usenix
THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

23rd USENIX Security Symposium

Sponsored by USENIX

August 20–22, 2014, San Diego, CA

Important Dates

Paper submissions due: *Thursday, February 27, 2014, 8:59 p.m. EST (firm deadline)*

Invited talk proposals due: *Thursday, February 27, 2014, 8:59 p.m. EST*

Panel proposals due: *Friday, April 18, 2014, 8:59 p.m. EDT*

Notification to authors: *Friday, May 9, 2014*

Final papers due: *Tuesday, July 8, 2014, 8:59 p.m. EDT (firm deadline)*

Poster proposals due: *Tuesday, July 15, 2014, 8:59 p.m. EDT*

Notification to poster presenters: *Thursday, July 24, 2014*

Rump session submissions due: *Wednesday, August 20, 2014, 11:59 a.m. PDT (San Diego)*

Conference Organizers

Program Chair

Kevin Fu, *University of Michigan*

Deputy Program Chair

Jaeyeon Jung, *Microsoft Research*

Program Committee

Bill Aiello, *University of British Columbia*
Steven Bellovin, *Columbia University*
Emery Berger, *University of Massachusetts Amherst*
Dan Boneh, *Stanford University*
Nikita Borisov, *University of Illinois at Urbana-Champaign*
David Brumley, *Carnegie Mellon University*
Kevin Butler, *University of Oregon*
Srdjan Capkun, *ETH Zürich*
Stephen Checkoway, *Johns Hopkins University*
Nicolas Christin, *Carnegie Mellon University*
George Danezis, *University College London*
Srini Devadas, *Massachusetts Institute of Technology*
Roger Dingledine, *The Tor Project*
David Evans, *University of Virginia*
Nick Feamster, *Georgia Institute of Technology*
Adrienne Porter Felt, *Google*
Simson Garfinkel, *Naval Postgraduate School*
Virgil Gligor, *Carnegie Mellon University*
Rachel Greenstadt, *Drexel University*
Steve Gribble, *University of Washington and Google*
Carl Gunter, *University of Illinois at Urbana-Champaign*
Nadia Heninger, *University of Pennsylvania*
Thorsten Holz, *Rühr-Universität Bochum*
Jean-Pierre Hubaux, *École Polytechnique Fédérale de Lausanne*
Cynthia Irvine, *Naval Postgraduate School*
Jaeyeon Jung, *Microsoft Research*
Chris Kanich, *University of Illinois at Chicago*
Engin Kirda, *Northeastern University*
Tadayoshi Kohno, *Microsoft Research and University of Washington*
Farinaz Koushanfar, *Rice University*
Zhenkai Liang, *National University of Singapore*
David Lie, *University of Toronto*
Stephen McCamant, *University of Minnesota*
Damon McCoy, *George Mason University*
Patrick McDaniel, *Pennsylvania State University*
Cristina Nita-Rotaru, *Purdue University*
Christof Paar, *Rühr-Universität Bochum*
Zachary N. J. Peterson, *California Polytechnic State University*
Niels Provos, *Google*
Raj Rajagopalan, *Honeywell Labs*
Ben Ransford, *University of Washington*
Thomas Ristenpart, *University of Wisconsin—Madison*
Prateek Saxena, *National University of Singapore*
Patrick Schaumont, *Virginia Polytechnic Institute and State University*
Stuart Schechter, *Microsoft Research*
Simha Sethumadhavan, *Columbia University*
Cynthia Sturton, *University of North Carolina at Chapel Hill*
Mohammad Tehranipoor, *University of Connecticut*
Wade Trappe, *Rutgers University*
Eugene Y. Vasserman, *Kansas State University*
Ingrid Verbauwhede, *Katholieke Universiteit Leuven*
Giovanni Vigna, *University of California, Santa Barbara*
David Wagner, *University of California, Berkeley*
Dan Wallach, *Rice University*
Rui Wang, *Microsoft Research*
Matthew Wright, *University of Texas at Arlington*
Wenyuan Xu, *University of South Carolina*

