11TH USENIX SECURITY SYMPOSIUM

Symposium at a Glance

Sunday, August 4

5:00 p.m.–8:00 p.m.	Registration
6:00 p.m.–8:00 p.m.	Welcome Get-Together

Monday, August 5

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

Tuesday, August 6

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

Wednesday, August 7

7:30 a.m.–5:00 p.m.	Registration
8:45 a.m.–10:30 a.m.	Opening Remarks, Awards, Keynote Address
11:00 a.m.–5:30 p.m.	Technical Sessions
7:00 p.m.–11:00 p.m.	Birds-of-a-Feather Sessions

Thursday, August 8

7:30 a.m.–5:00 p.m.	Registration
9:00 a.m.–5:30 p.m.	Technical Sessions
6:00 p.m.–8:00 p.m.	Symposium Reception
8:00 p.m.–11:00 p.m.	Birds-of-a-Feather Sessions

Friday, August 9

7:30 a.m.–12:00 p.m.	Registration
9:00 a.m.–2:00 p.m.	Technical Sessions
11:00 a.m.–12:30 p.m.	Work-in-Progress Reports
12:30 p.m.–2:00 p.m.	Closing Keynote Session

Important Date to Remember

Early Bird Registration & Hotel Discount Deadline: Wednesday, July 10, 2002

Contents

Art by Robin Jareaux

DAN BONEH

Symposium Organizers

Program Chair

Dan Boneh, *Stanford University*

Program Committee

Steve Bellovin, *AT&T Labs–Research*
Matt Blaze, *AT&T Labs–Research*
Drew Dean, *SRI International*
Kevin Fu, *M.I.T.*
Brian LaMacchia, *Microsoft Corporation*
Patrick Lincoln, *SRI International*
Vern Paxson, *ACIRI/ICSI*
Radia Perlman, *Sun Microsystems Laboratories*
Mike Reiter, *Bell Labs, Lucent*
Avi Rubin, *AT&T Labs–Research*
Adam Stubblefield, *Rice University*
Leendert van Doorn, *IBM T.J. Watson Research Center*
Wietse Venema, *IBM T.J. Watson Research Center*
Dan Wallach, *Rice University*
Bennet Yee, *University of California, San Diego*
Elizabeth Zwicky, *Counterpane Internet Security*

Invited Talks Coordinator

Dan Wallach, *Rice University*

An Invitation from the Program Chair

Dear Colleague,

The field of computer security is evolving at a phenomenal rate. New services, new systems, and new networking architectures continuously add new dimensions to the field and completely change previously held assumptions. This symposium addresses cutting-edge research ranging in topics from making ordinary programs more robust through protecting whole networks against worms and denial of service attacks.

Want to hear about new ideas for adding security hooks to software systems? Learn about sandboxing malicious applications? Understand how to secure new web services? Curious about privacy issues or dealing with law enforcement? Come to the 2002 USENIX Security Symposium and find out about these topics and many more.

Learn the latest techniques, best tools and effective strategies from the experts at our Security tutorials – over half of which are new including: Building Honey Pots, IPSs, Unix Security Solutions, Building Secure Software and others.

Keynote speaker Whitfield Diffie, co-inventor of public key cryptography and a distinguished engineer at Sun Microsystems, will talk about security policy and challenges for the 21st century.

From the Invited Talks, find out how common security systems fail; how to validate and test security designs; how to make biometrics authentication work; legal aspects of the DMCA; and much more.

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

Whether you're a researcher, a system administrator, or a policy wonk, come find out how computer security is going to affect you in the future.

We look forward to seeing you in San Francisco, August 5–9, 2002.

For the Security '02 Program Committee,

Dan Boneh, *Stanford University*
Program Chair

About USENIX/Symposium Activities

About USENIX & SAGE

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 and its members are engaged in problem-solving, in innovation, and in research that works.

About SAGE

http://www.sage.org/

SAGE, the System Administrators Guild, is a special technical group within USENIX. SAGE is dedicated to the recognition and advancement of the system administration profession.

Upcoming Events

16th Systems Administration Conference (LISA '02)

Sponsored by USENIX, The Advanced Computing Systems Association and SAGE, The System Administrators Guild

NOVEMBER 3–8, 2002, Philadelphia, PA, USA
Webite: *http://www.usenix.org/events/lisa02/*

5th Smart Card Research and Advanced Application (CARDIS '02)

Sponsored by USENIX
Co-sponsored by IFIP Working Group 8.8 (Smart Cards)

NOVEMBER 20–22, 2002, San Jose, CA, USA
Web site: *http://www.usenix.org/events/cardis02*

2nd Workshop on Industrial Experiences with Systems Software (WIESS '02)

Sponsored by USENIX
Co-sponsored by ACM SIGOPS in cooperation with IEEE TCOS

DECEMBER 8, 2002, Boston, MA, USA
Web site: *http://www.usenix.org/events/wiess02*

5th Symposium on Operating Systems Design and Implementation (OSDI '02)

Sponsored by USENIX
Co-sponsored by ACM SIGOPS in cooperation with IEEE TCOS

DECEMBER 9–11, 2002, Boston, MA, USA
Web site: *http://www.usenix.org/events/osdi02*

Symposium Activities

Birds-of-a-Feather Sessions (BoFs)

Tuesday, Wednesday, and Thursday evenings, August 6–8

Lead or attend a BoF! Meet with your peers! Present new work! Don't miss these special activities designed to maximize the value of your time at the conference. The always popular evening Birds-of-a-Feather sessions are very informal gatherings of persons interested in a particular topic. BoFs may be scheduled during the conference at the registration desk or in advance by contacting the USENIX Conference Dept. by email (bofs@usenix.org). BoFs are open to all attendees. Topics are announced at the conference.

