28th USENIX Security Symposium

August 14–16, 2019 • Santa Clara, CA, USA

Sponsored by USENIX, the Advanced Computing Systems Association

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 28th USENIX Security Symposium will be held August 14–16, 2019, in Santa Clara, CA.

Important: *The USENIX Security Symposium is moving to multiple submission deadlines for USENIX Security '19. This change includes changes to the review process and submission policies. Detailed information is available on the USENIX Security Publication Model Changes web page at www.usenix.org/conference/usenixsecurity19/publication-model-change.*

All researchers are encouraged to submit papers covering novel and scientifically significant practical works in computer security. There will be two quarterly submission deadlines for USENIX Security '19. The fall quarter submissions deadline is **Thursday, November 15, 2018, 5:00 pm PST**. The winter quarter submissions deadline is **Friday, February 15, 2019, 5:00 pm 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 events will precede the Symposium on August 12 and 13.

Important Dates

Fall Quarter Deadline

- Refereed paper submissions due: **Thursday, November 15, 2018, 5:00 pm PST**
- Early reject notification: **Friday, December 14, 2018**
- Author responses due: **Tuesday, December 18, 2018**
- Notification to authors: **Friday, January 18, 2019**
- Final papers due: **Monday, February 18, 2019, 9:00 pm PST**

Winter Quarter Deadline

- Refereed paper submission due: **Friday, February 15, 2019, 5:00 pm PST**
- Early reject notification: **Thursday, March 21, 2019**
- Author responses due: **Tuesday March 26, 2019**
- Notification to authors: **Wednesday, May 1, 2019**
- Final papers due: **Saturday, June 1, 2019, 9:00 pm PDT**
- Invited talk and panel proposals due: **Friday, February 15, 2019, 5:00 pm PST**
- Poster proposals due: **Tuesday, July 9, 2019, 9:00 pm PDT**
- Notification to poster presenters: **Tuesday, July 16, 2019**
- Lightning Talks submissions due: **Wednesday, August 14, 2019, 12:00 pm PDT**

Symposium Organizers

Program Co-Chairs

Nadia Heninger, *University of Pennsylvania*
Patrick Traynor, *University of Florida*

Program Committee

Yasemin Acar, *Leibniz University Hannover*
Sadia Afroz, *University of California, Berkeley/International Computer Science Institute*
Devdatta Akhawe, *Dropbox*
Johanna Amann, *International Computer Science Institute*
Adam Aviv, *United States Naval Academy*
Michael Bailey, *University of Illinois at Urbana–Champaign*
Adam Bates, *University of Illinois at Urbana–Champaign*
Vincent Bindschaedler, *University of Florida*
Joseph Bonneau, *Princeton University*
Nikita Borisov, *University of Illinois at Urbana–Champaign*
Sven Bugiel, *CISPA Helmholtz Center i.G.*
Kevin Butler, *University of Florida*
Joe Calandrino, *Federal Trade Commission*
Stefano Calzavara, *Università Ca' Foscari Venezia*
Yinzhi Cao, *Johns Hopkins University*
Srdjan Capkun, *ETH Zurich*
Lorenzo Cavallaro, *King's College London*
Stephen Checkoway, *Oberlin College*
Bill Cheswick, *AT&T Labs—Research*
Marshini Chetty, *Princeton University*
Mihai Christodorescu, *VISA Research*
Erinn Clark, *First Look Media*
George Danezis, *University College London*
Nathan Dautenhahn, *Rice University*
Roger Dingledine, *The Tor Project*
Adam Doupe, *Arizona State University*
Thomas Dullien, *Google*
Zakir Durumeric, *Stanford University*
Manuel Egele, *Boston University*
William Enck, *North Carolina State University*

Roya Ensafi, *University of Michigan*
David Evans, *University of Virginia*
Sascha Fahl, *Leibniz University Hannover*
Giulia Fanti, *Carnegie Mellon University*
Nick Feamster, *Princeton University*
Adrienne Porter Felt, *Google*
Earlence Fernandes, *University of Washington*
David Freeman, *LinkedIn Corporation*
Daniel Genkin, *University of Michigan*
Neil Gong, *Iowa State University*
Matthew Green, *Johns Hopkins Information Security Institute*
Rachel Greenstadt, *Drexel University*
Daniel Gruss, *Graz University of Technology*
Joseph Lorenzo Hall, *Center for Democracy & Technology*
Xiali (Sharon) Hei, *University of Louisiana at Lafayette*
Thorsten Holz, *Ruhr-University Bochum*
Trent Jaeger, *The Pennsylvania State University*
Rob Jansen, *U.S. Naval Research Laboratory*
Mobin Javed, *Lahore University of Management Sciences*
Chris Kanich, *University of Illinois at Chicago*
Vasileios Kemerlis, *Brown University*
Yongdae Kim, *Korea Advanced Institute of Science and Technology (KAIST)*
Lea Kissner, *Google*
Yoshi Kohno, *University of Washington*
Farinaz Koushanfar, *University of California, San Diego*
Katharina Krombholz, *CISPA Helmholtz Center i.G.*
Ben Laurie, *Google*
Tancrde Lepoint, *Google*
Martina Lindorfer, *Technische Universität Wien*
Allison Mankin, *Salesforce*
Ivan Martinovic, *Oxford University*
Stephen McCamant, *University of Minnesota*
Jon McCune, *Google*
Patrick McDaniel, *The Pennsylvania State University*
Sarah Meiklejohn, *University College London*
Jelena Mirkovic, *USC/Information Sciences Institute*
Prateek Mittal, *Princeton University*
Veelasha Moonsamy, *Utrecht University*
Adwait Nadkarni, *College of William & Mary*
Yossi Oren, *Ben-Gurion University of the Negev*
Nicolas Papernot, *The Pennsylvania State University*
Kenny Paterson, *Royal Holloway*
Mathias Payer, *École Polytechnique Fédérale de Lausanne (EPFL)*
Giancarlo Pellegrino, *Stanford University*
Christina Pöpper, *New York University Abu Dhabi*
Brad Reaves, *North Carolina State University*
Elissa Redmiles, *University of Maryland*
Konrad Rieck, *Technische Universität Braunschweig*
Tom Ristenpart, *Cornell Tech*
Tom Ritter, *Mozilla*
Franziska Roesner, *University of Washington*
Ahmad-Reza Sadeghi, *Technische Universität Darmstadt*
Prateek Saxena, *National University of Singapore*
Nolen Scaife, *University of Florida*
Wendy Seltzer, *W3C/Massachusetts Institute of Technology*
Micah Sherr, *Georgetown University*
Deian Stefan, *University of California, San Diego*
Ben Stock, *CISPA Helmholtz Center i.G.*
Gianluca Stringhini, *Boston University*
Dave 'Jing' Tian, *University of Florida*
Luke Valenta, *University of Pennsylvania*
Ingrid Verbauwhede, *Katholieke Universiteit Leuven*
David Wagner, *University of California, Berkeley*
Byron Williams, *University of Florida*
Eric Wustrow, *University of Colorado Boulder*
Wenyuan Xu, *Zhejiang University*
Yuval Yarom, *University of Adelaide and Data61*
Tuba Yavuz, *University of Florida*
Daniel Zappala, *Brigham Young University*
Mary Ellen Zurko, *MIT Lincoln Laboratory*

