30th USENIX Security Symposium
August 11–13, 2021 • Vancouver, B.C., Canada

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 30th USENIX Security Symposium will be held August 11–13, 2021, in Vancouver, B.C., Canada.

Important: The USENIX Security Symposium moved to multiple submission deadlines in 2019 and included 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/usenixsecurity21/publication-model-change.

All researchers are encouraged to submit papers covering novel and scientifically significant practical works in computer security. 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 9 and 10.

Important Dates
Summer Deadline
- Refereed paper submissions due: Thursday, June 11, 2020, 11:59 pm AoE
- Early reject notification: July 24, 2020
- Rebuttal Period: August 31 – September 2, 2020
- Notification to authors: September 11, 2020
- Final papers due: October 13, 2020

Fall Deadline
- Refereed paper submissions due: Thursday, October 15, 2020, 11:59 pm AoE
- Early reject notification: November 20, 2020
- Rebuttal Period: January 11–13, 2021
- Notification to authors: January 21, 2021
- Final papers due: February 22, 2021

Winter Deadline
- Refereed paper submissions due: Thursday, February 4, 2021, 11:59 pm AoE
- Early reject notification: March 12, 2021
- Rebuttal Period: April 19–21, 2021
- Notification to authors: April 30, 2021
- Final papers due: June 2, 2021

Symposium Organizers
Program Co-Chairs
Michael Bailey, University of Illinois at Urbana–Champaign
Rachel Greenstadt, New York University

Program Committee
Yousra Aafer, University of Waterloo
Ruba Abu-Salma, University College London and Inria
Gunes Acar, Katholieke Universiteit Leuven
David Adrian, Censys
Sadia Afroz, International Computer Science Institute (ICSI), University of California, Berkeley, and Avast
Devdatta Akhawe, Figma
Benjamin Andow, IBM T. J. Watson Research Center
Sebastian Angel, University of Pennsylvania
Pauline Anthonysamy, Google
Manos Antonakakis, Georgia Institute of Technology
Jethro G. Beekman, Fortanix
Matthew Bernhard, University of Michigan
Battista Biggio, University of Cagliari, Italy
Leyla Bilge, NortonLifeLock Research Group
Vincent Bindschaedler, University of Florida
Tamara Bonaci, Northeastern University
Joseph C. Bonneau, New York University
Sven Bugiel, CISPA Helmholtz Center for Information Security
Kevin Butler, University of Florida
Joseph Calandrino, Federal Trade Commission
Aylin Caliskan, George Washington University
Stefano Calzavara, Università Ca’ Foscari Venezia
Yinzhi Cao, Johns Hopkins University
Alvaro A. Cardenas, University of California, Santa Cruz
Nicholas Carlini, Google
Lorenzo Cavallaro, King’s College London
Rahul Chatterjee, University of Wisconsin—Madison
Qi Alfred Chen, University of California, Irvine
Marshini Chetty, University of Chicago
Sherman S. M. Chow, The Chinese University of Hong Kong
Omar Haider Chowdhury, The University of Iowa
Mihai Christodorescu, Visa Research
Erinn Clark, Google
Shaanan Cohney, Princeton University and University of Melbourne

Sponsored by USENIX, the Advanced Computing Systems Association
Deian Stefan, University of California, San Diego
Ben Stock, CISPA Helmholtz Center for Information Security
Gianluca Stringhini, Boston University
Cynthia Sturton, The University of North Carolina at Chapel Hill
Nick Sullivan, CloudFlare
Yixin Sun, University of Virginia
Paul Syverson, U.S. Naval Research Laboratory
Patrick Tague, Carnegie Mellon University
Kurt Thomas, Google
Dave (Jing) Tian, Purdue University
Yuan Tian, University of Virginia
Laura Tinnel, SR/International
Nils Ole Tippenhauer, CISPA Helmholtz Center for Information Security
Jacob Torrey, DARPA
Florian Tramèr, Stanford University
Patrick Traynor, University of Florida
Blase Ur, University of Chicago
Ingrid Verbauwhede, Katholieke Universiteit Leuven
Bimal Viswanath, Virginia Tech
David Wagner, University of California, Berkeley
Gang Wang, University of Illinois at Urbana–Champaign
Byron Williams, University of Florida
Matthew Wright, Rochester Institute of Technology
Eric Wustrow, University of Colorado Boulder
Dongyan Xu, Purdue University
Wenyuan Xu, Zhejiang University
Jason Minhui Xue, The University of Adelaide
Yuval Yarom, The University of Adelaide and Data61
Tuba Yavuz, University of Florida
Daniel Zappala, Brigham Young University
Mary Ellen Zurko, MIT Lincoln Laboratory

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
Nadia Heninger, University of California, San Diego
Thorsten Holz, Ruhr-Universität Bochum
Jaeyeon Jung, Samsung Electronics
Engin Kirda, Northeastern University
Tadayoshi Kohno, University of Washington
Thomas Ristenpart, Cornell Tech
Patrick Traynor, University of Florida
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
- Machine learning in a secure systems context
- 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
- Information manipulation
- Online abuse and harassment
- 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 of computing systems, 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. Alternative arrangements will be made if global health concerns persist. 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/sample_consent_form.pdf for the complete terms of publication.

