Announcement and Call for Papers **USENIX**

10th USENIX Security Symposium

http://www.usenix.org/events/sec01

August 13-17, 2001 **Washington, D.C., USA**

Important Dates for Refereed Papers

Paper submissions due: *February 1, 2001*
Author notification: *March 27, 2001*
Camera-ready final papers due: *May 2, 2001*

Symposium Organizers

Program Chair
Dan S. Wallach, *Rice University*
Program Committee
Dirk Balfanz, *Princeton University*
Steve Bellovin, *AT&T Labs—Research*
Carl Ellison, *Intel Corporation*
Ian Goldberg, *ZeroKnowledge Systems*
Peter Gutmann, *University of Auckland*
Trent Jaeger, *IBM T.J. Watson Research Center*
Teresa Lunt, *Xerox PARC*
Patrick McDaniel, *University of Michigan*
Mudge, *@stake Inc.*
Vern Paxson, *ACIRI*
Avi Rubin, *AT&T Labs—Research*
Fred Schneider, *Cornell University*
Jonathan Trostle, *Cisco*
Wietse Venema, *IBM T.J. Watson Research Center*
David Wagner, *University of California, Berkeley*
Invited Talks Coordinator
Greg Rose, *Qualcomm*

Symposium Overview

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

If you are working in any practical aspects of security or applications of cryptography, the program committee would like to encourage you to submit a paper. Submissions are due on February 1, 2001.

This symposium will last for four and a half days. Two days of tutorials will be followed by two and a half days of technical sessions including refereed papers, invited talks, works-in-progress, and panel discussions.

Symposium Topics

Refereed paper submissions are being solicited in all areas relating to system and network security, including but not limited to:

- Adaptive security and system management
- Analysis of malicious code
- Applications of cryptographic techniques
- Attacks against networks and machines
- Authentication and authorization of users, systems, and applications
- Denial-of-service attacks
- File and filesystem security
- Firewall technologies
- Intrusion detection
- IPSec and IPv6 security
- Privacy preserving (and compromising) systems
- Public key infrastructure
- Rights management and copyright protection
- Security in heterogeneous environments
- Security incident investigation and response
- Security of agents and mobile code
- Techniques for developing secure systems
- World Wide Web security

Papers covering "holistic security"—systems security, the security of entire large application systems, spread across many subsystems and computers, and involving people and environment—are particularly relevant. On the other hand, papers regarding new cryptographic algorithms or protocols, or electronic commerce primitives, are encouraged to seek alternative conferences.

Refereed Papers (August 15-17)

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 conference, will be available online to USENIX members and for purchase.

Best Paper Awards

Awards will be given at the conference for the best paper and for the best paper that is primarily the work of a student.

Tutorials, Invited Talks, WIPs, and BoFs

In addition to the refereed papers and the keynote presentation, the technical program will include tutorials, invited talks, panel discussions, a Work-in-Progress session (WIPs), and Birds-of-a-Feather Sessions. You are invited to make suggestions regarding topics or speakers for any of these formats to the program chair via email to *sec01chair@usenix.org*.

Tutorials (August 13-14)

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 Tutorial Coordinator, Dan Klein, by email to *dvk@usenix.org*.

Invited Talks (August 15-17)

There will be several outstanding invited talks at the symposium in parallel with the refereed papers. Please submit topic suggestions and talk proposals via email to *sec01it@usenix.org*.

Panel Discussions (August 15-17)

The technical sessions will also feature some panel discussions. Please send topic suggestions and proposals via email to *sec01chair@usenix.org*.

Work-in-Progress Reports (WIPs)

The last session of the symposium will be a Works-in-Progress session. This session will consist of short presentations about work-in-progress, new results, or timely topics. Speakers should submit a one- or two-paragraph abstract to *sec01wips@usenix.org* by 6:00 pm on Wednesday, August 15, 2001. Please include your name, affiliation, and the title of your talk. The accepted abstracts will appear on the symposium Web site after the symposium. The time available will be distributed among the presenters with a minimum of 5 minutes and a maximum of 10 minutes. The time limit will be strictly enforced. A schedule of presentations will be posted at the symposium. Experience has shown that most submissions are usually accepted.

Birds-of-a-Feather Sessions (BoFs)

There will be Birds-of-a-Feather sessions (BoFs) both Tuesday and Wednesday 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 on-site, but if you wish to preschedule a BoF, please email the conference office, *conference@usenix.org*. They will need to know the title of the BoF with a brief description, the name, title and company and email address of the facilitator, your preference of date, and whether an overhead projector and screen is desired.

How and Where to Submit Refereed Papers

Papers should represent novel scientific contributions in computer security with direct relevance to the engineering of secure systems and networks.

Authors must submit a mature paper. Any incomplete sections (there shouldn't be many) should be outlined in enough detail to make it clear that they could be finished easily. Full papers are encouraged, and should be about 8 to 15 typeset pages. Submissions must be received by February 1, 2001.

Papers will only be accepted electronically, via the symposium Web site, and must be in PDF format (e.g., processed by Adobe's Acrobat Distiller). We request that you follow the NSF FastLane guidelines in preparing your PDF.
http://www.fastlane.nsf.gov/a1/pdfcreat.htm

Submissions will be made with a Web-based form available on the symposium Web site: *http://www.usenix.org/events/sec01*

For more details on the submission process, authors are encouraged to consult the detailed author guidelines also located on the symposium Web site.

All submissions will be judged on originality, relevance, and correctness. 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. Authors will be notified of acceptance by March 27, 2001. Camera-ready final papers are due on May 2, 2001.

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 or subsequently published elsewhere. Papers accompanied by non-disclosure agreement forms are not acceptable and will be returned to the author(s) unread. All submissions are held in the highest confidentiality prior to publication in the Proceedings, both as a matter of policy and in accord with the U.S. Copyright Act of 1976.

Specific questions about submissions may be sent via e-mail to *sec01chair@usenix.org*.

Security 2001 Exhibition (August 15-16)

Demonstrate your security products to our technically astute attendees responsible for security at their sites. Meet with attendees in this informal setting and demonstrate in detail your security solutions. We invite you to take part. Contact: Dana Geffner, Email: *dana@usenix.org*, Phone: +1.831.457.8649

Registration Materials

Complete program and registration information will be available in April 2001 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*.