THE 8TH USENIX

Security Symposium

August 23-26, 1999 ▪ Washington D.C.

Securing The Future — Today

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

Keynote Address

The Next Generation of Security

Taher Elgamal, President, Information Security Group, Kroll-O'Gara

Technical Program

Over 20 refereed reports on the best new research in areas like:

Managing Access Control
Intrusion Detection
Creating Secure Environments for Software, and much more

Plus, invited talks by several of computer security's leading lights on topics including:

A Burglar Alarm Builder's Toolbox
A New Framework for Electronic Commerce
Public Key Infrastructure (PKI)
U.S. Crypto Policy

In-Depth Tutorials

Intrusion Detection and Network Forensics
Advanced Topics in Windows NT Security
An Introduction to Virtual Private Networks
How Attackers Break Programs, and How to Write Programs Securely
A Collection of Stuff Hackers Know About You
Cryptography — From the Basics Through PKI in 23,400 Seconds

Register Online

www.usenix.org/events/sec99

USENIX

THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

In Cooperation with the CERT Coordination Center

Sponsored by the USENIX Association in cooperation with the CERT Coordination Center

Important Dates to Remember

Pre-Registration Deadline: ***Friday, July 23, 1999***

Hotel Discount Deadline: ***Thursday, July 29, 1999***

Program at-a-Glance

8th USENIX Security Symposium

Sunday, August 22

6:00 pm – 9:00 pm ..... On-Site Registration
6:00 pm – 9:00 pm ..... Welcome Reception

Monday, August 23

7:30 am – 5:00 pm ..... On-Site Registration
9:00 am – 5:00 pm ..... Tutorial Program and Lunch

Tuesday, August 24

7:30 am – 5:00 pm ..... On-Site Registration
9:00 am – 5:00 pm ..... Tutorial Program and Lunch
6:00 pm – 10:00 pm ..... Birds-of-a-Feather Sessions

Wednesday, August 25

7:30 am – 5:00 pm ..... On-Site Registration
9:00 am – 10:30 am ..... Opening Remarks and Keynote
11:00 am – 5:30 pm..... USENIX Technical Sessions
12:00 pm – 7:00 pm ..... Security '99 Exhibition
7:00 pm – 9:00 pm ..... Symposium Reception
9:00 pm – 11:00 pm ..... Birds-of-a-Feather Sessions

Thursday, August 26

8:30 am – 5:00 pm ..... USENIX Technical Sessions
10:00 am – 2:00 pm ..... Security '99 Exhibition

Questions?

Email: conference@usenix.org
Phone: 1.949.588.8649
Fax: 1.949.588.9706
Web: http://www.usenix.org/events/sec99

Table of Contents

"...You'll come away with practical, immediate knowledge to improve the security of your systems and networks..."

Win Treese,
Program Chair

Program Committee

Program Chair
Win Treese, *Open Market, Inc.*

Committee Members
Fred Avolio, *Avolio Consulting*
Crispin Cowan, *Oregon Graduate Institute*
Jim Duncan, *Cisco Systems, Inc.*
Carl Ellison, *Intel Corporation*
Daniel Geer, *CertCo, Inc.*
Peter Gutmann, *University of Auckland*
Trent Jaeger, *IBM*
Wolfgang Ley, *DFN-CERT*
Alain Mayer, *Lucent Technologies, Bell Laboratories*
Christoph Schuba, *Sun Microsystems Laboratories*
Peter Trei, *Security Dynamics, Inc.*
Dan Wallach, *Rice University*

Invited Talks Coordinator
Aviel Rubin, *AT&T Labs — Research*

The 8th USENIX Security Symposium

Washington D.C. ▪ August 23-26, 1999

Dear Colleague:

Connecting to the Internet is no longer a luxury—it's a requirement. And security is the critical issue in using the Internet effectively.

With this in mind, we've designed the Security '99 tutorial and technical programs to help you learn about the latest research and contemporary solutions in security. Whether you're a computer security researcher, an application developer, or the system administrator everyone counts on to maintain a bulletproof network, you'll come away with practical, immediate knowledge to improve the security of your systems and networks. Plus you'll take home insight into the latest thinking in computer and network security.

The symposium begins with in-depth tutorials. Tutorial instructors are not only excellent teachers, they're experts in their fields: Matt Bishop, Brad Johnson, Aviel Rubin, Daniel Geer, Tina Bird, and Marcus Ranum, among others. The tutorials, which are intensely practical, cover such topics as intrusion detection, security for Windows NT, virtual private networks, public key infrastructure, developing secure software, and understanding what attackers are doing.

Keynote speaker Taher Elgamal, a leader in the field and former chief scientist of Netscape Communications, leads off the technical program. You'll gain valuable insights into some of the best research work in security today. You'll hear presentations of papers, selected for their quality from a large number of formal submissions, describing new results in using personal digital assistants (PDAs) to improve security, creating secure environments for software, certificates, public key infrastructure, managing access control, intrusion detection, and many other topics.

You'll also find an excellent selection of invited talks from some of computer security's leading lights — Edward Felten, Peter Neumann, Marcus Ranum, Susan Landau, Ross Anderson, and Paul Van Oorschot. Their talks are far-ranging and offer fresh and vital perspectives on groundbreaking security topics.

In addition to the formal presentations, you'll have plenty of chances to meet colleagues with similar interests. And you won't want to miss the vendor exhibits showcasing the latest in security products and technology.

All in all, we've assembled what's arguably the strongest program in the eight-year history of the USENIX Security Symposium. But don't take my word for it. Come to Washington, D.C., from August 23 through the 26th and see for yourself.

Win Treese, Program Chair
Open Market, Inc.
For the USENIX Security Symposium Program Committee

P.S. Register early for tutorials—they often fill up fast. You can use our on-line registration form at *http://www.usenix.org/events/sec99*

Tutorial Program

Monday–Tuesday, August 23-24, 1999

To meet your needs, the Tutorial Program at Security '99 provides you with in-depth, immediately-useful instruction in security techniques, effective tools, and best strategies. USENIX tutorials survey the topic, then dive right into the specifics of what-to-do and how-to-do-it. Instructors are well-known experts in their fields, selected for their ability to teach complex subjects. Attend the USENIX tutorials at Security '99 and take valuable skills back to your company or organization.