Work-in-Progress Reports (WiPs)

Friday, August 9, 11:00 a.m.–12:30 p.m.

Short, pithy, and fun, Work-in-Progress Reports introduce interesting new or ongoing work. If you have work you would like to share or a cool idea that's not quite ready for publication, send a one- or two-paragraph summary to sec02wips@usenix.org. We are particularly interested in presenting students' work. A schedule of presentations will be posted at the conference, and the speakers will be notified in advance. Work-in-Progress reports are five-minute presentations; the time limit will be strictly enforced.

Social Get-Togethers

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

Sunday, August 4	
Welcome Get-Together	6:00 p.m.–8:00 p.m.
Thursday, August 8	
Symposium Reception	6:00 p.m.–8:00 p.m.

Tutorial Program at a Glance

MONDAY		TUESDAY	
M1	Building Secure Software NEW	T1	A Crash Course in SSL and TLS NEW
M2	Practical Wireless IP: Concepts, Administration, and Security	T2	Building Honey Pots for Intrusion Detection NEW
M3	UNIX Security Threats and Solutions NEW	T3	Cisco's Security Features: What They Are, Where to Use Them, How to Configure Them NEW
M4	Network Security Protocols and Current Standards NEW	T4	IPSec NEW

To meet your needs, the Tutorial Program at the USENIX Security Symposium provides in-depth, immediately useful instruction in the latest 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 '02 and take valuable skills back to your company or organization. **Register now to guarantee your first choice—seating is limited.**

TUTORIAL FEES INCLUDE:

- Admission to the tutorials you select
- Lunch
- Printed and bound tutorial materials from your sessions

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 other available tutorial immediately.

CONTINUING EDUCATION UNITS (CEUs)

USENIX provides Continuing Education Units 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 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 CEUs tudents. CEUs are not the same as college credits. Consult your employer or school to determine their applicability.

MONDAY, AUGUST 5, 2002

M1 Building Secure Software NEW

Gary McGraw, *Cigital*

Who should attend: Developers, architects, and managers charged with developing code for security-critical and mission-critical projects (e.g., code that is intended to live on the Net), and security practitioners who must grapple with software security issues such as code review and risk analysis. Participants should have some familiarity with software development. Code examples include C, Java, and Python. This tutorial is based on material found in the book *Building Secure Software*, published by Addison-Wesley in their Professional Computing series.

What do wireless devices, cell phones, PDAs, browsers, operating systems, network services, public key infrastructure, and firewalls have in common? The answer is "software." Software is everywhere, and it is not usually built to be secure. This tutorial explains why the key to proactive computer security is making software behave. With software complexity growing alarmingly—the source code base for Windows XP is 40 million lines—we have our work cut out for us. Clearly, the penetrate-and-patch approach is non-optimal. Even worse is bolting security mechanisms on as an afterthought. Building software properly, both at the design and the implementation level, is a much better approach. This tutorial takes an in-depth look at some common software security risks, including buffer overflows, race conditions, and random number generation, and goes on to discuss essential guidelines for building secure software. A risk-driven approach to software security which integrates analysis and risk management throughout the software lifecycle is the key to better computer security.

Topics include:

- Aligning security goals and software project goals
- Software risk management
- Performing risk analysis
- Integrating securing into the software lifecycle
- Code-scanning technology
- Common software security risks
- Design versus implementation risks
- Building software security capability
- Open source and security
- Guidelines for building secure software

Upon completion of this tutorial, participants will understand why software security is essential to any organization building Net-enabled software, how to avoid common security problems, and how to design more secure software.

Gary McGraw (M1) Cigital Inc.'s CTO, researches

software security and sets technical vision in the area of software risk management. Dr. McGraw is co-author of four popular books: *Java Security* (Wiley, 1996), *Securing Java* (Wiley, 1999), *Software Fault Injection* (Wiley 1998), and *Building Secure Software* (Addison-Wesley, 2001). He consults with major e-commerce vendors, including Visa, MasterCard, and the Federal Reserve, functions as principal investigator on several government grants, and serves on commercial and academic advisory boards. Dr. McGraw holds a dual Ph.D. in cognitive science and computer science from Indiana University and a B.A. in philosophy from UVa. He regularly contributes to popular trade publications and is often quoted in national press articles.

M2 Practical Wireless IP: Concepts, Administration, and Security

Philip Cox and Brad C. Johnson, *SystemExperts Corporation*

Who should attend: Users, administrators, managers, and others interested in learning about some of the fundamental security and usage issues around wireless IP services. This tutorial assumes some knowledge of TCP/IP networking and client/server computing, the ability or willingness to use administrative GUIs to set up a device, and a general knowledge of common laptop environments.

