



# Announcement and Call for Papers USENIX

## 12th USENIX Security Symposium

<http://www.usenix.org/events/sec03>

August 4–8, 2003

Marriott Wardman Park Hotel, Washington, D.C

### Important Dates for Refereed Papers

Paper submissions due: *January 27, 2003*

Author notification: *March 20, 2003*

Camera-ready final papers due: *May 13, 2003*

### Symposium Organizers

#### Program Chair

Vern Paxson, *ICSI*

#### Program Committee

Steve Bellovin, *AT&T Labs—Research*

Dan Boneh, *Stanford University*

Crispin Cowan, *WireX*

Drew Dean, *SRI International*

Kevin Fu, *MIT*

Peter Gutmann, *University of Auckland, New Zealand*

Richard Kemmerer, *University of California, Santa Barbara*

Patrick McDaniel, *AT&T Labs—Research*

John McHugh, *CERT® Coordination Center*

Radia Perlman, *Sun Microsystems*

Niels Provos, *University of Michigan*

Dawn Song, *Carnegie Mellon University*

David Wagner, *University of California, Berkeley*

Dan S. Wallach, *Rice University*

Elizabeth Zwicky, *Greatcircle Associates*

#### Invited Talks Coordinator

Matt Blaze, *AT&T Labs—Research*

### 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 January 27, 2003.

This symposium will last for five days. Two days of tutorials will be followed by 2.5 days of technical sessions, including refereed papers, invited talks, Work-in-Progress reports, panel discussions, and Birds-of-a-Feather sessions.

### Symposium Topics

Refereed paper submissions are being 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
- 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

Since USENIX Security is primarily a systems security conference, papers regarding new cryptographic algorithms or protocols, or electronic commerce primitives, are in general discouraged.

### Refereed Papers (August 6–8)

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 [sec03chair@usenix.org](mailto:sec03chair@usenix.org).

### Tutorials (August 4–5)

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](mailto:dvk@usenix.org).

### Invited Talks (August 6–8)

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 [sec03it@usenix.org](mailto:sec03it@usenix.org).

### Panel Discussions (August 6–8)

The technical sessions will also feature some panel discussions. Please send topic suggestions and proposals to [sec03chair@usenix.org](mailto:sec03chair@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 [sec03wips@usenix.org](mailto:sec03wips@usenix.org) by 6:00 PM on Wednesday, August 6, 2003. 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 pre-schedule a BoF, please email the conference office, [conference@usenix.org](mailto: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) must 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 16 typeset pages. Submissions must be received by January 27, 2003.

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 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 20, 2003. Camera-ready final paper due date is May 13, 2003.

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 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 [sec03chair@usenix.org](mailto:sec03chair@usenix.org).

## Registration Materials

Complete program and registration information will be available in May 2003 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](mailto:conference@usenix.org).