Announcement and Call for Papers

www.usenix.org/sec15/cfp

24th USENIX Security Symposium

Sponsored by USENIX

August 12–14, 2015, Washington, D.C.

Important Dates

- Paper titles and abstracts due: *Monday, February 16, 2015, 9:00 p.m. EST*
- Complete paper submissions due: *Monday, February 23, 2015, 9:00 p.m. EST*
- Invited talk and panel proposals due: *Monday, February 16, 2015, 9:00 p.m. EST*
- Notification to authors: *Tuesday, May 12, 2015*
- Final papers due: *Tuesday, June 30, 2015, 9:00 p.m. EDT*
- Poster proposals due: *Thursday, July 9, 2015, 9:00 p.m. EDT*
- Notification to poster presenters: *Thursday, July 16, 2014*
- Work-in-Progress submissions due: *Wednesday, August 12, 2014, noon EDT*

Symposium Organizers

Program Chair

Jaeyeon Jung, *Microsoft Research*

Deputy Program Chair

Thorsten Holz, *Ruhr-Universität Bochum*

Program Committee

Sadia Afroz, *University of California, Berkeley*
Devdatta Akhawe, *Dropbox*
Davide Balzarotti, *Eurecome*
Igor Bilogrevic, *Google*
Sasha Boldyreva, *Georgia Institute of Technology*
Joseph Bonneau, *Princeton University*
Nikita Borisov, *University of Illinois at Urbana-Champaign*
David Brumley, *Carnegie Mellon University*
Kevin Butler, *University of Florida*
Juan Caballero, *IMDEA Software Institute*
Srdjan Capkun, *ETH Zürich*
Stephen Checkoway, *Johns Hopkins University*
Nicolas Christin, *Carnegie Mellon University*
Byung-Gon Chun, *Seoul National University*
George Danezis, *University College London*
Tamara Denning, *University of Utah*
Michael Dietz, *Google*
Adam Doupé, *Arizona State University*
Josiah Dykstra, *NSA Research*
Manuel Egele, *Boston University*
Serge Egelman, *University of California, Berkeley and International-Computer Science Institute*
William Enck, *North Carolina State University*
David Evans, *University of Virginia*
Matt Fredrikson, *University of Wisconsin—Madison*
Roxana Geambasu, *Columbia University*
Rachel Greenstadt, *Drexel University*
Chris Grier, *DataBricks*
Guofei Gu, *Texas A&M University*
Alex Halderman, *University of Michigan*
Nadia Heninger, *University of Pennsylvania*
Susan Hohenberger, *Johns Hopkins University*
Jean-Pierre Hubaux, *École Polytechnique Fédérale de Lausanne (EPFL)*
Cynthia Irvine, *Naval Postgraduate School*
Rob Johnson, *Stony Brook University*
Brent Byunghoon Kang, *Korea Advanced Institute of Science and Technology (KAIST)*
Taesoo Kim, *Georgia Institute of Technology*
Engin Kirda, *Northeastern University*
Tadayoshi Kohno, *University of Washington*
Farinaz Koushanfar, *Rice University*
Zhou Li, *RSA Labs*
David Lie, *University of Toronto*
Janne Lindqvist, *Rutgers University*
Long Lu, *Stony Brook University*
Stephen McCamant, *University of Minnesota*
Damon McCoy, *George Mason University*
Jonathan McCune, *Google*
Sarah Meiklejohn, *University College London*
David Molnar, *Microsoft Research*
Tyler Moore, *Southern Methodist University*
Nick Nikiforakis, *Stony Brook University*
Cristina Nita-Rotaru, *Purdue University*
Zachary N. J. Peterson, *California Polytechnic State University*
Michalis Polychronakis, *Stony Brook University*
Adrienne Porter Felt, *Google*
Georgios Portokalidis, *Stevens Institute of Technology*
Niels Provos, *Google*
Benjamin Ransford, *University of Washington*
Tom Ristenpart, *University of Wisconsin—Madison*
Will Robertson, *Northeastern University*
Franziska Roesner, *University of Washington*
Nitesh Saxena, *University of Alabama at Birmingham*
Prateek Saxena, *National University of Singapore*
R. Sekar, *Stony Brook University*
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*
Cynthia Sturton, *University of North Carolina at Chapel Hill*