Whether you like it or not, wireless services are popping up everywhere. And you and your organization will be responsible for understanding and managing the devices you possess. Since the purpose of wireless is to share data when you aren't directly attached to a wired resource, you need to understand the fundamental security and usage options. In this tutorial we will cover a number of topics that affect you in managing and using wireless services. Some of the topics will be demonstrated live using popular wireless devices.

Topics include:

- Cellular services basics
  - What's out there?
  - Who's using what?
  - What really matters?
- Wireless LAN fundamentals
  - Architecture
  - Threats
  - 802.11b
  - Configuration examples
  - Antennas
- Access points
  - Channels, placement
  - Bandwidth, aggregation
  - Congestion
  - Roaming, signals
- General issues
  - Sniffers
  - Building your own access point
  - 802.11a

Philip Cox (M2) is a consultant with SystemExperts

Corporation. Phil frequently writes and lectures on issues of UNIX and Windows NT integration and on information security. He is the lead author of *Windows 2000 Security Handbook, 2nd Edition* (Osborne McGraw-Hill), a contributing author of *Windows NT/2000 Network Security* (Macmillan Technical Publishing), and a featured columnist in *;login: The Magazine of USENIX & SAGE*. He has served on numerous USENIX program committees. Phil holds a B.S. in computer science from the College of Charleston, South Carolina.

Brad C. Johnson (M2) is vice president of

SystemExperts Corporation. He has participated in the Open Software Foundation, X/Open, and the IETF, and has often published about open systems. Brad has served as a security advisor to organizations such as Dateline NBC and CNN. He is a frequent tutorial instructor and conference speaker on network security, penetration analysis, middleware, and distributed systems. He holds a B.A. in computer science from Rutgers University and an M.S. in applied management from Lesley University.

M3 UNIX Security Threats and Solutions NEW

Matt Bishop, *University of California, Davis*

Who should attend: Anyone interested in threats to UNIX security and how to deal with them.

This tutorial uses case histories to show what vulnerabilities the attackers exploited, how the system administrators might have closed those loopholes, and how the intruders were discovered. Concepts and mechanisms, as well as publicly available tools, are discussed. This course focuses on non-network problems.

Topics include:

- Security policies vs. security mechanisms
- Password security and cracking
- Files and auditing
- Access control mechanisms
- Management of privileges
- Malicious logic and the UNIX system
- Basic vulnerabilities analysis
- Basic incident management
- Security holes past and current
- Managing the humans
- Where to get help

Matt Bishop (M3) began working on problems of computer security, including the security of the UNIX operating system, at Purdue, where he earned his doctorate in 1984. He worked in industry and at NASA before becoming a professor, teaching courses in computer security, cryptography, operating systems, and software engineering at both Dartmouth College and the University of California at Davis, where he teaches now. Matt's current research interests are analyzing vulnerabilities in operating systems, protocols, and software in general; denial of service; intrusion detection; and formal models of access control.

M4 Network Security Protocols and Current Standards NEW

Radia Perlman, *Sun Microsystems*

Who should attend: Anyone who wants to understand the theory behind network security protocol design, with an overview of the alphabet soup of standards and cryptography. This tutorial is especially useful for anyone who needs to design or implement a network security solution, but it is also useful to anyone who needs to understand existing offerings in order to deploy and manage them. Although the tutorial is technically deep, no background other than intellectual curiosity and a good night's sleep in the recent past are required.

First, without worrying about the details of particular standards, we discuss the pieces out of which all these protocols are built.

We then cover subtle design issues, such as how secure email interacts with distribution lists, how designs maximize security in the face of export laws, and the kinds of mistakes people generally make when designing protocols.

Armed with this conceptual knowledge of the toolkit of tricks, we describe and critique current standards.

Topics include:

- What problems are we trying to solve?
- Cryptography
- Key distribution
  - trust hierarchies
  - public key (PKI) vs. secret key solutions
- Handshake issues
  - Diffie-Hellman
  - Man-in-middle defense
  - Perfect forward secrecy
  - Reflection attacks
- PKI standards
  - X.509
  - PKIX
- Real-time protocols
  - SSL/TLS
  - IPsec (including AH, ESP, and IKE)
- Secure email
- Web security
  - URLs
  - HTTP, HTTPs
  - Cookies

Radia Perlman (M4) is a Distinguished Engineer at Sun Microsystems. She is known for her contributions to bridging (spanning tree algorithm) and routing (link state routing) as well as security (sabotage-proof networks). She is the author of "Interconnections: Bridges, Routers, Switches, and Internetworking Protocols", and co-author of Network Security: Private Communication in a Public World", two of the top 10 Networking reference books, according to Network Magazine. She is one of the 25 people whose work has most influenced the networking industry, according to Data Communications Magazine. She has about 50 issued patents, an S.B. and S.M in mathematics and a Ph.D. in computer science from MIT and an honorary doctorate from KTH, the Royal Institute of Technology in Sweden.

TUESDAY, AUGUST 6, 2002

T1 A Crash Course in SSL and TLS NEW

Eric Rescorla, *RTFM Inc.*

Who should attend: Programmers, designers and architects who want to acquire an in-depth knowledge of SSL and TLS. Attendees should be familiar with TCP/IP. Familiarity with basic cryptography (encryption, public key, message digests, etc.) is desirable. We'll start with a brief primer on cryptography if a substantial portion of the class needs it.