Invited Talks Chair
Devdatta Akhawe, *Dropbox*

Steering Committee
Matt Blaze, *University of Pennsylvania*
Dan Boneh, *Stanford University*
William Enck, *North Carolina State University*
Kevin Fu, *University of Michigan*
Casey Henderson, *USENIX Association*
Thorsten Holz, *Ruhr-Universität Bochum*
Jaeyeon Jung, *Samsung Electronics*
Engin Kirda, *Northeastern University*
Tadayoshi Kohno, *University of Washington*
Adrienne Porter Felt, *Google*
Thomas Ristenpart, *Cornell Tech*
David Wagner, *University of California, Berkeley*

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. By submitting a paper, you agree that at least one of the authors will attend the conference to present it. If the conference registration fee will pose a hardship for the presenter of the accepted paper, please contact conference@usenix.org.

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/2019_sample_consent.pdf for the complete terms of publication.

Symposium Activities

Invited Talks, Panels, Poster 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 co-chairs at sec19chairs@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 sec19it@usenix.org by Friday, February 15, 2019, 5:00 pm 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 web form linked from the USENIX Security '19 website at www.usenix.org/sec19/cfp by Friday, July 9, 2019, 9:00 pm PDT. Decisions will be made by Friday, July 16, 2019. 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 14, 2019. 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! 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 '19 website at www.usenix.org/sec19/cfp through July 27, 2019. Only talks submitted by this deadline will be considered for the awards. You can continue submitting talks through the submission form or by emailing sec19lightning@usenix.org until Wednesday, August 14, 2019, 12:00 pm PDT.

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 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

Fall quarter submissions are due by **Thursday, November 15, 2018, 5:00 pm PST (hard deadline).** Winter quarter submissions are due by **Friday, February 15, 2019, 5:00 pm PST (hard deadline).** All papers that are accepted by the end of the winter submission reviewing cycle (February–May 2019) will be invited to present at USENIX Security '19. All submissions will be made online via the web form linked from the USENIX Security '19 website at www.usenix.org/sec19/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, missing figures, etc.) or are submitted in violation of the Submission Instructions outlined below.

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.

New in 2019: Papers should be typeset on U.S. letter-sized pages in two-column format in 10-point Times Roman type on 12-point leading (single-spaced), in a text block 7" x 9" deep. Please note that this text block size has changed. If you wish, please make use of USENIX's LaTeX template and style files 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 (December 14, 2018 for papers submitted by November 15, 2018; March 21, 2019, for papers submitted by February 15, 2019).

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 responses will be due December 18, 2018 for papers submitted by November 15, 2018, and March 26, 2019, for papers submitted by February 15, 2019.

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.

While submitted papers must be anonymous, authors may choose to give talks about their work, post a preprint of the paper online, disclose security vulnerabilities to vendors or the public, etc. during the review process.

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 have already taken or 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 sec19chairs@usenix.org if you have any questions.

Submission Instructions

All submissions will be made online via the web form linked from the USENIX Security '19 website at www.usenix.org/sec19/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 sec19chairs@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.

Note that under the changes to the USENIX Security publication model in 2019, papers that have received a decision of Major Revisions from USENIX Security are still considered to be under review for the following two review cycles after notification; authors must formally withdraw their paper if they wish to submit to another venue. See the USENIX Security Publication Model Changes web page at www.usenix.org/conference/usenixsecurity19/publication-model-change for details. The changes to the submission model and new rules about resubmission timelines apply to papers submitted starting in November 2018; this means that papers that were rejected from USENIX Security '18 may submit to the November 2018 submission deadline for USENIX Security '19 without violating any rules.

Questions? Contact your program co-chairs, sec19chairs@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, that do not comply with resubmission policies, 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.

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, 2019.

Specific questions about submissions may be sent to the program co-chairs at sec19chairs@usenix.org. The chairs will respond to individual questions about the submission process if contacted at least a week before the submission deadline.