Tutorial Overview

All tutorials are full-day sessions

Monday, August 23

9:00 AM to 5:00 PM

M1 Intrusion Detection and Network Forensics
Marcus Ranum, *Network Flight Recorder, Inc.*

M2 Advanced Topics in Windows NT Security
Phil Cox, *Networking Technology Solutions*

M3 Secure Networking—An Introduction to Virtual Private Networks
Tina Bird, *Secure Networking Group*

Tuesday, August 24

9:00 AM to 5:00 PM

T1 How Attackers Break Programs, and How to Write Programs Securely
Matt Bishop, *University of California, Davis*

T2 Network Security Profiles: A Collection of Stuff Hackers Know About You
Brad Johnson, *SystemExperts Corporation*

T3 Cryptography—From the Basics Through PKI
Daniel Geer, *CertCo, Inc.*, and Aviel Rubin, *AT&T Labs—Research*

Tutorial fees include

- **Admission to the tutorials you select**
- **Printed and bound tutorial materials from your session**
- **Lunch**
- **Admission to the Security '99 Exhibition**

Our Guarantee: If you're not happy, we're not happy. If you feel a tutorial does not meet the high standards you have come to expect from USENIX, let us know by the first break and we will change you to any available tutorial immediately.

Continuing Education Units

USENIX provides Continuing Education Units (CEUs) for a small additional administrative fee. The CEU is a nationally recognized standard unit of measure for continuing education and training, and is used by thousands of organizations. Each full-day USENIX tutorial qualifies for 0.6 CEUs. You can request CEU credit by completing the CEU section on the registration form. USENIX provides a certificate for each attendee taking a tutorial for CEU credit and maintains transcripts for all CEU students. *CEUs are not the same as college credits. Consult your employer or school to determine their applicability.*

Register early for tutorials, as they often sell out.

Tutorial Program

Monday–Tuesday, August 23-24, 1999

Monday, August 23

M1 Intrusion Detection and Network Forensics

Marcus J. Ranum, Network Flight Recorder, Inc.

Who should attend: Network and system managers, security managers, and auditors. This tutorial assumes some knowledge of TCP/IP networking and client/server computing. What can intrusion detection do for you? Intrusion detection systems are designed to alert network managers to the presence of unusual or possibly hostile events within the network. Once you've found traces of a hacker, what should you do? What kind of tools can you deploy to determine what happened, how they got in, and how to keep them out? This tutorial provides a highly technical overview of the state of intrusion detection software and the types of products that are available, as well as the basic principles for building your own intrusion detection alarms. Methods of recording events during an intrusion are also covered.

Topics include:

What is IDS?
- Principles
- Prior art

Can IDS help?
- What IDS can and can't do for you
- IDS and the WWW
- IDS and firewalls
- IDS and VPNs

Types and trends in IDS design
- Anomaly and misuse detection
- Traps
- Future avenues of research

Concepts for building your IDS
- What you need to begin
- Performance issues

Tools for building your IDS
- Sniffers and suckers
- Host logging tools
- Log recorders

Reporting and recording
- Managing alerts
- What to throw away and what to keep

Network forensics
- So you've been hacked
- Forensic tools
- Brief overview of evidence handling
- Who can help you

Resources and references

Marcus J. Ranum *is CEO and founder of Network Flight Recorder, Inc. He is the principal author of several major Internet firewall products, including the DEC SEAL, the TIS Gauntlet, and the TIS Internet Firewall Toolkit. Marcus has been managing UNIX systems and network security for over 13 years, including configuring and managing whitehouse.gov. Marcus is a frequent lecturer and conference speaker on computer security topics, and is co-author with Daniel Geer and Aviel Rubin of* The Web Security Sourcebook.

M2 Advanced Topics in Windows NT Security

Phil Cox, Networking Technology Solutions

Who should attend: Programmers, network and systems administrators, and individuals who need a better understanding of the "why's" of Windows NT security. Anyone interested in Windows NT network protocols, details on "what" registry settings actually do, and other advanced topics. An intermediate knowledge of Windows NT security and experience dealing with network security are prerequisites for this course.

Many Windows NT security issues require more than a basic understanding of security exposures and potential control measures. This course is designed for system and network administrators and system programmers who are already technically proficient with Windows NT security and want to learn more about advanced features.

Topics include:

Details of Windows NT related to security and their implications
- The internal functionality of Windows NT
- Windows networking: SMB and NetBIOS

Tradeoffs in designing and implementing suitable solutions to address flaws

Practical exercise in defending NT using a firewall

Dealing with Windows NT authentication
- Passthrough authentication
- Derivation and protection of password hashes

Securing the Windows registry
- Advanced techniques
- Tradeoffs and pitfalls in each registry change

The Security Configuration Manager
- Default configurations
- Defining specialized templates

Phil Cox *is a consultant for Networking Technology Solutions, and is a member of a government incident response team. Phil frequently writes and lectures on issues bridging the gap between UNIX and Windows NT. He is a featured columnist in* ;login:*, the USENIX Association magazine, and is on the upcoming USENIX LISA program committee. Phil has a B.S. in Computer Science from the College of Charleston, South Carolina.*

M3 Secure Networking— An Introduction to Virtual Private Networks

Tina Bird, Secure Networking Group

Who should attend: System administrators and network managers responsible for remote access and wide-area networks within their organization. Participants should be familiar with TCP/IP networking and fundamental network security, although some review is provided. The purpose of this tutorial is to provide a step-by-step guide to evaluating an organization's VPN requirements, selecting the appropriate technology, and implementing it within a pre-existing security infrastructure.

"I can trace a good portion of my professional success to what I learned and whom I met at the USENIX Security Symposium. It has been invaluable."

Daniel Geer, Senior Strategist for CertCo, Inc.

Virtual private networking technology provides a flexible mechanism for addressing connectivity needs within many organizations. This class focuses on assessing business and technical requirements for remote access and extranet connections, evaluating VPN technology, integrating VPNs within an existing network infrastructure, and common implementation difficulties.

Topics include:

- VPN security features (encryption, access control, NAT) and how they protect against common Internet threats
- Assessing your organization's needs for remote access
- VPN architectures and where they fit
- A brief review of commercial VPN products
- Implementing VPN technology within your organization's network
- Common VPN difficulties

After completing this course, students will be ready to evaluate their requirements for remote access and begin testing commercial VPN implementations.

