Review the Program. See the quality. Join us at the Security Symposium.

Papers Presented at USENIX Conferences are Refereed.

The refereed papers were reviewed by the Program Committee and selected for their quality from a large number of submissions. We thank the Program Committee for their hard work.

Program Committee

Program Chair

Avi Rubin, *AT&T Labs – Research*

Committee

Carlisle Adams, *Entrust Technologies*
Dave Balenson, *Trusted Information Systems*
Steve Bellovin, *AT&T Labs – Research*
Dan Boneh, *Stanford University*
Diane Coe, *Concept Five Technologies*
Ed Felten, *Princeton University*
Li Gong, *JavaSoft*
Peter Honeyman, *CITI, University of Michigan*
Hugo Krawczyk, *Technion*
Jack Lacy, *AT&T Labs – Research*
Hilarie Orman, *DARPA/ITO*
Mike Reiter, *AT&T Labs – Research*
David Wagner, *University of California, Berkeley*

Readers

Katherine T. Fithen, *CERT*
Trent Jaeger, *IBM Watson Labs*

Invited Talks Coordinator

Greg Rose, *QUALCOMM Australia*

Questions?
Email: *conference@usenix.org*
Phone: 714.588.8649
Fax: 714.588.9706
Updates: *http://www.usenix.org/events/sec98/*

Important Dates to Remember:

Hotel Discount Deadline: *Monday, January 5, 1998*

Pre-Registration Deadline: *Monday, January 5, 1998*

Program at-a-Glance

Sunday, January 25	
6:00 pm – 9:00 pm	On-Site Registration
6:00 pm – 9:00 pm	Welcome Reception
Monday, January 26	
7:30 am – 5:00 pm	On-Site Registration
9:00 am – 5:00 pm	Tutorial Program and Lunch
Tuesday, January 27	
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, January 28	
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
Noon – 7:00 pm	Security '98 Exhibition
7:00 pm – 9:00 pm	Symposium Reception
Thursday, January 29	
8:30 am – 5:00 pm	USENIX Technical Sessions
10:00 am – 2:00 pm	Security '98 Exhibition

"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,
1996 Attendee

Table of Contents

4–7 Tutorials
7–8 About the Speakers
9 Exhibition
10 Keynote Address
10–11 Technical Program
12 About USENIX
13 Conference Activities & Services
14 Hotel and Travel Information
15 Registration

A Letter from the Program Chair

"This is the place where you will hear, discuss, then put to use the latest research, well-thought-out approaches, and tools and techniques for practical system security."

Dear Colleague:

I invite you to the USENIX Security Symposium. This is the place where you will hear, discuss, then put to use the latest research, well-thought-out approaches, and tools and techniques for practical system security. Take home lessons from real-world security practice on how to assess what needs protecting, from whom, and how best to go about it.

As the 7th USENIX Security Symposium approaches, we find ourselves in exciting times. More and more companies are realizing the importance of securing their networks, their data and their computers. Long-awaited electronic commerce is becoming a reality, and people are actually making money on the net. The advent of Java and other platform-independent languages has enabled computational models that only existed in theory to be rapidly developed and deployed. The inherent security risks have jump-started researchers into action.

The conference kicks off with your opportunity for in-depth study. Choose among tutorials led by Bruce Schneier, Carl Ellison, Daniel Geer, Jon Rochlis, Brad Johnson, Jim Duncan, Gary McGraw, and Rik Farrow, all experienced, respected instructors. You'll master both theory and effective approaches and techniques in areas you need: Security on the Web; Windows NT Security; Certification; Java Security; Handling Security Incidents; Network Security Profiles; Introduction to Cryptography; and Internet Crypto Protocols.

Expect to hear about the latest research. The Program Committee had the pleasure of selecting the best among 65 high-quality submissions. These reports of research and new implementations cover a wide range, including:

- Security of mobile code
- Electronic commerce in actuality: how money is being made on the net
- Intrusion detection: implementations of superior new systems
- Security of the world wide web

Alongside the refereed papers, you'll find an incredible line-up of invited speakers: Bill Cheswick; Daniel Geer; Arjen Lenstra; Alfred Menezes; Clifford Neuman; JoAnn Perry; Marcus Ranum; and Shabbir Safdar. This is your chance to hear it from the real pioneers of our field.

Meet colleagues with similar interests at the Tuesday Birds-of-a-Feather Session or present your own on-going research in the Work-In-Progress Session. You'll want to check out the Exhibition where vendors will be demonstrating products they hope will help you practice security more efficiently and effectively. Give them your feedback on what works and what is still needed.

Please join us. I hope to see you in San Antonio on January 26–29, 1998.

Aviel D. Rubin, Program Chair
AT&T Labs – Research
For Security Symposium Program Committee

PS: Register early for tutorials—they often fill up fast.
You can use our on-line registration form: http://www.usenix.org/events/sec98/

Tutorial Program *Monday–Tuesday, January 26–27, 1998*

Gain command of the newest security tools, techniques, and approaches, then put them to work in your organization immediately.

Security is one of the most urgent topics in today's computing environments. USENIX tutorials at Security '98 provide you with the in-depth and immediately-useful instruction you need to meet the demands. These tutorials survey the topic and then dive into the specifics of what-to-do and how-to-do it. Instructors are well-known experts in their topics and selected with care for their ability to teach complex subjects. Attend the USENIX tutorials.

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 of 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 now to guarantee your first choice. Seating is limited. Register by January 5, and save $50.