Invited Talks Committee

Sandy Clark, *University of Pennsylvania*
Matthew Green, *Johns Hopkins University*
Thorsten Holz, *Rühr-Universität Bochum*
Ben Laurie, *Google*
Damon McCoy, *George Mason University*
Jon Oberheide, *Duo Security*
Patrick Traynor (Chair), *Georgia Institute of Technology*

Steering Committee

Matt Blaze, *University of Pennsylvania*
Dan Boneh, *Stanford University*
Casey Henderson, *USENIX*
Tadayoshi Kohno, *University of Washington*
Fabian Monrose, *University of North Carolina, Chapel Hill*
Niels Provos, *Google*
David Wagner, *University of California, Berkeley*

Overview

The USENIX Security Symposium brings together researchers, practitioners, system administrators, system programmers, and others interested in the latest advances in the security and privacy of computer systems and networks. The 23rd USENIX Security Symposium will be held August 20–22, 2014, in San Diego, CA.

All researchers are encouraged to submit papers covering novel and scientifically significant practical works in computer security. Submissions are due on February 27, 2014. The Symposium will span three days, with a technical program including refereed papers, invited talks, posters, panel discussions, and Birds-of-a-Feather sessions. Workshops will precede the Symposium on August 18 and 19.

Symposium Topics

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

- Cloud computing security
- Cryptographic implementation analysis and construction, applied cryptography
- Distributed systems security
- Forensics and diagnostics for security
- Hardware security
    - Embedded systems security
    - Methods for detection of malicious or counterfeit hardware
    - Randomness
    - Secure computer architectures
    - Side channels
- Human-computer interaction, security, and privacy
- Intrusion and anomaly detection and prevention
- Malware
    - Detection, mitigation
    - Malicious code analysis, anti-virus, anti-spyware
- Mobile system security
- Network security
    - Botnets
    - Denial-of-service attacks and countermeasures
    - Network infrastructure security
- Operating system security
- Privacy-enhancing technologies, anonymity
- Programming language security
- Public good
    - Research on computer security law and policy
    - Research on security education and training
    - Research on social values, surveillance, and censorship
- Security analysis
    - Analysis of network and security protocols
    - Attacks with novel insights, techniques, or results
- Security applications
    - Security in critical infrastructures
    - Security in electronic voting
    - Security in health care and medicine
    - Security in ubiquitous computing, sensors, actuators
- Security economics, electronic commerce
- Security measurement studies
    - Large-scale measurement of fraud, malware, spam
    - Large-scale measurement of human behavior and security
- Security tools
    - Automated security analysis of hardware designs and implementation
    - Automated security analysis of source code and binaries, program analysis
    - Novel tools to improve the trustworthiness of computer systems
- Storage security
    - Database security and privacy
    - File systems
- Web security
- Wireless security

This topic list is not meant to be exhaustive; USENIX Security is interested in all aspects of computing systems security and privacy. Papers without a clear application to security or privacy, however, will be considered out of scope and may be rejected without full review.

The program chair is not permitted to be author or co-author of any paper submissions.

Refereed Papers

Papers that have been formally reviewed and accepted will be presented during the Symposium and published in the Symposium Proceedings. It is expected that one of the paper authors will attend the conference and present the work. It is the responsibility of the authors to find a suitable replacement presenter for their work, if the need arises.

A registration discount will be available for one author per paper. If the registration fee poses a hardship to the presenter, USENIX will offer complimentary registration.

A major mission of the USENIX Association is to provide for the creation and dissemination of new knowledge. In keeping with this and as part of USENIX's open access policy, the Proceedings will be available online for registered attendees before the Symposium and for everyone starting on the opening day of the technical sessions. USENIX also allows authors to retain ownership of the copyright in their works, requesting only that USENIX be granted the right to be the first publisher of that work. See our sample consent form at www.usenix.org/sites/default/files/usenix_sample_consent.pdf for the complete terms of publication.

Shadow PC (New This Year!)