Tina Bird *is a security analyst at Secure Network Group, a consulting firm in Lawrence, Kansas specializing in the installation and management of secure wide-area networks. She has implemented and managed a variety of wide-area-network security technologies, such as firewalls and VPN packages; built and supported extranet and intranet remote access packages; and developed, implemented, and enforced corporate IS security policies in a variety of environments. Her main focus in the last year has been on the evaluation and implementation of virtual private networking solutions in small- to mid-sized networks (40 to 4000 hosts). Tina is the moderator of the Virtual Private Networks mailing list. She has a B.S. in physics from Notre Dame and an M.S. and Ph.D. in astrophysics from the University of Minnesota.*

Tuesday, August 24

T1 How Attackers Break Programs, and How to Write Programs Securely

Matt Bishop, University of California, Davis

Who should attend: Software developers or managers who need to understand what it takes to write programs that can successfully withstand malicious attempts at intrusion. Attendees should be familiar with the C language and basic UNIX programming techniques.

Intrusions exploit vulnerabilities, and the vast majority of those vulnerabilities are the result of programming errors. Security professionals and developers who know the difference between safe and unsafe code can be key players in two critical endeavors—writing software that doesn't create new vulnerabilities and evaluating code to determine whether it is vulnerable.

The goal of this course is to enable the attendee to write a secure setuid or setgid program in C (or any code that runs as root with privileges), and to know when it is (and is not) appropriate to write such a program. The course covers common errors in designing and writing privileged programs, and presents them in the context of where they were discovered and exploited. In this way, the course provides a prescription for safe programming and anecdotal information about why ignoring each of the prescriptions can lead to real-world compromise. This course also exposes program errors and shows how to avoid them.

Topics include:

- When to write a privileged program
- Basic design principles
- Basic implementation rules; compartmentalization, modularization
- Common problems and attacks
- Environment problems
- Buffer and other overflows
- Inconsistencies
- Error handling
- Style
- Common system and library calls that can cause problems
- The most common security problems with setuid programs
- What to avoid, including descriptions of some known security flaws in existing setuid programs
- Alternate approaches, including servers
- Walk-through of some programs and functions: how they implement the privileged code, good points, and weak points

Matt Bishop *earned his Ph.D. at Purdue University, where he began working on problems of security in computer systems in general, and UNIX systems in particular. He subsequently worked at the Research Institute for Advanced Computer Science at NASA and taught courses in operating systems, computer security, and software engineering at Dartmouth College. He chaired the first USENIX Security Workshop and plays an active role in identifying and thwarting security threats. In 1993, Matt joined the faculty at the University of California at Davis.*

T2 Network Security Profiles: A Collection of Stuff Hackers Know About You

Brad Johnson, SystemExperts Corporation

Who should attend: Network, system, and firewall administrators; security auditors or audit recipients; people involved with responding to intrusions or responsible for network-based applications or systems which might be targets for hackers. Participants should understand the basics of TCP/IP networking. Examples may use UNIX commands or include C or scripting languages.

This course will be useful for people with any type of TCP/IP-based system, whether it is a UNIX, Windows NT, or mainframe operating system or a router, firewall, or gateway network host.

There are common stages to network-based host attacks, whether it comes from the Internet, Extranet, or Intranet reconnaissance,

vulnerability research, or exploitation. This tutorial will review the tools and techniques hackers use in performing these types of activities. You will learn how to be prepared for such attacks by becoming familiar with the methods employed. Specifically, the course will focus on how to generate profiles of your own systems over the network. Additionally, it will show some of the business implications of these network-based probes.

The course will focus primarily on tools that exploit many of the common TCP/IP-based protocols (such as WWW, SSL, DNS, ICMP, and SNMP) which support virtually all of the Internet applications, including Web technologies, network management, and remote file systems. Many topics will be addressed at a detailed technical and administrative level. This course will primarily use examples of public domain tools because these tools are widely available and commonly used in these situations.

Topics include:

- Review of attack methodology: reconnaissance, target selection, and exploitation
- Profiles: what an attack looks like
- Techniques: scanning, CERTs, TCP/IP protocol "mis"uses, denial of service, and hacking clubs
- Tools: scotty, strobe, netcat, SATAN, ISS, ToneLOC, SSLeay/upget, etc.
- Business exposures: integrity and confidentiality, audits, and intrusion resolution

Brad Johnson *is a well-known authority in the field of distributed systems.*

He has participated in seminal industry initiatives including the Open Software Foundation, X/Open, and the IETF, and has published often about open systems. At SystemExperts Brad has led numerous security probes for major companies, revealing significant unrealized exposures. Prior to joining SystemExperts, Brad was one of the original members of the OSF DCE Evaluation Team, the group that identified, evaluated, and selected technology to become the industry's first true interoperable middleware.

T3 Cryptography—From the Basics Through PKI in 23,400 Seconds

Daniel Geer, CertCo, Inc., and Aviel Rubin, AT&T Labs—Research

Who should attend: Corporate security officers, Webmasters, IT planners, and anyone who wants to augment their self-taught knowledge of modern security technology with an up-to-date, sophisticated look at what you have to work with.

This course addresses what is and is not possible in network security, and examines the tradeoffs between security, cryptographic complexity, accountability, and cost. We approach cryptography as a tool, not a calling, and we approach the idea of a Public Key Infrastructure as an investment you may or may not choose to make. Upon completing this course, you will be in a position to confidently evaluate and buy security technologies.

We will cover, as interactively as possible, what security really is and how to buy no more than you need. You will learn about alternatives for deploying and managing security in general and Public Key Infrastructure in particular, plus some guidance in evaluating them with respect to your needs. While we cannot solve your problems for you, we'd welcome students who are stalled out over seemingly unfathomable forks in the road, e.g., "How many CAs does a company need?" Possible answers include: one per hiring office, precisely one globally, it doesn't matter, none — you outsource, however many you already have plus one for cross-certification, etc. We'll help you discover which answers are better (and why), and which approach is right for you.

Daniel E. Geer, Jr., Sc.D., *is Vice President and Senior Strategist for CertCo, Inc., the market leader in digital certification for electronic commerce. Daniel was previously Director of Engineering at Open Market, Inc.*

He has been a successful entrepreneur in network security and distributed systems management culminating in the successful sale of his own company to OpenVision Technologies, where he subsequently served as Chief Scientist, Vice President of Technology, and Managing Director. He arranged the Public Key Infrastructure track of the Third USENIX Workshop on Electronic Commerce. His book with Marcus Ranum and Aviel Rubin, The Web Security Sourcebook *(Wiley & Sons). He co-chaired the recent USENIX workshops on Embedded Systems and Intrusion Detection.*

Aviel D. Rubin *is a Principal Technical Staff Member at AT&T Labs—Research, in the secure systems research department. He is also Adjunct Professor of Computer Science at New York University, where he teaches cryptography and computer security. He is the co-author of* The Web Security Sourcebook. *Avi holds a B.S., M.S.E., and Ph.D. from the University of Michigan in Ann Arbor ('89, '91, '94) in Computer Science and Engineering. He has served on several program committees for major security conferences and as the program chair for USENIX Security '98, USENIX Technical '99, and ISOC NDSS 2000. His URL is http://cs.nyu.edu/rubin.*

"The best conference around ... applying highbrow techniques to solve real security problems ... "

Greg Rose, Qualcomm, Australia

Technical Sessions

Wednesday–Thursday, August 25-26, 1999

The Technical Sessions program at Security '99 features some of the best minds in security research. Starting with the keynote address by Tahar Elgamal, former Chief Scientist at Netscape, the technical program offers two tracks for security professionals. The Refereed Papers Track provides the opportunity to hear over twenty research papers on security issues, presented by the authors. The refereed papers were reviewed by the USENIX Program Committee and selected for their quality from a large number of submissions. The Invited Talks Track brings together some of the foremost thinkers and scientists to discuss such topics as electronic commerce, multi-agent markets, and the U.S. government's cryptography export policy.