Tutorial Overview

Full day tutorials run from 9:00 AM to 5:00 PM. Half-day tutorials, marked "AM" or "PM" run either from 9:00 AM to 12:30 PM or from 1:30 PM to 5:00 PM. Full-day tutorials may not be split.

Register early for tutorials — they often sell out.

Monday, January 26

M1	Security on the World Wide Web
M2	Windows NT Security NEW
M3AM	Certification: Identity, Trust, and Empowerment NEW
M4PM	Towards Secure Executable Content: Java Security NEW

Tuesday, January 27

T1	Handling Computer and Network Security Incidents
T2	Network Security Profiles: What Every Hacker Already Knows About You, and What To Do About It
T3AM	Using Cryptography NEW
T4PM	Cryptography for the Internet NEW

Tutorial fees include:

- Admission to the tutorials you select
- Printed and bound tutorial materials from your session
- Lunch
- Admission to the Vendor Exhibition

Monday, January 26

M1 Security on the World Wide Web

Daniel Geer, *CertCo, LLC*, and Jon Rochlis, *SystemExperts Corp.*

Who should attend: Anyone responsible for running a web site who wants the understand the tradeoffs in making it secure. Anyone seeking to understand how the web is likely to be secured

> "Excellent execution of intro- to concept-to drill down facts. Both instructors were fabulous at responding to questions in the fly as well as establishing majority interest right away."
>
> Dolores Quade, *BTG Inc,* 1996 Tutorial Attendee

The World Wide Web is perhaps the most important enabler (so far) of electronic commerce. It has grabbed the popular imagination and the engineering and marketing efforts of a generation of on-line entrepreneurs and consumers. But it was initially designed with little if any thought to industrial strength security. Over the past several years numerous proposals have surfaced to secure the web. This course will survey them with the goal of understanding the strengths and weaknesses of each. The topics covered include:

- Client/server network security
- Brief overview of encryption and its role in all security
- Simple schemes: Basic Auth
- Prevailing protocols: SSL, S-HTTP, PCT
- IP Security
- Payment protocols: Cybercash, Digicash, Open Market, First Virtual, Visa/Mastercard (SET) and others
- Secure operation: configuration, containment, interaction with firewalls, replication, proxy servers, logging

M2 Windows NT Security NEW

Rik Farrow, *Consultant*

Who should attend: System and network administrators, and programmers, who must work with NT systems and need to understand its security principles.

Windows NT is the result of an unusual marriage between disparate operating systems: a completely reworked replacement for Digital Equipment's VMS and Windows 3.1. On the one hand, there are security features to satisfy the most avid control freak: centralized control over user accounts, file sharing, desktop appearance, fine grained object access, encryption, a security monitor, and auditing sensitive enough to capture most security related events. On the other hand, it provides support for an API that has been the main target for virus writers, and application programmers who have never even considered the notion of security.

This tutorial explains the security mechanisms in Windows NT, and how they can best be used to improve the security of networked NT systems. This is not just a review of NT's security-related GUIs (although they are included), we will go behind the scenes and discover the file and directory hierarchy of the trusted computing block, Web server (IIS), registry and event logs, and system files and libraries. Whenever possible, we will explore the command line interfaces and tools for controlling and auditing security of NT systems.

In particular, we will learn about:

- The NT registry, a file system-like construct for storing device and application configuration, passwords, and other system values, all of which are protected by access control lists (ACLs)
- User accounts, local and global groups, rights, and privileges
- Domains, domain controllers, local and network authentication
- NT Passwords, and collecting and cracking passwords
- ACLs for file, directories, and other objects
- NT's event and audit mechanism; and
- Correct configuration of IIS, RAS, network services, and protecting NT systems with firewalls

M3AM Certification: Identity, Trust, and Empowerment NEW

Carl M. Ellison, *CyberCash, Inc.*

Who should attend: Programmers and managers who have to design or select systems using public key cryptography for strong access control or other situations in which the guarantee of trust is critical.

In 1976, Diffie and Hellman postulated a telephone directory, but with public keys instead of phone numbers, to take the place of couriers carrying keys between people to open secure channels. This suggestion has grown into public key certificates, binding names to keys, and to suggestions for national or global Public Key Infrastructures (PKIs). Many people advocate using such certificates or PKIs without realizing what they are getting in return. They take the word of professional cryptographers.

Professional cryptographers, meanwhile, are sloppy in their use of words (using "name" and "identity" as if they were interchangeable) and using "trust" without any qualifiers (as in "In God We Trust").

In fact, each kind of certificate empowers a public key in some way. This tutorial will teach people how to identify what kind of empowerment they need for their public keys and how to achieve that empowerment. It will describe a variety of different certificate formats (X.509, Attribute Cert, PGP, SDSI, SPKI, PolicyMaker) and describe the kind of empowerment each offers.

Time and interest permitting, the tutorial will also cover US Government proposals for using PKIs to achieve Government Access to Keys—although this may be moot by the time of the tutorial (depending on congressional and judicial events).

M4PM Towards Secure Executable Content: Java Security NEW

Gary McGraw, *Reliable Software Technologies*

Who should attend: Programmers, webmasters, and network administrators interested in how Java security is implemented, and how the benefits of Java compare with its risks.

Executable content systems like Java, ActiveX, and Postscript have become a normal part of surfing the Web. These systems are often integrated so seamlessly into browsers that users are unaware that they are doing anything extraordinary. This means many users do not recognize the extra security risks they are taking on by using such systems.