Patrick Traynor, *University of Florida*
Ingrid Verbauwhede, *Katholieke Universiteit Leuven*
Giovanni Vigna, *University of California, Santa* Barbara
David Wagner, *University of California, Berkeley*
Ralf-Philipp Weinmann, *Comsecuris*
Xiaoyong Zhou, *Samsung Research America*

Work-in-Progress Reports (WiPs) Coordinator
Tadayoshi Kohno, *University of Washington*

Steering Committee
Matt Blaze, *University of Pennsylvania*
Dan Boneh, *Stanford University*
Casey Henderson, *USENIX Association*
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 24th USENIX Security Symposium will be held August 12–14, 2015, in Washington, D.C.

All researchers are encouraged to submit papers covering novel and scientifically significant practical works in computer security. Submissions are due on Monday, February 23, 2015, 9:00 p.m. EST. The title and abstract of a submission must be registered by Monday, February 16, 2015, 9:00 p.m. EST. The Symposium will span three days, with a technical program including refereed papers, invited talks, posters, panel discussions, and Birds-of-a-Feather sessions. Workshops will precede the Symposium on August 10 and 11.

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

Symposium Topics

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

- Systems security
  - Mobile systems security
  - Web security
  - Cloud computing security
  - Distributed systems security
  - Operating systems security
  - Storage security
- Cryptographic implementation analysis and construction, applied cryptography
- Language-based security
- Hardware security
  - Embedded systems security
  - Methods for detection of malicious or counterfeit hardware
  - Randomness
  - Secure computer architectures
  - Side channels
- Network security
  - Intrusion and anomaly detection and prevention
  - Network infrastructure security
  - Denial-of-service attacks and countermeasures
  - Wireless network security
- Privacy-enhancing technologies, anonymity
  - Research on surveillance and censorship
- Human-computer interaction, security, and privacy
- Social issues and security
  - Research on computer security law and policy
  - Ethics of computer security research
  - Research on security education and training
- 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
- Others
  - Security in critical infrastructures
  - Security in electronic voting
  - Security in health care and medicine
  - Security in ubiquitous computing, sensors, actuators
  - Security in electronic commerce

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 will 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/usenix_sample_consent.pdf for the complete terms of publication.

Shadow PC

Continuing the success of the previous year, the USENIX Security '15 PC would like to make submitted papers available to shadow PCs. Shadow PCs allow students and others interested in future PC service to read submitted papers and go through the reviewing process, ultimately arriving at a shadow conference program. This is an opportunity for future PC members to learn about the peer-review process and gain experience as a reviewer.

Shadow PCs will not have any access to the real reviews, the names of the real reviewers, or any other data such as relative rankings. They will have to abide by the same rules and restrictions applicable to regular PC members. This includes, but is not limited to, rules against discussing the papers outside of the PC context, or using in any way results from reviewed papers before such papers have been published. Subreviews (i.e., external reviews) are not allowed for the

shadow PC. If you are given a paper to review as a student/shadow PC member, you must review it yourself. Making a submitted paper available to shadow PCs is optional; authors will have the opportunity to opt-in during the paper submission process. Shadow reviews for papers that are reviewed by shadow PCs will be sent out after the actual USENIX Security '15 notifications.

Authors that have participated in previous shadow PCs have found the additional reviews helpful. However, note that not all papers that volunteer for the shadow review process will receive shadow reviews; the shadow reviews may not be returned for several weeks after the notification deadline; and these reviews will have no direct bearing on acceptance to the technical program. If you would like to organize a shadow PC at your host institution, please contact Yoshi Kohno via sec15shadow@usenix.org.

