracking documents, passwords, and zip files for which there are no keys or decrypted copies, hence the software you'll see presented at the conference. Long ago in his youth, bernz wrote an article for *2600 Magazine* on the topic of social engineering. Bernz grew up near the sea and currently lives beneath it.

Bernie S. has been hacking computers, phones, radios, and the authorities for over 25 years — sometimes pushing the envelope too far. In 1995 he was imprisoned for one and a half years by the Secret Service for possessing hardware and software they said had the potential for abuse. Later the U.S. government admitted "there were no victims in the offense" and

that they were more concerned about his exposing their covert activities. Bernie continues to investigate and report on communications technologies and government activities.

Jello Biafra has now been to three of the five HOPE conferences. He is the former lead singer for the Dead Kennedys, a spoken word activist who campaigns for free speech and against corporate dictatorships, and a media hacker who knows exactly how the industry works and how it can be manipulated Despite his admitted lack of technical prowess, Jello manages to see the big picture and how it relates to the hacker culture.

Big-E, a Miami native, has been in the scene since late 1998, having discovered the wide world of hacking and phreaking at age 11. Today he is still in the scene, frequenting the Phone Losers of America forums and reading all the others. His main interests include reclaiming the word "hacker" from mainstream media and social engineering. You can hear Big-E on *Hax0r Radio.*

Binary is a network engineer from Boston with over 12 years experience with data communication. He is currently dividing his time between laboring for a large telecommunications equipment manufacturer which develops circuit-to-packet convergence technologies and being a divergent trance DJ on weekends. He is a founding member of a Boston-based workspace of technophiles.

Matt Blaze has been involved in all sorts of stuff, from evaluating Carnivore and Key Escrow for the government to writing the crypto file system to writing dozens of papers on crypto. He was the codesigner of swIPe, a predecessor of the now standard IPSEC protocol for protecting Internet traffic. In 1994, he discovered a serious flaw in the U.S. government's "Clipper" encryption system, which had been proposed as a mechanism for the public to encrypt their data in a way that would still allow law enforcement to have access to it.

Stephen Cass was born and raised in Dublin, but now hails from Brooklyn. He cut his programming teeth on a TI 99-4/A and a totally pimped out BBC Model B+, but is currently smitten by his G4 PowerBook. He covers computers and space (among other things) for *IEEE Spectrum,* the flagship publication of the nice people who brought you 802.11, 1394, 1003, 754, and 802.3. (A very small prize will be awarded to the first HOPE attendee to correctly tell him what those standards actually refer to.)

Mike Castleman regularly appears on the *Off The Hook* radio show and participates in other *2600* related program activities. Beyond that, he is very secretive (despite not having any secrets worth keeping), and you'll have to ask him if you want to know more.

Richard Cheshire is known to the hacker and phone phreak community as "The Cheshire Catalyst." He was the last editor of the legendary *TAP Newsletter* which was published from 1971 to 1984. At that time he hacked his way into the world Telex network but had rested on his laurels since Telex was replaced by fax and e-mail. He came out of retirement, however, to get his own area code in 1998 (`http://CheshireCatalyst.Com/321/`).

Jim "Cipz" received an Associate's Degree in nanofabrication from PSU in 2000 (first graduating class in the United States for that degree). Since then he has earned various degrees and continued learning electronics, optoelectronics, computer networking, and computer security. He picked up skills in microradio, hacking, lockpicking, and other activities along the way.

Count Zero has been a member of the Cult of the Dead Cow since 1992. In 1993 he cofounded the innovative hacker group "The L0pht" in Boston, which has served as a model for successful hacker collaborative spaces. Today he is working to further develop collaborative real world hacker communities and has been working at "Hasty Pastry," a new hacker space in Cambridge.

In the mid 1990s, **Dharma Dailey** learned about an LPFM pirate radio station that broadcast out of a housing project in Illinois. As a teen mom who grew up in low income

housing projects, she immediately recognized the potential of LPFM and wondered why something that was so good for community building was illegal for those who could use it most. She's been researching LPFM ever since.

Christopher Davis graduated from Stony Brook University in 2000 with a degree in music performance. Davis is currently working in the field of computers. He has also written political and electronic music theory in his spare time. In 1999 he won an award for Outstanding Project in Music at the Celebration of Undergraduate Achievement at Stony Brook and now goes by the performance artist name of xpo8odx.