Java is especially cool since it is cross-platform, object oriented, network-savvy, and uses modern memory management. In addition, Java's designers have attempted to create a system that simultaneously ensures type safety and allows dynamic class loading. Type safety plays an essential role in Java's security approach.

Java clearly has exciting benefits, but with these benefits come new risks. It is critical that

Java perform in a secure fashion—something that its designers tried to ensure. How did they do it? How successful were they? Do the benefits of Java outweigh the risks?

This tutorial covers the three prongs of the fundamental Java security model, discusses some of Java's most famous flaws, covers the impact of code-signing on the Java sandbox, and talks about what to expect in the future from executable content systems in terms of security.

Tuesday, January 27

T1 Handling Computer and Network Security Incidents

Jim Duncan, *Penn State University*, and Rik Farrow, *Consultant*

Who should attend: System and network administrators, security managers and managers of computer resources. You should have some knowledge of current operating systems and networking.

Are you prepared to handle a security incident at your site? Responding to computer security incidents is a requirement for all organizations where computers and networks are an important part of the infrastructure. In this tutorial you will find out how to prepare for and handle security incidents with step-by-step information and examples from real-world incidents.

You will learn about the need for comprehensive computer security incident handling capability, how to communicate that need to management and the user community, how to investigate an incident (as a handler, not as law enforcement), and how to establish and maintain the capability. Even if you are the only person tasked with security, this tutorial will help you prepare yourself and your organization.

Topics include:

- Incidents and their cost: types of incidents, statistics on the frequency of incidents, targets of incidents (finance, research, educational, etc.). The costs for handling an incident poorly versus handling one well.
- A multilevel assessment of organizations including the hardware and software, operating systems, network components, types of links, locations, user base, knowledge level, experience, behavior. Also the business of each part of the organization and the corporate or organizational management structure.
- What not to do—real-life examples of incident handling done wrong.
- Post-mortem of incident and overview of computer ethics and law. Major missteps analyzed, possible violations and relevance to various statutes, e.g., ECPA, CFAA, FERPA, and newer legislation.
- How to develop and refine computer and network security policies, including practice and procedures for incident handling starting with what's already in place.
- Ten steps to incident handling: incident detection, reporting, the quick appraisal, flaw identification, countermeasures, decide about contacting law enforcement, investigation, notification of related RTs, evidence collection, and closure.
- Chain of custody: correct evidence handling, dealing with law enforcement, search warrants; deciding when to contact law enforcement.
- Building an incident handling capability in-house and outside. People, places, equipment, procedures, authority. Who to notify and determining who is responsible for what. Defining ethical behavior for the incident handling team.
- Incident handling through role playing.
- Other resources: FIRST teams, law enforcement, mailing lists and newsgroups, archives, vendor notifications and expectations.

T2 Network Security Profiles: What Every Hacker Already Knows About You, and What To Do About It

Jon Rochlis and Brad Johnson, *SystemExperts Corp.*

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 based operating system or whether it is a router, firewall, or gateway network host.

There are four common stages to network-based host attacks: reconnaissance, target selection, exploitation, and cover-up. This course will review the tools and techniques hackers use in performing these types of activities. You will understand how to either be prepared for such attacks or how to stay one step ahead of them. Specifically, the course will focus on how to generate profiles of your systems remotely. 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 ICMP, SNMP, RPC, HTTP, SMTP) which support virtually all of the Internet applications—such as mail, 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 they are widely available and commonly used in these types of situations.

Topics include:

- Review of attack methodology: reconnaissance, target selection, exploitation, and cover-up
- Profiles: what does one look like
- Techniques: scanning, CERTs, hacking clubs
- Tools: *scotty*, *strobe*, SATAN, ISS, etc.
- Business exposures: integrity and confidentiality, audits, intrusion resolution
- Demos of some tools

T3AM Using Cryptography NEW

Bruce Schneier, *Counterpane Systems*

Who should attend: Those who need to understand what cryptography: does and how it works. I stress the engineering discipline, and do not assume a strong background in mathematics.

From encryption to digital signatures to electronic commerce to secure voting, cryptography has become the enabling technology that allows us to take existing business and social constructs and move them to computer networks. But a lot of cryptography is bad, and the problem with bad cryptography is that it looks just like good cryptography; most people cannot tell the difference. Security is a chain: only as strong as the weakest link.

This tutorial is about cryptography as it is used in the real world: the algorithms, the protocols, and the implementations. I'll stress the whats and the hows rather than the whys. People building (or using) cryptography need to understand what it can do and can't do, and that it's not the panacea it's often made out to be. Topics covered include:

- Basics of cryptography
- Symmetric cryptography: DES, triple-DES, IDEA, Blowfish, RC2, RC4, RC5, AES
- Public-key cryptography: encryption and digital signatures, RSA, Diffie-Hellman, ElGamal, DSA
- Hash functions and message authentication codes: MD4, MD5, SHA, CBC-MAC, HMAC, NMAC
- Random number generation
- Protocols: key exchange, authentication, secret sharing, key escrow, certificates, digital cash
- What cryptography can do for you
- What cryptography can't do for you

No single tutorial can teach someone to be a cryptographer. After completing this tutorial, participants will be intelligent consumers of cryptography. They will understand cryptography's building blocks, how those building blocks are put together to make cryptographic system, and what the limitations of the science are.

T4PM Cryptography for the Internet NEW

Bruce Schneier, *Counterpane Systems*

Who should attend: Those who need to understand how cryptography is used over the Internet to secure communications, establish authenticity, and provide for integrity. I stress the engineering discipline, and do not assume a strong background in mathematics.

