Announcement and Call for Papers

usenix
THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

22nd USENIX Security Symposium

www.usenix.org/conference/sec13

August 14–16, 2013 **Washington, DC**

Important Dates

Paper submissions due: *Thursday, February 21, 2013, 11:59 p.m. EST (firm deadline)*
Invited talk proposals due: *Thursday, February 21, 2013, 11:59 p.m. EST*
Panel proposals due: *Friday, April 12, 2013, 11:59 p.m. EDT*
Notification to authors: *Tuesday, April 30, 2013*
Final papers due: *Tuesday, June 25, 2013, 11:59 p.m. EDT (firm deadline)*
Poster proposals due: *Tuesday, July 9, 2013, 11:59 p.m. EDT*
Notification to poster presenters: *Thursday, July 18, 2013*
Rump session submissions due: *Wednesday, August 14, 2013, 11:59 a.m. EDT*

Symposium Organizers

Program Chair
Sam King, *University of Illinois at Urbana-Champaign*

Program Committee
Nikita Borisov, *University of Illinois at Urbana-Champaign*
Elie Bursztein, *Google*
Srdjan Capkun, *ETH Zurich*
Shuo Chen, *Microsoft Research*
Sonia Chiasson, *Carleton University*
Adam Chlipala, *Massachusetts Institute of Technology*
William Enck, *North Carolina State University*
Adrienne Porter Felt, *Google*
Kevin Fu, *University of Michigan*
Roxana Geambasu, *Columbia University*
Ian Goldberg, *University of Waterloo*
Matthew Green, *John Hopkins University*
Chris Grier, *University of California, Berkeley*
Thorsten Holz, *Ruhr-Universität Bochum*
Jaeyeon Jung, *Microsoft Research*
Benjamin Livshits, *Microsoft Research*
Jonathan McCune, *Google*
Fabian Monrose, *University of North Carolina, Chapel Hill*
Niels Provos, *Google*
Prateek Saxena, *National University of Singapore*
Stuart Schechter, *Microsoft Research*
Hovav Shacham, *University of California, San Diego*
Micah Sherr, *Georgetown University*
Elaine Shi, *University of Maryland, College Park*
Cynthia Sturton, *University of California, Berkeley*
Shuo Tang, *University of Illinois at Urbana-Champaign*
Patrick Traynor, *Georgia Institute of Technology*
David Wagner, *University of California, Berkeley*
Tara Whalen, *Carleton University*
Michal Zalewski, *Google*
Nickolai Zeldovich, *Massachusetts Institute of Technology*

Invited Talks Committee
Michael Bailey (Chair), *University of Michigan*
Elie Bursztein, *Google*
Wenke Lee, *Georgia Institute of Technology*
Stefan Savage, *University of California, San Diego*

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 of computer systems and networks. The 22nd USENIX Security Symposium will be held August 14–16, 2013, in Washington, DC.

All researchers are encouraged to submit papers covering novel and scientifically significant practical works in computer security. Submissions are due on February 21, 2013. 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 12 and 13.

Symposium Topics

Refereed paper submissions are solicited in all areas relating to systems and network security, including:

- Analysis of network and security protocols
- Applications of cryptographic techniques
- Attacks with novel insights, techniques, or results
- Authentication and authorization of users, systems, and applications
- Automated tools for source code analysis
- Botnets
- Cryptographic implementation analysis and construction
- Denial-of-service attacks and countermeasures
- Embedded systems security
- File and filesystem security
- Forensics and diagnostics for security
- Hardware security
- Human-computer interaction, security, and privacy
- Intrusion and anomaly detection and prevention
- Malicious code analysis, anti-virus, anti-spyware
- Mobile system security
- Network infrastructure security
- Operating system security
- Privacy-enhancing technologies
- Security architectures
- Security education and training
- Security for critical infrastructures
- Security in heterogeneous and large-scale environments
- Security in ubiquitous computing environments
- Security policy
- Self-protecting and self-healing systems
- Techniques for developing secure systems
- Technologies for trustworthy computing
- Wireless security
- Web security, including client-side and server-side security

The USENIX Security Symposium is primarily a systems security conference. Papers whose contributions are primarily new cryptographic algorithms or protocols, cryptanalysis, electronic commerce primitives, etc., may not be appropriate for this conference.

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.

The Proceedings will be available online for registered attendees before the Symposium and for everyone starting on the opening day of the technical sessions. Attendees may choose also to receive a USB drive pre-loaded with the Proceedings.

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 sec13chair@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 sec13it@usenix.org by Thursday, February 21, 2012, 11:59 p.m. EST.

Panel Discussions

The technical sessions may include topical panel discussions. Please send topic suggestions and proposals to sec13chair@usenix.org. The deadline for panel proposals is Friday, April 12, 2013, 11:59 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 linked from www.usenix.org/conference/usenixsecurity13/symposium-activities by Tuesday, July 9, 2013, 11:59 p.m. EDT. Decisions will be made by Thursday, July 18, 2013. 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 14, 2013. 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 sec13rump@usenix.org by Wednesday, August 14, 2012, 11:59 a.m. EDT.

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 21, 2013, at 11:59 p.m. EST (firm deadline). All submissions will be made online via the Web form on the Call for Papers Web site, https://www.usenix.org/conference/usenixsecurity13/submitting-papers. 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 on the Call for Papers Web site when preparing your paper for submission.

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. Note that while submissions will remain anonymous during the review process, authors' names and affiliations will be revealed to the reviewers after the reviews are complete, before the program committee meeting.

New in 2013: 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 sec13chair@usenix.org if you have any questions.

Papers that do not comply with the submission requirements, including length and anonymity, may be rejected without review.

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 sec13chair@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. See the USENIX Conference Submissions Policy at www.usenix.org/conferences/submissions-policy for details. Questions? Contact your program chair, sec13chair@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 '13 Web site; rejected submissions will be permanently treated as confidential.

Authors will be notified of acceptance by Tuesday, April 30, 2013. The final paper due date is Tuesday, June 25, 2013, 11:59 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 14, 2013.

Specific questions about submissions may be sent to the program chair at sec13chair@usenix.org.

Rev. 11/19/12