USENIX Security '16: 25th USENIX Security Symposium

August 10–12, 2016 • Austin, TX

Sponsored by USENIX, the Advanced Computing Systems Association

usenix THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

Important Dates

- Paper submissions due: **Thursday, February 18, 2016, 9:00 pm EST**
- Invited talk and panel proposals due: **Thursday, February 18, 2016, 9:00 pm EST**
- Early reject notification and author appeal period: **April 6-8, 2016**
- Notification to authors: **Monday, May 16, 2016**
- Final papers due: **Tuesday, June 28, 2016, 9:00 pm EDT**
- Poster submissions due: **Thursday, July 7, 2016, 9:00 pm EDT**
- Notification to poster presenters: **Thursday, July 14, 2016**
- Work-in-Progress submissions due: **Wednesday, August 10, 2016, noon CDT**

Conference Organizers

Program Co-Chairs

Thorsten Holz, *Ruhr-Universtät Bochum*
Stefan Savage, *University of California, San Diego*

Program Committee

Michael Backes, *CISPA, Saarland University & MPI-SWS*
Michael Bailey, *University of Illinois at Urbana-Champaign*
Davide Balzarotti, *Eurecom*
Lujo Bauer, *Carnegie Mellon University*
Leyla Bilge, *Symantec*
Dan Boneh, *Stanford University*
Joseph Bonneau, *Stanford University and The Electronic Frontier Foundation*
Nikita Borisov, *University of Illinois at Urbana-Champaign*
Elie Bursztein, *Google*
Juan Caballero, *IMDEA Software Institute*
Srdjan Capkun, *ETH Zürich*
Stephen Checkoway, *University of Illinois at Chicago*
Nicolas Christin, *Carnegie Mellon University*
Manuel Costa, *Microsoft Research*
George Danezis, *University College London*
Tamara Denning, *University of Utah*
Adam Doupé, *Arizona State University*
Tudor Dumitraş, *University of Maryland, College Park*
Manuel Egele, *Boston University*
Serge Egelman, *University of California, Berkeley, and International Computer Science Institute*
David Evans, *University of Virginia*
Cédric Fournet, *Microsoft Research*
Matthew Fredrikson, *Carnegie Mellon University*
Cristiano Giuffrida, *Vrije Universiteit Amsterdam*
Matthew Green, *Johns Hopkins University*
Chris Grier, *DataBricks*
Guofei Gu, *Texas A&M University*
Saikat Guha, *Microsoft Research India*
Alex Halderman, *University of Michigan*
Nadia Heninger, *University of Pennsylvania*
Cynthia Irvine, *Naval Postgraduate School*
Martin Johns, *SAP Research*
Engin Kirda, *Northeastern University*
Tadayoshi Kohno, *University of Washington*
Farinaz Koushanfar, *University of California, San Diego*
Per Larsen, *University of California, Irvine*
Wenke Lee, *Georgia Tech*
Nektarios Leontiadis, *Facebook*
Janne Lindqvist, *Rutgers University*
Ben Livshits, *Microsoft Research*
Michelle Mazurek, *University of Maryland, College Park*
Stephen McCamant, *University of Minnesota*
Damon McCoy, *George Mason University*
Jonathan McCune, *Google*
Sarah Meiklejohn, *University College London*
Prateek Mittal, *Princeton University*
Tyler Moore, *University of Tulsa*
Arvind Narayanan, *Princeton University*
Nick Nikiforakis, *Stony Brook University*
Cristina Nita-Rotaru, *Northeastern University*
Mathias Payer, *Purdue University*
Zachary N. J. Peterson, *California Polytechnic State University*
Frank Piessens, *Katholieke Universiteit Leuven*
Michalis Polychranakis, *Stony Brook University*
Raluca Popa, *University of California, Berkeley*
Christina Pöpper, *New York University*
Adrienne Porter Felt, *Google*
Georgios Portokalidis, *Stevens Institute of Technology*
Niels Provos, *Google*
Tom Ristenpart, *Cornell Tech*
Will Robertson, *Northeastern University*
Franziska Roesner, *University of Washington*

Andrei Sabelfeld, *Chalmers University of Technology*
Ahmad-Reza Sadeghi, *Technische Universität Darmstadt*
Felix Schuster, *Microsoft Research*
Jörg Schwenk, *Ruhr-Universität Bochum*
Hovav Shacham, *University of California, San Diego*
Micah Sherr, *Georgetown University*
Elaine Shi, *University of Maryland, College Park*
Reza Shokri, *The University of Texas at Austin*
Deian Stefan, *University of California, San Diego*
Gianluca Stringhini, *University College London*
Cynthia Sturton, *The University of North Carolina at Chapel Hill*
Kurt Thomas, *Google*
Patrick Traynor, *University of Florida*
Giovanni Vigna, *University of California, Santa Barbara*
David Wagner, *University of California, Berkeley*
Nick Weaver, *International Computer Science Institute*

Invited Talks Chair
Adrienne Porter Felt, Google

Invited Talks Committee
Tyrone Grandison, *US Department of Commerce*
Alex Halderman, *University of Michigan*
Franziska Roesner, *University of Washington*
Elaine Shi, *Cornell University*

