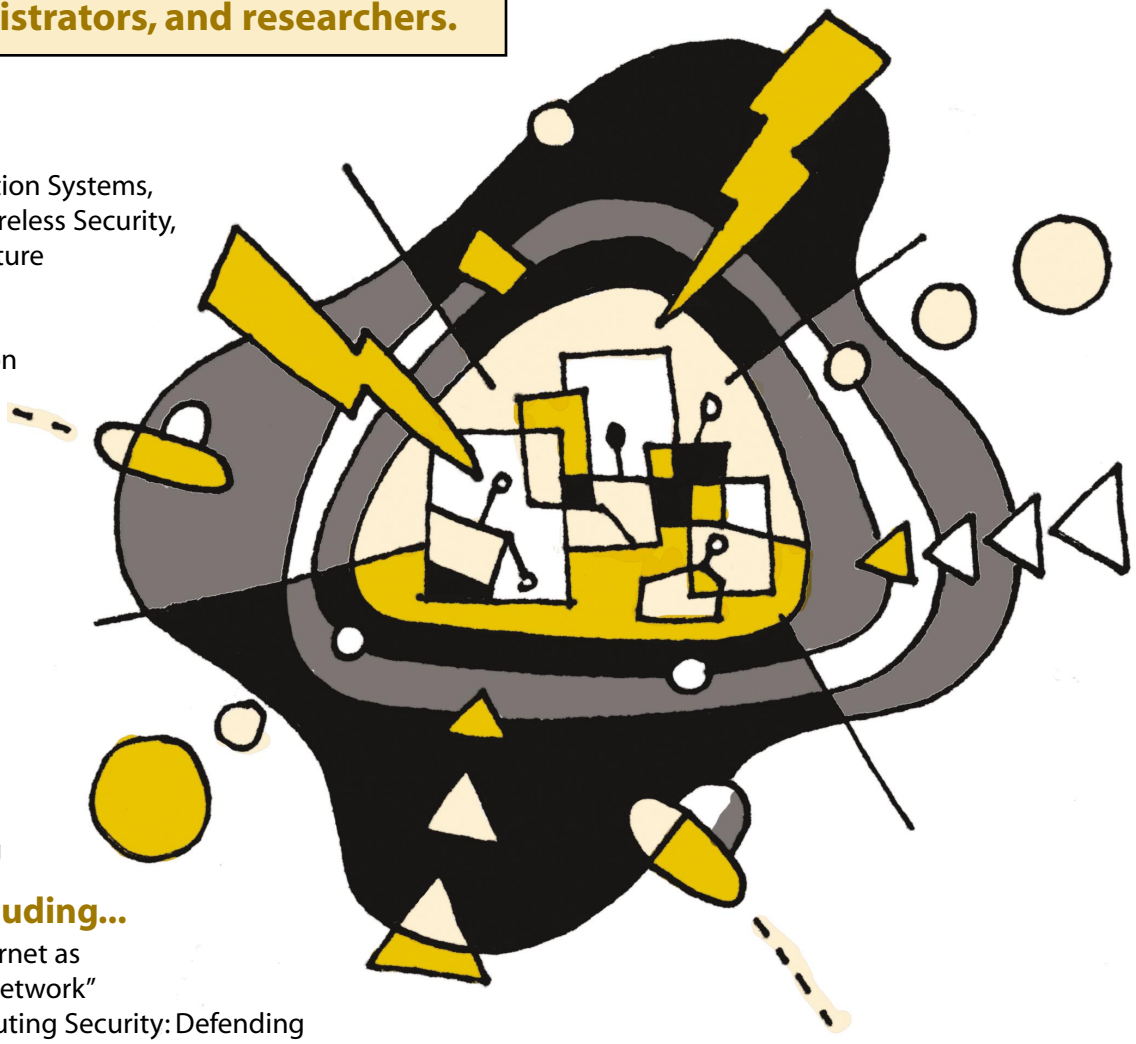
12th USENIX Security Symposium

August 4–8, 2003 • Washington, DC • USA

A five-day tutorial and refereed technical program for security professionals, system and network administrators, and researchers.



In-Depth Tutorials

Intrusion Detection & Prevention Systems, DDoS Attacks & Defenses, Wireless Security, Building a Logging Infrastructure

Keynote Speaker

Black Unicorn's "Reflections on a Decade of Pseudonymity"

Technical Program

21 refereed papers on the best new research, with sessions on Coping with the Real World, Hardening, Applied Crypto, and more …

Panels

Should the U.S. Elections Go Electronic?
and
Revisiting Trusted Computing

Plus Invited Talks, including...