Security is essential for business and social interactions, and the pre-computer world has developed many techniques to establish security: voice recognition on the telephone provides authentication, signatures on paper provide proof of intent, closed doors and walks in the park provide privacy, unforgeable currency provides for fairness. As more and more business and social interactions move onto the Internet, the challenge is to mirror these techniques as much as possible in this new world.

This tutorial shows how cryptography can help. By allowing for confidentiality, authentication, integrity, fairness, and many other things, cryptography can transform the Internet into a serious business tool. The Internet community has developed protocols to secure electronic mail, World Wide Web interactions, electronic commerce transactions, etc., which you will learn about.

After completing this tutorial, you will understand how cryptography is currently used on the Internet. You will be able to vigorously debate the pros and cons of different systems, and cause commotions at IETF meetings.

Topics include:

- Cryptography in a networked world
- Tools of Internet cryptography
- Threat modeling
- Email security: PGP, S/MIME
- Trust management: X.509, SDSI, SPKI
- IP security
- World Wide Web security
- Electronic commerce: Cybercash, Digicash, First Virtual, SET

About the Tutorial and Invited Talks Speakers

Steven M. Bellovin is the co-author of the recent book, *Firewalls and Internet Security: Repelling the WilyHacker*, and holds several patents on cryptographic protocols. He is a member of the Internet Architecture Board, and is currently focusing on how to write systems that are inherently more secure. Despite the fact that he has not changed jobs since joining AT&T Labs – Research in 1982, he is still working on networks, security, and why the two don't get along.


Jim Duncan

Jim Duncan is manager of Network and Information Systems and principal systems administrator for Pennsylvania State University's Applied Research Laboratory. He is a contributor to the Site Security Policy Handbook and has developed numerous policies, guidelines, and presentations on computer security, incident handling, and ethics. Jim is an active member of the Penn State CERT team.


Carl Ellison

Carl Ellison is a professional cryptographer who has been researching certification for over two years now. He is draft author for the IETF standard track certificate structure known as SPKI. In addition to his cryptography background, Carl has expertise in networking, operating systems, real time computer graphics, fault tolerance and digital signal processing.


Rik Farrow

Rik Farrow provides UNIX and Internet security consulting and training. He has been working with UNIX system security since 1984, and with TCP/IP networks since 1988. He is the author of *UNIX System Security* and *System Administrator's Guide to System V*. Farrow writes two columns for *;login:*, and a network security column for *Network* magazine.

About the Tutorial and Invited Talks Speakers


Daniel E. Geer, Jr.

Daniel E. Geer, Jr. is vice president of CertCo, LLC, a market leader in digital certification for electronic commerce. He has a long history in network security and distributed computing management as an entrepreneur, consultant, teacher and architect. He is a co-author of the recently-published *Web Security Sourcebook*.


Brad Johnson

Brad Johnson is a well-known authority in the field of distributed systems. He has participated in seminal industry initiatives like the Open Software Foundation, X/Open, and the IETF. At SystemExperts he has led numerous security probes for major companies, revealing significant unrealized exposures.


Arjen K. Lenstra

Arjen K. Lenstra's major research interest is computational number theory, in particular algorithms for factoring integers and computing discrete logarithms. He developed a portable toolkit for experimenting with cryptographic protocols; this software was used in 1994 to break the famous 1977 RSA-Challenge number. He is one of the co-developers of the recent number field sieve factoring algorithm.


Gary McGraw

Gary McGraw is a research scientist with a dual PhD in Cognitive Science and Computer Science. He recently completed *Java Security: Hostile Applets, Holes, & Antidotes* and *Software Fault Injection: Inoculating Programs Against Errors*. Dr. McGraw has published his research in over forty technical publications. He is principal investigator on grants from the National Science Foundation, Rome Labs, and the Defense Advanced Research Projects Agency (DARPA).


Alfred Menezes

Alfred Menezes is co-author of *Handbook of Applied Cryptography* and *Elliptic Curve Public Key Cryptosystems*. He is actively involved in cryptographic research, consults on a regular basis for Certicom Corp., and participates in IEEE and ANSI standards forums. He is a professor of mathematics at Auburn University.


Clifford Neuman

Clifford Neuman is a senior research scientist at the Information Sciences Institute of the University of Southern California (USC), a faculty member in the Computer Science Department at USC, and Chief Scientist for CyberSafe Corporation. Dr. Neuman's recent work includes the development of a security infrastructure supporting authorization, accounting, and the NetCheque® electronic payment system.


JoAnn Perry

JoAnn Perry was vice president and head of computer scurity for Goldman Sachs for eight years. During that time the organization was expanded to handle global issues with teams set up in London and Tokyo. JoAnn managed the expansion teams from the London office. She is currently a security consultant with her own firm.


Marcus Ranum

Marcus Ranum is CEO 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. 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*.


Jon Rochlis

Jon Rochlis is a senior consultant for SystemExperts Corp. He provides high level advice to businesses in the areas of network security, distributed systems design and management, high-availability, and electronic commerce. Before joining SystemExperts, Mr. Rochlis was engineering Manager with BBN Planet, a major national Internet service provider.


Avi Rubin

Avi Rubin is a senior technical staff member in the secure systems research department at AT&T Labs – Research and an adjunct professor of computer science at New York University where he teaches cryptography and computer security. His past research includes trusted distribution of software in hostile environments, one-time password schemes, key management, worldwide web security, anonymity and privacy, and formal methods for cryptographic protocol analysis. He is a co-author of the *Web Security Sourcebook*.