In order to train the next generation of program committee (PC) members and to expose students to the review process, the USENIX Security '14 PC would like to make submitted papers available to shadow PCs. Shadow PCs allow students and others interested in future PC service to read submitted papers and go through the reviewing process, ultimately arriving at a shadow conference program. This is an opportunity for future PC members to learn about the peer-review process and gain experience as a reviewer. Shadow PCs will not have any access to the real reviews, the names of the real reviewers, or any other data such as relative rankings. They will have to abide by the same rules and restrictions applicable to regular PC members. This includes, but is not limited to, rules against discussing the papers outside of the PC context, or using in any way results from reviewed papers before such papers have been published. Subreviews (i.e., external reviews) are not allowed for the shadow PC. If you are given a paper to review as a student/shadow PC member, you must review it yourself. Making a submitted paper available to shadow PCs is optional; authors will have the opportunity to opt-in during the paper submission process. Shadow reviews for papers that are reviewed by shadow PCs will be sent out after the actual USENIX Security '14 review process. Authors that have participated in previous shadow PCs have found the additional reviews helpful; however, these reviews will have no direct bearing on acceptance to the technical program. If you would like to organize a shadow PC at your host institution, please contact Yoshi Kohno via sec14shadow@usenix.org.

Symposium Activities

Invited Talks, Panels, Poster Session, Rump Session, and BoFs

In addition to the refereed papers and the keynote presentation, the technical program will include invited talks, panel discussions, a Poster Session, and Birds-of-a-Feather sessions (BoFs). You are invited to make suggestions regarding topics or speakers in any of these sessions via email to the contacts listed below or to the program chair at sec14chair@usenix.org.

Invited Talks

Invited talks will be held in parallel with the refereed paper sessions. Please submit topic suggestions and talk proposals via email to sec14it@usenix.org by Thursday, February 27, 2014, 8:59 p.m. EST.

Panel Discussions

The technical sessions may include topical panel discussions. Please send topic suggestions and proposals to sec14chair@usenix.org. The deadline for panel proposals is Friday, April 18, 2014, 8:59 p.m. EDT.

Poster Session

Would you like to share a provocative opinion, interesting preliminary work, or a cool idea that will spark discussion at this year's USENIX Security Symposium? The poster session is the perfect venue to introduce such new or ongoing work. Poster presenters will have the entirety of the evening reception to discuss their work, get exposure, and receive feedback from attendees.

To submit a poster, please submit a draft of your poster, in PDF (maximum size 36" by 48"), or a one-page abstract via the poster session submission form, which will be available here soon, by Tuesday, July 15, 2014, 8:59 p.m. EDT. Decisions will be made by Thursday, July 24, 2014. Posters will not be included in the proceedings but may be made available online if circumstances permit. Poster submissions must include the authors' names, affiliations, and contact information. At least one author of each accepted poster must register for and attend the Symposium to present the poster.

Rump Session

We will host a rump session on the evening of Wednesday, August 20, 2014. This is intended as an informal session for short and engaging presentations on recent unpublished results, work in progress, or other topics of interest to the USENIX Security attendees. As in the past, talks do not always need to be serious. To submit a rump session talk, email sec14rump@usenix.org by Wednesday, August 20, 2014, 11:59 a.m. PDT (San Diego).

Doctoral Colloquium (New This Year!)

What opportunities await security students graduating with a PhD? On Thursday evening, students will have the opportunity to listen to informal panels of faculty and industrial researchers providing personal perspectives on their post-PhD career search. Learn about the academic job search, the industrial research job search, research fund raising, dual-career challenges, life uncertainty, and other idiosyncrasies of the ivory tower.

Birds-of-a-Feather Sessions (BoFs)

Birds-of-a-Feather sessions (BoFs) will be held 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 or in advance. To preschedule a BoF, please send email to the USENIX Conference Department at bofs@usenix.org with the title and a brief description of the BoF; the name, title, affiliation, and email address of the facilitator; and your preference of date and time.

How and Where to Submit Refereed Papers

Important: Note that some past USENIX Security Symposia have had different anonymity policies and page limits.

Papers are due by Thursday, February 27, 2014, at 8:59 p.m. EST (firm deadline). All submissions will be made online via the Web form, which will be available here soon. Submissions should be finished, complete papers.