- Richard M. Smith: "The Internet as the Ultimate Surveillance Network"
- Andy Ellis, Akamai: "Distributing Security: Defending Web Sites with 13,000 Servers"
- Mike Godwin, Public Knowledge: "When Policies Collide: Will the Copyright Wars Roll Back the Computer Revolution?"
- Mark Seiden, MSB Associates: "Physical Security: The Good, the Bad, and the Ugly"
- Eric Rescorla, RTFM, Inc.: "The Internet Is Too Secure Already"

Register Online by July 14 and SAVE Up to $425

USENIX Sponsored by USENIX, The Advanced Computing Systems Association

http://www.usenix.org/sec03

Security ’03 Invitation from the Program Chair

Security ’03 • August 4–8, 2003 • Marriott Wardman Park Hotel • Washington, DC • USA

Vern Paxson

Dear Colleague,

Computer security today evolves at a brisk pace, as both its operational relevance and the arms-race tension between attackers and defenders continue to grow. New services, new systems, and new networking architectures continuously add new dimensions to the field and subvert previously held assumptions. This symposium offers cutting-edge research on topics that range from making ordinary programs more robust through new classes of denial-of-service attacks.

Want to hear about new ideas for adding security hooks to software systems? Learn about sandboxing malicious applications? Understand new security issues with 802.11 and SSL? Curious about where Trusted Computing is going, or the realities of how responsive sites are when security patches are announced? Come to the 2003 USENIX Security Symposium and find out about these topics and many others.

Do you need to prevent and detect intrusions? Ensure WiFi security? Deal with DDoS attacks? Are you thinking about building honey pots, or would you like to understand the theory behind network security protocols? In our Security tutorials, experts such as Marcus Ranum, Radia Perlman, and Tina Bird will give you the information, techniques, tools, and strategies you need to practice effective security today—and tomorrow.

Keynote speaker “Black Unicorn” will talk about the central role played in security by notions of identity, reputation, and trust, drawing not only upon his cypherpunk background but also on his fascinating studies of the dynamics of money-laundering, black markets, and narcotics smuggling.

From the Invited Talks, discover the realities of physical security; how the rules change when your job is to defend, not a handful of servers, but 13,000; why the Internet is too secure already; whether the Internet is the ultimate surveillance network; and much more.

Join colleagues with similar interests for stimulating discussions at the evening Birds-of-a-Feather sessions. From the Work-in-Progress reports, get a preview of next year's news, or present fledgling work of your own and get feedback from the audience.

Whether you’re a researcher, a system administrator, or a policy wonk, come to the 12th USENIX Security Symposium to find out how computer security is going to affect you in the future.

We look forward to seeing you in Washington, D.C., August 4–8, 2003.

For the Security ’03 Program Committee,

Vern Paxson, *International Computer Science Institute*
Security ’03 Program Chair

Security ’03 Symposium Organizers

PROGRAM CHAIR

Vern Paxson, *International Computer Science Institute*

PROGRAM COMMITTEE

Steve Bellovin, *AT&T Labs—Research*
Dan Boneh, *Stanford University*
Crispin Cowan, *WireX Communications*
Drew Dean, *SRI International*
Kevin Fu, *MIT*
Peter Gutmann, *University of Auckland, New Zealand*
Richard Kemmerer, *University of California, Santa Barbara*
Patrick McDaniel, *AT&T Labs—Research*
John McHugh, *CERT® Coordination Center*
Radia Perlman, *Sun Microsystems*
Niels Provos, *University of Michigan*
Dawn Song, *Carnegie Mellon University*
David Wagner, *University of California, Berkeley*
Dan S. Wallach, *Rice University*
Elizabeth Zwicky, *Great Circle Associates*

INVITED TALKS COORDINATOR

Matt Blaze, *AT&T Labs—Research*

REGISTER EARLY AND SAVE

Early Registration Deadline:
July 14, 2003

Hotel Discount Deadline:
July 11, 2003

Security '03 Tutorials

For complete information and updates see
www.usenix.org/sec03

Monday, August 4 – Tuesday, August 5, 2003, 9:00 a.m.–5:00 p.m.