This tutorial is an in-depth look at SSL and TLS. In this tutorial, we'll cram as much SSL/TLS knowledge into your head as possible in a single day. Topics covered will include:

Topics include:

- An in-depth look at the SSL handshake and its major variants
  - session resumption
  - client auth
  - export modes
- Data transfer and alerts
- Known attacks
- Performance
  - tuning
  - hardware acceleration
- Integrating SSL into protocols
  - generic philosophy
  - HTTPS
  - SMTP/TLS
- Programming with SSL
- The future of SSL/TLS

After completing this tutorial, you will know enough about SSL to be seriously dangerous to your friends, neighbors, and co-workers.

Eric Rescorla (T1) is Principal Engineer of RTFM, Inc., an independent security consulting firm. He has been working in Internet Security since 1993. He has been a member of the TLS working group from before the beginning and has written several commercial SSL implementations as well as the free Java toolkit PureTLS and the SSL protocol analyzer sslsdump. He is the author of "SSL and TLS: Designing and Building Secure Systems" (Addison-Wesley 2000) as well as the RFCs defining Secure-HTTP and HTTP over TLS.

T2 Building Honey Pots for Intrusion Detection NEW

Marcus Ranum, *NFR Security, Inc.*

Who should attend: System and network managers with administrative skills and a security background. The tutorial examples will be based on UNIX/Linux. While the materials may be of interest to a Windows/NT administrator, attendees will benefit most if they have at least basic UNIX system administration skills.

This class provides a technical introduction to the art of building honey pot systems for intrusion detection and burglar-alarming networks. Students completing this class will come away armed with the knowledge that will enable them to easily assemble their own honey pot, install it, maintain it, keep it secure, and analyze the data from it.

Topics include:

- Introduction
  - IDSes
  - Fundamentals of burglar alarms
  - Fundamentals of honey pots
  - Fundamentals of log-data analysis
  - Spoofing servers
- Overview of our honey pot's design
  - System initialization
  - Services
  - Spoofing server implementation walkthrough
  - Multiway address/traffic manipulation
  - Logging architecture: syslogs, XML logs, statistical processing
  - Simple tricks for information visualization
- Crunchy implementation details
  - How to write spoofing rules
  - How to write log filtering rules
- Management
  - How to get help in analyzing attacks
  - Keeping up to date

Auxiliary materials: Attendees will receive a bootable CD-ROM containing a mini UNIX kernel and preconfigured software, and will also have source-code access to the honey pot building toolkit. Attendees may also wish to review The Honeynet Project, eds., *Know Your Enemy: Revealing the Security Tools, Tactics, and Motives of the Blackhat Community* (Addison-Wesley, 2001).

Marcus Ranum (T2) is founder and CTO of NFR Security, Inc. He has been working in the computer/network security field for over 14 years and is credited with designing and implementing the first commercial Internet firewall product. Marcus also designed and implemented other significant security technologies, including the TIS firewall toolkit and the TIS Gauntlet firewall. As a researcher for ARPA, Marcus set up and managed the Whitehouse.gov email server. Widely known as a teacher and industry visionary, he has been the recipient of both the TISC Clue award and the ISSA lifetime achievement award. Marcus lives in Woodbine, Maryland, with his wife, Katrina, and a small herd of cats.

T3 Cisco's Security Features: What They Are, Where to Use Them, How to Configure Them NEW

John Stewart, *Digital Island, Inc.*

Who should attend: Network and system administrators running Cisco networks, and security professionals.

It's common knowledge that over 85% of all Internet traffic crosses a Cisco product at one time or another. Given this fact, it is obvious that improving security on Cisco products can improve the overall security of your site as well as the overall security of the Internet. However, the security features available in Cisco products can be a discipline in themselves. This class takes a nuts-and-bolts approach to deciding which Cisco security features to use, and when and where to use them. A sample network is used as the basis for the class. For each area, sample uses and actual configuration techniques are discussed.

Topics include:

- Perimeter Security
  - Cisco Access Control Lists (ACLs)
  - Lock and key
  - TCP intercept
  - Context-Based Access Control (CBAC)
  - Firewalling technologies compared and contrasted
  - PIX
  - IOS
- Access Lists revealed
  - Basic vs. extended
  - Where and how to use ACLs
  - Event logging
  - Per-user ACLs on dial-up ports
- Router-to-router security
  - Shared symmetrical application keys
  - Distributed Director
  - Remote access
  - Route authentication
- User security
  - Authentication, Authorization, Accounting (AAA)
  - TACACS
  - Fixed, OTP, SecureCard
  - RADIUS
  - Kerberos
- IPSec
  - Current standards update
  - Deploying IPSec with other technologies
  - ISAKMP/Oakley
  - Availability
  - Configuring and using IPSec
- Network Address Translation (NAT)
  - Hiding your company
  - Hiding your Web servers
  - Using NAT over dial-up
- VPN
  - VPDNs
  - GRE tunnels
  - Layer 2 Forwarding (L2F)
  - L2TP tunnels

John Stewart (T3) is responsible for investigating emerging technologies and helping to set future direction for Exodus, a Cable & Wireless Service. Previous to this position, Mr. Stewart was Digital Island's Chief Security Office. He also managed the core team and company-wide Security Council for auditing and adherence. As part of his involvement with the Center for Information Security (CIS), Mr. Stewart co-developed the Cisco Router Auditing Tool, an industry security analysis tool to help network administrators protect their Cisco routers, switches, and PIX firewalls. He serves on advisory boards for CloudShield, Tripwire Security, and hotU, Inc. Mr. Stewart holds a Master of Science degree in Computer and Information Science from Syracuse University, Syracuse, New York.

