

MAY 21-23, 2018 AT THE HYATT REGENCY, SAN FRANCISCO, CA

39th IEEE Symposium on Security and Privacy

Call For Papers

New submissions are no longer being accepted for the 2018 Symposium. Rolling submissions for the 2019 Symposium begin on January 1, 2018. See the 2019 Call for Papers (<http://www.ieee-security.org/TC/SP2019/cfpapers.html>) for more information.

Since 1980 in Oakland, the IEEE Symposium on Security and Privacy has been the premier forum for computer security research, presenting the latest developments and bringing together researchers and practitioners. We solicit previously unpublished papers offering novel research contributions in any aspect of security or privacy. Papers may present advances in the theory, design, implementation, analysis, verification, or empirical evaluation and measurement of secure systems.

Topics of interest include:

- Access control and authorization
- Accountability
- Anonymity
- Application security
- Attacks and defenses
- Authentication
- Censorship resistance
- Cloud security
- Distributed systems security
- Economics of security and privacy
- Embedded systems security
- Forensics
- Hardware security
- Intrusion detection and prevention
- Malware and unwanted software
- Mobile and Web security and privacy
- Language-based security
- Network and systems security
- Privacy technologies and mechanisms
- Protocol security
- Secure information flow
- Security and privacy for the Internet of Things
- Security and privacy metrics
- Security and privacy policies
- Security architectures

- Usable security and privacy

This topic list is not meant to be exhaustive; S&P is interested in all aspects of computer 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.

Systematization of Knowledge Papers

As in past years, we solicit systematization of knowledge (SoK) papers that evaluate, systematize, and contextualize existing knowledge, as such papers can provide a high value to our community. Suitable papers are those that provide an important new viewpoint on an established, major research area, support or challenge long-held beliefs in such an area with compelling evidence, or present a convincing, comprehensive new taxonomy of such an area. Survey papers without such insights are not appropriate. Submissions will be distinguished by the prefix “SoK:” in the title and a checkbox on the submission form. They will be reviewed by the full PC and held to the same standards as traditional research papers, but **they will be accepted based on their treatment of existing work and value to the community, and not based on any new research results they may contain**. Accepted papers will be presented at the symposium and included in the proceedings.

Workshops

The Symposium is also soliciting submissions for co-located workshops. Further details on submissions can be found at <https://www.ieee-security.org/TC/SP2018/workshops.html> (workshops.html) .

Ongoing Submissions

To enhance the quality and timeliness of the scientific results presented as part of the Symposium, and to improve the quality of our reviewing process, IEEE S&P now accepts paper submissions 12 times a year, on the first of each month. The detailed process is as follows.

- A rolling deadline occurs on the 1st of each month, at 3:00 PM (UTC-7, i.e., PDT). This deadline is strict and no extensions will be granted.
- Within two months of submission, author notifications of Accept/Revise/Reject decisions will be sent out.
- Within one month of acceptance, all accepted papers must submit a camera-ready copy incorporating reviewer feedback. The papers will immediately be published, open access, in the Computer Society’s Digital Library, and they may be cited as “To appear in the IEEE Symposium on Security & Privacy, May 20XX”.
- A limited number of papers will be invited to submit a revision; such papers will receive a specific set of expectations to be met by that revision. Authors may take up to three months from decision notification to produce a revised manuscript and submit it as part of the standard deadline on the 1st of the month. Authors will receive decisions on revisions within one month. See below for additional details on the resubmission procedure.
- Rejected papers must wait for one year, from the date of original submission, to resubmit to IEEE S&P.
 - A paper will be judged to be a resubmit (as opposed to a new submission) if the paper is from the same or similar authors, and a reviewer could write a substantially similar summary of the paper compared with the original submission. As a rule of thumb, if there is more than 40% overlap between the original submission and the new paper, it will be considered a resubmission.
- All papers **accepted** by February 1st, 2018, or that are submitted as a revision by February 1st, 2018 and the revision is then accepted, will be included in the proceedings of the symposium in May, 2018 and invited to present their work. Other papers will be included in the 2019 proceedings.
 - As a result, for authors who anticipate using the full three months to respond to a Revision decision, the final submission deadline for possible inclusion in the 2018 proceedings is September 1st, 2017.

- For authors who anticipate using only one month to respond to a Revision decision, the final submission deadline for possible inclusion in the 2018 proceedings is November 1st, 2017.
- The final submission deadline for possible inclusion in the 2018 proceedings is December 1st, 2017, but only for papers accepted without revision.