Monday, August 4, 2003

M1: INTRUSION DETECTION AND PREVENTION SYSTEMS **NEW!**

Marcus Ranum, *Consultant*

Who should attend: Network or security managers responsible for an IDS roll-out, security auditors interested in assessing IDS capabilities, security managers involved in IDS product selection.

Overview: Attendees will learn the advantages and disadvantages of popular approaches to Intrusion Detection Systems (IDSes), how to deal with false positives and noise, where to deploy IDSes, how to test them, how to build out-of-band IDS management networks, and how they interact with switches, routers, and firewalls.

Topics include technologies, deployment issues, and management issues.

Marcus J. Ranum (http://www.ranum.com) is the inventor of the proxy firewall and the implementer of the first commercial firewall product. He holds both the TISC "Clue" award and the ISSA Hall of Fame award.

M2: LOGGING & SECURITY: BUILDING AN ENTERPRISE LOGGING INFRASTRUCTURE

Tina Bird, *Stanford University*

Who should attend: System administrators and network managers responsible for monitoring and maintaining computers and network devices in an enterprise environment. Participants should be familiar with the UNIX and Windows operating systems and basic network security.

Overview: Every device on your network spits out millions of lines of audit information a day. Hidden within that data are the first clues that systems are breaking down, attackers are breaking in, and end users are breaking up. This class will teach you how to build a log management infrastructure and how to figure out what your log data means.

Topics include the extent of the audit problem, logfile generation, log management, and legal issues.

Tina Bird is a Computer Security Officer at Stanford University. She designs and implements security infrastructure for University systems; provides security alerts for machines on the 40,000-host network; and works on healthcare information security and the university's logging infrastructure.

M3: WIFI SECURITY: THE TRIALS AND TRIBULATIONS OF DESIGNING, DEPLOYING, AND USING WIFI NETWORKS SECURELY **NEW!**

William Arbaugh, *University of Maryland, College Park*

Who should attend: Anyone who needs to design, deploy, and/or operate a WiFi network. Previous experience with or knowledge of wireless networking is helpful but not required.

Overview: This tutorial presents security problems with WiFi equipment and explains standards changes designed to mitigate or eliminate those problems. Attendees will be shown how to design, deploy, and test wireless architectures using legacy, WPA, and RSN equipment and open source software.

Topics include known attacks and the tools that implement them, WiFi Protected Access and RSN, designing and deploying a secure WiFi network, and testing your network using open source tools.

William A. Arbaugh has spent over 15 years performing security research and engineering. He and his students were among the first to identify security flaws contained in the IEEE 802.11 standard, as well as proposed fixes to the standard.

M4: DDOS ATTACKS AND DEFENSES: OVERVIEW, TAXONOMY, AND FUTURE DIRECTIONS **NEW!**

Jelena Mirkovic and Peter Reiher, *UCLA*

Who should attend: Researchers intending to contribute to DDoS defense, and field and security officers who need to understand and deal with DDoS attacks.

Overview: Distributed denial of service (DDoS) attacks are a great threat to the Internet, because their diffuse nature makes it difficult to control or stop them. This tutorial will describe how DDoS attacks work, based on analysis of actual attacks and the tools used to perpetrate them.

Topics include the best uses of the tools available today; research that is likely to produce more powerful tools; probable future trends in DDoS attacks; and a taxonomy for classifying DDoS attack and defense mechanisms, which will aid in understanding the scope of the threat and the possible range of responses.

Jelena Mirkovic is completing her doctorate at UCLA. She has designed and implemented a source-end DDoS defense system that stops outgoing DDoS attacks while preserving legitimate traffic.

Peter Reiher is an adjunct associate professor at UCLA. His reseach focuses on distributed systems and security. Dr Reiher was a co-recipient of the Award for the Top 100 R&D Projects in the United States.

Tuesday, August 5, 2003

T1: BUILDING HONEY POTS FOR INTRUSION DETECTION

Marcus Ranum, *Consultant*

Who should attend: System and network managers with administrative skills and a security background. Attendees will benefit if they have at least basic UNIX system administration skills.

Overview: This class provides a technical introduction to the art of building honey pot systems for intrusion detection and burglar-alarming networks. Attendees will learn how to assemble their own honey pot, install it, maintain it, keep it secure, and analyze the data from it.

Topics include the fundamentals of IDSes, burglar alarms, honey pots, and log-data analysis; a detailed explanation of honey pot design, including tools and techniques, services, spoofing, honeyd, LaBrea tarpitting, logging architecture, and simple tricks for information visualization; how to get help in analyzing data; and legal issues of entrapment, privacy, and liability.