Shabbir J. Safdar

Shabbir J. Safdar is a senior member of the worldwide information security department at Goldman, Sachs & Co. He is responsible for building the GS CERT organization. He has also been active in working to obtain more favorable regulations regarding encryption for the industry.


Bruce Schneier

Bruce Schneier is president of Counterpane Systems, a cryptography and computer security consulting company. He is the author of *Applied Cryptography*, the seminal work in its field. He has written dozens of articles on cryptography for major magazines and designed the popular Blowfish encryption algorithm, still unbroken after years of cryptanalysis.

Security '98 Exhibition

Wednesday, January 28 12:00 noon–7:00 pm
Thursday, January 29 10:00 am–2:00 pm

- *See demonstrations of innovative solutions that will put you ahead in providing critically-needed security at your site.*
- *Enjoy the relaxed atmosphere where you can get in-depth answers from well-informed company representatives.*
- *Publishers and booksellers will be there to provide the latest print and software releases.*
- *Several companies will be recruiting or contracting employment.*

Questions About the Exhibition?
Contact Cynthia Deno
Phone: 408.335.9445
Email: *display@usenix.org*

Come See the Security Solutions Offered by:

Axent Technologies *www.axent.com*
BDM International Inc. *www.bdm.com*
CheckPoint Software Technologies, Inc. *www.checkpoint.com*
Computer Security Institute *www.gocsi.com*
Cygnus Support *www.cygnus.com*
InfoExpress, Inc. *www.infoexpress.com*
Information Security Institute *www.misti.com*
Information Systems Security Association *www.uhsa.uh.edu/issa*
IntelliSoft Corporation *www.isoft.com*
ISS (Internet Security Systems) *www.iss.net*
Miller Freeman, Inc. *www.mfi.com*
O'Reilly & Associates, Inc. *www.ora.com*
Platinum Technology, Inc. *www.platinum.com*
Prentice Hall PTR *www.prenhall.com*
RiskWatch, Inc. *www.riskguard.com*
SAGUS Security Inc. *www.sagus-security.com*
Secure Networks Inc. *www.securenetworks.com*
Symark Software *www.symark.com*
Technologic Software Concepts Inc. *www.technologic.com*
TimeStep Corporation *www.timestep.com*
Touch Technologies, Inc. *www.ttinet.com*
Trident Data Systems *www.tds.com*
WheelGroup Corporation *www.wheelgroup.com*
Wiley Computer Publishing *www.wiley.com*

Current participants as of October 15, 1997

FREE EXHIBIT HALL PASS — Be Our Guest

Please complete. Information is confidential.

Open: Wednesday, January 28, 12 noon–7 pm
Thursday, January 29, 10 am–2 pm
Location: Grand Ballroom, 3rd Floor Marriott River Center Hotel, 101 Bowie Street, San Antonio, TX, 210.223.1000

USE THIS PASS ONLY if you do not register for the Symposium's Tutorials or Technical Sessions. Please copy and share with your colleagues.
BRING THIS PASS to the Exhibits for FREE Admission.

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/bulletin board 3. ❑ *;login:*
4. ❑ Web 5. ❑ from a colleague 6. ❑ magazine 7. ❑ from a vendor

Name First Last

Company

Work Address

City State Zip Country

Telephone No. Fax

Email Address (1 only please)

❑ *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.*

Wednesday, Jan. 28

9:00am–10:30am

Opening Remarks

Avi Rubin, *AT&T Labs – Research*

Keynote Address: Security Lessons From All Over

Bill Cheswick, *Lucent Technologies, Bell Labs*

From a security viewpoint, there is little new about the Internet. The same security rules apply to the Internet, castles, walls, and even the immune system. We will explore a number of security lessons from many sources.

Bill Cheswick *logged into his first computer in 1969 and has worked on operating system security for more than 25 years. Since joining Bell Laboratories in 1987, he has worked on network security, PC viruses, mailers, the Plan 9 operating system, and kernel hacking. With Steve Bellovin, he co-authored the first full book on Internet security,* Firewalls and Internet Security, Repelling the Wily Hacker. *Cliff Stoll has called Ches "one of the seven avatars of the Internet." Ches's current work includes various Internet munitions, a new edition of the book, and maybe a way to hunt down anonymous denial-of-service attacks.*