T4 IPSec NEW

John Ioannidis, *AT&T Labs;*
Angelos Keromytis, *Columbia University*

Who should attend: Network administrators, system managers, developers of network applications, and anyone interested in network security. Some familiarity with networking principles is required, but cryptography is not.

The IPSec protocol suite provides network-layer security for the Internet and is an IETF standard. It is already widely used to implement Virtual Private Networks (VPNs), and is beginning to make its way into commercial implementations of desktop operating systems. This tutorial covers every feature of IPSec and its key management protocol, IKE, gives many real-life examples drawn from a variety of environments and operating systems, and aims to clear a lot of myths and misunderstandings about IPSsec.

Topics include:

- Justification of network-layer security
- Encapsulation, tunneling, and overlay networks
- The IPSec transforms (ESP and AH)
- Transport and tunnel modes
- Key management
- IKE, the Internet Key Exchange protocol
- Interaction between IPSec/IKE and firewall/NAT boxes
- Examples
- Performance considerations (software and hardware)
- Comparison with TLS/SSL
- About PKIs
- Miscellaneous topics
- Future developments
  - Policy
  - Additional Key Management protocols

John Ioannidis (T4) is a researcher at AT&T Labs – Research. He has been contributing in the IETF for over 10 years, and has been with the IPsec effort since the very beginning, and wrote the first SunOS, BSD and Linux implementations. He has also worked on policy mechanisms for IPsec, and more recently on JFK, a proposed successor to the Internet Key Exchange protocol. His many research interests include security of large distributed systems, wireless and mobile networking, micropayment systems, and high-speed network monitoring.

Angelos Keromytis (T4) is an Assistant Professor of Computer Science at Columbia University. He has been working on IPsec since 1995, both in defining and refining the standards in the IETF, and in implementing and measuring its performance. He developed the OpenBSD IPsec stack, and wrote the first free implementations of the Photuris and IKE key management protocols for IPsec. More recently, he has been working on a proposed successor to IKE, named JFK, and has designed and implemented a cryptographic acceleration framework for IPsec (and other cryptography-heavy applications). His other research interests include scalable access control mechanisms, security policy composition and enforcement, and distributed system virtualization.

Refereed Papers | Invited Talks

WEDNESDAY

8:45 AM–10:30 AM

Opening Remarks, Awards, and Keynote

Keynote Address: Information Security in the 21st Century

Whitfield Diffie, *Distinguished Engineer at Sun Microsystems*

Although its origins may be ancient, the first component of information security, communication security, was so expanded by the First World War that we might reasonably count its birth from that event. The second component, computer security, appeared with shared, on-line computer use in the 1960s. Now, in the early 21st century, many of the problems that plagued information security in the 20th century have receded, while others have expanded or changed. We will assess the field inherited from the past century and look at its prospects for the future.

10:30 AM–11:00 AM Break

11:00 AM–12:30 PM

OS Security

Security in Plan 9
Russ Cox, *MIT LCS*; Eric Grosse, *Bell Labs*; Rob Pike, *Bell Labs;* Dave Presotto, *Avaya Labs and Bell Labs;* Sean Quinlan, *Bell Labs*

Linux Security Modules: General Security Support for the Linux Kernel
Chris Wright and Crispin Cowan, *WireX;* Stephen Smalley, *NAI Labs;* James Morris, *Intercode Pty.;* Greg Kroah-Hartman, *IBM*

Using CQUAL for Static Analysis of Authorization Hook Placement
Xiaolan Zhang, Antony Edwards, and Trent Jaeger, *IBM Research*

Wireless Access Point Mapping

Simon D. Byers, *AT&T Labs—Research*

This talk relates our experiences in 2.4 GHz wireless AP mapping, giving a broad sweep through various motivations, implementations, analyses, and applications. This includes practical description of software, hardware, antennae, and other devices that we have found useful to interact with and measure wireless devices. We employ a very hands-on philosophy in our work and the talk. Given the current explosion in wireless deployment, formal research in this area has come to be important. This talk will attempt to illustrate some of our directions.

12:30 PM–2:00 PM Lunch (on your own)

2:00 PM–3:30 PM

Intrusion Detection/Protection

Using Text Categorization Techniques for Intrusion Detection
Yihua Liao, V. Rao Vemuri, *University of California at Davis*

Detecting Manipulated Remote Call Streams
Jonathon Giffin, Somesh Jha, Bart Miller, *University of Wisconsin, Madison*

Type-Assisted Dynamic Buffer Overflow Detection
Kyung-Suk Lhee, Steve J. Chapin, *Syracuse University*

Freedom to Tinker

Ed Felten, *Princeton University*

"Freedom to Tinker" is the freedom to understand, discuss, repair, and improve the technological devices you own. This freedom, which has been eroded by recent changes in market practices and the law, is the organizing principle behind an increasing political and legal awareness among technologists. In this talk, Professor Felten will outline the ideas behind the freedom to tinker movement, using examples drawn from the current battles over copy protection.