See **M1** for **Marcus Ranum**'s bio.

T2: HACKING AND SECURING WEB-BASED APPLICATIONS **NEW!**

David Rhoades, *Maven Security Consulting, Inc.*

Who should attend: People who are auditing Web application security or are developing or managing the development of a Web application.

Overview: Although numerous commercial and freeware tools assist in locating network-level security vulnerabilities, these tools are incapable of locating application-level issues. This course will demonstrate how to identify security weaknesses for Web-enabled services that could be exploited by remote users.

Topics include information-gathering attacks; user sign-off verification; OS and Web server weaknesses; finding the weakest link in encryption; session tracking; authentication; and transaction-level issues.

David Rhoades is a principal consultant with Maven Security Consulting, which provides information security assurance and training services. His work has taken him across the U.S. and to Europe and Asia, where he has lectured and consulted in various areas of information security.

Tuesday's Tutorials Continue →

Security '03 Tutorials

For complete information and updates see
www.usenix.org/sec03

Monday, August 4 – Tuesday, August 5, 2003, 9:00 a.m.–5:00 p.m.

Tuesday, August 5, 2003 (continued)

T3: NETWORK SECURITY PROTOCOLS: THEORY AND CURRENT STANDARDS

Radia Perlman, *Sun Microsystems*

Who should attend: Anyone who wants to understand the theory behind network security protocol design and get an overview of the alphabet soup of standards and cryptography. Although the tutorial is technically deep, no background other than intellectual curiosity and a good night's sleep is required.

Overview: This tutorial first convers the conceptual problems and solutions, and then specifics of the standards. It describes the pieces out of which all these protocols are built, discusses subtle design issues, and covers the kinds of mistakes people make when designing protocols.

Topics include cryptography, key distribution, handshake issues, PKI standards, real-time protocols, secure email, and Web security.

Radia Perlman is a Distinguished Engineer at Sun Microsystems. She is one of the 25 people whose work has most influenced the networking industry, according to *Data Communications Magazine,* and she holds about 50 issued patents.

T4: USING FREEBSD'S ADVANCED SECURITY FEATURES **NEW!**

Mike DeGraw-Bertsch, *Consultant*

Who should attend: System administrators and managers responsible for securing IT assets whose requirements have outgrown their existing infrastructure. Participants should be familiar with basic system security.

Overview: This tutorial addresses the risks companies face today, discusses how to evaluate and lessen those risks, and shows how to use FreeBSD to create cost-effective, secure computing environments.

Topics include assessing risks; TrustedBSD for security evaluation; using FreeBSD's ports system for patches; jails and virtual machines; firewalls; access controls; authentication via PAM or POPIE; and configuring secure firewalls, log hosts, servers, and clients.

Mike DeGraw-Bertsch is a security and networking consultant who has been working with FreeBSD for ten years and has been active in security for the past five years.

Security '03 Technical Sessions

WEDNESDAY, AUGUST 6 – FRIDAY, AUGUST 8

Wednesday, August 6, 2003

9:00 a.m. – 10:30 a.m.

OPENING REMARKS, AWARDS, AND KEYNOTE
Keynote Address: Reflections on a Decade of Pseudonymity
Black Unicorn (a.k.a. A.S.L. von Bernhardi)

What is identity? What is reputation? What is trust? Are these concepts as self-explanatory as they generally appear? This talk will examine the shortcomings of several identity and reputation systems and explore their importance from the perspective of the practitioner designing critical systems and security architectures. We will also direct an eye to evolving social, legal, and technical expectations and how they impact our perceptions of these concepts.

Black Unicorn has served as a "Big 5" consultant, an entrepreneur, an intelligence professional, a banker, a lobbyist, and a sometime cypherpunk. A survey of his recent work includes modeling narcotics smuggling and money laundering dynamics, a study of concepts of money throughout history, and research into the behavioral economics of black markets. He is currently at work developing political risk-hedging methodologies for foreign exchange markets. 2003 marks the 10-year anniversary of the pseudonym "Black Unicorn."

10:30 a.m. – 11:00 a.m. **Break**

Refereed Papers

Invited Talks

11:00 a.m. – 12:30 p.m.