10:30am–11:00am — Break

	Refereed Papers Track	Invited Talks Track
11:00am–Noon	**Architecture** Session Chair: Steve Bellovin, *AT&T Labs – Research* A Comparison of Methods for Implementing Adaptive Security Policies Brian Loe and Michael Carney, *Secure Computing Corporation* The CRISIS Wide Area Security Architecture Eshwar Belani, Amin Vahdat, Thomas E. Anderson, Michael Dahlin, *University of California at Berkeley*	**Invited Talk: The Security Product Market: Trends and Influences** Marcus Ranum, *Network Flight Recorder, Inc.* The computer security products market is expected to grow from a $100m/year market in 1995 to a $1b/year market by the year 2000. Such a magnitude in growth will trigger major changes in the industry. I will outline the main factors influencing different aspects of the security products market, and describe how those factors are likely to direct product and technology trends.
Noon–1:30pm	Lunch (on your own)	
1:30pm–3:30pm	**Intrusion Detection** Session Chair: Mike Reiter, *AT&T Labs – Research* Bro: A System for Detecting Network Intruders in Real-Time Vern Paxson, *Lawrence Berkeley National Laboratory* Cryptographic Support for Secure Logs on Untrusted Machines Bruce Schneier and John Kelsey, *Counterpane Systems* StackGuard: Automatic Adaptive Detection and Prevention of Buffer-Overflow Attacks Crispan Cowan, *Oregon Graduate Institute* Data Mining Approaches for Intrusion Detection Wenke Lee and Salvatore J. Stolfo, *Columbia University*	**Panel: Computer Security and Legal Liability** Moderator: Steve Bellovin, *AT&T Labs – Research* Because of buggy, vendor-supplied software, someone breaks into your site and causes damage. Who is liable? You? The hacker? The vendor? Some real live lawyers will try to answer this question. Panelists: Ed Cavazos, *Interliant Corporation* Others to be announced.
3:30pm–4:00pm	Break	
4:00pm–5:30pm	**Network Security** Session Chair: Dave Balenson, *Trusted Information Systems* Securing Classical IP Over ATM Networks Carsten Benecke and Uwe Ellermann, *Universitaet Hamburg, Fachbereich Informatik* A Java Beans Component Architecture for Cryptographic Protocols Pekka Nikander and Arto Karila, *Helsinki University of Technology* Secure Videoconferencing Peter Honeyman, Andy Adamson, Kevin Coffman, Janani Janakiraman, Rob Jerdonek, and Jim Rees, *CITI, University of Michigan*	**Invited Talk: Factoring: Facts and Fables** Arjen K. Lenstra, *Citibank, N.A.* In theory, the security of most Public Key Cryptosystems is based on the assumption that a number theoretical problem (such as integer factorization or computing discrete logarithms) is hard. In practice, when using Public Key Cryptosystems to secure Internet traffic for instance, the situation is not so clear. In this talk I will discuss various security assumptions and I will show how our credulity may lead to interesting business opportunities.

Refereed Papers Track

Invited Talks Track

Thursday, Jan. 29

8:30am–10:00am

Distributed Systems

Session Chair: Hilarie Orman, *DARPA/ITO*

Unified Support for Heterogeneous Security Policies in Distributed Systems
Victoria Ungureanu and Naftaly H. Minsky, *Rutgers University*

Operating System Protection for Fine-Grained Programs
Trent Jaeger, Jochen Liedtke, and Nayeem Islam, *IBM T.J. Watson Research Center*

Expanding and Extending the Security Features of Java
Karen R. Sollins and Nimisha V. Mehta, *MIT Laboratory for Computer Science*

Invited Talk: Elliptic Curves—Ready for Prime Time

Alfred Menezes, *Auburn University*

In this talk I will give a quick introduction to elliptic curve cryptosystems, discuss their advantages, mention recent work done on studying their security, and some of the implementations being done.

10:00am–10:30am — Break

10:30am–Noon

World Wide Web Security

Session Chair: Diane Coe, *Concept5 Technologies*

Towards Web Security Using PLASMA
A. Krannig, *Fraunhofer-Institute for Computer Graphics IGD*

Security of Web Browser Scripting Languages: Vulnerabilities, Attacks, and Remedies
Vinod Anupam and Alain Mayer, *Bell Labs, Lucent Technologies, Bell Labs*

Finite-State Analysis of SSL 3.0
John C. Mitchell, Vitaly Shmatikov, and Ulrich Stern, *Stanford University*

Invited Talk: Securing Electronic Commerce: Applied Computer Security or Just Common Sense

Clifford Neuman, *University of Southern California*

Internet commerce has made security critical and organizations finally recognize the need to provide security. Because electronic commerce often involves access to privileged data by customers, it is harder to secure these applications than traditional ones. Authentication, authorization, and encryption can be used to secure computers and communication channels, but there will always be vulnerabilities at the end points; attackers will break into the service provider's and end user's systems to steal or modify data. Once these basic security techniques have been applied, the greatest improvements in security can be obtained through the common sense technique of partitioning protected data so that authoritative and highly sensitive data is stored on computers that aren't directly connected to the internet. In this talk Dr. Neuman will describe the application of distributed system security techniques and data partitioning to the development electronic commerce applications.

Noon–1:30pm — Lunch (on your own)

1:30pm–3:00pm

Cryptography

Session Chair: Carlisle Adams, *Nortel*

Certificate Revocation and Certificate Update
Kobbi Nissim and Moni Naor, *Weizmann Institute of Science*

Attack-Resistant Trust Metrics for Public Key Certification
Raph Levien and Alex Aiken, *University of California at Berkeley*

Software Generation of Random Numbers for Cryptographic Purposes
Peter Gutmann, *University of Auckland*

Invited Talk: Real World Security Practices

JoAnn Perry, *Independent Consultant,* and Shabbir Safdar, *Goldman, Sachs & Co.*

You have completed testing and are ready to recommend the implementation of a near-perfect technical solution to a control issue in your company. How confident are you that your management will allocate the dollars and manpower for your project? Will management support the implementation with the end users? Effective security controls must meet business objectives. We will discuss how we have successfully achieved this. You will learn ways to form a close alliance with management and key people to assure that security objectives are met and supported.

3:00pm–3:30pm — Break

JOINT SESSION

3:30pm–5:00pm

Work-In-Progress Reports (WIPs)

The Works-In-Progress session will consist of five minute presentations. Speakers should submit a one or two paragraph abstract to *sec98wips@usenix.org* by January 15. Please include your name, affiliation, and the title of your talk. Please note this is a change from the original instructions in the Call for Papers. A schedule of presentations will be posted at the conference by Noon on January 29. Experience at other conferences has shown that most submissions are usually accepted. The five minute time limit will be strictly enforced.

