Announcement and Call for Papers www.usenix.org/soups2019/cfp

SOUPS 2019: Fifteenth Symposium on Usable Privacy and Security

AUGUST 11–13, 2019 • Santa Clara, CA, USA

In-cooperation with USENIX, the Advanced Computing Systems Association

SOUPS 2019 will be co-located with the 28th USENIX Security Symposium, August 11–13, 2019, in Santa Clara, CA, USA.

Important Dates

All dates are at 23:59 AoE (Anywhere on Earth) time.

- Paper registration deadline: **Thursday, February 21, 2019**
- Paper submission deadline: **Thursday, February 28, 2019**
- Early rejection notification: **Saturday, March 30, 2019**
- Rebuttal period: **Friday, April 26–Friday, May 3, 2019**
- Notification of paper acceptance: **Tuesday, May 14, 2019**
- Camera ready papers due: **Tuesday, June 18, 2019**

Symposium Organizers

General Chair

Heather Richter Lipford, *University of North Carolina at Charlotte*

Invited Talks Chair

Serge Egelman, *International Computer Science Institute*

Technical Papers Co-Chairs

Michelle Mazurek, *University of Maryland*
Rob Reeder, *Google*

Technical Papers Committee

Yasemin Acar, *Leibniz Universität Hannover*
Adam Aviv, *United States Naval Academy*
Lujo Bauer, *Carnegie Mellon University*
Konstantin Beznosov, *The University of British Columbia*
Tamara Bonaci, *Northeastern University and University of Washington*
Joe Calandrino, *Federal Trade Commission*
Sonia Chiasson, *Carleton University*
Nicolas Christin, *Carnegie Mellon University*
Lynne Coventry, *Northumbria University*
Serge Egelman, *International Computer Science Institute (ICSI) and University of California, Berkeley*
Sascha Fahl, *Ruhr-Universität Bochum*
Carrie Gates, *Bank of America*
Rachel Greenstadt, *New York University*
Iulia Ion, *Google*
Apu Kapadia, *Indiana University Bloomington*
Bart Knijnenburg, *Clemson University*
Katharina Krombholz, *Helmholtz Center for Information Security (CISPA)*
Susan McGregor, *Columbia University Graduate School of Journalism*
Emilee Rader, *Michigan State University*
Scott Ruoti, *The University of Tennessee, Knoxville*
Florian Schaub, *University of Michigan*
Kent Seamons, *Brigham Young University*
Manya Sleeper, *Google*
Matthew Smith, *University of Bonn*
Jessica Staddon, *Google*
Elizabeth Stobert, *National Research Council Canada*
Jose Such, *King's College London*
Nina Taft, *Google*
Mary Theofanos, *National Institute of Standards and Technology (NIST)*
Blase Ur, *The University of Chicago*
Kami Vaniea, *The University of Edinburgh*
Emanuel von Zezschwitz, *University of Bonn and Fraunhofer FKIE*
Rick Wash, *Michigan State University*

Lightning Talks and Demos Chair

Yousra Javed, *Illinois State University*
Scott Ruoti, *University of Kentucky*

Karat Award Chair

Kent Seamons, *Brigham Young University*

Posters Co-Chairs

Yasemin Acar, *Leibniz University Hannover*
Heather Crawford, *Florida Institute of Technology*

Tutorials and Workshops Co-Chairs

Elissa Redmiles, *University of Maryland*
Daniel Zappala, *Brigham Young University*

Publicity Co-Chairs

Nalin Asanka Gamagedara Arachchilage, *University of New South Wales*
Joe Calandrino, *Federal Trade Commission*

Program Committee Local Arrangements Chair

Kami Vaniea, *University of Edinburgh*

Email List Chair

Lorrie Cranor, *Carnegie Mellon University*

USENIX Liaison

Casey Henderson, *USENIX Association*

Steering Committee

Robert Biddle, *Carleton University*
Sonia Chiasson, *Carleton University*
Sunny Consolvo, *Google*
Lorrie Cranor, *Carnegie Mellon University*
Patrick Gage Kelley, *Google*
Jaeyeon Jung, *Samsung Electronics*
Apu Kapadia, *Indiana University Bloomington*
Michelle Mazurek, *University of Maryland*
Rob Reeder, *Google*
Mike Reiter, *University of North Carolina, Chapel Hill*
Heather Richter Lipford, *University of North Carolina at Charlotte*
Matthew Smith, *University of Bonn, Fraunhofer FKIE*
Rick Wash, *Michigan State University*

usenix
THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

Rev. 1/17/19

Overview

The 2019 Symposium on Usable Privacy and Security (SOUPS) will bring together an interdisciplinary group of researchers and practitioners in human computer interaction, security, and privacy. The program will feature:

- technical papers, including replication papers and systematization of knowledge papers
- workshops and tutorials
- a poster session
- lightning talks

Technical Papers

We invite authors to submit previously unpublished papers describing research or experience in all areas of usable privacy and security. We welcome a variety of research methods, including both qualitative and quantitative approaches. Papers will be judged on their scientific quality, overall quality, and value to the community. Topics include, but are not limited to:

- Innovative security or privacy functionality and design
- Field studies of security or privacy technology
- Usability evaluations of new or existing security or privacy features
- Security testing of new or existing usability features
- Longitudinal studies of deployed security or privacy features
- Studies of administrators or developers and support for security and privacy
- The impact of organizational policy or procurement decisions
- Lessons learned from the deployment and use of usable privacy and security features
- Foundational principles of usable security or privacy
- Ethical, psychological, sociological aspects of usable security and privacy
- Usable security and privacy implications/solutions for specific domains (e.g., IoT, medical, vulnerable populations)
- Replicating or extending important previously published studies and experiments
- **NEW in 2019:** Systematization of knowledge papers that integrate and systematize existing knowledge to provide new insight into a previously studied area

Paper Registration: Technical papers must be registered by the deadline listed above. Registration is mandatory for all papers. Registering a paper in the submission system requires filling out all the fields of the online form that describe the submission, but does not require uploading a PDF of the paper. This information is used to facilitate the assignment of reviewers. **Placeholder or incomplete titles and abstracts may be rejected without review.**

Paper Submission: Technical papers must be uploaded as PDF by the deadline listed above. All submissions must follow the guidelines described below. **Submissions that violate any of the requirements below may be rejected without review.**

Contact the program chairs at soups19chairs@usenix.org if you have any questions about these requirements.

Format and Page Limits: Papers must use the SOUPS formatting template (available for MS Word or LaTeX), and be submitted as a PDF via the online submission system linked from the SOUPS 2019 Call for Papers web page, www.usenix.org/soups2019/cfp. Submissions must be no more than 12 pages (excluding acknowledgements, bibliography, and appendices) and up to 20 pages total including acknowledgements, bibliography, and appendices. For the body of your paper, brevity is appreciated, as evidenced by the fact that many papers in prior years have been well under this limit.

Paper Content: Papers need to describe the purpose and goals of the work, cite related work, show how the work effectively integrates usability or human factors with security or privacy, and clearly indicate the innovative aspects of the work or lessons learned as well as the contribution of the work to the field. The paper abstracts should contain a sentence summarizing the contribution to the field and literature.

All submissions must clearly relate to the human aspects of security or privacy. Papers on security or privacy that do not address usability or human factors will not be considered. Likewise, papers on usability or human factors that do not address security or privacy will not be considered. The determination of whether a paper is within scope will be solely at the discretion of the program committee chairs.

Systematization of Knowledge Papers: New for SOUPS 2019, we are soliciting Systematization of Knowledge (SoK) papers that integrate and systematize existing knowledge to provide new insight into a previously studied area of usable security or privacy. SoK papers should draw on prior work to put forth a new taxonomy, argument, or observation in an area in which substantial work has already been done. SoK papers should be more than a survey or summary of prior work in an area. SoK papers will be held to the same scientific and presentation standards as other technical papers. Please prefix the title of these papers with "SoK:" and check the SoK checkbox on the submission form to flag them for the review process.

Replication Papers: In addition to original work, we are soliciting well-executed replication studies that meaningfully confirm, question, or clarify the result under consideration. Please prefix the title of these papers with the word "Replication:" for the review process.

Replication papers should aim to replicate important/influential findings from the literature. They may not necessarily offer new or unexpected findings; papers confirming previous findings are also considered contributions. Replication of a result that has already been replicated many times is less valuable. Replication of an obscure study that originally had only minimal influence on the community is less valuable. Authors should clearly state why they conducted a replication study, describe the methodological differences precisely, and compare their findings with the results from the original study.

Replications paper will be held to the same scientific standards as other technical papers. They should use currently accepted methodologies and technologies. Authors should not reuse outdated methods/technologies simply because they were used in the original paper. Replications may follow the same protocol as the original study, or may vary one or more key variables to see whether the result is extensible (e.g., re-running a study with a sample from a different population).

Anonymization: Reviewing is double blind. No names or affiliations should appear on the title page or in the body of the paper, acknowledgements should be blinded, and papers should avoid revealing the authors' identities in the text. Any references to the authors' own work should be made in the third person, as if it was work by someone else. Appendices and figures should also be blinded (e.g., do not leave logos or contact info on study materials, and remove de-anonymizing URLs from screenshots). Contact the program chairs at soups19chairs@usenix.org if you have any questions about how to anonymize your submission.