ATTACKS
Session Chair: John McHugh, *CERT*

Remote Timing Attacks Are Practical
David Brumley and Dan Boneh, *Stanford University*

802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions
John Bellardo and Stefan Savage, *University of California, San Diego*

Denial of Service via Algorithmic Complexity Attacks
Scott Crosby and Dan Wallach, *Rice University*

DISTRIBUTING SECURITY: DEFENDING WEB SITES WITH 13,000 SERVERS
Speaker: Andy Ellis, *Akamai*

Early models of Web site defense focused on the challenges of appropriately hardening a small cluster of machines and a simple network infrastructure against attack. With 13,000 distributed servers, a different set of challenges need to be overcome, from robust system management and monitoring to providing protection to backend servers.

12:30 p.m. – 2:00 p.m. **Lunch (on your own)**

Wednesday, August 6, 2003 (continued)

Refereed Papers

2:00 p.m. – 3:30 p.m.

COPING WITH THE REAL WORLD
Session Chair: Crispin Cowan, *WireX Communications*

Plug-and-Play PKI: A PKI Your Mother Can Use
Peter Gutmann, *Auckland University*

Analyzing Integrity Protection in the SELinux Example Policy
Trent Jaeger, Reiner Sailer, and Xiaolan Zhang, *IBM Research*

Security Holes . . . Who Cares?
Eric Rescorla, *RTFM, Inc.*

Invited Talks

PROTECTING THE INTERNET INFRASTRUCTURE
Speaker: John Ioannidis, *AT&T Labs—Research*

All Internet services depend on two infrastructure components: the Domain Name System and the routing system. Neither has evolved with much security in mind. Both have depended instead on the friendly cooperation of the people who "run the network." These two essential components are increasingly the target of attacks. Even worse, they are frequently subject to misconfigurations (routing more so than DNS), and also heavily affected by distributed denial of service attacks. This talk gives an overview of the DNS and Internet routing, discusses their security vulnerabilities, and explores where we are and where we should be going to improve the situation.

3:30 p.m. – 4:00 p.m. **Break**

4:00 p.m. – 5:30 p.m.

PANEL: ELECTRONIC VOTING

Moderator: Dan Wallach, *Rice University*
Panelists: David Elliot, *Washington State, Office of the Secretary of State*; David Dill, *Stanford University*; Douglas Jones, *University of Iowa*; Sanford Morganstein, *Populex*; Jim Adler, *VoteHere*; Brian O'Connor, *Sequoia*

The U.S. national elections in 2000 demonstrated numerous problems with punch-card voting systems. Many states are replacing such systems with new, computerized ones. Most of these record and tally the votes completely in software, which raises concerns if the software is either simply buggy or has been subjected to malicious tampering. Hundreds of computer scientists signed a petition demanding that these machines have a "voter-verifiable audit trail." Academic experts, government election specialists, and voting system manufacturers will discuss security requirements and mechanisms for managing our elections.

AN OPTIMIST GROPES FOR HOPE
Speaker: Bill Cheswick, *Lumeta*

By all accounts the Internet has grown more dangerous since its inception. Most of the expected attacks have appeared and become commonplace. Increasingly sophisticated malware has learned to hide in the deep bushes of verdant, wild software. Users can't keep up with these dangers, and it is hard enough for the professionals. Yet there are indications that things can get better. Many important Web sites get security right enough to support large business models. Those who run our most secure networks report that they repeatedly pass the pop quizzes of the attack du jour. We can use crypto when we want to, and many do. We can do better, and many of us are starting to.

Thursday, August 7, 2003

9:00 a.m. – 10:30 a.m.

HARDENING I
Session Chair: David Wagner, *University of California, Berkeley*

PointGuard: Protecting Pointers from Buffer Overflow Vulnerabilities
Crispin Cowan, Steve Beattie, John Johansen, and Perry Wagle, *WireX Communications*

Address Obfuscation: An Approach to Combat Buffer Overflows, Format-String Attacks, and More
Sandeep Bhatkar, Daniel C. DuVarney, and R. Sekar, *Stony Brook University*

High Coverage Detection of Input-Related Security Faults
Eric Larson and Todd Austin, *University of Michigan*

WHEN POLICIES COLLIDE: WILL THE COPYRIGHT WARS ROLL BACK THE COMPUTER REVOLUTION?
Speaker: Mike Godwin, *Public Knowledge*

The last two years have seen an unprecedented effort by content companies—notably the movie studios—to press for legislative or regulatory requirements that could have closed down the open-platform, general-purpose computer as such. Where are these efforts going? What do they signify? What should we do about it?