USENIX Membership Information

About USENIX

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 grounds 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.

The USENIX Association
2560 Ninth Street, Suite 215
Berkeley, CA 94710
Phone: 510.528.8649
Fax: 510.548.5738
Email: *office@usenix.org*
Web: *http://www.usenix.org/*

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 can also send email to *office@usenix.org* or phone 510.528.8649. Visit our Web site: *http://www.usenix.org/*.

T H A N K Y O U

USENIX and SAGE Thank Their Supporting Members

USENIX Supporting Members

Adobe Systems Inc.
Advanced Resources
ANDATACO
Apunix Computer Services
Auspex Systems, Inc.
Boeing Company
Crosswind Technologies, Inc.
Digital Equipment Corp.
Earthlink Network, Inc.
Invincible Technologies Corp.
Lucent Technologies, Bell Labs
Motorola Research & Development
MTI Technology Corporation
Nimrod AS
O'Reilly & Associates, Inc.
Sun Microsystems, Inc.
Tandem Computers, Inc.
UUNET Technologies, Inc.

SAGE Supporting Members

Atlantic Systems Group
Digital Equipment Corp.
ESM Services, Inc.
Global Networking and Computing, Inc.
Great Circle Associates
Online Staffing
Sprint Paranet
Texas Instruments, Inc.
TransQuest Technologies, Inc.
UNIX Guru Universe

About SAGE

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

SAGE co-sponsors system and network administration conferences, publishes SAGE News in the Association's bimonthly magazine, conducts an annual system administration salary survey, fosters relationships with international affiliates, facilitates the work of regional system administration groups, and publishes an on-going series of practical booklets and resource guides covering topics of interest to system administrators.

Mark Your Calendar For These USENIX Events

3rd Workshop on Electronic Commerce
Aug. 31 – Sept. 3, 1998
Boston, MA

12th Systems Administration Conference (LISA '98)
December 6 – 11, 1998
Boston, MA

23rd USENIX Annual Technical Conference
June 15 – 19, 1998
New Orleans, LA

USENIX sponsors as many as ten refereed technical meetings every year!

Need detailed information? Visit our Web site: *www.usenix.org/events/event_calendar.html*

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

Magda De Jong, *Hewlett-Packard,* 1996 Symposium Attendee

"The Security 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.,* 1996 Symposium Attendee

Birds-of-a-Feather Sessions (BoFs)

Tuesday Evening

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. Schedule your BoF in advance by telephoning the USENIX Conference Office at 714.588.8649 or sending email to: *conference@usenix.org*.

Work-In-Progress Reports (WIPs)

Thursday, January 29 3:30pm–5:00pm

Submission deadline: *January 15, 1998*

Submissions to: *sec98wips@usenix.org*

The Works-in-Progress session will consist of five minute presentations. Speakers should submit a one or two paragraph abstract to *sec98wips@usenix.org* by January 15. Please include your name, affiliation, and the title of your talk. This is a change from the original instructions in the Call for Papers. A schedule of presentations will be posted at the conference by Noon on January 29. Experience has shown that most submissions are usually accepted. The five-minute time limit will be strictly enforced.

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/*, 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 510.528.8649, or send email to: *office@usenix.org*

Social Activities

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

There will be a Welcome Reception on Sunday evening, a luncheon on Monday and Tuesday for tutorial attendees, and a reception on Wednesday evening.

Special Event

Meet the Authors

Sponsored by Wiley Computer Publishing

The authors of these books, all speakers at the Symposium, will be available to meet, talk with, and sign copies of their books at the Symposium. Check the schedule on-site for the time and location of the booksigning. Books will be available for purchase at the conference.

Web Security Sourcebook
Avi Rubin, Daniel Geer, and Marcus Ranum

Java Security
Gary MacGraw and Edward Felten

The Electronic Privacy Papers
Bruce Schneier

Applied Cryptography
Bruce Schneier
"The classic reference in cryptography"
—New York Times

Hotel and Travel Information

Hotel Information

Hotel Discount Reservation Deadline:

→ Monday, January 5, 1998 ←

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

San Antonio Marriott Rivercenter
Bowie Street
San Antonio, TX 78205

Toll Free: 800.648.4462
Local Telephone: 210.223.1000
Reservation Fax: 210.554.6248

Single/Double Occupancy $142.00
(*plus state and local taxes, currently at 15%*)

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

Travel to San Antonio

Discount Air Fares

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

JNR, Inc.
Toll Free in US and Canada:
800.343.4546
Telephone: 714.476.2788

Airport to Hotel Transportation

The San Antonio Marriott Rivercenter is located 15 minutes from the San Antonio International Airport. Star Shuttle Service provides 24 hr. daily shuttle service every 15–30 minutes to all the downtown San Antonio hotels. Tickets must be purchased for $6.00 one way at the Star Shuttle Booth located near the baggage claim area. Reservations not required.

Taxi service costs approximately $13.50 one way. Four can ride for the price of one.

San Antonio Attractions

You can plan what to see and where to eat when you are not in conference sessions. Visit CityNet for restaurants, maps, and more: *http://city.net/countries/united_states/texas/san_antonio/*. Some of the most well-knwn sites include:

The Alamo—Perhaps the best-known site in Texas History.

Missions of San Antonio—Visit all four missions, which were started in the 18th century by Spanish priests, and are still active parish churches.

River Walk and Rivercenter Mall—Enjoy the charm and history of San Antonio by strolling along the River Walk. Enjoy the many outdoor cafes and hundreds of shops plus an IMAX theater adjoining the Marriott Rivercenter Hotel.