Serving as @stake's Lead Software Architect, **DilDog** came to @stake as a founder from L0pht Heavy Industries, a renowned security think-tank. While at @stake and L0pht, he developed the best selling Windows password auditing tool LC3, and the AntiSniff product. He is also responsible for numerous security advisories in many applications, operating systems, and environments. He is a recognized authority in the areas of Windows product vulnerability assessment, application optimization, and program analysis. His current responsibilities include design and development of the SmartRisk Analyzer (SRA).

An original member of the now famous Homebrew Computer Club where he designed his own computers and helped create the "blue box" tone generator, **John Draper** (aka Captain Crunch) has over 30 years of programming and security expertise. One of the first security pioneers, John developed his interest while learning how to penetrate phone networks. He became the 13th employee of Apple Computers, designing telephone interface boards and developing both hardware and software for the Apple II. A cofounder of ShopIP, John now performs security audits and is an architect of the CrunchBox firewall/IPS system. He also does database, Python, and secure GUI programming for SpamCruncher and CrunchBox.

Dragorn is the author of Kismet, a wireless sniffer and IDS tool. He's a fan of improving security in general, and wireless security particularly.

Jon Erickson has been involved in computer security for over a decade. He has spoken at computer security conferences around the world and is the author of the book *Hacking: The Art of Exploitation.* He has contributed to various magazines and currently works as a vulnerability researcher for an enterprise vulnerability management company in northern California.

Rob T. Firefly is an amateur hacker, prankster, and comedian from Long Island. Formerly known as Rufus T. Firefly, he has been active in the scene for over a decade. Rob went on to become a staff member and occasional editor of the PLA's spinoff zine, *United Phone Losers.* Rob's personal site can be found at `http://rtf.phonelosers.org`.

Before becoming a member of the Cult of the Dead Cow, **Freqout** was a founding member of "New Hack City." NHC had three incarnations, the first in Boston, and two in San Francisco. Freqout built his first hacker space just after going to the first HOPE conference and is now a member of the "Hasty Pastry."

Emmanuel Goldstein is the editor and cofounder of *2600,* as well as the chief organizer of the HOPE conferences. He also is a radio host for WBAI's *Off The Hook* and WUSB's *Off The Wall* and directed/produced the documentary on the Kevin Mitnick story entitled *Freedom Downtime.* Emmanuel to this day enjoys playing with phones, operators, and customer service representatives worldwide. His passions include urban exploration, mind exploration, and space exploration.

Rop Gonggrijp was editor and publisher of the Dutch hacker magazine *Hack-Tic* from 1989 to 1993. He also cofounded XS4ALL (one of the first European ISPs) and cofounded ITSX (a computer security consultancy). Along with partner Barry Wels, Rop initiated work on the CryptoPhone in 2001.

Gonzo is a veteran of the Underground and is the editor-in-chief of the e-zine *Reprimand.* It can be found at `http://reprimandmag.com`.

Virgil Griffith spends most of his time as a student in brain and computer sciences at the University of Alabama. He is an avid fan of AI and biologically inspired techniques in computer security (Internet immune system withstanding). He was one of the plaintiffs in the Blackboard college ID card system lawsuit last year. After researching the system, Blackboard filed a restraining order preventing the details from being revealed at a conference in Atlanta.

Eric Grimm and his law firm CyberBrief, PLC, specialize in the resolution of technology related legal disputes. Back in 2001 he represented *2600* when Ford decided to sue for redirecting fuckgeneralmotors.com to their site. His victory in that case probably saved others from the horrors of a lawsuit, at least for now.

Born in Germany, **Frederic Guimont** moved to Canada at an early age where he developed an interest in comic books and computer programming. After having fully explored his parents' Commodore 64c, he focused on developing his drawing skills and went on to study art in college near Quebec City. He has worked on a comic book series entitled Candyappleblack and is currently adapting George Orwell's *1984* as an independent comic book project (`http://www.1984comic.com`).

Gweeds is a hacker activist and wants to be your friend. Contributor to the rise and fall of New Hack City 415, he currently spends his time cooking for poor people and writing software for anarchist foaf networks.

Seth Hardy is involved in both research and implementation in the field of cryptology, both as part of a university research group and independently. Although he enjoys programming, his primary interest is the mathematics side of cryptography. For this reason, he's been involved in a number of projects which involve translating mathematical concepts and algorithms into working implementations in code. Seth has presented his work at a number of conferences, usually with his good friend Jose.