10:30 a.m. – 11:00 a.m. **Break**

11:00 a.m. – 12:30 p.m.

DETECTION
Session Chair: Dawn Song, *Carnegie Mellon University*

Storage-based Intrusion Detection: Watching Storage Activity for Suspicious Behavior
Adam Pennington, John Strunk, John Griffin, Craig Soules, Garth Goodson, and Gregory Ganger, *Carnegie Mellon University*

Detecting Malicious Java Code Using Virtual Machine Auditing
Sunil Soman, Chandra Krintz, and Giovanni Vigna, *University of California, Santa Barbara*

Static Analysis of Executables to Detect Malicious Patterns
Mihai Christodorescu and Somesh Jha, *University of Wisconsin, Madison*

PHYSICAL SECURITY: THE GOOD, THE BAD, AND THE UGLY
Speaker: Mark Seiden, *MSB Associates*

Physical security is an oft-overlooked but critical prerequisite for good information security. A bad guy with a console root login can obviously adversely affect behavior in basic or profound ways, but you may not know how trust can be completely breached by brief and seemingly limited physical exposure using spiffy/inexpensive tools available on Ebay. Another dirty little secret: When critically examined, physical security policies/mechanisms perhaps have *always* oozed snake oil, including back doors relying on "security through obscurity" and ignoring environmental context—the need to function in a system. Outsourcing/colocation often presents only the perception (seldom the actuality) of security. A badging system implementation turns out to be >200K LOC, rather than simply "wave badge at the reader and maybe let 'em in," and is as buggy as any large program.

12:30 p.m. – 2:00 p.m. **Lunch (on your own)**

Thursday, August 7, 2003 (continued)

Refereed Papers

2:00 p.m. – 3:30 p.m.

APPLIED CRYPTO
Session Chair: Patrick McDaniel, *AT&T Labs—Research*

SSL Splitting: Securely Serving Data from Untrusted Caches
Chris Lesniewski-Laas and M. Frans Kaashoek, *MIT*

A New Two-Server Approach for Authentication with Short Secrets
John Brainard, Ari Juels, Burt Kaliski, and Michael Szydlo, *RSA Laboratories*

Domain-Based Administration of Identity-Based Cryptosystems for Secure Email and IPSEC
D. K. Smetters and Glenn Durfee, *PARC*

Invited Talks

THE INTERNET AS THE ULTIMATE SURVEILLANCE NETWORK
Speaker: Richard M. Smith

This session will look at the economic, technological, and political forces which are changing the Internet into a worldwide surveillance network. As more intelligent devices are connected to the Internet, the Internet will become less of an information publisher and more of an information collector. Technologies which are pushing along this transformation include ubiquitous wireless IP networking, RFID tags, low-cost digital sensors, and XML. This session will look at trends in technology to help understand how this surveillance network will be used, who will control it, how it will be secured, and its potential impact on personal privacy.

3:30 p.m. – 4:00 p.m. **Break**

4:00 p.m. – 6:00 p.m.

PANEL: REVISITING TRUSTED COMPUTING

Moderator: David Farber, *University of Pennsylvania*
Panelists: Lucky Green; Leendert van Doorn, *IBM*; Bill Arbaugh, *University of Maryland*; Peter Biddle, *Microsoft*

Suddenly, cybersecurity is on the lips of senior government officials, high-level corporate executives, and even casual computer users who hadn't a clue what it was six months ago. Secure systems proposals, most notably the Trusted Computer Platform Alliance (TCPA), can generate considerable controversy. The hazy debate forming about this area ends up sounding like a choice between no secure computer systems and potential damage to our established copyright mechanisms and freedom of speech. Professor Farber will moderate an examination of this complex set of issues and the question of how to find an acceptable path forward.

Friday, August 8, 2003

9:00 a.m. – 10:30 a.m.