Refereed Papers

Invited Talks

3:30 PM–4:00 PM Break

4:00 PM–5:30 PM

Access Control

A General and Flexible Access-Control System for the Web
Lujo Bauer, Michael Schneider, Ed Felten, *Princeton University*

Access and Integrity Control in a Public-Access High-Assurance Configuration Management System
Jonathan S. Shapiro and John Vanderburgh, *Systems Research Laboratory Johns Hopkins University*

Biometric Authentication Technologies: Hype Meets the Test Results

James L. Wayman, *Director, Biometric Test Center, San Jose State University*

Biometric authentication is automatic identification or identity verification based on behavioral and physiological characteristics. Its potential for securing financial transactions and controlling physical access has been recognized for over 40 years, but adoption has been considerably slower than predicted. One reason for this has been the unrealistic performance expectations placed on the technologies by both vendors and users. This talk will discuss biometric technologies and applications, performance metrics, and the results of the last 10 years of pilot projects and independent testing. We will explore what has worked, what hasn't, and why, with particular emphasis on the impact of biometrics on privacy.

THURSDAY

9:00 AM–10:30 AM

Hacks/Attacks

Deanonymizing Users of the SafeWeb Anonymizing Service
David Martin, *Boston University*; Andrew Schulman, *Software Litigation Consultant*

VeriSign CZAG: Privacy Leak in X.509 Certificates
Scott Renfro, *Yahoo! Inc.*

How to Own the Internet in Your Spare Time
Stuart Staniford, *Silicon Defense;* Vern Paxson, *ICIR / ICSI*

Network Telescopes: Observing Small or Distant Security Events

David Moore, *CAIDA, San Diego Supercomputer Center*

A network telescope is a portion of routed IP address space on which little or no legitimate traffic exists. Monitoring unexpected traffic arriving at a network telescope yields a view of certain remote network events. Among the visible events are various forms of flooding DoS attacks, infection of hosts by Internet worms, and network scanning. In this presentation, we'll examine questions such as: How large should my network telescope be? How well can one go backwards from a local view to an estimate of the global phenomenon? How big (in packets sent) or long (in duration) must an event be to be seen? What can I see from my own backyard telescope?

10:30 AM–11:00 AM Break

11:00 AM–12:30 PM

Sandboxing

Setuid Demystified
Hao Chen, David Wagner, *UC Berkeley;* Drew Dean, *SRI International*

Secure Execution Via Program Shepherding
Vladimir Kiriansky, Derek Bruening, Saman Amarasinghe, *MIT*

A Flexible Containment Mechanism for Executing Untrusted Code
David S. Peterson, *University of Cailfornia at Davis;* Matt Bishop, Raju Pandey, *University of California at Davis*

Illusions of Security

Paul Kocher, *Cryptography Research, Inc.*

For years, the standard yardstick for measuring cryptographic security has been key length. Unfortunately, real adversaries lack the propriety to limit themselves to tidy attacks such as brute force, factoring, and differential cryptanalysis. Worse, Moore's Law is driving vendors to build systems of exponentially increasing complexity without making security experts exponentially smarter to compensate. The resulting products have a minuscule chance of being extremely secure, and a large chance of being critically flawed. This talk will review basic engineering approaches that can improve assurance and will show how evaluators and attackers break overly complex, poorly tested designs.

Refereed Papers

Invited Talks

12:30 PM–2:00 PM LUNCH (ON YOUR OWN)

2:00 PM–3:30 PM

WEB SECURITY

SSLACC: A Clustered SSL Accelerator
Eric Rescorla, *RTFM, Inc.;* Adam Cain, *Nokia Inc.;* Brian Korver, *Xythos Software, Inc.*

Infranet: Circumventing Web Censorship and Surveillance
Nick Feamster, Magdalena Balazinska, Greg Harfst, Hari Balakrishnan, David Karger, *MIT Laboratory for Computer Science*

Trusted Paths for Browsers: An Open-Source Solution to Web Spoofing
Zishuang (Eileen) Ye, Sean Smith, *Dartmouth College*

FORMAL METHODS AND COMPUTER SECURITY

John C. Mitchell, *Stanford University*

Formal methods are variously considered to be arcane, tedious, and oblivious to practical concerns. However, such techniques as specification, type checking, proofs of correctness, and model checking, offer the power to analyze system properties under many or even infinitely many possible inputs and execution conditions without running an implemented system through all of the associated test cases. This talk will summarize some of the successful applications of formal methods for security problems such as protocol analysis, mobile code security, access control, and rights specifications.

3:30 PM–4:00 PM BREAK

4:00 PM–5:30 PM

GENERATING KEYS AND TIMESTAMPS

Toward Speech-Generated Cryptographic Keys on Resource Constrained Devices
Fabian Monrose, *Bell Labs, Lucent Technologies;* Michael K. Reiter, *Carnegie Mellon University;* Qi Li, Daniel P. Lopresti, Chilin Shih, *Bell Labs, Lucent Technologies*

Secure History Preservation through Timeline Entanglement
Petros Maniatis, Mary Baker, *Computer Science Department, Stanford University*

"HOW COME WE STILL DON'T HAVE IPSEC, DAMMIT?"