Overlap with previous papers: Submitted papers must not significantly overlap papers that have been published or that are simultaneously submitted to a peer-reviewed venue or publication. Any overlap between your submitted paper and other work either under submission, previously published, or submitted elsewhere before the SOUPS notification deadline must be documented in an explanatory note sent to the chairs. State precisely how the two works differ in their goals, share experiments or data sources, and offer unique contributions. If the other work is under submission elsewhere, the program committee may ask to review that work to evaluate the overlap. Please note that program committees frequently share information about papers under review and reviewers usually work on multiple conferences simultaneously. Technical reports, e.g., arXiv reports, are exempt from this rule. If in doubt, please contact the program chairs at soups19chairs@usenix.org for advice.

Self-plagiarism includes verbatim or near-verbatim use of one's own published work without citing the original source, and is generally not acceptable. In some cases, it may be acceptable to include a **brief** portion of selected content from the introduction, background, related work, or methods of a closely related paper. In these cases, the original paper must be explicitly referenced and the overlap should be clear to the reader. The reused content must not be part of the main contributions of the paper and, where possible, rewriting the text is prefered. Papers with significant text reuse may be rejected because of too much overlap. If in doubt, please contact the program chairs at soups19chairs@usenix.org for advice.

Appendices: Authors may attach to their paper supplementary appendices containing study materials (e.g., survey instruments, interview guides, etc.) that would not otherwise fit within the body of the paper. These appendices may be included to assist reviewers with questions that fall outside the stated contribution of your paper on which your work is to be evaluated. Reviewers are not required to read any appendices, so your paper should be self contained without them. Accepted papers will be published online with their supplementary appendices included.

Conflicts of Interest: The submission system will request information about conflicts of interest between the paper's authors and program committee (PC) members. It is the full responsibility of all authors of a paper to identify 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 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 four years.
3. The PC member has been a collaborator within the past four years.
4. The PC member is or was an author's thesis advisor, no matter how long ago.
5. An author is or was the PC member's thesis advisor, no matter how long ago.
6. The PC member is a relative or close personal friend of the author.

Ethical Research: User studies should follow the basic principles of ethical research, including beneficence (maximizing the benefits to an individual or to society while minimizing harm to the individual), minimal risk (appropriateness of the risk versus benefit ratio), voluntary consent, respect for privacy, and limited deception. Studies that rely on crowdworkers can incur additional ethical obligations, including but not limited to paying a fair wage. Some example ethical guidelines generated by Mechanical Turk crowdworkers can be found at http://wiki.wearedynamo.org/index.php/Guidelines_for_Academic_Requesters.

Authors are encouraged to include in their submissions explanation of how ethical principles were followed, and may be asked to provide such an explanation should questions arise during the review process. If your organization or institution requires formal clearance for research with human subjects, your paper may be rejected if clearance was not obtained. However, such clearance alone does not guarantee acceptance and the program committee may reject a paper on ethical grounds.

Early Rejections: Papers that receive substantially negative initial reviews will be rejected early. The authors of early-rejected papers, and only such papers, will receive a copy of their initial reviews. At this point, papers are no longer considered under submission (except if authors appeal).

Authors who substantively disagree with the reviews can appeal to the program committee chairs. Authors' appeals must clearly and explicitly identify concrete disagreements with factual statements in the initial reviews. 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.

Rebuttals: The rebuttal period will be held after the second round of reviews, so the authors will be given a chance to see and correct factual errors in all reviews. Authors may provide a short rebuttal that will be considered in subsequent discussions. Authors' rebuttals must clearly and explicitly identify concrete issues with factual statements in the initial reviews, or provide clarification to explicit reviewer questions. Due to time constraints, the rebuttal period is fairly short. **Please ensure that you reserve enough time between April 26 and May 3 for the rebuttal process. Late rebuttals will not be accepted.**

Publication: Accepted papers will be published by the USENIX Association, and will be freely available on the USENIX and SOUPS websites. Authors will retain copyright of their papers. Authors may also release pre-prints of their accepted work to the public at their discretion.

Presentation: For accepted papers, at least one of the paper authors must attend the conference and present the work.

* Conflict of Interest and Early Rejection policies adapted from IEEE Symposium on Security and Privacy 2017

* Replication papers description adapted from Elsevier *Journal of Molecular and Cellular Cardiology*.

* SoK papers description adapted from IEEE Symposium on Security and Privacy 2018