John Henry is a founding member of the Institute for Applied Autonomy (`http://www.appliedautonomy.com`) and was a young lad at the first HOPE conference. The IAA was founded in 1998 as a technological research and development organization dedicated to individual and collective self determination. IAA projects to date have included robots that write graffiti in high profile locations, a cute robot that distributes subversive literature, a vehicle that prints six foot tall letters on the ground while driving, and a website which generates maps that avoid surveillance cameras in cities.

Sharon Hom is Executive Director of Human Rights In China and Professor of Law Emerita at the City University of New York School of Law. She has over 14 years of experience in USA-China legal exchanges and training programs. Sharon was a Fulbright Scholar in the People's Republic of China and a Scholar-in-Residence at the Rockefeller Foundation's Bellagio Center. She also participated as an independent expert in the WSIS International Symposium on the Information Society and Human Dignity. As a delegate of the International Federation of Human Rights Leagues, Sharon also presented at several parallel NGO events at the WSIS, and participated in the EU-China Human Rights Seminar in Venice, Italy. She served on the USA-China Committee on Legal Education Exchange with China, and sits on the boards of Human Rights Watch/Asia, and on the Committees on Asian Affairs and International Human Rights of the Bar Association of the City of New York.

IrishMASMS is an old school hardware and network guy. He has degrees in Management of Information Systems, computer programming, networking technology, microcomputer programming, and aviation/aerospace management. Certainly not a bit-head by any means, but he will write some code if forced. After exploring the wonders of the early years with TRS-80s, Mac Plus, and even some Unisys mainframes and a clustered DEC VAX, he is currently frustrated as a miracle worker for a government library with no IT budget, and looking for a better opportunity in the information/network security realm. During off time

and when not working any consultant jobs on the side, he helps with the local Linux Users' Group and other local IT organizations. He also enjoys a few LAN parties, his NES, and his cat. No one can confirm or deny that he is a founding member of the 241_Crew, a locally based group of misfits who explore technology and the local music and epicurean scene.

Judas Iscariot hails from Delaware and is a moderator on the Phone Losers of America forums as well as a prestigious Telecom-munist member. Judas started back in the BBS days reading up on text files and he still holds them close to his heart. After being persecuted as a teenager for being a "black-hat" hacker he decided to research and learn telephony. His first encounter with the PLA was back in the mid 1990s when he started red boxing after reading a PLA text file. His current interests are Voice over IP (VoIP) technology, the Electronic Frontier Foundation, and the Telecom-munists.

Javaman is a Philadelphian who attempts balance living in academia, the security community, and the real world. He can usually be found in his office trying to stay on top of current research, the local diner drinking too much coffee, or the Philadelphia Walnut Factory wasting time on IRC. He also likes long walks on the beach and engaging in romantic candlelight dinners with various monomaniacal despots extracted from the course of history, brought to life by neurotransmitter imbalances.

Brad Johnson is a science and technology writer as well as an activist. He coauthored, as Adam Brate, *Making the Cisco Connection,* a business history of the datacom giant, and *Technomanifestos,* a history of the information revolution from Alan Turing and J.C.R. Licklider to Abbie Hoffman and Richard Stallman. In recent months he has volunteered for the Howard Dean and John Kerry campaigns in addition to the Democratic National Convention.

Jason Kroll arrived at the present through a C64-Amiga-Mac-Linux trajectory. He even spent his dotcom year as the technical editor of *Linux Journal.* The crash sent him back to complete his B.A. in economics at the University of Washington and he is now finishing his M.S. in computer science at Tufts. His research interests are mostly machine learning and game theory, but he finds it hard to focus on research with the world in its current state.

Lazlow produces a daily radio program called *Technofile* which is heard every day on 80 radio stations nationwide as well as on XM Satellite Radio. This 60 second news feature frequently covers hacker issues and items overlooked by the mainstream press. Lazlow is a contributing writer to *Playboy* and has been published in several magazines. He is most famous for cowriting and producing audio for *Grand Theft Auto 3* and *Grand Theft Auto Vice City.* His production company and recording studios are in Long Beach, New York.

John Leita aka Archivist graduated with a bachelors in engineering from SUNY Stony Brook. He has done some work for Brookhaven National Labs as well as other engineering companies. He has been an avid urban explorer for many years and is currently editor and webmaster for *Long Island Oddities,* a magazine and website devoted to odd finds, urban exploring, and forgotten history. Much like many urban explorers, he also shares a strong love of computers and hacking.