John Ioannidis, *AT&T Labs—Research*

It has been over ten years since the IPSec effort was started at the IETF, and the question of why it is still not a universally deployed protocol has been haunting us for about half that time. I shall talk about what has gone wrong (as well as what has gone right) for IPSec, how SSL/TLS and SSH have affected the development and deployment of IPSec, why IPSec is still viewed as good only for VPNs, and other popular myths. I shall not point too many fingers (eight, plus two thumbs, will be enough); I *will* try to explore, however, what has to happen in the next couple of years in order to see the desired widespread deployment of the protocol.

Refereed Papers

Invited Talks

FRIDAY

9:00 AM–10:30 AM

Deploying Crypto

Lessons Learned in Implementing and Deploying Crypto Software
Peter Gutmann, *University of Auckland*

Side-Channel Attacks on Symmetric Encryption Schemes: The Case for Authenticated Encryption
John R. Black and Hector Urtubia, *University of Nevada, Reno*

Making Mix Nets Robust For Electronic Voting By Randomized Partial Checking
Markus Jakobsson, Ari Juels, *RSA Labs;* Ron Rivest, *MIT*

Implications of the DMCA Anti-Circumvention for Security, Research, and Innovation

Pam Samuelson, *University of California at Berkeley*

The Digital Millennium Copyright Act of 1998 makes it illegal to circumvent access controls and to make or distribute circumvention technologies. It contains exceptions to enable legitimate computer security research, computer security testing, and interoperability among programs. This talk will look closely at the exceptions and at the DMCA caselaw to determine whether they adequately balance the interests of copyright owners and of follow-on innovators and researchers. It will also consider whether the U.S. Constitution may limit the application of the DMCA to some research- and innovation-related activities.

10:30 AM–11:00 AM **Break**

11:00 AM–12:30 PM

Work-in-Progress Reports (WiPs)

Short, pithy, and fun, Work-in-Progress Reports introduce interesting new or ongoing work, and the USENIX audience provides valuable discussion and feedback. A schedule of presentations will be posted at the Symposium. See page 4 for submission instructions.

Registration, Hotel, and Travel Information

Registration Information

Early Bird Registration Deadline: Wednesday, July 10, 2002

Save Up to $100: Register on the Web

TUTORIAL FEES (AUGUST 5–6)

Tutorial registration fees include:

- Admission to the tutorials you select
- Lunch
- Printed tutorial materials for your courses

Select only one tutorial per day.

Members/Nonmembers

Per day	$600
Multi-day discount:	$100
Two days	$1100
CEU credit (optional)	$15/day

After July 10, add $150 to the tutorial fee.

TECHNICAL SESSIONS FEES (AUGUST 7–9)

Technical sessions registration fees include:

- Admission to all technical sessions
- Free USENIX T-shirt
- Copy of Symposium Proceedings
- Admission to the Symposium Reception

Early Bird Registration Fees (before July 10)

Member*	$645
Nonmember**	$745
Student	$100

After July 10, members and nonmembers add $150 to the technical sessions fee.

** The member fee applies to current members of USENIX, EurOpen.SE, and NUUG.*
*** The nonmember fee includes a free one-year membership in the USENIX Association.*

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

Student Discounts & Stipends

TECHNICAL SESSIONS

USENIX offers full-time students a special discount rate of $100 for its technical sessions. You must include a copy of your current student I.D. card with your registration. This special fee is not transferable.

STUDENT STIPENDS

The USENIX student stipend program covers travel, hotel, and registration fees to enable full-time students to attend USENIX meetings. Application information is posted on comp.org.usenix 6–8 weeks before the conference, and is also available on the Web at *http://www.usenix.org/students/stipend.html*.

Symposium Services

SYMPOSIUM PROCEEDINGS

One copy of the Proceedings is included with your technical sessions registration fee. Additional copies may be purchased at the symposium. To purchase copies after the symposium, email orders@usenix.org or visit us on the Web at http://www.usenix.org/publications/ordering/.

INTERNET CONNECTIVITY

USENIX is pleased to offer Internet connectivity and a terminal room at the Security Symposium. The terminal room will be furnished with PCs running OpenBSD, drops for you to connect your laptop to our switches, and 802.11b wireless connectivity.

During the tutorials there will be limited hours of operation covering peak times. On Wednesday and Thursday we will be open from 7 a.m. until midnight, except for all-inclusive symposium functions such as the Opening Session and the Symposium Reception. We will close on Friday at 12:30 p.m. If you are interested in volunteering to work in the terminal room in exchange for free registration for the technical sessions, please contact Lynda McGinley at mcginley@usenix.org.

Hotel and Travel Information

Hotel Discount Reservation Deadline: Wednesday, July 10, 2002

USENIX has negotiated special rates for attendees at the 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.

San Francisco Marriott
55 Fourth St.
San Francisco, CA 94103
Toll-free: 1.800.228.9290
Local telephone: 1.415.896.1600

Room Rates
Single/double: $215.00
(plus local and state taxes, currently 14.5%)

Note: All requests for hotel reservations made after the July 10 deadline (or after the room block is sold out) will be handled on a space-available basis at the hotel's standard rate. You are encouraged to make your reservations as soon as possible in order to get the special discount rate.

