Announcement and Call for Papers www.usenix.org/sec18/cfp

27th USENIX Security Symposium

August 15–17, 2018 • Baltimore, MD, USA

Sponsored by USENIX, the Advanced Computing Systems Association

Important Dates

- Paper submissions due: **Thursday, February 8, 2018, 5:00 p.m. PST**
- Invited talk and panel proposals due: **Thursday, February 8, 2018, 5:00 p.m. PST**
- Early reject notification: **Tuesday, March 20, 2018**
- Author responses: **March 20–22, 2018**
- Notification to authors: **Friday, May 4, 2018**
- Final papers due: **Thursday, June 28, 2018, 9:00 p.m. PDT**
- Poster proposals due: **Thursday, July 5, 2018, 9:00 p.m. PDT**
- Notification to poster presenters: **Thursday, July 12, 2018**
- Lightning Talks submissions due: **Wednesday, August 15, 2018, 12:00 pm EDT**

Symposium Organizers

Program Co-Chairs

William Enck, *North Carolina State University*
Adrienne Porter Felt, *Google*

Program Committee

Sadia Afroz, *International Computer Science Institute*
Devdatta Akhawe, *Dropbox*
Johanna Amann, *International Computer Science Institute*
Adam Aviv, *US Naval Academy*
Michael Bailey, *University of Illinois Urbana-Champaign*
David Barrera, *École Polytechnique de Montréal*
Adam Bates, *University of Illinois Urbana-Champaign*
Lujo Bauer, *Carnegie Mellon University*
Steven Bellovin, *Columbia University*
Joseph Bonneau, *New York University*
Herbert Bos, *Vrije Universiteit Amsterdam*
Kevin Butler, *University of Florida*
Joe Calandrino, *Federal Trade Commission*
Srdjan Capkun, *ETH Zurich*
Justin Cappos, *New York University*
Lorenzo Cavallaro, *Royal Holloway, University of London*
Neha Chachra, *Facebook*
Weidong Cui, *Microsoft Research*
Nathan Dautenhahn, *University of Pennsylvania*
Lucas Davi, *University of Duisburg-Essen*
Razvan Deaconescu, *University POLITEHNICA of Bucharest*
Brendan Dolan-Gavitt, *New York University*
Adam Doupe, *Arizona State University*
Tudor Dumitras, *University of Maryland, College Park*
Zakir Durumeric, *Stanford University*
Manuel Egele, *Boston University*
Sascha Fahl, *Leibniz University Hannover*
Kassem Fawaz, *University of Wisconsin–Madison*
Earlence Fernandes, *University of Washington*
Carrie Gates, *Securelytix*
Guofei Gu, *Texas A&M University*
Nadia Heninger, *University of Pennsylvania*
Thorsten Holz, *Ruhr-Universität Bochum*
Cynthia Irvine, *Naval Postgraduate School*
Trent Jaeger, *Pennsylvania State University*
Suman Jana, *Columbia University*
Mobin Javed, *Lahore University of Management Sciences (LUMS) and International Computer Science Institute, Berkeley*
Alex Kapravelos, *North Carolina State University*
Aniket Kate, *Purdue University*
Taesoo Kim, *Georgia Institute of Technology*
Yongdae Kim, *Korea Advanced Institute of Science and Technology*
Engin Kirda, *Northeastern University*
Yoshi Kohno, *University of Washington*
Farinaz Koushanfar, *University of California, San Diego*
Bo Li, *University of California, Berkeley*
Kangjie Lu, *University of Minnesota, Twin Cities*
Long Lu, *Northeastern University*
Mohammad Mannan, *Concordia University, Montreal*
Ivan Martinovic, *Oxford University*
Stephen McCamant, *University of Minnesota*
Damon McCoy, *New York University*
Jon McCune, *Google*
Patrick McDaniel, *Pennsylvania State University*
Prateek Mittal, *Princeton University*
Tom Moyer, *University of North Carolina, Charlotte*
Adwait Nadkarni, *College of William and Mary*
Muhammad Naveed, *University of Southern California*
Nick Nikiforakis, *Stony Brook University*
Cristina Nita-Rotaru, *Northeastern University*
Alina Oprea, *Northeastern University*
Mathias Payer, *Purdue University*
Zachary Peterson, *Cal Poly*
Raluca Popa, *University of California, Berkeley*

Rev. 1/25/18

Christina Pöpper, *NYU Abu Dhabi*
Brad Reaves, *North Carolina State University*
Tom Ristenpart, *Cornell Tech*
Ahmad Sadeghi, *Technischen Universität Darmstadt*
Alessandra Scafuro, *North Carolina State University*
Vyas Sekar, *Carnegie Mellon University*
Micah Sherr, *Georgetown University*
Matthew Smith, *Universität Bonn, Fraunhofer FKIE*
Jessica Staddon, *Google*
Emily Stark, *Google*
Gianluca Stringhini, *University College London*
Cynthia Sturton, *University of North Carolina, Chapel Hill*
Nick Sullivan, *Cloudflare*
Patrick Tague, *Carnegie Mellon University, Silicon Valley*
Gang Tan, *Pennsylvania State University*
Vanessa Teague, *University of Melbourne*
Kurt Thomas, *Google*
Yuan Tian, *University of Virginia*
Patrick Traynor, *University of Florida*
Tanvi Vyas, *Mozilla*
Dan Wallach, *Rice University*
Gang Wang, *Virginia Tech*
Eric Wustrow, *University of Colorado Boulder*
Dongyan Xu, *Purdue University*