Laura Cummings-Leita aka ShadowCat graduated with a bachelors in English from SUNY Stony Brook. Since then she has held various jobs from computer instructor for the blind to English teacher. She is now coeditor and webmaster of *Long Island Oddities,* a magazine and website dedicated to the strange and unusual on Long Island. She has been an avid urban explorer for many years.

Leo aka I-baLL originally hails from Moscow. He is a phreaker whose introduction to the scene occurred a decade ago when he began frequenting various bulletin boards in the New York City area. He is a jack-of-all-trades who knows something about everything but not enough to get a job. Currently Leo edits, writes, and updates (sporadically) the *Reprimand* e-zine (`http://www.reprimandmag.com`), hangs out at Cal's forums (`http://`

`cal.phonelosers.org`), and is generally seen hanging around the New York City *2600* meeting with his two liter bottle of soda.

Peter Leung joined CryptoMail.org in 2000 as the webmaster and the project manager. His main task in the organization is to direct, manage, and organize the software release process. Peter collaborates with other members to document the e-mail system and informs everyone about the organization's activities. Peter holds a BS in mechanical engineering, a BS in mathematics, and an MBA from SFSU.

D. Kall Loper is coauthor of *Digital Crime Digital Terrorism* and Professor of Criminal Justice at the University of North Texas. He has thought far too much about hacker culture and would be happy to hear your thoughts on it. Before turning a hacking hobby into a life's work, he worked for the Michigan Department of Corrections teaching inmates how to write lawsuits and administrating employment and life skills training for female prisoners. He currently teaches and trains in the areas of digital forensics and computer crime investigation because they are fun and easy.

Mike Lynn has been involved in wireless security research from the early days of 802.11. His accomplishments in the field include authoring the first publicly available 802.11 intrusion detection system, writing device drivers for almost all types of 802.11 cards, and developing the Airjack toolkit for 802.11 security research. Mike is the primary inventor for a variety of patents in the area of wireless security and cocreator of the first commercial 802.11 intrusion detection system. Mike is currently a member of Internet Security Systems' X-Force Security research and development team.

Todd MacDermid is a serial open source security software author and speaker, and a member of Syn Ack Labs (`http://www.synacklabs.net`). Current research areas include covert channels, interface design, and other privacy protecting topics. Past work includes kernel module rootkit detection and source routing.

Mangala is a native New Yorker who has been working with information technologies since 1984 and is presently working part time as a C++ software developer and a Unix system administrator. The other part of his time is spent as a geophysics student at a university in Germany. He is a member of the German Chaos Computer Club and also part of other hacker groups such as 't-Klaphek, based in Utrecht. In addition, he's helped to organize the Orange County (California) *2600* meetings.

Josh Marcus is a community activist and programmer living in Philadelphia. He has been a developer on the open source projects that underlie the Philadelphia Independent Media Center, including the Slashcode-based open publishing system and the studio-transmitter link software that powers WPEB 88.1 FM. He is also a contributor to various open source projects, and the Director of Technology of Datarealm Internet Services, a Philadelphia based webhosting company.

Nathan Martin is a new media artist, collective experimenter, technologist, designer, writer, and programmer currently living in Pittsburgh as a Research Fellow at Carnegie Mellon University's Studio for Creative Inquiry. Nathan is a founding member of the media arts collective Carbon Defense League (CDL) and the hactivist.com network. Nathan is currently working on the CDL project MapHub and is writing a book called *Parasites, Splinters, and Thieves.*

Dan Matthews has been in the semiconductor sales and manufacturing industry for over 20 years. He is an engineer and an engineering manager over field engineers for the past 14 years, having been a director of engineering for a major microcontroller (embedded CPU) manufacturer for the past eight years. He spent much of his time traveling the world training in seminars about embedded design using microcontrollers and has been exposed to thousands of embedded systems.

Nick Mathewson is one of the main designers of the Type III anonymous remailer protocol, the one that has been selected to replace the type II protocol currently used by the

Mixmaster software. He is the lead developer on the Mixminion remailer software and a core developer on the Tor anonymizing proxy.

