Since 1980, the IEEE Symposium on Security and Privacy has been the premier forum for computer security research, presenting the latest developments and bringing together researchers and practitioners.

We solicit previously unpublished papers offering novel research contributions in any aspect of computer security or privacy. S&P is interested in all aspects of computer security and privacy. Papers may present advances in the theory, design, implementation, analysis, or empirical evaluation of secure systems. Papers without a clear application to security or privacy will be considered out of scope and may be rejected without full review.

Topics of interest include, but are not limited to:

- Access control
- Attacks and defenses
- Embedded system security
- Information flow
- Malicious code
- Physical security
- Secure protocols
- System security
- Anonymity
- Authentication
- Forensics
- Information security
- Language-based security
- Privacy-preserving systems
- Security architectures
- Usability and security
- Application-level security
- Distributed systems security
- Hardware-based security
- Intrusion detection
- Network security
- Recovery
- Security and privacy policies
- Web security

The Symposium is also soliciting submissions for colocated workshops, tutorials, posters, and work-in-progress talks (see back for details).

Call for Papers

Papers, workshop proposals, and tutorial proposals due Monday, 10 November 2008 11:59PM PST (UTC-8)

Symposium Organizers

General Chair
David Du
University of Minnesota, National Science Foundation

Program Chairs
Andrew Myers
Cornell University
David Evans
University of Virginia

Registration Chair
Ulf Lindqvist
SRI International

Treasurer
David Shambroom
Intersystems Corporation

Publications Chair
Carrie Gates, CA Labs

Poster Session Chair
Cristina Nita-Rotaru
Purdue University

Web Design Chair
Adrienne Felt
UC Berkeley

Program Committee

Ben Adida, Harvard U.
William Aiello, U. of British Columbia
Ross Anderson, Cambridge U.
Michael Backes, Saarland U.
Srdjan Capkun, ETH Zürich
Miguel Castro, MSR Cambridge
Hao Chen, UC Davis
Jed Crandall, U. of New Mexico
Bruno Crispo, U. of Trento
Weidong Cui, MSR Redmond
George Danezis, MSR Cambridge
Úlfar Erlingsson, Reykjavik U.
Michael Freedman, Princeton U.
Kevin Fu, U. of Massachusetts
Jonathan Giffin, Georgia Tech
Ian Goldberg, U. of Waterloo, Canada
Andrew D. Gordon, MSR Cambridge
Steve Gribble, U. of Washington
Guofei Gu, Texas A&M U.
Peter Gutmann, U. of New Auckland
Michael Hicks, U. of Maryland
Farnam Jahanian, U. of Michigan
Xuxian Jiang, North Carolina State U.
Jonathan Katz, U. of Maryland
Sam King, U. of Illinois, Urbana-Champaign
Tadayoshi Kohno, U. of Washington
Farinaz Koushanfar, Rice U.
Wenke Lee, Georgia Tech
Kristen LeFevre, U. of Michigan
David Lie, U. of Toronto
John Mitchell, Stanford U.
Greg Morrisett, Harvard U.
Peng Ning, North Carolina State U.
Reiner Sailer, IBM TJ Watson Research Center
Stefan Savage, UC San Diego
R. Sekar, Stony Brook U.
Umesh Shankar, Google, New York
Abhi Shelat, U. of Virginia
Vitaly Shmatikov, U. of Texas, Austin
Radu Sion, Stony Brook U.
Patrick Traynor, Georgia Tech
Doug Tygar, UC Berkeley
Giovanni Vigna, UC Santa Barbara
David Wagner, UC Berkeley
Haining Wang, College of William and Mary
Brent Waters, U. of Texas, Austin
Rebecca Wright, Rutgers U.
Steve Zdancewic, U. of Pennsylvania

http://oakland09.cs.virginia.edu
Awards

There will be awards for the best paper, best student paper, and best practical paper from the accepted program. These awards will be chosen by the program committee. The best paper award will be given to the paper judged to have the highest overall quality. A student must be the first author to be eligible for the best student paper. The best practical paper award will be for the paper judged most likely to immediately improve current security practice.

Instructions for Paper Submission

Submissions received after the submission deadline or failing to conform to the submission guidelines risk rejection without consideration of their merits.

All submissions must reflect original work and must precisely document any overlap with previously published or simultaneously submitted papers from any of the authors. Simultaneous submission of the same paper to another venue with proceedings or a journal is not allowed. Failure to clearly document such overlaps will lead to automatic rejection. If authors have any doubts regarding such overlaps, they should contact the program chairs prior to submission.

Papers must not exceed 12 pages, excluding the bibliography and well-marked appendices. Reviewers are not required to read appendices, so papers must be self-contained without them. Papers should be submitted in Portable Document Format (.pdf) in US letter (not A4) paper size with a margin width of at least 3/4 inch. The text must be formatted in a two-column layout, with columns no more than 9 in. high and 3.25 in. wide. The text must be in Times font, 10-point or larger, with 12-point or larger line spacing. Authors are encouraged to use the IEEE standard Latex template, found at: http://www.ieee.org/web/publications/authors/txnsl/index.html. Authors should pay special attention to unusual fonts, images, and figures that might create problems for reviewers.

Papers must be submitted in a form suitable for anonymous review: remove author names and affiliations from the title page, and avoid explicit self-referencing in the text. When referring to your previous work, do so in the third person, as though it were written by someone else. Only blind the reference itself in the (unusual) case that a third-person reference is infeasible. Contact the program chairs you have any questions.

Please submit your paper through the submissions website at http://firefly01.cs.cornell.edu/oakland09. Submissions are accepted in .pdf form only. If you have any difficulty submitting a paper or have any questions about the submission process, please contact the program chairs at oakland09-pccchairs@cs.virginia.edu. Authors are responsible for obtaining appropriate publication clearances; authors of accepted papers will be asked to sign IEEE copyright release forms.

Workshops and Tutorials

Workshop and tutorial proposals should be sent to oakland09-pccchairs@cs.virginia.edu by Monday, 10 November, 2008. Workshops may be half-day or full-day in length. Submissions should include the title, a short description of the topic of the workshop, and a short biography of the organizer(s).

Tutorials may be 90 minutes or 3 hours long. Submissions should include the title, a brief description of the topic for the tutorial and intended audience, the intended length, and a short biography of the presenter(s).

Posters

There will be a poster session at an evening reception during the conference. Posters are solicited that present recent and ongoing research on security and privacy related topics. Posters are nice opportunities for students to obtain feedback on ongoing work. More information on submissions will be available on the conference website soon.

Work-in-Progress Talks

A continuing feature of the symposium is a session of 5-minute talks where attendees can present preliminary research results and new ideas. More information on work-in-progress talk submissions will be available on the conference website soon.