Invited Talks Committee

Frank Chen, *Andreessen Horowitz*
Kevin Fu (Chair), *University of Michigan*
Casey Henderson, *USENIX Association*
Matthew Scholl, *National Institute of Standards and Technology (NIST)*

Steering Committee

Matt Blaze, *University of Pennsylvania*
Dan Boneh, *Stanford University*
Kevin Fu, *University of Michigan*
Casey Henderson, *USENIX Association*
Thorsten Holz, *Ruhr-Universität Bochum*
Jaeyeon Jung, *Microsoft Research*
Engin Kirda, *Northeastern University*
Tadayoshi Kohno, *University of Washington*
Niels Provos, *Google*
Thomas Ristenpart, *Cornell Tech*
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 27th USENIX Security Symposium will be held August 15–17, 2018, in Baltimore, MD, USA.

All researchers are encouraged to submit papers covering novel and scientifically significant practical works in computer security. Submissions are due on Thursday, February 8, 2018, 5:00 p.m. PST. The Symposium will span three days, with a technical program including refereed papers, invited talks, posters, panel discussions, and Birds-of-a-Feather sessions. Co-located workshops will precede the Symposium on August 13 and 14.

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
- 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
- Data-driven security and 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
- Applications of cryptography
  - Analysis of deployed cryptography and cryptographic protocols
  - Cryptographic implementation analysis
  - New cryptographic protocols with real-world applications

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.

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/2018_sample_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 sec18chairs@usenix.org.

Invited Talks and Panel Discussions

Invited talks and panel discussions will be held in parallel with the refereed paper sessions. Please submit topic suggestions and talk and panel proposals via email to sec18it@usenix.org by Thursday, February 8, 2018, 5:00 p.m. PST.

Poster Session

Would you like to share a provocative opinion, an 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 the USENIX Security '18 website at www.usenix.org/sec18/cfp by Thursday, July 5, 2018, 9:00 p.m. PDT. Decisions will be made by Thursday, July 12, 2018. 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.

Lightning Talks

We will host a Lightning Talks session (also previously known as Work-in-Progress/Rump session) on the evening of Wednesday, August 15, 2018. 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 USENIX Security attendees. As in the past, talks do not always need to be serious and funny talks are encouraged! This year, USENIX will generously sponsor awards for the most engaging talks. Bragging rights and small cash prizes can be yours for a great talk! For full consideration, submit your lightning talk via the lighting talk submission form linked from the USENIX Security '18 website at www.usenix.org/sec18/cfp through July 27, 2018. Only talks submitted by this deadline will be considered for the awards. You can continue submitting talks via the submission form or by emailing sec18lightning@usenix.org until Wednesday, August 15, 2018, 12:00 pm EDT.

Doctoral Colloquium

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. If you would like to speak in the Doctoral Colloquium, please email sec18dc@usenix.org.

Birds-of-a-Feather Sessions (BoFs)

Birds-of-a-Feather sessions (BoFs) will be held Tuesday, Wednesday, and Thursday evenings. BoFs are informal gatherings of persons interested in a particular topic and 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 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.

Submission Policies and Instructions

Submission Policies

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 8, 2018, 5:00 p.m. PST (hard deadline).** All submissions will be made online via the web form linked from the USENIX Security '18 website at www.usenix.org/sec18/cfp. Do not email submissions. Submissions should be finished, complete papers, and we may reject papers without review that have severe editorial problems (broken references, egregious spelling or grammar errors, figures, etc.).

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" x 9", on 8.5" x 11" (letter-sized) paper. If you wish, please make use of USENIX's LaTeX template and style files, 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 to identify members of the program committee with whom they share a conflict of interest. This includes: (1) anyone who shares an institutional affiliation with an author at the time of submission, (2) anyone who was the advisor or advisee of an author at any time in the past, (3) anyone the author has collaborated or published with in the prior two years, (4) anyone who is serving as the sponsor or administrator of a grant that funds your research, or (5) close personal friendships. For other forms of conflict, authors must contact the chairs and explain the perceived conflict.

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.

Early Rejection Notification

The review process will consist of several reviewing rounds. In order to allow authors time to improve their work and submit to other venues, authors of submissions for which there is a consensus on rejection will be notified earlier (March 20, 2018).

Author Responses

Authors of papers that have not been rejected early will have an opportunity to respond to an initial round of reviews. We encourage authors to focus on questions posed by reviewers and significant factual corrections. The response period is March 20–22, 2018.

Anonymous Submission

The review process will be double blind. Papers must be submitted in a form suitable for anonymous review:

- The title page should not contain any author names or affiliations.
- Authors should carefully review figures and appendices (especially survey instruments) to ensure affiliations are not accidentally included.
- 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.

- Authors may include links to websites that contain source code, tools, or other supplemental material. The link in the paper should not contain the author's name or affiliation. However, the website itself may contain the authors' names and affiliations.

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

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 '18 paper submission for consideration for the Prize as part of the regular submission process. More details will be available here soon. Find out more about the Internet Defense 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 (e.g., an IRB).
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 personally 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.

Contact the program co-chairs at sec18chairs@usenix.org if you have any questions.

Submission Instructions

All submissions will be made online via the web form linked from the USENIX Security '18 website at www.usenix.org/sec18/cfp. Do not email submissions. 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 sec18chairs@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 for details. Questions? Contact your program co-chairs, sec18chairs@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 Friday, May 4, 2018. The final paper due date is Thursday, June 28, 2018, 9:00 p.m. PDT. 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.