Poster Session Chair
Raluca Popa, *University of California, Berkeley*

Poster Session Committee Members
Nikita Borisov, *University of Illinois at Urbana-Champaign*
Mathias Payer, *Purdue University*

Steering Committee
Matt Blaze, *University of Pennsylvania*
Dan Boneh, *Stanford University*
Kevin Fu, *University of Michigan*
Casey Henderson, *USENIX Association*
Jaeyeon Jung, *Microsoft Research*
Tadayoshi Kohno, *University of Washington*
Niels Provos, *Google*
David Wagner, *University of California, Berkeley*
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 the security and privacy of computer systems and networks. The 25th USENIX Security Symposium will be held August 10–12, 2016, in Austin, TX.

All researchers are encouraged to submit papers covering novel and scientifically significant practical works in computer security. Submissions are due on Thursday, February 18, 2016, 9:00 pm EST. The Symposium will span three days, with a technical program including refereed papers, invited talks, panel discussions, posters, a Work-in-Progress session, Doctoral Colloquium, and Birds-of-a-Feather sessions (BoFs). Workshops will precede the Symposium on August 8 and 9.

Symposium Topics

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

- System security
  - Operating systems security
  - Web security
  - Mobile systems security
  - Distributed systems security
  - Cloud computing security
- Network security
  - Intrusion and anomaly detection and prevention
  - Network infrastructure security
  - Denial-of-service attacks and countermeasures
  - Wireless security
- Cryptographic implementation analysis and construction
- Applied cryptography
- Security analysis
  - Malware analysis
  - Analysis of network and security protocols
  - Attacks with novel insights, techniques, or results
  - Forensics and diagnostics for security
  - Automated security analysis of hardware designs and implementation
  - Automated security analysis of source code and binaries
  - Program analysis
- Security measurement studies
  - Measurements of fraud, malware, spam
  - Measurements of human behavior and security
- Privacy-enhancing technologies and anonymity
- Usable security and privacy
- Language-based security
- Hardware security
  - Secure computer architectures
  - Embedded systems security
  - Methods for detection of malicious or counterfeit hardware
  - Side channels
- Research on surveillance and censorship
- Social issues and security
  - Research on computer security law and policy
  - Ethics of computer security research
  - Research on security education and training

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.

Given the rapidly expanding and maturing security and privacy community, we hope to increase the acceptance rate of papers that are more "far-reaching" and "risky," as long as those papers also show sufficient promise for creating interesting discussions and questioning widely-held beliefs.

Refereed Papers

Papers that have been formally reviewed and accepted will be presented during the Symposium and published in the Symposium Proceedings. It is required that one of the paper authors 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/2016_consent_author.pdf for the complete terms of publication.

Symposium Activities

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 co-chairs at sec16chairs@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 sec16it@usenix.org by Thursday, February 18, 2016, 9:00 pm EST.

Panel Discussions

The technical sessions may include topical panel discussions. Please send topic suggestions and proposals to sec16chairs@usenix.org by Thursday, February 18, 2016, 9:00 pm EST.

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 on the Call for Papers Web site, www.usenix.org/usenixsecurity16/cfp, by Thursday, July 7, 2016, 9:00 pm EDT. Decisions will be made by Thursday, July 14, 2016. 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.

Work-in-Progress Session

We will host a WiP session (previously known as rump session) on the evening of Wednesday, August 10, 2016. 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 and funny talks are encouraged! To submit a WiP talk, email sec16wips@usenix.org by Wednesday, August 10, 2016, noon CDT.

Doctoral Colloquium

What opportunities await security students graduating with a Ph.D.? On Thursday evening, students will have the opportunity to listen to informal panels of faculty and industrial researchers providing personal perspectives on their post-Ph.D. 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. If you are interested in speaking about your post-Ph.D. experiences at the Doctoral Colloquium, please email sec16dc@usenix.org.

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 onsite or in advance. To schedule 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 policies and requirements. Please read the following text carefully.

Submissions are due by **Thursday, February 18, 2016, 9:00 pm EST (hard deadline);** no abstract submission is required. All submissions will be made online via the Web form on the Call for Papers Web site, www.usenix.org/usenixsecurity16/cfp. Submissions should be finished, complete papers.

Paper submissions should be at most 13 typeset pages, excluding bibliography and well-marked appendices. These appendices may be included to assist reviewers who may have questions that fall outside the stated contribution of the paper on which your work is to be evaluated or to provide details that would only be of interest to a small minority of readers. There is no limit on the length of the bibliography and appendices, but reviewers are not required to read any appendices so the paper should be self-contained without them. Once accepted, papers must be reformatted to fit in 18 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/conferences/author-resources/paper-templates when preparing your paper for submission. Failure to adhere to the page limit and formatting requirements can be grounds for rejection.

Conflicts of Interest

The program co-chairs require cooperation from both authors and program committee members to prevent submissions from being evaluated by reviewers who have a conflict of interest. During the submission process, we will ask authors identify members of the program committee with whom they share a conflict of interest. This includes anyone who shares an institutional affiliation with an author at the time of submission, anyone who was the advisor or advisee of an author at any time in the past, or anyone the author has collaborated or published with in the prior two years.

