Announcement and Call for Papers USENIX

9th USENIX Security Symposium

Sponsored by USENIX in cooperation with The CERT Coordination Center

http://www.usenix.org/events/sec2000

August 14-17, 2000 **Denver, Colorado, USA**

Important Dates for Refereed Papers

Paper submissions due: *February 10, 2000*
Author notification: *March 23, 2000*
Camera-ready final papers due: *June 15, 2000*

Symposium Organizers

Program Co-Chairs
Steven Bellovin, *AT&T Labs—Research*
Greg Rose, *QUALCOMM Australia*
Program Committee
Carl Ellison, *Intel Corporation*
Ian Goldberg, *UC Berkeley*
Peter Gutmann, *University of Auckland*
Trent Jaeger, *IBM T.J.Watson Research Center*
Markus Kuhn, *University of Cambridge*
Marcus Leech, *Nortel*
Alain Mayer, *Lucent Technologies, Bell Laboratories*
Avi Rubin, *AT&T Labs—Research*
Jeff Schiller, *MIT*
Jonathan Trostle, *Cisco*
Wietse Venema, *IBM T.J.Watson Research Center*
Dan Wallach, *Rice University*
Tara Whalen, *Communications Research Centre Canada*
Elizabeth Zwicky
Invited Talks Coordinator
Win Treese, *Open Market Inc.*

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.

Dr. Blaine Burnham, director of the Georgia Tech Information Security Center (GTISC), will give the keynote address. Dr. Burnham most recently served as program manager for the National Security Agency (NSA) at Ft. Meade, Maryland.

If you are working in any practical aspects of security or applications of cryptography, the program committee would like to urge you to submit a paper. Submissions are due on February 10, 2000.

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

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
- File and filesystem security
- Firewall technologies
- Intrusion detection
- IPSec and IPv6 security
- 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
- Trust management
- 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

Papers that have been formally reviewed and accepted will be presented during the symposium and published in the symposium proceedings. The proceedings are provided free to technical session attendees. Additional copies will be available for purchase from USENIX.

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 *securitychairs@usenix.org*.

Tutorials

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 phone at +1.412.422.0285 or by email to *dvk@usenix.org*.

Submitting an Invited Talk Proposal

These survey-style talks given by experts range over many interesting and timely topics. The Invited Talk Coordinator, Win Treese, welcomes suggestions for topics and requests proposals for particular talks. In your proposal state the main focus, including a brief outline, and be sure to emphasize why your topic is of general interest to our community. Please submit via email to *securityit@usenix.org*.

Work-in-Progress Session (WIPs)

The last session of the symposium will be a Work-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 *securitywips@usenix.org* by 6:00 pm on Wednesday, August 16, 2000. Please include your name, affiliation, and the title of your talk. The accepted abstracts will appear on the conference Web page 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 by noon on August 17. 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.

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 in PostScript format. 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 10, 2000.

Along with your paper, please submit a separate email message in ASCII containing:

- The title, all authors of the manuscript, and their affiliations.
- The name of one author who will serve as a contact, with regular and electronic mail addresses, daytime and evening telephone numbers, and a fax number.
- Indicate any authors who are full-time students.

For more details on the submission process, authors are encouraged to consult the detailed author guidelines on the symposium website at: *http://www.usenix.org/events/sec2000/*.

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. Camera-ready final papers are due on June 15, 2000.

Authors will be notified of acceptance by March 23, 2000.

The 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 to the program chairs via email to *securitychairs@usenix.org*.

For reliability, please send one copy of your paper to the program committee via **both** of the following two methods. All submissions will be acknowledged.

1. **Email (PostScript) to:**
   securitypapers@usenix.org
2. **Send a hard copy to:**
   Security Symposium
   USENIX Association
   2560 Ninth Street, Suite 215
   Berkeley CA 94710
   U.S.A.
   Phone: +1.510.528.8649

Security 2000 Exhibition

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

Materials containing all details of the technical and tutorial programs, registration fees and forms, and hotel information will be available in May 2000. If you wish to receive the registration materials, please visit the symposium Web site or contact:

USENIX Conference Office
22672 Lambert Street, Suite 613
Lake Forest, CA 92630, USA
Phone: +1.949.588.8649
Fax: +1.949.588.9706
Email: *conference@usenix.org*