Wednesday, August 25

9:00am–10:30am

Opening Remarks and Best Paper Awards
Win Treese, *Open Market, Inc.*

Keynote Address — The Next Generation of Security
Taher Elgamal, *President, Information Security Group, Kroll-O'Gara*

The one predictable thing about the security industry is that it will remain unpredictable, because every new device or application adds new holes and vulnerabilities. The security industry is developing from a static model of shared secrets and acl's to PKIs, to single sign-on, and policy-based applications. The growth of E-commerce will not only drive the security industry but shape it towards risk-based thinking. We are moving from "this is a secure network because of the firewall" to "this is an adequate (or acceptable level of risk) IT system for our type of business."

As Chief Scientist of Netscape Communications Corporation, Dr. Elgamal pioneered Internet security technologies such as SSL, developed a number of Internet payment schemes, and participated in the "SET" credit card payment protocol. He has a long career in cryptography and security, which started with a Ph.D. at Stanford, where he pioneered original public key cryptography and digital signature technology, inventing the Elgamal cryptography technology which was adopted by NIST in the DSS digital signature standard. He was director of engineering at RSA Data Security, Inc., where he produced the RSA cryptographic toolkits, the industry standards for developers of security-enabled applications and systems.

	Refereed Papers Track	Invited Talks Track
10:30am–11:00am	**Break**	**Break**
11:00am–12:30pm	**PDAs** Session Chair: Jim Duncan, *Cisco Systems, Inc.* **The Design and Analysis of Graphical Passwords** Ian Jermyn, *New York University*; Alain Mayer, *Bell Laboratories, Lucent Technologies*; Fabian Monrose, *New York University;* Michael K. Reiter, *Bell Laboratories, Lucent Technologies;* Aviel Rubin, *AT&T Labs—Research* **Hand-Held Computers Can Be Better Smart Cards** Dirk Balfanz, Edward W. Felten, *Princeton University* **Offline Delegation** Arne Helme, Tage Stabell-Kulø, *University of Tromsø, Norway*	**The Burglar Alarm Builder's Toolbox** Marcus Ranum, *CEO, Network Flight Recorder, Inc.* When you're protecting your site, don't ignore the home court advantage! One of the best ways to detect attackers is by instrumenting your system with unexpected booby traps and alarm bells. Make your system or network into a virtual minefield for hackers to play in. I will present a few useful tools and sick, twisted ideas for building burglar alarms.
12:30pm–2:00pm	**Lunch (on your own)**	**Lunch (on your own)**
2:00pm–3:30pm	**Cages** Session Chair: Crispin Cowan, *Oregon Graduate Institute* **Vaulted VPN: Compartmented Virtual Private Networks on Trusted Operating Systems** Tse-Huong Choo, *Hewlett-Packard Laboratories* **Enforcing Well-Formed and Partially-Formed Transactions for UNIX** Dean Povey, *Cooperative Research Centre for Distributed Systems Technology* **Synthesizing Fast Intrusion Prevention/Detection Systems from High-Level Specifications** R. Sekar, Prem Uppuluri, *Iowa State University*	**Jikzi — A New Framework for Security Policy, Trusted Publishing, and Electronic Commerce** Ross Anderson, *Computer Laboratory, Cambridge University* The goal of enabling people to build integrated publishing and e-commerce services using appropriate, simple and uniform mechanisms requires a new way to deal with security policy on the Web. In this talk, we explain Jikzi, a single transparent markup language that supports multiple security policies — even in the same document.

3:30pm–4:00pm Break | Break

4:00pm–5:30pm

Keys
Session Chair: Carl Ellison, *Intel Corporation*

Building Intrusion Tolerant Applications
Tom Wu, Michael Malkin, Dan Boneh, *Stanford University*

Designing a Secure Multi-Agent Market
Edward W. Felten, *Princeton University*

Brute Force Attack on UNIX Passwords with SIMD Computer
Gershon Kedem, Yuriko Ishihara, *Duke University*

Antigone: A Flexible Framework for Secure Group Communication
Patrick McDaniel, Atul Prakash, Peter Honeyman, *University of Michigan*

Designing a Secure Multi-Agent Market
Edward W. Felten, *Professor, Princeton University*

Recently, a group at Princeton designed a secure electronic stock market that allows clients to inject trading "agent" programs that monitor the market and act on the client's behalf. Systems of this type raise some very difficult security issues. By allowing traders to write their agents in a general-purpose programming language, we allow great flexibility in designing trading strategies, which makes the market more interesting and efficient. However, giving so much freedom to the agents forces us to rigorously control what agents can do and what resources they can use. This talk will discuss the problems encountered in building a secure agent trading market, present the solutions our group devised and the compromises we made, and point the way to future research needed to build and deploy such systems in the real world.

Thursday, August 26

Refereed Papers Track

Invited Talks Track

8:30am–10:00am

Potpourri
Session Chair: Trent Jaeger, *IBM*

A Secure Station for Network Monitoring and Control
Vassilis Prevelakis, *Network Management Center, University of Piraeus*

The Flask Security Architecture: System Support for Diverse Security Policies
Ray Spencer, *Secure Computing Corporation*; Stephen Smalley, Peter Loscocco, *National Security Agency;* Mike Hibler, Dave Andersen, Jay Lepreau, *University of Utah*

A Study in Using Neural Networks for Anomaly and Misuse Detection
Anup K. Ghosh, Aaron Schwartzbard, *Reliable Software Technologies*

Apples, Oranges and the Public Key Infrastructure (PKI)
Paul C. Van Oorschot, *Chief Scientist, Entrust Technologies*

The unprecedented growth of the Internet is surpassed only by the confusion resulting from the rapid introduction of new technologies. A prime example is the application of Public Key Infrastructure (PKI) to a wide array of products, systems, and services. Many experts are positioning the Public Key Infrastructure as the answer to all security questions; other experts dismiss PKI as a poor fit for commercial problems. Both groups are correct — within their own unspoken definitions — and this is precisely the problem, namely the lack of common understanding of what PKI encompasses. In an attempt to clear the smoke (rather than to just move it around), this talk outlines the components of a baseline architecture for a managed PKI, explores standard features, and examines how these match the security requirements in a commercial world where public key certificates form the basis for security.