During the first HOPE conference in 1994, **Kevin Mitnick** was a fugitive. In 1997 during Beyond HOPE, he was in prison. Although released in 2000, he was denied permission to come to H2K to see the prerelease of *Freedom Downtime*. And in 2002, Kevin missed H2K2 because he was still on supervised release, which tends to keep one away from hacker events. But now it's 2004 and there are no legal barriers to keep Kevin away from The Fifth HOPE, where he'll be delivering the Friday keynote address. Since his legal troubles ended (not exactly helped by the mass media's portrayal of him as the "world's most dangerous hacker"), Kevin has been extremely productive, working as a radio talk show host, testifying in front of Congress, working on two books, and doing security consulting. While he's in great demand as a speaker worldwide, this is the conference he's waited the longest for.

Monk is a corporate burnout. He started Boulder Free Radio in his basement in 2000 and has been on the air pretty much 24/7 (with occasional breaks due to FCC busts) since then. Monk has developed a group of 40 plus DJs rocking the Boulder Airwaves with great live music, local on-air band jams, and some of the best music west of the Mississippi. The group's tech team has developed an Internet studio transmitter link system that's successfully thwarted the FCC for over two years.

Dan Morgan published the leading satellite TV hacking newsletter, *Satellite Watch News.* He also produced the *DB1* radio show and a series of related videotapes. In 1997 DirecTV filed a cease and desist order to stop publication of the newsletter. When Dan refused on First Amendment grounds, DirecTV (owned by General Motors) sued him for a million dollars. Unable to afford effective counsel, Dan lost the case and nearly everything he owned. Dan Morgan now operates a small network consulting firm in Michigan.

James Mulvenon is a political scientist at the RAND Corporation in Washington, DC and Deputy Director of RAND's Center for Asia-Pacific Policy. A specialist on the Chinese military, his current research focuses on Chinese C4ISR, defense research/development/acquisition organizations and policy, strategic weapons doctrines (computer network attack and nuclear warfare), patriotic hackers, and the military and civilian implications of the information revolution in China. James' most recent book, entitled *Soldiers of Fortune,* examines the Chinese military's multi-billion dollar business empire. He received his Ph.D. in political science from the University of California, Los Angeles.

Murd0c is an Allentown, Pennsylvania based phone phreak with a real interest in Direct Access Test Units (DATUs), vintage telecom, and now VoIP protocol. His real love is that of comedy. Murd0c has been following and interacting with the Phone Losers of America since 1998. His prank calls and other shenanigans are often heard on the PLA's website.

Viki Navratilova has spent seven years in the security community and in the meantime has gotten a C.S. degree, lots of useless knowledge, and some free t-shirts. After working for a year or two at a Leading National University, she has learned the fine art of not caring about security. Oh, and she's published a bunch of stuff on Linux and security in book, magazine, newspaper, and online formats.

Dr. Greg Newby is an information scientist with an interest in hacker ethics and education for hackers. He has taught college courses ranging from Unix security to systems administration, and has also published papers and led workshops. He has helped organize the last few HOPE conferences and still believes in the promise of information technology for a free and empowered society.

Annalee Newitz is a policy analyst at the Electronic Frontier Foundation. She conducts research, talks to the media, propagandizes, and writes policy recommendations and white papers. Although she is a digital rights generalist, her special areas of interest are expanding the public domain, free speech, and network regulation. Previously, she was Culture Editor

at the *San Francisco Bay Guardian* and was the recipient of a Knight Science Journalism Fellowship in 2002. She writes a syndicated column called "Techsploitation" (`http://www.techsploitation.com`) and is published regularly in national magazines and newspapers. In her off hours, she edits an indie magazine called *Other.* She has a Ph.D. in English and American Studies from UC Berkeley.

Sam Nitzberg is a computer security analyst who has presented and published on subjects relating to information security, information warfare, and technology and society. His papers and presentations have been conducted in both national and international venues, and he has attended or participated in each of the HOPE conferences since their inception. His website is `http://www.iamsam.com`.

Tyler Nordgren is a media artist who uses the application of the malfunction (or glitch) in technology as a theatrical tool and performance tactic. His work forms a discourse that is constitutive of an obsession with the intersection of human and machine and an ironic, but critical, analysis of the mass media and corporate control. One of his projects, Re-Code.com gained the attention of the mainstream media in such places as *USA Today,* CNN, and BBC World.

Nothingface is formally educated in electrical and computer engineering and informally (i.e., not) educated in automotive maintenance and repair. He has been known to earn his keep doing software design, hardware design, and security consulting. Nothingface is currently employed designing hardware and software for two-way radio communication networks.