Need a Roommate?
Usenet facilitates room-sharing. If you wish to share a room, post to and check *comp.org.usenix.roomshare*.

DISCOUNT AIRFARES

Special airfares with discounts of 5–10% have been negotiated with United Airlines. Contact United directly at 1.800.521.4041 and refer to Meeting ID number 510Ch.

TRANSPORTATION

San Francisco: SFO is approximately 25 minutes (13 miles) from the Marriott. Please visit http://www.flysfo.com/ for more information about transportation service to and from SFO.

Oakland: The Oakland airport (OAK) is approximately 35 minutes (19 miles) from the Marriott. Please visit http://www.oaklandairport.com/ for more information about transportation service to and from the Oakland airport.

BART: The nearest BART station is at Powell street, one block north of the Marriott.

PARKING

Valet parking is offered at the Marriott for $35, including in-and-out privileges. Self-parking is available near the Marriott at the Fifth and Mission Parking Garage, at $18.00 per day, *without* in-and-out privileges.

Registration Questions?

USENIX Conference Department
2560 Ninth St., Suite 215
Berkeley, CA 94710
Phone: 1.510.528.8649
Fax: 1.510.548.5738
Email: conference@usenix.org

Refund & Cancellation Policy

Substitutions are welcome at any time. If you must cancel: All refund requests must be in writing, postmarked no later than Monday, July 29, 2002. You may fax or email your cancellation, but telephone cancellations cannot be accepted.

Registration Form Security '02 August 5–9, 2002

Copy this form as needed. Type or print clearly.

This address will be used for all USENIX mailings unless you notify us in writing.

First name | Last name | First Name for Badge

Job Title | Member Number

Company/Institution

Mail Stop | Mail Address

City | State | Zip | Country

Telephone No. | Fax

Email Address (one only, please) | Priority Code*

*Your Priority Code appears just above the address on the mailing label of this brochure.

Attendee Profile

Would you like to receive email about USENIX activities? ❑ Yes ❑ No

Would you like us to provide your name to carefully selected partners? USENIX does not sell its mailing lists. ❑ Yes ❑ No

Would you like to be included on the Attendee list? ❑ Yes ❑ No

Would you like information about onsite child care? ❑ Yes ❑ No

What is your affiliation (check one):

1. ❑ academic 2. ❑ commercial 3. ❑ gov't 4. ❑ R&D 5. ❑ consultant

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 10. ❑ other

How did you *first* hear about this meeting (check one):

1. ❑ Conference brochure 2. ❑ Email from USENIX
3. ❑ USENIX/SAGE Web site 4. ❑ Newsgroup
5. ❑ Local user group 6. ❑ *UnixReview.com* 7. ❑ Ad in *Info Security*
8. ❑ Ad in *SC Security Magazine* 9. ❑ Colleague

What publications or Web sites do you read related to the topics of this conference? _____

Payment Must Accompany This Form

Payment (U.S. dollars only) must accompany this form. Purchase orders, vouchers, email, or 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

You may fax your registration form to 1.510.548.5738 if paying by credit card. To avoid duplicate billing, please do not mail an additional copy.

Tutorial Program *(Monday–Tuesday, August 5–6)*

Select only one tutorial per day (9:00 a.m.–5:00 p.m.)

Monday, August 5

❑ M1 Building Secure Software
❑ M2 Practical Wireless IP: Concepts, Administration, and Security
❑ M3 UNIX Security Threats and Solutions
❑ M4 Network Security Protocols and Current Standards

Tuesday, August 6

❑ T1 A Crash Course in SSL and TLS
❑ T2 Building Honey Pots for Intrusion Detection
❑ T3 Cisco's Security Features
❑ T4 IPSec

EARLY BIRD TUTORIAL FEES (until July 10)

$600.00 per day ..... $_____
Multi-day Discount: Deduct $100.00 for 2 days: $1100 total $_____
CEU fee (optional) .....$15.00 per day $_____

LATE FEE (after July 10)

Add $150 to the above rates if registering after July 10.... $_____

Technical Program *(Wednesday–Friday, August 7–9)*

EARLY BIRD REGISTRATION (until July 10)

Current member fee ..... $645.00 $_____
(applies to individual members of USENIX, EurOpen.SE, and NUUG)
Non-member fee (includes FREE one-year membership) $745.00 $_____
I do ***NOT*** wish to join USENIX at this time (check here): ❑

LATE FEE (after July 10)

Add $150 to the above rates if registering after July 10.... $_____

SPECIAL STUDENT RATE $100.00

$_____
**Students: Attach a photocopy of current student I.D.*

Membership Renewal

Renew your USENIX membership..... $100.00 $_____

STUDENTS:
Join USENIX or renew your student membership..... $30.00 $_____
**Students: Attach a photocopy of current student I.D.*

TOTAL DUE $_____

Refund & Cancellation Policy

Substitutions are welcome at any time.
If you must cancel: All refund requests must be in writing, postmarked no later than Monday, July 29, 2002.
You may fax or email your cancellation, but telephone cancellations cannot be accepted.

PLEASE COMPLETE THIS FORM AND RETURN IT, ALONG WITH FULL PAYMENT, TO:

USENIX Conference Department
2560 Ninth Street, Suite 215
Berkeley, CA 94710