10:00am–10:30am Break | Break

10:30am–Noon

Security Practicum
Session Chair: Wolfgang Ley, *DFN-CERT*

The Design of a Cryptographic Security Architecture
Peter Gutmann, *University of Auckland*

Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0
Alma Whitten, *Carnegie Mellon University*

Jonah: Experience Implementing PKIX Reference Freeware
Mary Ellen Zurko, John Wray, *Iris Associates*; Ian Morrison, *IBM;* Mike Shanzer, *Iris Associates*; Mike Crane, *IBM*; Pat Booth, *Lotus;* Ellen McDermott, *IBM;* Warren Macek, *Iris Associates;* Ann Graham, Jim Wade, Tom Sandlin, *IBM*

Experience Is the Best Teacher
Peter G. Neumann, *Principal Scientist, SRI International*

Everyone involved in information security and overall system survivability can learn more from the historical evolution of computer operating systems, distributed systems, databases, networks, and the associated risks. Yet, somehow the most valuable would-be lessons from the past keep getting lost. Consequently, our "generally accepted"' principles are sub-optimal without an understanding of their deeper implications. However, our understanding of experience may also be flaky in the absence of guiding principles. This talk considers some of the lost horizons and assesses why the advancement of the state of the art in security has been so difficult.

Technical Sessions

Wednesday–Thursday, August 25-26, 1999

Noon–1:30pm — Lunch (on your own) / Lunch (on your own)

1:30pm–3:00pm

Access Control

Session Chair: Christoph Schuba, *Sun Microsystems Laboratories*

Scalable Access Control for Distributed Object Systems
Daniel Sterne, Gregg Tally, Durward McDonell, David Sames, David Sherman, Pierre Pasturel, E. John Sebes, *TIS Labs at Network Associates*

Certificate-based Access Control for Widely Distributed Resources
Mary R. Thompson, William Johnston, Srilekha Mudumbai, Gary Hoo, Keith Jackson, *Lawrence Berkeley National Laboratory*

Digital-Ticket-Controlled Digital Ticket Circulation
Ko Fujimura, Hiroshi Kuno, Masayuki Terada, Kazuo Matsuyama, Yasunao Mizuno, Jun Sekine, *NTT Information Sharing Platform Laboratories*

U.S. Crypto Policy: Explaining the Inexplicable

Susan Landau, *Sun Microsystems Laboratories*

The richest, strongest, most electronically vulnerable nation on earth persists in a policy that effectively restricts the use of encryption technology domestically as well as abroad. Even while the security of transactions over telephone and computer networks has become a source of wide public concern, the U.S. government continues to work against the proliferation of unbreakable cryptography (and thus perfectly concealable communications). Why? In this talk, I attempt to explain today's inexplicable U.S. crypto policy in a perhaps more explicable context of U.S. history.

3:00pm–3:30pm — Break / Break

Joint Session
3:30pm–5:00pm

Works-In-Progress Reports

Session Chair: Greg Rose, *Qualcomm, Inc.*
This session will consist of short presentations from researchers about work-in-progress, new results, or timely topics.
To participate, please see Works-In-Progress description on page 12.

About Invited Talks Speakers

Ross Anderson

Ross Anderson leads research in computer security at the University of Cambridge Computer Laboratory. His most innovative recent work is on "soft tempest" — software techniques to reduce the Tempest leakage from PCs, now used in a number of products including PGP. He is a coauthor of Serpent, a leading candidate cipher in the Advanced Encryption Standard competition, and has well-known publications on the tamper resistance of smartcards, techniques for removing copyright marks from digital media, medical information security, the robustness of cryptographic protocols, and how real-world cryptosystems fail. He is both a Chartered Engineer and a Chartered Mathematician.

Peter G. Neumann

Peter G. Neumann is a Principal Scientist in the Computer Science Lab at SRI International in Menlo Park. He has a Ph.D. from Harvard and a Dr. rerum naturarum from the Technische Hochschule Darmstadt. He has worked on system security, safety, reliability, and survivability. He is the author of *Computer-Related Risks*, the Moderator of Risks Forum (comp.risks), Chairman of the ACM Committee on Computers and Public Policy, and Fellow of the ACM, IEEE, and AAAS. His Web site (http://www.csl.sri.com/~neumann/) contains pointers to his list of risks cases, Congressional testimonies, and other background.

Edward W. Felten

Edward W. Felten is Assistant Professor of Computer Science at Princeton University. He has published more than forty papers in the research literature, and has won awards for his research including a National Young Investigator award from the National Science Foundation and an Alfred P. Sloan Fellowship. He received his B.S. (with honors) in Physics from the California Institute of Technology, and his Ph.D. in Computer Science and Engineering from the University of Washington.

Paul C. Van Oorschot

Paul C. Van Oorschot is Vice President and Chief Scientist for Entrust Technologies. Over the past 15 years he has been involved in research, consulting, standardization, and product R&D in cryptography and information security, and in particular in the area of authentication, key management, and public key certificate systems. He has a Ph.D. in computer science, is a member of the Board of Directors of the International Association for Cryptologic Research (IACR), and co-author of the *Handbook of Applied Cryptography*.

Susan Landau

Susan Landau is Senior Staff Engineer at Sun Microsystems Laboratories. She and Whitfield Diffie have written *Privacy on the Line: The Politics of Wiretapping and Encryption*. Landau is also primary author of the 1994 Association for Computing Machinery report *Codes, Keys, and Conflicts: Issues in US Crypto Policy*. Landau has done extensive work in symbolic computation and algebraic algorithms. Landau received her Ph.D. from MIT, her M.S. from Cornell, and her B.A. from Princeton.

Marcus J. Ranum

Marcus J. Ranum is CEO of Network Flight Recorder, Inc. (http://www.nfr.net/) He is the principal author of several major Internet firewall products, including the DEC SEAL, the TIS Gauntlet, and the TIS Internet Firewall Toolkit. He has been managing UNIX systems and security for over 13 years, including configuring and managing whitehouse.gov. He is a co-author of *The Web Security Sourcebook*.