Program committee members who are conflicts of interest with a paper, including program co-chairs, will be excluded from both online and in-person evaluation and discussion of the paper by default. With the program committee's transition from one to two program chairs, the program co-chairs may now submit papers, so long as there is one chair who is not an author of the submission. The program co-chair who is not the author of the paper will be responsible for managing the other program co-chair's paper.

Early Rejection and Appeals (New This Year!)

There will be no conventional rebuttal process. Papers that receive substantially negative initial reviews will be rejected early, and at the same time, the initial reviews of all submissions will be sent to the authors. Authors who substantively disagree with the reviews can appeal to the PC chairs. Authors' appeals must clearly and explicitly identify concrete disagreements with factual statements in the initial reviews that should be adjudicated by a special arbitration reviewer who may be recruited by the PC chairs. Appealing a submission that was rejected early will keep it under consideration, and it cannot be withdrawn or resubmitted elsewhere until the final notification of acceptance or rejection.

Anonymous Submission

Papers 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. Papers that are not properly anonymized may be rejected without review.

While authors will not be identified during the bulk of the review process, anonymity will expire after the great majority of reviews have been submitted and preliminary outcomes decided. While USENIX Security required authors to disclose their identities during the first two decades, we transitioned to anonymous submission in 2011 to prevent knowledge of authors' identities from biasing reviewers. In 2014, we began revealing the identities of authors to reviewers toward the end of the review process—after reviewers had submitted their evaluations of the paper. This allows reviewers to identify mistaken assumptions they have made about the authorship of the paper, identify conflicts

of interest that might have otherwise gone unnoticed, and to ameliorate any other damage caused by false assumptions about a paper's authorship. To ensure transparency and determine the effectiveness of this approach, changes to reviews and paper outcomes that follow, and potentially result from, revelations of the authors' identities will be monitored and reported on.

Facebook Internet Defense Prize

The Internet Defense Prize recognizes and rewards research that meaningfully makes the internet more secure. Created in 2014, the award is funded by Facebook and offered in partnership with USENIX to celebrate contributions to the protection and defense of the internet. Successful recipients of the Internet Defense Prize will provide a working prototype that demonstrates significant contributions to the security of the internet, particularly in the areas of prevention and defense. This award is meant to recognize the direction of the research and not necessarily its progress to date. The intent of the award is to inspire researchers to focus on high-impact areas of research.

You may submit your USENIX Security '16 paper submission for consideration for the Prize as part of the regular submission process. Find out more about the Prize at internetdefenseprize.org.

Human Subjects and Ethical Considerations

Submissions that describe experiments on human subjects, that analyze data derived from human subjects (even anonymized data), or that otherwise may put humans at risk should

1. Disclose whether the research received an approval or waiver from each of the authors' institutional ethics review boards (IRB)—if applicable.
2. Discuss steps taken to ensure that participants and others who might have been affected by an experiment were treated ethically and with respect.

If the submission deals with vulnerabilities (e.g., software vulnerabilities in a given program or design weaknesses in a hardware system), the authors need to discuss in detail the steps they plan to take to address these vulnerabilities (e.g., by disclosing vulnerabilities to the vendors). The same applies if the submission deals with personal identifiable information (PII) or other kinds of sensitive data. If a paper raises significant ethical and legal concerns, it might be rejected based on these concerns.

Authors seeking ways to reduce the ethical risks of their experiments may optionally consider reaching out to the Ethics Feedback Panel for Networking and Security at www.ethicalresearch.org/efp/netsec/. The panel's mission is to help researchers identify ethics-related risks, find prior research that provides precedent or data to inform ethical decision making, to suggest ways to improve experimental designs to reduce ethical risks, and provide any other information that may assist the researchers in meeting their ethical obligations. The best time to reach out to this panel is before conducting your experiments, but they may be able to assist if concerns arise during an experiment. Contact the program co-chairs at sec16chairs@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 co-chairs at sec16chairs@usenix.org. Simultaneous submission of the same work to multiple venues, submission of previously published work, or plagiarism constitutes dishonesty or fraud. Failure to point out and explain overlap will be grounds for rejection. 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/author-resources/submissions-policy for details. Questions? Contact your program co-chairs, sec16chairs@usenix.org, or the USENIX office, submissionspolicy@usenix.org.

The program committee and external reviewers are required to treat all submissions as confidential. However, the program co-chairs or designated committee members may share submissions outside the program committee to allow chairs of other conferences to identify dual submissions.

Papers that do not comply with the submission requirements, including length and anonymity, or that do not have a clear application to security or privacy may be rejected without review. Papers accompanied by nondisclosure agreement forms will not be considered.

Authors will be notified of acceptance by Monday, May 16, 2016. The final paper due date is Tuesday, June 28, 2016, 9:00 pm EDT. 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 10, 2016.

Specific questions about submissions may be sent to the program co-chairs at sec16chairs@usenix.org. The chair will respond to individual questions about the submission process if contacted at least a week before the submission deadline.