As a security engineer and researcher, **Laurent Oudot** has been a security expert for the past seven years, working for the French equivalent of the U.S. Department of Energy. He is also an instructor in French high schools on computer security. He cofounded the French Honeynet Project which is part of the Honeynet Alliance. He has also written many security articles in places like securityfocus.com. He has been a presenter at numerous international computer security and academic conferences as well. His research focuses on defensive technologies like honeypots, intrusion prevention, intrusion detection, firewalls, sandboxes, mandatory access control, etc. In his spare time, he is a member of a weird security team called Rstack (`http://www.rstack.org/oudot/`).

Phar has been working in the electronic security and telecom fields for most of his life. He is a resident of the Hacker Halfway House and enjoys long walks on the beach and pina coladas.

Weld Pond was one of the L0pht members who testified before the U.S. Senate under his pseudonym (and he wasn't even in the witness protection program). He was on the original L0phtCrack team and also wrote Netcat for Windows. Now he specializes in software security and automated vulnerability discovery tools.

Porkchop has been involved with *2600* since 1997 helping with the HOPE conferences, the *Off The Hook* radio show and the documentary *Freedom Downtime.* He earns his bread at a liberal arts college in New York toying with grid computing infrastructure and writing software for collaboration between research scientists in the field of bioinformatics.

Steven Rambam is a licensed private investigator and the owner and CEO of Pallorium, Inc., an investigative agency with offices and affiliates throughout the world. During the past 23 years, he has conducted and coordinated investigations in more than 50 countries and in nearly every U.S. state and Canadian province. For the past 13 years, he has also been the owner and director of PallTech, an online service which provides database and investigative support services to investigative agencies, special investigative units (SIUs), and law enforcement. PallTech offers interactive and non-interactive access to nearly 600 data sources, including five major proprietary databases such as Skiptrace America and BusinessFinder America. The Skiptrace America database, which currently contains more

than 5.3 billion unique records, is believed to be the largest individual reference database in the United States, excluding those databases maintained by the three U.S. credit bureaus. More than a decade ago Rambam forced the tightening of airport security in Texas airports by publicly exposing those airports' security flaws. In 1997 he exposed the presence in Canada of 162 Nazi war criminals and also conducted investigations which resulted in the prosecution and conviction of war criminals on murder charges. He is also the inspiration for "Rambam the detective" in Kinky Friedman's series of murder mysteries.

Rev. Sergey, having emigrated from Russia, is a member of the Barbelith Underground, founding member of the Weird Science Club, and is an ordained minister with the Universal Light Church.

Oxblood Ruffin is the Founder and Executive Director of Hacktivismo, an international coalition of hackers and human rights activists that develops circumvention technologies and consults with NGOs. He is also a member of the Cult of the Dead Cow t-file and security group. Oxblood is a coauthor of the Hacktivismo Enhanced Source Software License Agreement (HESSLA). The license enables both Hacktivismo and its end users to go to court if a third party (read Government) attempts to use the software in a malicious manner or to introduce harmful changes into the software in such a way that it violates the licensee's human rights. Oxblood participated in the United Nations World Summit on the Information Society in Geneva and recently delivered a paper on hacktivism at the Yale Law School Conference on Cybercrime. He is based in Munich where he works as a strategist for a cryptography firm.

Hannah Sassaman is an organizer with the Prometheus Radio Project. She has spearheaded national campaigns against the Clear Channel coalition and partnered with local, national, and international individuals and organizations to bring people out in force to the FCC hearings on "localism and diversity" in Texas and South Dakota. She also develops a variety of web tools to bring people's voices to power structures in the U.S. government.

Len Sassaman is a communication security consultant specializing in Internet privacy and anonymity technologies. Len has been a strong defender of personal rights through technology. As a volunteer, he has lent his expertise to human rights organizations, victim support groups, and civil liberties organizations. He is a frequent contributor to online discussions of electronic privacy issues and has contributed to the development of free software privacy utilities. Len is an anonymous remailer operator and is currently project manager for Mixmaster, the most advanced remailer software available. Previously, he was a software engineer for PGP Security, the provider of the world's best known personal cryptography software.