Zoological Gardens and Aquarium—One of the largest animal collections in the US.

Museums—Hertzberg Circus Collections; Institute of Texas Cultures; McNay Art Museum; San Antonio Museum of Art; Witte Museum.

Registration Information

Tutorial Fees (January 26–27)

Tutorial fees include:

- Admission to the tutorials you select
- Printed and bound tutorials materials for your selected courses
- Lunch
- Admission to the Vendor Exhibition

Early Registration deadline is January 5, 1998. After January 5, add $50 to the Tutorial fee.

To calculate your tutorial fees:

One half-day tutorial = 1 unit
One full-day tutorial = 2 units

To determine your total tutorial registration fee, add the total number of units you have selected and refer to the fee schedule shown below. A maximum of 2 units per day may be selected. The tutorials may be on different days if you wish, so long as there is no overlap (i.e. selecting two AM tutorials on the same day). Full-day tutorial classes cannot be split.

# Units Selected	*Tutorial Fee (until Jan. 5)*	*Tutorial Fee (after Jan. 5)*	*CEU Credit (optional)*
1 unit	$190.00	$240.00	$15.00
2 units	$335.00	$385.00	$15.00
3 units	$480.00	$530.00	$23.00
4 units	$620.00	$670.00	$30.00

Technical Sessions Fees (January 28–29)

Technical sessions fees include:

- Admission to all Technical Sessions
- Copy of the Symposium Proceedings
- Admission to Symposium Reception
- Admission to Vendor Exhibition

Early registration deadline is January 5, 1998. After January 5, add $50 to the Technical Sessions fee.

Registration	*Until Jan. 5*	*After Jan. 5*
Member*	$325	$375
Non-Member or Renewing Member**	$395	$445
Full-Time Student (Must provide copy of current student ID Card)	$ 75	$ 75

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

***Join USENIX or renew your membership. 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.

REFUND/CANCELLATION POLICY

If you must cancel, all refund requests must be in writing, with your signature, and postmarked no later than January 16, 1998. 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 information, contact:

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

Phone: 714.588.8649
Fax: 714.588.9706
Email: *conference@usenix.org*
Hours: M–F, 8:30 am–5:00 pm PST

Copy this form as needed. Type or print clearly.

Registration Form *USENIX Security Symposium '98 January 26–29, 1998*

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

Name First Last

First Name for Badge Member Number

Company / Institution

Mail Stop Mail Address

City State Zip Country

( ) ( )

Telephone No. Fax

Email Address (1 only please) *WWW*

Attendee Profile

Please help us serve you better. By answering the following questions, you help us plan our activities to meet members' needs. All 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/bulletin board 3. ❑ *;login:*
4. ❑ Web 5. ❑ from a colleague 6. ❑ magazine 7. ❑ vendor

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

REFUND/CANCELLATION POLICY If you must cancel, all refund requests must be in writing, with your signature, and postmarked no later than January 16, 1998. Telephone and email cancellations cannot be accepted. You may fax your cancellation or substitute another in your place. Call the conference office for details: 714.588.8649.

Payment must accompany this form

Payment (U.S. dollars only) must accompany this form. Purchase orders, vouchers, email, and telephone 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 either one full-day tutorial on each day or no more than one AM and one PM tutorial on each day. Full-day tutorials cannot be split. Check the box next to the tutorial(s) you wish to attend:

Carry total units to end of each column for each day.

Monday	Tuesday	
❑ M1 Security on the World Wide Web ❑ M2 Windows NT Security	❑ T1 Handling Computer and Network Security Incidents ❑ T2 Network Security Profiles: What Every Hacker Already Knows About You, and What To Do About It	*Full-day = 2 units*
❑ M3AM Certification: Identity, Trust, and Empowerment ❑ M4PM Towards Secure Executable Content: Java Security	❑ T3AM Using Cryptography ❑ T4PM Cryptography for the Internet	*Each Half-day class = 1 unit*
_____ units/day (max. 2)	_____ units/day (max. 2)	
	TOTAL UNITS (max 4): _____	

Tutorial Program Fee Schedule

Full-day = 2 units; Each Half-day class = 1 unit

*After January 5th add $50 to total fee	*Units*	*Tutorial Fee (until Jan. 5*)*	*CEU Fee (optional)*
	1 unit	$190.00	$15.00
	2 units	$335.00	$15.00
	3 units	$480.00	$23.00
	4 units	$620.00	$30.00

Tutorial Program Fees (Monday–Tuesday, Jan. 26–27)

Enter total tutorial fee from fee schedule above $ _____

CEU units surcharge from fee schedule above $ _____

Late fee applies if postmarked after Monday, January 5, 1998.....Add $50.00 $ _____

Technical Sessions Fees (Wednesday–Thursday, Jan. 28–29)

Current member fee..... $325.00 $ _____
(Applies to individual members of USENIX, EurOpen national groups, JUS, and AUUG)

Non-member fee* ..... $395.00 $ _____
*Join or renew your USENIX membership, AND attend the symposium for the same low price. Check here: ❑

Late fee applies if postmarked after Monday, January 5, 1998 ..... Add $50.00 $ _____

Full-time student** fee, pre-registered or on-site..... $75.00 $ _____

Full-time student** fee including USENIX membership fee..... $100.00 $ _____
***Students: Attach a photocopy of current student ID*

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: 714.588.8649 Fax: 714.588.9706

You may fax your registration form if paying by credit card. To avoid duplicate billing, please do not mail an additional copy.