

# 34th USENIX Security Symposium

August 13–15, 2025, Seattle, WA, USA



*Sponsored by USENIX, the Advanced Computing Systems Association*

The USENIX Security Symposium brings together researchers, practitioners, system programmers, and others interested in the latest advances in the security and privacy of computer systems and networks. The 34th USENIX Security Symposium will be held on August 13–15, 2025, in Seattle, WA, USA.

## Summary of main changes from previous editions

1. Two submission cycles instead of three.
2. New open science policy: Research results should be available to the public or explain why this is not possible. The artifact evaluation process is adjusted to accommodate this.
3. New guidelines for ethics considerations.
4. Extra page to discuss ethics considerations and compliance with open science policy.
5. Revisions are reviewed within the same submission cycle instead of the next.
6. New approach to presenting accepted papers (see the public RFC at <https://github.com/USENIX-Security-2025/conference-format> about the plans for this new model).

## Important Dates

New in 2025, there will be two submission cycles.

### Cycle 1

- Paper submissions due: **Wednesday, September 4, 2024**
- Early reject notification: **Tuesday, October 15, 2024**
- Rebuttal period: **November 18–25, 2024**
- Notification to authors: **Wednesday, December 11, 2024**
- Shepherding/revision period: **Thursday, December 12, 2024–Thursday, January 16, 2025**
- Artifacts due for availability verification: **Thursday, January 16, 2025**
- Shepherding/revision author notification: **Thursday, January 23, 2025**
- Final papers due: **Thursday, January 30, 2025**

### Cycle 2

- Paper submissions due: **Wednesday, January 22, 2025**
- Early reject notification: **Tuesday, March 4, 2025**
- Rebuttal period: **April 7–14, 2025**
- Notification to authors: **Wednesday, April 30, 2025**
- Shepherding/revision period: **Thursday, May 1, 2025–Thursday, May 29, 2025**
- Artifacts due for availability verification: **Thursday, May 29, 2025**
- Shepherding/revision author notification: **Thursday, June 5, 2025**
- Final papers due: **Thursday, June 12, 2025**

## Symposium Topics

Refereed paper submissions are solicited in all areas relating to systems research in security and privacy. 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.

- 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
  - Analysis of network and security protocols
- Software analyses
  - Malware analysis
  - Forensics and diagnostics for security
  - Automated security analysis of source code and binaries
  - Program analysis
  - Fuzzing and vulnerability discovery



- ML and AI security and privacy
  - ML and AI applications to security and privacy
  - Privacy risks in ML and AI
  - Security of AI
- Data-driven security and measurement studies
  - Measurements of fraud, malware, spam
  - Measurements of human behavior and security
- Privacy
  - Privacy metrics
  - Anonymity
  - Web and mobile privacy
  - Privacy-preserving computation
  - Privacy attacks
- Usable security and privacy
  - User studies related to security and privacy
  - Human-centered security and privacy design
- Formal methods and language-based security
- Hardware security
  - Secure computer architectures
  - Embedded systems security
  - Cyber-physical systems security
  - Methods for detection of malicious or counterfeit hardware
  - Side channels
  - Automated security analysis of hardware designs and implementation
- Surveillance and censorship
- Social issues and security
  - Security and privacy law and policy
  - Information manipulation, misinformation, and disinformation
  - Protecting and understanding at-risk users
  - Emerging online threats, harassment, extremism, and abuse
- Applications of cryptography
  - Analysis of deployed cryptography and cryptographic protocols
  - Cryptographic implementation analysis
  - New cryptographic protocols with real-world applications
- Blockchains and distributed ledger security
- Meta-science in security and privacy
  - Ethics of computer security research
  - Security education and training
  - Replication and reproduction
- Attacks with novel insights, techniques, or results

### **New Topics: Meta-science in Security and Privacy**

Meta-science, or the study of scientific research itself, aims to enhance the efficiency, quality, and outcomes of research activities in our community. Submissions in this broad topic should focus on evaluations of research practices, replicability/reproducibility, ethics, research methodologies, data transparency, and peer-review processes.

Contributions should extend beyond analysis, aiming to influence future research practices.

**Replication and Reproduction:** Contributions to this sub-topic should primarily consist of studies that verify, refute, or refine

prior technical results or widely-held beliefs. We encourage submissions that not only replicate studies but also offer meta-analyses that assess the replicability of research. Additionally, while replication studies often replicate original findings, we also value novel investigations into why certain studies fail to replicate. Papers that critically examine the conditions under which replication is feasible, or those that propose innovative methods to enhance the reliability of scientific findings, are especially welcome.

### **Systematization of Knowledge**

USENIX Security solicits the submission of Systematization of Knowledge (SoK) papers, which have been very valuable to help our community to clarify and put into context complex research problems.