Security '99 Exhibition

Wednesday–Thursday, August 25-26, 1999

The Security '99 Exhibition puts company representatives at your fingertips. See demonstrations, ask questions, and pick up a copy of the latest print and software releases from book and software publishers alike. Tomorrow's solutions start with today's technology, so be sure to browse the booths and learn more about commercial applications in the security field. Shopping for something more than a security solution? Several companies are also looking for contractors and new members of their teams.

Exhibit Hours

Wednesday, August 25
12:00 noon–7:00 pm

Thursday, August 26
10:00 am–2:00 pm

Come Test Security Solutions Offered by:

Association Book Exhibit

Computer Associates International, Inc.
www.cai.com

Computer Security Institute
www.gocsi.com

CounterPane Systems
www.counterpane.com

Covalent Technologies, Inc.
www.covalent.net

Data Fellows Corporation
www.datafellows.com

InfoExpress, Inc.
www.infoexpress.com

Intellisoft Corporation
www.isoft.com

International Network Services
www.ins.com

Internet Devices, Inc.
www.internetdevices.com

Internet Security Systems, Inc.
www.iss.com.net

MIS Training Institute
www.misti.com

Norman Data Defense Systems Inc.
www.norman.com

Secure Computing Corporation
www.securecomputing.com

SOLsoft, Inc.
www.solsoft.com

Symark Software
www.symark.com

Trend Micro Inc.
www.antivirus.com

Tripwire Security Systems
www.tripwiresecurity.com

Participants as of May 14, 1999

Questions About Exhibiting?

Demonstrate your products to the most technically astute professionals in computing.

Contact: Dana Geffner, Phone: 1.831.457.8649
Email: dana@usenix.org

FREE EXHIBIT HALL PASS

Please complete. Information is confidential.

Open: Wednesday, August 25, 12 noon–7 pm
Thursday, August 26, 10 am–2 pm

Location: JW Marriott Hotel, 1331 Pennsylvania Avenue N.W.,
Washington, D.C. 20004, 1.202.393.2000

USE THIS PASS ONLY if you do not register for the conference.
Please copy and share freely with your colleagues.
Bring this pass with you to the Exhibit.

What is your affiliation (check one):
❑ academic ❑ commercial ❑ gov't ❑ R&D

What is your role in the purchase decision (check one):
1. ❑ final 2. ❑ specify 3. ❑ recommend 4. ❑ influence 5. ❑ no role

What is your primary job function (check one):
1. ❑ system/network administrator 2. ❑ consultant 3. ❑ academic/researcher
4. ❑ developer/programmer/architect 5. ❑ system engineer
6. ❑ technical manager 7. ❑ student 8. ❑ security 9. ❑ Webmaster

Name First Last

Company

Work Address

City State Zip Country

Telephone No. Fax

Email Address (1 only please)

❑ *I do not want my address available for other than USENIX mailings.*

❑ *I do not want USENIX to email me notices of Association activities.*

Symposium Activities and Services

"The fact that people with different backgrounds and perspectives gave their vision made this symposium a very vivid, rich, and colorful one."

Magda De Jong,
Hewlett-Packard,
Symposium Attendee

"The conference exceeded my expectations. It was a great way to see and meet many of the people whose work I reference constantly."

David W. Ford,
Vision Development Group, Inc.,
Symposium Attendee

Birds-of-a-Feather Sessions (BoFs)

Tuesday and Wednesday Evenings

Do you have a topic that you'd like to discuss with others? Our Birds-of-a-Feather sessions may be perfect for you. BoFs are very interactive and informal gatherings for attendees interested in a particular topic. BoFs may be scheduled during the symposium at the registration desk or in advance by contacting the USENIX Conference Office at 1.949.588.8649, or by sending email to: *conference@usenix.org*.

Works-In-Progress Reports (WIPs)

Thursday, August 26, 3:30pm–5:00pm

Submission deadline: August 25, 1999

Submissions to: securitywips@usenix.org

This session will consist of short presentations about work-in-progress, new results, or timely topics. Speakers should submit a one- or two-paragraph abstract to securitywips@usenix.org by 6:00 pm on Wednesday, August 25, 1999, or to Greg Rose, at the conference, by 11 am Thursday, August 26. Please include your name, affiliation, and the title of your talk. The accepted abstracts will appear on the conference Web page after the symposium. The time available will be distributed among the presenters with a minimum of 5 minutes and a maximum of 10 minutes. The time limit will be strictly enforced. A schedule of presentations will be posted at the symposium by noon on August 26. Experience has shown that most submissions are usually accepted.

Student Stipends Available

The USENIX student stipend program covers travel, living expenses, and registration fees to enable full-time students to attend USENIX meetings. Detailed information about applying for a stipend is available at the USENIX Web site: *http://www.usenix.org/students/stipend.ann.html*, by reading *comp.org.usenix*, or by sending email to *students@usenix.org*.

Symposium Proceedings

One copy of the proceedings is included with your Technical Sessions registration fee. To order additional copies, contact the USENIX Association at 1.510.528.8649, or send email to: *office@usenix.org*.

Social Activities

Meet the symposium speakers and connect with your peers in the community.

There will be a Welcome Reception on Sunday evening and a luncheon on both Monday and Tuesday for tutorial attendees. All symposium attendees are invited to the reception on Wednesday evening in the JW Marriott Hotel.

Security Symposium Terminal Room

USENIX is pleased to provide a terminal room for your convenience. The terminal room will feature 30 PCs with a UNIX operating system. There will be a dial-in network from your Marriott hotel room, laptop drops, and a live Webcam. All of these will be connected to the internet via a T1 line sponsored by Earthlink Network Services.

The terminal room is staffed by volunteers. If you are interested in helping with this effort please send email to mcginley@usenix.org for more information.

Registration Discount Deadline: July 23, 1999

Hotel Discount Deadline: July 29, 1999

About USENIX and CERT/CC

About USENIX

http://www.usenix.org/

USENIX is the Advanced Computing Systems Association. Since 1975 USENIX has brought together the community of system administrators, engineers, scientists, and technicians working on the cutting edge of the computing world.

USENIX conferences are the essential meeting ground for the presentation and discussion of the most advanced information on the latest developments in computing.

USENIX and its members are dedicated to:

- Problem-solving with a practical bias
- Fostering innovation that works
- Communicating rapidly the results of both research and innovation
- Providing a neutral forum for the exercise of critical thought and the airing of technical issues

About SAGE

SAGE, the System Administrators Guild, is a special technical group within USENIX. To join SAGE, you must be a member of USENIX. SAGE is an international membership society dedicated to the recognition and advancement of the system administration profession.