Bruce Schneier is both a founder and the chief technical officer of Counterpane Internet Security, Inc. which provides managed security monitoring services to organizations worldwide. Bruce is the author of six books, including *Secrets & Lies: Digital Security in a Networked World* and *Applied Cryptography*, now in its second edition and the seminal work in its field which has sold over 150,000 copies and been translated into five languages. He writes the free e-mail newsletter *Crypto-Gram*, which has over 70,000 readers. Bruce has presented papers at many international conferences and he is a frequent writer, contributing editor, and lecturer on the topics of cryptography, computer security, and privacy. He also designed the popular Blowfish encryption algorithm. His Twofish was a finalist for the new federal Advanced Encryption Standard (AES). Bruce served on the board of directors of the International Association for Cryptologic Research and is an Advisory Board member for the Electronic Privacy Information Center. He holds an MS degree in computer science from American University and a BS degree in physics from the University of Rochester.

Jason Scott is curator of textfiles.com, a website that collects files and other artifacts from the "BBS Era" of the late 1970s to mid 1990s. Over the last six years, his mission has expanded into many different historical projects, including a massive BBS documentary currently being edited for release later in 2004. He is, at this point, beyond saving.

Wendy Seltzer is a staff attorney with the Electronic Frontier Foundation, specializing in intellectual property and free speech issues. As a Fellow with Harvard's Berkman Center for Internet and Society, Wendy founded and leads the Chilling Effects Clearinghouse, helping Internet users to understand their rights in response to cease-and-desist threats. Prior to joining EFF, Wendy taught Internet Law as an adjunct professor at St. John's University School of Law and practiced intellectual property and technology litigation with Kramer, Levin, Naftalis, and Frankel in New York. Wendy speaks frequently on copyright, trademark, open source, and the public interest online. She has an A.B. from Harvard College and J.D. from Harvard Law School, and occasionally takes a break from legal code to program (Perl).

ShapeShifter is most well known as one of three alleged "ringleaders" of the 2000 RNC protests in Philadelphia, where he was charged with "Possession of an Instrument of Crime" (a cell phone) and held on half a million dollars bail. The charges against him were dismissed when prosecutors failed to prove that cell phones are dangerous and that he conspired to break the law. In addition to being a menace to society, ShapeShifter is currently studying electrical engineering and has recently spawned "the BUG," a.k.a. Zoe Olivia. ShapeShifter is also the layout artist for *2600.*

Michael Sims has been an editor at Slashdot.org since 1999 and is a student of technology, privacy, and free software. His interests include censorship issues, digital rights management, and electronic communications. He lives in New York City.

Sl1pm0de began his interest in technology with a pinball machine that his family had since his birth. The fascination of the lights, sounds, and the game gave him an understanding of some of the wonderful things technology could create. Like most typical old school geeks, sl1pm0de graduated to a Commodore 64 and later to an Apple IIE. Since then he has dabbled in many aspects of technology including electronics, ham radio, graphics, multimedia, systems administration, networking, and computer security. He has been involved in the *2600* meetings in Arizona since 1995 and has been an avid reader of the current state of technology and the politics surrounding the technical world. He has also done a hacker radio show called *In The Now* hosted at `http://slipnet.org` since 2001.

StankDawg is a senior programmer/analyst who has worked for Fortune 500 companies and large universities. He has been published in *2600 Magazine* on several occasions, as well as other hacking zines and numerous websites. He is founder of "The Digital DawgPound" (the DDP) which is a group of white-hat/gray-hat hackers who produce their own magazine, radio show, TV show, and other projects at `http://www.binrev.com/`.

Robert Steele is the author of *On Intelligence: Spies and Secrecy in an Open World* and *The New Craft of Intelligence: Personal, Public, & Political.* He is the founder and CEO of OSS.Net, a global intelligence partnership and network that excels at both teaching and performing legal ethical intelligence collection, processing, and analysis. In the course of a 25 year national security career, Robert has served as a Marine Corps infantry officer and service level plans officer; fulfilled clandestine, covert action, and technical collection duties; been responsible for programming funds for overhead reconnaissance capabilities; contributed to strategic signals intelligence operations; managed an offensive counterintelligence program; initiated an advanced information technology project; and been the senior civilian responsible for founding a new national intelligence production facility. He was one of the first clandestine officers assigned the terrorist target on a full time basis in the 1980s and the first person, also in the 1980s, to devise advanced information technology applications relevant to clandestine operations.