HARDENING II
Session Chair: Steve Bellovin, *AT&T Labs—Research*

Preventing Privilege Escalation
Niels Provos, *University of Michigan;* Markus Friedl, *GeNUA mbH;* Peter Honeyman, *University of Michigan*

Dynamic Detection and Prevention of Race Conditions in File Accesses
Eugene Tsyrklevich, *Security Architects, Inc.;* Bennet Yee, *University of California, San Diego*

Improving Host Security with System Call Policies
Niels Provos, *University of Michigan*

THE INTERNET IS TOO SECURE ALREADY
Speaker: Eric Rescorla, *RTFM, Inc.*

The cryptographers and COMSEC engineers have given us an incredible number of fundamental security primitives. We now have good versions of essentially all the tools we know how to build at all. These tools are so good that attacks which are either impractical or entirely theoretical are nevertheless considered major successes. At the same time, the vast majority of traffic on the Internet is completely unprotected. These two phenomena are not unrelated. The flip side of the praise given for finding relatively small vulnerabilities is the massive amount of effort that developers feel they have to expend on fixing (and preventing) even quite small vulnerabilities. The inevitable result is that designers spend much more time enhancing security protocols than figuring out how to deploy them in real applications.

10:30 a.m. – 11:00 a.m. **Break**

11:00 a.m. – 12:30 p.m.

THE ROAD LESS TRAVELED
Session Chair: Dan Boneh, *Stanford University*

Scrash: A System for Generating Secure Crash Information
Pete Broadwell, Matt Harren, and Naveen Sastry, *University of California, Berkeley*

Implementing and Testing a Virus Throttle
Jamie Twycross and Matthew M. Willia, *HP Labs, Bristol*

Establishing the Genuinity of Remote Computer Systems
Rick Kennell and Leah Jamieson, *Purdue University*

THE CASE FOR ASSURANCE IN SECURITY PRODUCTS
Speaker: Brian Snow, *National Security Agency*

Security products need to work as intended, especially in the presence of malice. This requires considerable effort during all phases of the life cycle, from design, through evaluation and field use, to the eventual retirement of the product. The mechanisms that assure the customer of robust performance differ from one part of the life cycle to the next. They include technical enhancements, human processes, and legal constraints, among others. The talk offers views from three perspectives: research, security service and product provisioning, and education and training.

12:30 p.m. – 2:00 p.m. **Lunch (on your own)**

2:00 p.m. – 3:30 p.m.

WORK-IN-PROGRESS REPORTS
Chair: Kevin Fu, *MIT*

Short, pithy, and fun, Work-in-Progress Reports introduce interesting new or ongoing work, and the USENIX audience provides valuable discussion and feedback. If you have work you would like to share or a cool idea that's not quite ready for publication, send a one- or two-paragraph summary to sec03wips@usenix.org. We are particularly interested in presenting students' work. A schedule of presentations will be posted at the conference, and the speakers will be notified in advance. Work-in-Progress reports are five-minute presentations; the time limit will be strictly enforced.

Security '03

Registration Information / Student Discounts and Stipends / Hotel Information

REGISTRATION INFORMATION

Tutorial Fees (August 4–5)

Online Early Bird Rates with Multi-Day Discounts (members & nonmembers)

- One day: $575
- Two days: $1100
- CEU credit (optional): $15/day

After July 14, add $150 to the tutorial fee.

Standard Early Bird Rates with Multi-Day Discounts (members & nonmembers)

- One day: $625
- Two days: $1150
- CEU credit (optional): $15/day

After July 14, add $150 to the tutorial fee.

Student Tutorial Rates

- Students, with Tutorial Codes: $150/day
- CEU credit (optional): $15/day

Technical Sessions Fees (August 6–8)

Online Early Bird Registration Fees (before July 14)

- Member*: $695
- Nonmember**: $805
- Student member: $310
- Student nonmember: $350

After July 14, members and nonmembers (not students) add $150 to their technical sessions fee.

* For current members of USENIX, EurOpen.SE, and NUUG.

** The nonmember fee includes a one-year membership in the USENIX Association.

MULTIPLE EMPLOYEE DISCOUNT

We offer discounts for organizations sending 5 or more employees to Security '03. Please contact conference@usenix.org for more details.

GOVERNMENT EMPLOYEE DISCOUNT

USENIX is offering a $150 discount to federal government employees.

STUDENT DISCOUNTS AND STIPENDS

A limited number of tutorial seats are reserved for full-time students at the very special rate of $150 for a full-day tutorial. You must email the Conference Department, conference@usenix.org, to confirm availability.

The USENIX student stipend program covers travel, accommodations, and registration fees to enable full-time students to attend USENIX conferences. Application information will be available 6–8 weeks before the conference at **www.usenix.org/students/stipend.html.**

HOTEL INFORMATION

Hotel Reservation Discount Deadline: Friday, July 11, 2003

Marriott Wardman Park Hotel
2660 Woodley Road, NW, Washington, DC 20008
(202) 328-2000 / (800) 228-9290

Special Attendee Room Rate: $157 single/double

You must mention USENIX or Security '03 to get the special rate. See **www.usenix.org/sec03** for details. All requests for reservations received after the deadline of July 11 will be handled on a space-available basis.