Revised Submissions

As described above, some number of papers will receive a Revise decision, rather than Accept or Reject. This decision will be accompanied by a detailed summary of the expectations for the revision, in addition to the standard reviewer comments. Authors may take up to three months to prepare a revision, which may include running additional experiments, improving the paper's presentation, or other such improvements. Papers meeting the expectations will typically be accepted. Those that do not will be rejected. Only in exceptional circumstances will additional revisions be requested.

Upon receiving a Revise decision, authors can choose to withdraw their paper or not submit a revision within three months, but they will be asked to not submit the same or similar work again (following the same rules as for Rejected papers) for 1 year from the date of the original submission.

Revised submissions should be submitted on the first of the month, just as with new submissions. Revisions must be accompanied by a summary of the changes that were made.

Submission Statistics

Statistics on the submissions and decisions made thus far are available here (<https://www.ieee-security.org/TC/SP2018/submissions.html>).

Student Program Committee

Following a successful model used at last year's conference, as well as other premier technical conferences, some paper submissions will be reviewed by a "shadow PC" of students and junior researchers, this year chaired by Thorsten Holz of Ruhr-University Bochum, Germany. For more information see <https://www.ieee-security.org/TC/SP2018/studentpc.html> (studentpc.html).

Instructions for Paper Submission

These instructions apply to both the research papers and systematization of knowledge papers.

All submissions must be original work; the submitter must clearly document any overlap with previously published or simultaneously submitted papers from any of the authors. Failure to point out and explain overlap will be grounds for rejection. Simultaneous submission of the same paper to another venue with proceedings or a journal is not allowed and will be grounds for automatic rejection. Contact the program committee chairs if there are questions about this policy.

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 papers 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. Publication as a technical report or in an online repository does not constitute a violation of this policy. Contact the program chairs if you have any questions. Papers that are not properly anonymized may be rejected without review.

Conflicts of Interest

Drawn from the ACM SIGMOD 2015 CFP

During submission of a research paper, the submission site will request information about conflicts of interest of the paper's authors with program committee (PC) members. It is the full responsibility of all authors of a paper to identify all and only their potential conflict-of-interest PC members, according to the following definition. A paper author has a conflict of interest with a PC member when and only when one or more of the following conditions holds:

1. The PC member is a co-author of the paper.
2. The PC member has been a co-worker in the same company or university within the past two years.
 - For student interns, the student is conflicted with their supervisors and with members of the same research group. If the student no longer works for the organization, then they are not conflicted with a PC member from the larger organization.
3. The PC member has been a collaborator within the past two years.
4. The PC member is or was the author's primary thesis advisor, no matter how long ago.
5. The author is or was the PC member's primary thesis advisor, no matter how long ago.
6. The PC member is a relative or close personal friend of the author.

For any other situation where the authors feel they have a conflict with a PC member, they must explain the nature of the conflict to the PC chairs, who will mark the conflict if appropriate. Papers with incorrect or incomplete conflict of interest information as of the submission closing time are subject to immediate rejection.

Human Subjects and Ethical Considerations

Drawn from the USENIX Security 2016 CFP

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 have 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 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.

Contact the program co-chairs oakland18-pcchairs@ieee-security.org (mailto:oakland18-pcchairs@ieee-security.org) if you have any questions.

Page Limit and Formatting

Submitted papers may include up to 13 pages of text and up to 5 pages for references and appendices, totalling no more than 18 pages. The same applies to camera-ready papers, although, at the PC chairs' discretion, additional pages may be allowed for references and appendices. Reviewers are not required to read appendices.

Papers must be formatted for US letter (not A4) size paper. The text must be formatted in a two-column layout, with columns no more than 9.5 in. tall and 3.5 in. wide. The text must be in Times font, 10-point or larger, with 11-point or larger line spacing. Authors are encouraged to use the IEEE conference proceedings templates.

LaTeX submissions should use IEEEtran.cls version 1.8. All submissions will be automatically checked for conformance to these requirements. Failure to adhere to the page limit and formatting requirements are grounds for rejection without review.

Reviews from Prior Submissions

Authors may optionally submit a document (PDF or text) containing:

1. the complete reviews they received from prior submission(s) and
2. a page of up to 500 words documenting the improvements made since the prior submission(s).

Also starting this year, if a submission is derived in any way from a submission submitted to another venue (conference, journal, etc.) in the past twelve months, we require that the authors provide the name of the most recent venue to which it was submitted. **This information will not be shared with reviewers.** It will only be used (1) for aggregate statistics to understand the percent of resubmissions among the set of submitted (and accepted) papers; (2) at the Chairs' discretion, to identify dual submissions and verify the accuracy of prior reviews provided by authors regarding previously rejected papers.

