

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

# 13<sup>th</sup> USENIX SECURITY SYMPOSIUM

August 9-13, 2004  
San Diego, CA USA

Cutting-Edge Security Developments from Industry Experts

Join us in San Diego for the latest advances in computer system security. In addition to the in-depth tutorials and informative invited talks and refereed papers, keynote speaker William "Earl" Boebert of Sandia National Laboratories will remind us how far we've gone—and yet how little we've actually progressed—since the early days of Multics. Register today for insight into the newest security developments.

## SYMPOSIUM ORGANIZERS

### Program Chair

Matt Blaze, *University of Pennsylvania*

### Program Committee

Bill Aiello, *AT&T Labs—Research*

Tina Bird, *Stanford University*

Drew Dean, *SRI International*

Carl Ellison, *Microsoft*

Eu-Jin Goh, *Stanford University*

Sotiris Ioannidis, *University of Pennsylvania*

Angelos Keromytis, *Columbia University*

Patrick McDaniel, *AT&T Labs—Research*

Adrian Perrig, *Carnegie Mellon University*

Niels Provos, *Google*

Greg Rose, *Qualcomm*

Sean Smith, *Dartmouth College*

Leendert van Doorn, *IBM Research*

Paul van Oorschot, *Carleton University*

Dave Wagner, *University of California, Berkeley*

Rebecca Wright, *Stevens Institute of Technology*

### Invited Talks Co-Chairs

Vern Paxson, *ICSI*

Avi Rubin, *Johns Hopkins University*

## IN-DEPTH TUTORIALS

- **Building a Software Security Capability: How to Foster Best Practices in Software Security**

Gary McGraw, *Digital*

- **Intrusion Detection and Prevention Systems**

Marcus Ranum, *Trusecure Corp.*

- **Malicious Cryptography**

Moti Yung, *Columbia University*

- **Network Security Assessments Workshop**

David Rhoades, *Maven Security Consulting, Inc.*

- **Network Security Monitoring with Open Source Tools**

Richard Bejtlich, *TaoSecurity*

- **Network Security Profiles: Protocol Threats, Intrusion Classes, and How Hackers Find Exploits**

Brad Johnson, *SystemExperts Corp.*

- **Network Security Protocols: Theory and Current Standards**

Radia Perlman, *Sun Microsystems*

- **System Log Aggregation, Statistics, and Analysis**

Marcus Ranum, *Trusecure Corp.*

SPONSORED BY

# USENIX

THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

Register Online by July 16, 2004, and Save!

[www.usenix.org/sec04](http://www.usenix.org/sec04)

# SECURITY '04 TECHNICAL SESSIONS

WEDNESDAY, AUGUST 11 – FRIDAY, AUGUST 13

## WEDNESDAY, AUGUST 11

9:00 a.m.–10:30 a.m.

### OPENING REMARKS, AWARDS, KEYNOTE

#### Keynote Address: Back to the Future

William "Earl" Boebert, *Sandia National Laboratory*

11:00 a.m.–12:30 p.m.

### REFEREED PAPERS: ATTACK CONTAINMENT

#### A Virtual Honeypot Framework

Niels Provos, *Google, Inc.*

#### Collapsar: A VM-Based Architecture for Network Attack Detention Center

Xuxian Jiang and Dongyan Xu, *Purdue University*

#### Very Fast Containment of Scanning Worms

Nicholas Weaver, *International Computer Science Institute*; Stuart Staniford, *Silicon Defense*; Vern Paxson, *International Computer Science Institute and Lawrence Berkeley National Laboratory*

### INVITED TALKS

#### RFID: Security and Privacy for Five-Cent Computers

Ari Juels, *Principal Research Scientist, RSA Laboratories*

2:00 p.m.–3:30 p.m.

### PANEL: CAPTURE THE FLAG

Moderator: Tina Bird, *Stanford University*

Panelists: Major Ronald Dodge, *United States Military Academy*; Marc Dougherty, *Northeastern University*; Chris Eagle, *Naval Postgraduate School*; Riley Eller, *Special Projects Manager, CoCo Communications Corp.*

### INVITED TALKS

#### Fighting Computer Virus Attacks

Peter Szor, *Chief Researcher, Symantec Corporation*

4:00 p.m.–5:30 p.m.

### REFEREED PAPERS: PROTECTING SOFTWARE I

#### TIED, LibsafePlus: Tools for Dynamic Buffer Overflow Protection

Kumar Avijit, Prateek Gupta, and Deepak Gupta, *IIT Kanpur*

#### Privtrans: Automatically Partitioning Programs for Privilege Separation

David Brumley and Dawn Song, *Carnegie Mellon University*

#### Avfs: An On-Access Anti-Virus File System

Yevgeniy Miretskiy, Abhijith Das, Charles P. Wright, and Erez Zadok, *Stony Brook University*

### INVITED TALKS

#### I Voted? How the Law Increasingly Restricts Independent Security Research

Cindy Cohn, *Legal Director, Electronic Frontier Foundation*

## THURSDAY, AUGUST 12

9:00 a.m.–10:30 a.m.