How to Join

Joining is easy. When you register, be sure to check off the membership box on the registration form and pay the non-member fee. You may also join at the symposium or send email to *office@usenix.org* or phone 1.510.528.8649.

About the CERT Coordination Center

http://www.cert.org/

CERT/CC is part of the Software Engineering Institute, a federally funded research and development center at Carnegie Mellon University. It was started in December 1988 after the Morris Worm incident and originally was almost exclusively involved with incident response. Since then, the work has grown to include helping to start other incident response teams, coordinating the efforts of teams in responding to large-scale incidents, providing training to incident response professionals, researching the causes of security vulnerabilities, preventing vulnerabilities, improving system security, and increasing the survivability of large-scale networks.

t h a n k y o u

USENIX and SAGE Thank Their Supporting Members

USENIX Supporting Members

C++ Users Journal
Cirrus Technologies
Cisco Systems, Inc.
CyberSource Corporation
Deer Run Associates
Greenberg News Networks/MedCast Networks
Hewlett-Packard India Software Operations
Internet Security Systems, Inc.
Microsoft Research
MKS, Inc.
Motorola Australia Software Centre
NeoSoft, Inc.
New Riders Press
Nimrod AS
Performance Computing Magazine
Questra Consulting
Sendmail, Inc.
Server/Workstation Expert Magazine
TeamQuest Corporation
UUNET Technologies, Inc.
Windows NT Systems Magazine
WITSEC, Inc.

SAGE Supporting Members

Atlantic Systems Group
Collective Technologies
D.E. Shaw & Co.
Deer Run Associates
Electric Lightwave, Inc.
ESM Services, Inc.
GNAC, Inc.
Mentor Graphics Corp.
Microsoft Research
MindSource Software Engineers
Motorola Australia Software Centre
New Riders Press
O'Reilly & Associates, Inc.
Remedy Corporation
SysAdmin Magazine
Taos Mountain
TransQuest Technologies, Inc.
UNIX Guru Universe

Mark Your Calendar for These Upcoming 1999 USENIX Events

LISA-NT—2nd Large Installation System Administration of Windows NT Conference

July 14–17, 1999
Seattle, Washington

2nd Symposium on Internet Technologies and Systems (USITS '99)

October 11–14, 1999
Boulder, Colorado

13th Systems Administration Conference (LISA '99)

November 7 – 12, 1999
Seattle, Washington

Visit Our Calendar:

www.usenix.org/events

Registration Information

Tutorial Program (August 23-24)

Tutorial Registration Fees include:

- Admission to the tutorials you select
- Printed and bound tutorial materials for your selected courses
- Lunch
- Admission to the Security '99 Exhibition
- Admission to Symposium Activities

Early Registration fee (until Friday, July 23, 1999)

Tutorial Program for one day $395
CEU credit (optional) $15
Tutorial Program for two days $690
CEU credit (optional) $30

After July 23, add $50 to the tutorial fee

Technical Sessions (August 25-26)

Technical Sessions Registration Fees include:

- Admission to all Technical Sessions
- Copy of the Symposium Proceedings
- Admission to Security '99 Exhibition
- Admission to Symposium Reception
- Admission to Symposium Activities

Early Registration fee (until Friday, July 23, 1999)

Member* $360
Non-Member or Renewing Member** . . . $440
Full-time student $75
(Must provide copy of current student ID Card)

After July 23, add $50 to the technical sessions fee.

**The member fee applies to current individual members of USENIX, EurOpen national groups, JUS, or AUUG.*

***Non-Members: Join USENIX or renew your membership at no additional charge. Pay the non-member technical sessions fee and check the USENIX membership box on the registration form to renew your existing membership or receive a one-year individual association membership.*

Current USENIX members who wish to join SAGE: You may join SAGE at the USENIX Membership Booth during the conference.

Payment

Payment by check or credit card must accompany the registration form. Purchase orders, vouchers, telephone reservations, and email registrations cannot be accepted.

Student Stipends and Discounts

USENIX offers a special discount rate of $75 for its technical sessions for full-time students. You must include a copy of your current student I.D. card with your registration. This special fee is not transferable.

A limited number of student stipends are available to pay for travel, living expenses, and registration fees to enable full-time students to attend the conference. To apply for a stipend, read comp.org.usenix 6 to 8 weeks before the conference, visit our Web site, www.usenix.org/students/, or email students@usenix.org for more information.

Refund/Cancellation Policy

If you must cancel, all refund requests must be in writing, with your signature, and postmarked no later than Friday, August 13, 1999. Telephone and email cancellations cannot be accepted. You may fax your cancellation or substitute another in your place. Contact the Conference Office for details.

For more conference information, please contact:

USENIX Conference Office
22672 Lambert St., Suite 613
Lake Forest, CA USA 92630

Phone: 1.949.588.8649
Fax: 1.949.588.9706
Email: *conference@usenix.org*
Web: *http://www.usenix.org*
Hours: M–F, 8:30 am–5:00 pm PST

Hotel and Travel Information

Hotel Discount Reservation Deadline: Thursday, July 29, 1999

Note: *Requests for hotel reservations made after the deadline will be handled on a space- and rate-available basis only.*

Hotel Information

USENIX has negotiated special rates for attendees at the JW Marriott Hotel. Contact the hotel directly to make your reservation. You must mention USENIX to get the special rate. A one-night room deposit must be guaranteed to a major credit card. *To cancel your reservation, you must notify the hotel at least 24 hours before your planned arrival date.*

JW Marriott Hotel
1331 Pennsylvania Avenue N.W.
Washington, D.C. 20004

Toll Free: 1.800.228.9290
Local Telephone: 1.202.393.2000
Reservation Fax: 1.202.626.6943

Single Occupancy $139.00

Double Occupancy $149.00
(*plus state and local taxes, currently 14.5%*)

Travel to Washington, D.C.

Discount Air Fares

Special airline discounts will be available for USENIX attendees. Please call for details:

JNR, Inc.
Toll Free in US and Canada:
1.800.343.4546
Telephone: 1.949.476.2788

Airport to Hotel Transportation

Both National and Dulles Airports service the Washington, D.C. area.

National Airport

Metro Light Rail service is available. Take the Blue Line to the Metro Center Station stop. Hotel is located on the left one block from that stop. Super Shuttle runs every half-hour with an $8 one-way fare. Taxi service costs approximately $12 one way.

