Announcement and Call for Papers **USENIX**

13th USENIX Security Symposium

http://www.usenix.org/sec04

August 9–13, 2004 **San Diego, California, USA**

Important Dates for Refereed Papers

Paper submissions due: *February 1, 2004, 23:59 PST*
Notification to authors: *March 31, 2004*
Camera-ready final papers due: *May 18, 2004*

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*

Symposium Overview

The USENIX Security Symposium brings together researchers, practitioners, system administrators, system programmers, and others interested in the latest advances in security of computer systems.

If you are working on any practical aspects of security or applications of cryptography, the program committee encourages you to submit a paper. Submissions are due on January 25, 2004, 11:59 p.m. PST. The Symposium will span five days: a two-day training program will be followed by a two and one half day technical program, which will include refereed papers, invited talks, Work-in-Progress reports, panel discussions, and Birds-of-a-Feather sessions.

Symposium Topics

Refereed paper submissions are solicited in all areas relating to systems and network security, including:

- Adaptive security and system management
- Analysis of malicious code
- Analysis of network and security protocols
- Applications of cryptographic techniques
- Attacks against networks and machines
- Authentication and authorization of users, systems, and applications
- Automated tools for source code analysis
- Denial-of-service attacks and countermeasures
- File and filesystem security
- Firewall technologies
- Intrusion detection
- Privacy preserving (and compromising) systems
- Public key infrastructure
- Rights management and copyright protection
- Security in heterogeneous and large-scale environments
- Security of agents and mobile code
- Security of Internet voting systems
- Techniques for developing secure systems
- World Wide Web security

Note that the USENIX Security Symposium is primarily a systems security conference. Papers whose contributions are primarily in the area of new cryptographic algorithms or protocols, cryptanalysis, electronic commerce primitives, etc., may not be appropriate for this conference.

Refereed Papers & Awards

Papers that have been formally reviewed and accepted will be presented during the Symposium and published in the Symposium Proceedings. The Proceedings will be distributed to attendees and, following the Symposium, will be available online to USENIX members and for purchase.

One author per paper may take a registration discount of $200. If the registration fee poses a hardship to the presenter, USENIX can offer complimentary registration.

Awards may be given at the Symposium for the best overall paper and for the best paper for which a student is the lead author.

Training Program, Invited Talks, WiPs, and BoFs

In addition to the refereed papers and the keynote presentation, the technical program will include a training program, invited talks, panel discussions, a Work-in-Progress session (WiPs), and Birds-of-a-Feather sessions (BoFs). You are invited to make suggestions regarding topics or speakers in any of these sessions via email to the contacts listed below or to the program chair at sec04chair@usenix.org.

Training Program

Tutorials for both technical staff and managers will provide immediately useful, practical information on topics such as local and network security precautions, what cryptography can and cannot do, security mechanisms and policies, firewalls, and monitoring systems. If you are interested in proposing a tutorial or suggesting a topic, contact the USENIX Training Program Coordinator, Dan Klein, by email to dvk@usenix.org.

Invited Talks

There will be several outstanding invited talks in parallel with the refereed papers. Please submit topic suggestions and talk proposals via email to sec04it@usenix.org.

Panel Discussions

The technical sessions may include topical panel discussions. Please send topic suggestions and proposals to sec04chair@usenix.org.

Work-in-Progress Reports (WiPs)

The last session of the Symposium will consist of Work-in-Progress reports (WiPs). This session offers short presentations about work in progress, new results, or timely topics. Speakers should submit a one- or two-paragraph abstract to sec04wips@usenix.org by 6:00 p.m. PDT on Wednesday, August 11, 2004. Make sure to include your name, affiliation, and the title of your talk. The accepted abstracts will be posted on the Symposium Web site. The time available will be distributed among the presenters, with each speaker allocated between 5 and 10 minutes. The time limit will be strictly enforced. The schedule of presentations will be posted at the Symposium and on the Symposium Web site.

Birds-of-a-Feather Sessions (BoFs)

Birds-of-a-Feather sessions (BoFs) will be held Tuesday, Wednesday, and Thursday evenings. Birds-of-a-Feather sessions are informal gatherings of persons interested in a particular topic. BoFs often feature a presentation or a demonstration followed by discussion, announcements, and the sharing of strategies. BoFs can be scheduled onsite, but if you wish to preschedule a BoF, please email the USENIX Conference Department, conference@usenix.org. They will need the title of the BoF with a brief description, the name, title, affiliation, and email address of the facilitator, your preference of date, and whether an overhead projector and screen are desired.

Paper Submission Instructions

Papers should represent novel scientific contributions in computer security with direct relevance to the engineering of secure systems and networks. Submissions should be finished, complete papers. Papers should be about 8 to a maximum of 16 typeset pages, formatted in 2 columns, using 10 point Times Roman type on 12 point leading, in a text block of 6.5" by 9". Submissions must be received by January 25, 2004, 11:59 p.m. PST.

Submissions will only be accepted electronically via the Symposium Web form, and must be in PDF format (i.e., processed by Adobe's Acrobat Distiller or equivalent). Note that LaTeX users can use the "dvipdf" command to convert a DVI file into PDF format. Please make sure your submission can be opened using Adobe Acrobat 4.0. For more details on the submission process, authors are encouraged to consult the detailed author guidelines at http://www.usenix.org/events/sec04/cfp/guidelines.html.

To insure that we can read your PDF file, authors are urged to follow the NSF "Fastlane" guidelines for document preparation (http://www.fastlane.nsf.gov/a1/pdfcreat.htm), and to pay special attention to unusual fonts.

A link to the Web submission system will be available on the Symposium Web site at http://www.usenix.org/sec04.

All submissions will be judged on originality, relevance, and correctness. The USENIX Security Symposium, like most conferences and journals, requires that papers not be submitted simultaneously to another conference or publication and that submitted papers not be previously published elsewhere, or subsequently published within 12 months of acceptance at the Symposium. (We may share information about submissions with the program chairs of other conferences considering papers during the review period.) Papers accompanied by nondisclosure agreement forms will not be considered. All submissions are treated as confidential, both as a matter of policy and in accord with the U.S. Copyright Act of 1976.

Authors will be notified of acceptance by March 31, 2004. The camera-ready final paper due date is May 18, 2004. Each accepted submission may be assigned a member of the program committee to act as its shepherd through the preparation of the final paper. The assigned member will act as a conduit for feedback from the committee to the authors.

Specific questions about submissions may be sent via email to the program chair at sec04chair@usenix.org.

Program and Registration Information

Complete program and registration information will be available in May 2004 on the Symposium Web site. The information will be in both HTML and a printable PDF file. If you would like to receive the program booklet in print, please email your request, including your postal address, to conference@usenix.org.