DISCOUNT AIRFARES

Special discounted airfares have been negotiated with United Airlines:

* 5% off any published fare on United Airlines, United Express, or Shuttle by United.
* 10% off coach fares (BUA) when reservations are made in "M" class and utilize the MTGUA Unique Fare Basis Code.

Make reservations through your travel agent or directly with United Airlines at 1.800.521.4041. Refer to Meeting ID Number 510CH.

Security '03 Symposium at a Glance

SUNDAY, AUGUST 3

5:00 p.m.–8:00 p.m.	Registration
6:00 p.m.–8:00 p.m.	Welcome Meet & Greet

MONDAY, AUGUST 4

7:30 a.m.–5:00 p.m.	Registration
9:00 a.m.–5:00 p.m.	Tutorial Program
12:30 p.m.–1:30 p.m.	Tutorial Luncheon

TUESDAY, AUGUST 5

7:30 a.m.–5:00 p.m.	Registration
9:00 a.m.–5:00 p.m.	Tutorial Program
12:30 p.m.–1:30 p.m.	Tutorial Luncheon
6:00 p.m.–10:00 p.m.	Birds-of-a-Feather Sessions

WEDNESDAY, AUGUST 6

7:30 a.m.–5:00 p.m.	Registration
9:00 a.m.–10:30 a.m.	Opening Remarks, Awards, and Keynote

WEDNESDAY, AUGUST 6 (continued)

11:00 a.m.–5:30 p.m.	Technical Program
12:00 noon–4:00 p.m.	Vendor Exhibition
6:00 p.m.–7:00 p.m.	Casual Reception
7:00 p.m.–11:00 p.m.	Birds-of-a-Feather Sessions

THURSDAY, AUGUST 7

7:30 a.m.–5:00 p.m.	Registration
9:00 a.m.–6:00 p.m.	Technical Program
10:00 a.m.–4:00 p.m.	Vendor Exhibition
6:00 p.m.–7:00 p.m.	Casual Reception
7:00 p.m.–11:00 p.m.	Birds-of-a-Feather Sessions

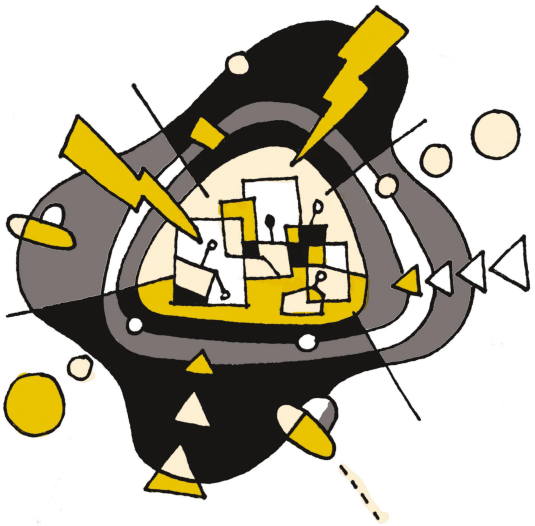
FRIDAY, AUGUST 8

9:00 a.m.–12:30 p.m.	Technical Program
2:00 p.m.–3:30 p.m.	Work-in-Progress Reports

12th USENIX Security Symposium

August 4–8, 2003 • Washington, DC • USA

Sponsored by USENIX, The Advanced Computing Systems Association



Join computer security's insiders (and outsiders), exchanging ideas and learning new, practical ways to improve the security of your systems and networks.

A high-level, five-day tutorial and refereed technical program for security professionals, system and network administrators, and researchers.

REGISTER ONLINE BY JULY 14, 2003, AND SAVE UP TO $400
http://www.usenix.org/sec03

Enter the priority code on the mailing label below and receive an immediate additional $25 discount!

USENIX ASSOCIATION
2560 Ninth Street, Suite 215
Berkeley, CA 94710
p 510.528.8649
f 510.548.5738
w www.usenix.org

NON–PROFIT ORGANIZATION
US POSTAGE
PAID
PERMIT #110
HOPKINS, MN

INTERESTED IN EXHIBITING? CONTACT EXHIBITS@USENIX.ORG