Symposium Activities

Invited Talks, Panels, Poster Session, Doctoral Colloquium, 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 chair at sec15chair@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 sec15it@usenix.org by Monday, February 16, 2015, 9:00 p.m. EST.

Panel Discussions

The technical sessions may include topical panel discussions. Please send topic suggestions and proposals to sec15chair@usenix.org by Monday, February 16, 2015, 9:00 p.m. 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 submission form on the Call for Papers Web site, www.usenix.org/sec15/cfp, by Thursday, July 9, 2015, 9:00 p.m. EDT. Decisions will be made by Thursday, July 16, 2014. 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 (as also previously known as rump session) on the evening of Wednesday, August 12, 2014. 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 sec15wips@usenix.org by Wednesday, August 12, 2015, noon EDT.

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 would like to speak in Doctoral Colloquium, please email sec15dc@usenix.org.

Birds-of-a-Feather Sessions (BoFs)

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

Submitting Papers

How and Where to Submit Refereed Papers

Important: Note that some past USENIX Security Symposia have had different policies and requirements.

Submissions are due by Monday, February 23, 2015, 9:00 p.m. EST (hard deadline). The title and abstract of a submission must be registered by Monday, February 16, 2015, 9:00 p.m. EST (hard deadline). All submissions will be made online via the Web form on the Call for Papers Web site, www.usenix.org/sec15/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 (e.g., the 2,000 applications that make up your benchmark or the exact wording of the instructions and 50 questions in a survey). 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 16 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.

Conflicts of Interest

The program 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 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 steering committee has modified the conflict of interest policies to allow all members of the program committee (including program chairs) to submit papers, so long as there is one chair who is not an author of the submission.

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.

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.

Reviews from Prior Submissions (New This Year!)

The rapidly increasing number of papers being submitted to security conferences has put a strain on both authors' and reviewers' time, with both sides concerned about the implications on the fairness of the process. Concerned reviewers worry that authors will give into the temptation to resubmit rejected papers without addressing prior reviewers' concerns, hoping that different reviewers will lead to a different outcome. Authors are concerned that reviewers who helped to reject an earlier draft of a paper will not read an improved draft as diligently as they would read an unfamiliar submission,and may miss or disregard improvements. The broad set of peer-reviewed publication venues in security make it hard to quantify, understand, or correct for these problems.

Starting this year, authors can 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). To reduce any potential bias, this document will be only available to reviewers after the bulk of reviews have been submitted, at the same time authors' identities are revealed.

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 be used (1) for aggregate statistics to understand the percent of resubmissions among the set of submitted (and accepted) papers; (2) at the chair's discretion, to identify dual submissions and verify the accuracy of prior reviews provided by authors regarding previously rejected papers.

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 '15 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 Prize at http://internetdefenseprize.org/.

Human Subjects

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).
2. Discuss steps taken to ensure that participants and others who might have been affected by an experiment were treated ethically and with respect.

Authors seeking ways to reduce the ethical risks of their experiments may optionally consider reaching out to the newly formed Ethics Feedback Panel for Networking and Security, 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 panel is before conducting your experiments, but they may be able to assist if concerns arise during an experiment. Contact the program chair at sec15chair@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 chair at sec15chair@usenix.org.

Simultaneous submission of the same work to multiple venues, submission of previously published work, or plagiarism constitutes dishonesty or fraud. 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/submissions-policy for details. Questions? Contact your program chair, sec15chair@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 chair 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 Tuesday, May 12, 2015. The final paper due date is Tuesday, June 30, 2015, 9:00 p.m. 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 12, 2015.

Specific questions about submissions may be sent to the program chair at sec15chair@usenix.org. The chair will respond to individual questions about the submission process if contacted at least a week before the submission deadline.