Announcement and Call for Papers **USENIX**

11th USENIX Security Symposium

http://www.usenix.org/events/sec02

August 5-9, 2002 **San Francisco, California**

Important Dates for Refereed Papers

Paper submissions due: *Extended to February 1, 2002*
Author notification: *March 25, 2002*
Camera-ready final papers due: *May 13, 2002*

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*

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 would like to encourage you to submit a paper. Submissions are due on February 1, 2002.

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, Work-in-Progress reports, Birds-of-a-Feather sessions, and panel discussions.

Symposium Topics

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

- 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
- File and filesystem security
- Firewall technologies
- Intrusion detection
- Privacy preserving systems
- Public key infrastructure
- Rights management and copyright protection
- Security in heterogeneous environments
- Security of agents and mobile code
- Security of Internet voting systems
- Techniques for developing secure systems
- World Wide Web security

Since USENIX Security is primarily a systems security conference, papers focusing on cryptographic primitives or electronic commerce models are encouraged to seek alternative conferences.

Refereed Papers (August 7-9)

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 symposium will include tutorials, invited talks, panel discussions, a Work-in-Progress session, 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 *sec02chair@usenix.org*.

Tutorials (August 5-6)

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: *dvk@usenix.org*.

Invited Talks (August 7-9)

These survey-style talks given by experts range over many interesting and timely topics. The invited talks track also may include panel presentations. Please submit topic suggestions and talk proposals via email to *sec02it@usenix.org*.

Panel Discussions (August 7-9)

The technical sessions will also feature some panel discussions. Please send topic suggestions and proposals via email to *sec02chair@usenix.org*.

Work-in-Progress Reports (WiPs)

The last session of the symposium will be Work-in-Progress reports. 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 *sec02wips@usenix.org* by 6:00 pm on Wednesday, August 7, 2002. 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) on 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 on-site, but if you wish to pre-schedule 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, 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. Both the work described in the paper and the paper itself must be substantially complete at the time of the submission. Full papers are encouraged, and should be about 8 to 14 typeset pages using an 11pt font or larger. Submissions must be received by February 1, 2002.

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). 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 available at *http://www.usenix.org/events/sec02/cfp/guidelines.html*

All submissions will be judged on originality, contribution to the field, 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 25th, 2002. Camera-ready final paper due date is May 13th, 2002.

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. When appropriate, authors should arrange for a release for publication from their employer prior to submission. Papers accompanied by non-disclosure agreement forms are not acceptable and will be returned to the author(s) unread. Submissions will be read by the program committee and other selected members of the technical community for the purposes of technical review, but otherwise will be held in confidentiality.

Specific questions about submissions may be sent via email to *sec02chair@usenix.org*.

Registration Materials

Complete program and registration information will be available in May 2002 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*.