Joshua Teitelbaum developed the CryptoMail e-mail system and founded CryptoMail.org in 2000. He is the primary developer and technical lead of the e-mail system. Besides information security, Joshua holds an active interest in building scalable trading systems for broker/dealers and portfolio managers.

The Prophet aka TProphet has been a *2600* writer since the early 1990s, primarily on telecommunications and related subjects. When he is not traveling abroad, he lives in the beautiful Pacific Northwest.

Marc Tobias is an investigative attorney from Sioux Falls, South Dakota. He has a bachelor's degree with a major in law enforcement and a Juris Doctor from Creighton Law School in Omaha. He was admitted to the Nebraska and South Dakota bars as well as federal courts. He has specialized in technical fraud investigations for 30 years, is a polygraph examiner, has written five police textbooks (including the treatise on locks and safes entitled *Locks, Safes, and Security).* Marc has worked around the world in investigations involving security issues and the bypass of high security locks.

Pete Tridish is one of the founders of pirate station Radio Mutiny, 91.3 FM in Philadelphia, and its legal successor RadioVolta.org. He is also a founder of the Prometheus Radio Project, an organization that organizes for low power radio and provides free assistance to LPFM applicants. He actively participated in the FCC rulemaking and the grassroots organizing campaign that led up to the adoption of LPFM. He tours the country regularly to help start community radio stations and fight for democratization of media, speaking at colleges, coffee shops, living rooms, garages, and even the CATO Institute.

Nart Villeneuve is Director of Technical Research at the Citizen Lab, an interdisciplinary laboratory at the Munk Centre for International Studies at the University of Toronto. He is currently documenting Internet content filtering and surveillance practices worldwide with the OpenNet Initiative (ONI). Nart designed the software and methods used by the ONI to enumerate Internet filtering and is currently investigating Internet filtering in more than 15 countries worldwide. In addition, he has been documenting and evaluating existing circumvention technologies as well as developing them. His research interests include hacktivism, cyberterrorism, and Internet security. He is a graduate of the University of Toronto's Peace and Conflict Studies program.

Kathy Wang broke into programming with BASIC on the Apple IIgs. She has a bachelor's and master's degree in electrical engineering from the University of Michigan, where she specialized in VLSI chip design and semiconductor device physics and fabrication. She worked at Digital as part of the Next Generation Alpha Chip Design Team, and got to spend an entire wonderful summer blowing up Alpha chips. She has published a paper on some of the work she did there at an IEEE conference. Kathy has instructed courses ranging from "Semiconductor Device Physics" to "Vulnerability Assessment and Penetration Testing." Since Digital got broken up by Compaq and Intel, Kathy has focused on the software side of things. She has worked at Counterpane Internet Security and currently works as a Senior Infosec engineer at the MITRE Corporation. Kathy is also a founder of Syn Ack Labs, a computer security research group focused on cryptography, steganography, and low-level packet hijinks.

Peter Wayner is the author of 13 books including *Translucent Databases,* an exploration of how databases can do useful work while protecting privacy, and *Policing Online Games,* a book exploring how P2P networks can enforce rules and prevent cheating. He's also a frequent contributor to publications like *The New York Times, Wired,* and *BYTE.*

Barry "The Key" Wels has many passions. Lockpicking, safecracking, voice encryption, radio monitoring, and bug sweeping (TSCM) are a few of them. He spends most of his time on the Cryptophone project (`http://www.cryptophone.de/`) and on Toool, the Dutch lockpick sportgroup he is chairman of (`http://www.toool.nl/`).

Steve Wozniak has a long history in Silicon Valley and is respected worldwide as a visionary and philanthropist. He built the first Apple prototype himself and later started Apple Computers. He was also a major force behind the Electronic Frontier Foundation. Steve personifies what a true hacker is and his becoming incredibly successful has done nothing to

negate that. (And yes, he did build Blue Boxes and take a keen interest in phone phreaking back in the 1970s after reading that infamous article in *Esquire.)* Steve currently runs Wheels of Zeus (wOz) and is on the board of directors of Jacent and Danger, Inc.

Bill Xia is president of Dynamic Internet Technology Inc., which helps Chinese web users get around the firewalls the authorities have erected to control access to information on the web. Since he left China in the 1990s, he has devoted his time to researching Internet censorship in China and developing information technology that can penetrate such efforts in totalitarian regimes. Xia is also involved with `http://www.freenet-china.org` and is the founder of DynaWeb.