Submission

Submissions must be in Portable Document Format (.pdf). Authors should pay special attention to unusual fonts, images, and figures that might create problems for reviewers. Your document should render correctly in Adobe Reader 9 and when printed in black and white.

Conference Submission Server

Papers must be submitted at <https://oakland18.seclab.cs.ucsb.edu> (<https://oakland18.seclab.cs.ucsb.edu>).

Publication and Presentation

Authors are responsible for obtaining appropriate publication clearances. One of the authors of the accepted paper is expected to present the paper at the conference.

Program Committee

Chairs

Bryan Parno Carnegie Mellon University

Christopher Kruegel UC Santa Barbara

Associate Chairs

Lujo Bauer Carnegie Mellon University

Srdjan Capkun ETH Zurich

David Evans University of Virginia

Michael Hicks University of Maryland

Members

Manos Antonakakis	Georgia Institute of Technology
Michael Backes	CISPA
Davide Balzarotti	Eurecom
Gilles Barthe	IMDEA Software Institute
Karthik Bhargavan	INRIA
Leyla Bilge	Symantec Research Labs
Marina Blanton	University at Buffalo (SUNY)
Nikita Borisov	University of Illinois at Urbana-Champaign
Herbert Bos	Vrije Universiteit Amsterdam
Kevin Butler	University of Florida
Juan Caballero	IMDEA Software Institute
David Cash	Rutgers University
Haibo Chen	Shanghai Jiao Tong University
Stephen Chong	Harvard University
Manuel Costa	Microsoft Research
Cas Cremers	University of Oxford
Rob Cunningham	MIT Lincoln Laboratory
George Danezis	University College London
Antoine Delignat-Lavaud	Microsoft Research
Srini Devadas	Massachusetts Institute of Technology
Tudor Dumitras	University of Maryland, College Park
Manuel Egele	Boston University
Serge Egelman	UC Berkeley / ICSI
Sascha Fahl	Leibniz University Hannover
Cédric Fournet	Microsoft Research
Matt Fredrikson	Carnegie Mellon University
Kevin Fu	University of Michigan

Cristiano Giuffrida	Vrije Universiteit Amsterdam
Virgil Gligor	Carnegie Mellon University
Andreas Haeberlen	University of Pennsylvania
Nadia Heninger	University of Pennsylvania
Matthew Hicks	Virginia Tech
Thorsten Holz	Ruhr-University Bochum
Amir Houmansadr	University of Massachusetts Amherst
Trent Jaeger	Penn State University
Somesh Jha	University of Wisconsin, Madison
Rob Johnson	VMware Research
Brent Byunghoon Kang	KAIST
Engin Kirda	Northeastern University
Farinaz Koushanfar	University of California San Diego
Wenke Lee	Georgia Institute of Technology
Ruby Lee	Princeton University
Kirill Levchenko	UC San Diego
Jay Lorch	Microsoft Research
Long Lu	Northeastern University
Matteo Maffei	TU Wien
Bruce Maggs	Duke University and Akamai Technologies
Michelle Mazurek	University of Maryland
Andrew Miller	University of Illinois at Urbana-Champaign
Prateek Mittal	Princeton University
Payman Mohassel	Visa Research
Greg Morrisett	Cornell University
Michael Naehrig	Microsoft Research, USA
Arvind Narayanan	Princeton University
Muhammad Naveed	University of Southern California
Cristina Nita-Rotaru	Northeastern University

Marcus Peinado	Microsoft Research
Adrian Perrig	ETH Zurich
Christina Pöpper	New York University Abu Dhabi
Niels Provos	Google
Mariana Raykova	Yale University
Rob Reeder	Google
Ulrich Rührmair	Ruhr University Bochum
Andrei Sabelfeld	Chalmers University of Technology
Prateek Saxena	National University of Singapore
Simha Sethumadhavan	Columbia University/Chip Scan
Hovav Shacham	UC San Diego
Elaine Shi	Cornell
Asia Slowinska	IBM Security
Matthew Smith	University of Bonn, Fraunhofer FKIE
Adam Smith	Pennsylvania State University
Alex Snoeren	UC San Diego
Deian Stefan	UC San Diego
Gianluca Stringhini	University College London
Cynthia Sturton	University of North Carolina at Chapel Hill
Gang Tan	Pennsylvania State University
Stefano Tessaro	University of California, Santa Barbara
Kurt Thomas	Google
Carmela Troncoso	IMDEA Software Institute
Dan Wallach	Rice University
XiaoFeng Wang	Indiana University
Tao Xie	University of Illinois at Urbana-Champaign
Danfeng (Daphne) Yao	Virginia Tech
Yinqian Zhang	The Ohio State University