Dulles International Airport

The Washington Flyer provides transportation to the JW Marriott. The shuttle runs every half-hour with a one-way fare of $16. Taxi service costs approximately $40 one way.

Sights and Special Attractions in Washington, D.C.

National Air and Space Museum

The world's most visited museum houses the Wright Brothers' 1903 Flyer, Lindbergh's Spirit of St. Louis, the Apollo 11 lunar command module, and other aviation and space technology spectaculars.

National Geographic Society

Explorers Hall features Geographica, an interactive exhibit about the earth and the fragile balance among its inhabitants.

Georgetown Walking Tours

The romance, history, and magic of an earlier time in America comes alive in this walking tour of Georgetown.

Kenilworth Aquatic Gardens

Thousands of waterplants, waterlilies, lotuses, water hyacinths and bamboo grow in ponds along the Anacostia River.

Copy this form as needed. Type or print clearly.

Registration Form

8th USENIX Security Symposium
August 23–26, 1999
JW Marriott Hotel, Washington, D.C.

The address you provide will be used for all future USENIX mailings unless you notify us in writing.

Name First Last (surname)

First Name for Badge Member Number

Company / Institution

Mail Stop Mail Address

City State Zip Country

( ) ( )
Telephone No. Fax

Email Address (1 only please)

Important: If there is a mailing label (see other side), please tell us the single letter in the upper right corner (2nd line): _____

Attendee Profile

Help us meet your needs by answering the following questions.
Information is confidential.

❑ *I do not want to be on the attendee list.*
❑ *I do not want my address made available except for USENIX mailings.*
❑ *I do not want USENIX to email me notices of Association activities.*

What is your affiliation (check one):
❑ academic ❑ commercial ❑ gov't ❑ R&D

What is your role in the purchase decision (check one):
1.❑ final 2.❑ specify 3.❑ recommend 4.❑ influence 5.❑ no role

What is your primary job function (check one):
1.❑ system/network administrator 2.❑ consultant 3.❑ academic/researcher
4.❑ developer/programmer/architect 5.❑ system engineer
6.❑ technical manager 7.❑ student 8.❑ security 9.❑ Webmaster

How did you first hear about this meeting (check one):
1.❑ USENIX brochure 2.❑ newsgroup/mailing list 3.❑ *;login:*
4.❑ WWW 5.❑ from a colleague 6.❑ magazine

What publications or newsgroups do you read related to security issues?

Payment must accompany this form

Payment by check or credit card MUST accompany the registration form.

Purchase orders, vouchers, telephone and email registrations cannot be accepted.

❑ **Payment enclosed.** Make check payable to USENIX Conference.

Charge to my: ❑ VISA ❑ MasterCard ❑ American Express ❑ Discover

Account No. Exp. Date

Print Cardholder's Name

Cardholder's Signature

Tutorial Program

Select only one full-day tutorial per day (9:00 am–5:00 pm)

Monday, August 23, 1999	Tuesday, August 24, 1999
❑ M1 Intrusion Detection and Network Forensics *Marcus J. Ranum, Network Flight Recorder, Inc.*	❑ T1 How Attackers Break Programs, and How to Write Programs Securely *Matt Bishop, University of California, Davis*
❑ M2 Advanced Topics in Windows NT Security *Phil Cox, Networking Technology Solutions*	❑ T2 Network Security Profiles: A Collection of Stuff Hackers Know About You *Brad Johnson, SystemExperts Corporation*
❑ M3 Secure Networking—An Introduction to Virtual Private Networks *Tina Bird, Secure Networking Group*	❑ T3 Cryptography—From the Basics Through PKI in 23,400 Seconds *Daniel Geer, CertCo, Inc., and Aviel Rubin, AT&T Labs—Research*

REFUND/CANCELLATION POLICY If you must cancel, all refund requests must be in writing, with your signature, and postmarked no later than Friday, August 13, 1999. Telephone and email cancellations cannot be accepted. You may substitute another in your place. Call the USENIX Conference Office for details: 1.949.588.8649.

Tutorial Program Fees

August 23-24, 1999 (Monday & Tuesday)

One-day tutorial fee	$395.00	$_____
CEU credit (optional)	$15.00	$_____
Two-day tutorial fee	$690.00	$_____
CEU credit (optional)	$30.00	$_____
Late fee applies if postmarked after Friday, July 23, 1999	Add $50.00	$_____

Technical Sessions Fees

August 25-26, 1999 (Wednesday & Thursday)

Current member fee *(Applies to individual members of USENIX, EurOpen national groups, JUS, and AUUG)*	$360.00	$_____
Non-member or renewing member fee*	$440.00	$_____
***Join or renew your USENIX membership, for no additional fee, AND attend the symposium.** Check here: ❑		
Late fee applies if postmarked after Friday, July 23, 1999	Add $50.00	$_____
Full-time student** fee, pre-registered or on-site	$75.00	$_____
Full-time student** fee including USENIX membership fee ***Students: Attach a photocopy of current student ID*	$100.00	$_____
TOTAL DUE		**$**_____

Please complete this registration form and return it along with full payment to:

USENIX Conference Office
22672 Lambert St., Suite 613
Lake Forest, CA USA 92630
Phone: 1.949.588.8649 Fax: 1.949.588.9706

You may fax your registration form to 1.949.588.9706 if paying by credit card. To avoid duplicate billing, please DO NOT mail an additional copy.

The 8th USENIX Security Symposium

Washington D.C. ▪ August 23-26, 1999

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

Securing the Future — Today

Join computer security's insiders (and outsiders) to examine the issues, tools, policies, threats, twisted tricks, and opportunities shaping tomorrow's system and network security landscape.

Whether you are an Internet security guru or the system administrator everyone counts on to maintain a bulletproof network, the 8th USENIX Security Symposium is the place to be.

- Gain command of leading-edge tools and techniques at specifics-driven tutorials.
- Explore the latest advances in security and applications of cryptography, intrusion detection, Public Key Infrastructure (PKI), distributed systems, and Web security.
- Exchange ideas with computing security's foremost experts.

Register Online

www.usenix.org/events/sec99

or call 1.949.588.8649 for more information

USENIX

USENIX Conference Office
22672 Lambert Street, Suite 613
Lake Forest, CA 92630
Phone: 1.949.588.8649
Fax: 1.949.588.9706
Email: conference@usenix.org
Office Hours: 8:30 am to 5:00 pm, Pacific Time

Non-Profit
Organization
US Postage
PAID
USENIX
Association

THE 8TH USENIX
Security
Symposium

August 23-26, 1999 ▪ Washington D.C.