### REFEREED PAPERS: PROTECTING SOFTWARE II

#### Side Effects Are Not Sufficient to Authenticate Software

Umesh Shankar, Monica Chew, and J.D. Tygar, *UC Berkeley*

#### On Gray-Box Program Tracking for Anomaly Detection

Debin Gao, Michael K. Reiter, and Dawn Song, *Carnegie Mellon University*

#### Finding User/Kernel Pointer Bugs with Type Inference

Rob Johnson and David Wagner, *UC Berkeley*

11:00 a.m.–12:30 p.m.

### REFEREED PAPERS: THE HUMAN INTERFACE

#### Graphical Dictionaries and the Memorable Space of Graphical Passwords

Julie Thorpe and Paul van Oorschot, *Carleton University*

#### On User Choice in Graphical Password Schemes

Darren Davis and Fabian Monrose, *Johns Hopkins University*; Michael K. Reiter, *Carnegie Mellon University*

#### Design of the EROS Trusted Window System

Jonathan S. Shapiro, John Vanderburgh, and Eric Northup, *Johns Hopkins University*; David Chizmadia, *Promia Inc.*

11:00 a.m.–12:30 p.m. (continued)

### INVITED TALKS

#### Exploiting Software

Gary McGraw, *Cigital*

2:00 p.m.–3:30 p.m.

### PANEL: PATCH MANAGEMENT

Moderator: Patrick McDaniel, *AT&T Research*

Panelists: Crispin Cowan, *Immunix*; Bob Cowles, *Stanford Linear Accelerator*; Eric Schultz

### INVITED TALKS

#### Military Strategy in CyberSpace

Stuart Staniford, *Nevis Networks*

4:00 p.m.–6:00 p.m.

### REFEREED PAPERS: SECURITY ENGINEERING

#### Copilot, a Coprocessor-based Kernel Runtime Integrity Monitor

Nick L. Petroni, Jr., Timothy Fraser, Jesus Molina, William A. Arbaugh, *University of Maryland*

#### Fixing Races for Fun and Profit

Drew Dean, *SRI International*; Alan Hu, *University of British Columbia*

#### Network-in-a-Box: How to Set Up a Secure Wireless Network in Under a Minute

Dirk Balfanz, Glenn Durfee, Rebecca E. Grinter, Diana K. Smetters, and Paul Stewart, *PARC*

#### Design and Implementation of a TCG-based Integrity Measurement Architecture

Reiner Sailer, Xiaolan Zhang, Trent Jaeger, and Leendert van Doorn, *IBM T.J. Watson Research Center*

### INVITED TALKS

#### What Biology Can (and Can't) Teach Us About Security

David Evans, *University of Virginia*

## FRIDAY, AUGUST 13

9:00 a.m.–10:30 a.m.

### REFEREED PAPERS: FORENSICS AND RESPONSE

#### Privacy-Preserving Sharing and Correlation of Security Alerts

Patrick Lincoln, Phillip Porras, and Vitaly Shmatikov, *SRI*

#### Static Disassembly of Obfuscated Binaries

Christopher Kruegel, William Robertson, Fredrik Valeur, and Giovanni Vigna, *UC Santa Barbara*

#### Autograph: Toward Automated, Distributed Worm Signature Detection

Hyang-Ah Kim, *Carnegie Mellon University*, and Brad Karp, *Intel Research and Carnegie Mellon University*

### INVITED TALKS

#### Nuclear Weapons, Permissive Action Links, and the History of Public Key Cryptography

Steve Bellovin, *AT&T Labs—Research*

11:00 a.m.–12:30 p.m.

### REFEREED PAPERS: DATA PRIVACY

#### Fairplay: A Secure Two-Party Computation System

Dahlia Malkhi and Noam Nisan, *Hebrew University*; Benny Pinkas, *HP Labs*; Yaron Sella, *Hebrew University*

#### Tor: The Second-Generation Onion Router

Roger Dingledine and Nick Mathewson, *The Free Haven Project*; Paul Syverson, *Naval Research Lab*

#### Understanding Data Lifetime via Whole System Simulation

Jim Chow, Ben Pfaff, Tal Garfinkel, Kevin Christopher, and Mendel Rosenblum, *Stanford University*

2:00 p.m.–4:00 p.m.

### WORK-IN-PROGRESS REPORTS (WIPS) & CLOSING REMARKS