Go to Paper Submission Policies and Instructions page at www.usenix.org/conference/usenixsecurity21/submission-policies-and-instructions for more information.

Artifact Evaluation
The Call for Artifacts will be available soon.

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.
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 sec21chairs@usenix.org by February 4, 2021.

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, which will be available here soon, by July 6, 2021. Decisions will be made by July 13, 2021. 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
Information about lightning talks will be available soon.

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

Important: The USENIX Security Symposium moved to multiple submission deadlines in 2019 and included changes to the review process and submission policies. Detailed information is available at USENIX Security Publication Model Changes at www.usenix.org/conference/usenixsecurity21/publication-model-change.

USENIX Security ‘21 submissions deadlines are as follows:

- Summer Deadline: Thursday, June 11, 2020, 11:59 pm AoE
- Fall Deadline: Thursday, October 15, 2020, 11:59 pm AoE
- Winter Deadline: Thursday, February 4, 2021, 11:59 pm AoE

All papers that are accepted by the end of the winter submission reviewing cycle (February–May 2021) will be invited to present at USENIX Security ‘21. All submissions will be made online via their respective web forms: Summer Quarter, Fall Quarter, Winter Quarter. 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.

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.

Prepublication of Papers
Prepublication versions of papers accepted for USENIX Security ‘21 will be published and open and accessible to everyone without restrictions on the following dates:

- Summer Deadline: Wednesday, November 11, 2020
- Fall Deadline: Monday, April 5, 2021
- Winter Deadline: TBD (final papers will be published with the full conference proceedings)

Embargo Requests
Authors may request an embargo for their papers by the deadline dates listed below. All embargoed papers will be released on the first day of the conference, Wednesday, August 11, 2021.

- Summer Deadline: Wednesday, November 3, 2020
- Fall Deadline: Monday, March 29, 2021
- Winter Deadline: Thursday, July 1, 2021

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.

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.

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. Neither the link in the paper nor the website itself should contain the authors’ names or 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.

**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 '21 paper submission for consideration for the Prize as part of the regular submission process. 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 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 sec21chairs@usenix.org if you have any questions.

**Reviews from Prior Submissions**

**Drawn from the ACM CCS 2020 CFP, IEEE S&P 2021**

For papers that were previously submitted to, and rejected from, another conference, authors are required to submit a separate document containing the prior reviews along with a description of how those reviews were addressed in the current version of the paper. Authors are only required to include reviews from the last time the paper was submitted. Reviewers will be asked to complete their reviews before reading the provided supplementary material to avoid being biased in formulating their own opinions; once their reviews are complete, however, reviewers will be given the opportunity to provide additional comments based on the submission history of the paper. Authors who try to circumvent this rule (e.g., by changing the title of the paper without significantly changing the contents) may have their papers rejected without further consideration, at the discretion of the PC chairs.

**Submission Instructions**

All submissions will be made online via their respective web forms. 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.

For resubmissions of Major Revisions, authors must submit an appendix that includes a list of changes to the paper and a statement of how the changes address the review comments. For papers that were previously submitted to, and rejected from, another conference, the required document (see “Reviews from Prior Submissions” above) should be submitted as a PDF file using the “Prior Reviews” field in the submission forms, not via an appendix.

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 sec21chairs@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, 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/usenixsecurity21/publication-model-change for details. For submissions that received Reject or Reject and Resubmit decisions from USENIX Security '20, resubmissions must follow the rules laid out for when they can be resubmitted (i.e., not in the next two deadlines for Reject and Resubmit, and not in the next three deadlines for Reject). Questions? Contact your program co-chairs, sec21chairs@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 be available online before the symposium. If your accepted paper should not be published prior to the event, please notify production@usenix.org after you submit your final paper. See the Embargo Requests section of this document for deadlines.

Specific questions about submissions may be sent to the program co-chairs at sec21chairs@usenix.org. The chairs will respond to individual questions about the submission process if contacted at least a week before the submission deadline.