Paper submissions should be at most 13 typeset pages, excluding bibliography and well-marked appendices. There is no limit on the length of the bibliography and appendices, but reviewers are not required to read them. Once accepted, papers must be reformatted to fit in 16 pages, including bibliography and any appendices. The submission must be formatted in 2 columns, using 10-point Times Roman type on 12-point leading, in a text block of 6.5" by 9", on 8.5"x11" (letter-sized) paper. If you wish, please make use of the LaTeX file and style file available at www.usenix.org/templates-conference-papers when preparing your paper for submission.

Blind Review and Unblinding

Paper submissions must be submitted in a form suitable for anonymous review: no author names or affiliations may appear on the title page, and authors should avoid revealing their identity 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.

This year, we are using a hybrid approach to double-blind review. While submissions will remain anonymous during the review process, authors' names and affiliations will be revealed to the reviewers after the reviews are received, but before the program committee meeting. USENIX Security followed a single-blind reviewing process (anonymity explicitly disallowed) for its first two decades of symposia. The double-blind process was introduced in 2011 to increase reviewing fairness by reducing actual and perceived bias. However, it has become apparent that authors can also be unfairly penalized when reviewers make inadvertent assumptions about authorship of related work. Unblinding prior to the PC meeting also provides transparency to mitigate potential abuses in which committee members end up advancing the cause of a paper with which they have a conflict (e.g., a paper from a close colleague). Borrowing from the approach of PLDI, reviewers can now correct their reviews if they indeed have penalized the authors inappropriately. In order to ensure transparency and determine the effectiveness of this approach, the chair will measure the changes to paper outcomes that result from unblinding.

Human Subjects

Papers that describe experiments on human subjects, or that analyze non-public data derived from human subjects (even anonymized data), should disclose whether an ethics review (e.g., IRB approval) was conducted and discuss steps taken to ensure that participants were treated ethically. Contact the program chair at sec14chair@usenix.org if you have any questions.

How and Where to Submit

Submissions must be in PDF format. LaTeX users can use the "pdflatex" command to convert a LaTeX document into PDF format. Please make sure your submission can be opened using Adobe Reader. Please also make sure your submission and all embedded figures are intelligible when printed in grayscale.

All submissions will be judged on originality, relevance, correctness, and clarity. In addition to citing relevant published work, authors should relate their submission to any other relevant submissions of theirs in other venues that are under review at the same time as their submission to the Symposium. These citations to simultaneously submitted papers should be anonymized; non-anonymous versions of these citations must, however, be emailed to the program chair at sec14chair@usenix.org. Simultaneous submission of the same work to multiple venues, submission of previously published work, or plagiarism constitutes dishonesty or fraud. USENIX, like other scientific and technical conferences and journals, prohibits these practices and may take action against authors who have committed them. Program committee members will be instructed not to reject a paper solely on the basis of the existence of an unrefereed technical report, short workshop paper, job talk, or poster by the author. Program committee members have pledged to the PC chair to provide constructive and positive reviews. See the USENIX Conference Submissions Policy for details. Questions? Contact your program chair, sec14chair@usenix.org, or the USENIX office, submissionspolicy@usenix.org.

Papers accompanied by nondisclosure agreement forms will not be considered. Accepted submissions will be treated as confidential prior to publication on the USENIX Security '14 Web site; rejected submissions will be permanently treated as confidential. Papers that do not comply with the submission requirements, including length and anonymity, may be rejected without review.

Authors will be notified of acceptance by Friday, May 9, 2014. The final paper due date is Tuesday, July 8, 2014, 8:59 p.m. EDT (firm deadline). 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.

All papers will by default be available online to registered attendees before the symposium. If your accepted paper should not be published prior to the event, please notify production@usenix.org. The papers will be available online to everyone beginning on the first day of the symposium, August 20, 2014.

Specific questions about submissions may be sent to the program chair at sec14chair@usenix.org. The chair will respond to individual questions about the submission process if contacted at least a week before the submission deadline. Please contact the chair's assistant Jessica Patterson at 734-936-8875 (USA) if you do not receive an email response within a couple business days (perhaps a spam filter ate it).

Rev. 01/15/14