It is important to stress that SoK papers go beyond simply summarizing previous research (like in a survey); they also include a thorough examination and analysis of existing approaches, identify gaps and limitations, and offer insights or new perspectives on a given, major research area.

While both SoK and survey papers may involve summarizing existing research, the key difference is that an SoK paper provides a more structured and insightful overview, which might also involve new experiments to replicate and compare previous solutions. For examples, please see the list of SoK papers that recently appeared at the IEEE Symposium on Security and Privacy at <https://oaklandsok.github.io/>.

The titles of SoK submissions should be prefixed with "SoK:".

### **Research Ethics**

Authors of *all* submissions must consider the ethics of their work even if, a priori, they do not think that this section on ethical considerations applies to them.

Without sufficient precautions, research endeavors can lead to negative outcomes. People or other entities, like companies, might experience negative outcomes during the research process itself, immediately after the research is published, or in the future. These negative outcomes might be in the form of tangible harms (e.g., financial loss or exposure to psychologically disturbing content). Or, these negative outcomes could be violations of human rights even if there are no directly tangible harms (e.g., the violation of a participants' right to informed consent or the violation of users' right to privacy via the study of data that users expect and desire to be private). Further, due to the complexity of today's computing systems, people could experience these negative outcomes either directly or indirectly in unexpected ways (see The Menlo Report at [https://www.dhs.gov/sites/default/files/publications/CSD-MenloPrinciplesCORE-20120803\\_1.pdf](https://www.dhs.gov/sites/default/files/publications/CSD-MenloPrinciplesCORE-20120803_1.pdf)).

We expect authors to carefully and proactively consider and address potential negative outcomes associated with carrying out their research, as well as potential negative outcomes that could stem from publishing their work. Failure to do so may result in rejection of a submission regardless of its quality and scientific value.

Although causing negative outcomes is sometimes a necessary and legitimate aspect of scientific research in computer security and privacy, authors are expected to document how they have addressed and mitigated the risks. This includes, but is not limited to, considering the impact of the research on deployed systems, understanding the costs the research imposes on others, safely and appropriately collecting data, considering the well-being of the research team, and following ethical disclosure practices.

Reviewers will be asked to evaluate the ethics of every submission. To facilitate their review, all papers must include a discussion of ethics and an argument for how their full research and publication process was ethical. For more information, see the submission policies and instructions and the ethics guideline sections below. Authors should understand that, sometimes, the right ethical decision is not to do a project or to change how a project is done. Thus, *authors are encouraged to read the ethics portion of the submission instructions and the ethics guidelines document as early as possible in their research process, ideally before initiating their research*, though it is understood that some projects may have been started before this CFP has been posted. Authors are further encouraged to revisit these guidelines throughout the research, publication, and post-publication processes.

### Open Science

This year, USENIX Security introduces a new open science policy, aiming to enhance the reproducibility and replicability of scientific findings: Authors are expected to openly **share their research artifacts by default**. This initiative is part of a broader commitment to foster open science principles, emphasizing the sharing of artifacts such as datasets, scripts, binaries, and source code associated with research papers. If, for some reason (such as licensing restrictions), artifacts cannot be shared, a detailed justification must be provided. Artifacts need to be available for the Artifact Evaluation committee after paper acceptance and before the final papers are due.

### Artifact Evaluation

Artifact evaluation will take place in two phases: Artifacts will be evaluated for availability after paper acceptance and before the final papers are due; artifacts will be evaluated for functionality and reproducibility after final papers are due. All artifacts mentioned in accepted papers will be checked for availability. Authors of accepted papers are encouraged to register their artifacts to also be checked for functionality and reproducibility.

Artifacts should be submitted in the same cycle as the accepted paper. Each submitted artifact will be reviewed by the Artifact Evaluation Committee (AEC).

The Call for Artifacts will be available soon.

### Conference Attendance and Publishing Accepted 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](mailto:conference@usenix.org).

A major mission of the USENIX Association is to provide for the creation and dissemination of new knowledge. USENIX 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 for the complete terms of publication.

Papers accepted during the first reviewing cycle will be published on the USENIX Security website shortly after the conclusion of the first reviewing cycle. Papers accepted during the second reviewing cycle will be published on the first day of the symposium.

See the Submission Policies and Instructions section below for more information.

### New Approach to Presentation of Papers

Motivated by rising conference costs and increasing numbers of submitted and accepted papers, USENIX Security '25 will implement a new approach to presenting accepted papers and fostering interactions at the conference. Some accepted papers will be presented as longer talks, tentatively 15 minutes long; others will be shorter presentations, tentatively between 30 seconds and one minute long. Accepted papers will additionally be presented as posters, during thematically organized discussion sessions that will run in parallel with talk sessions. Finally, authors of accepted papers will be invited to upload pre-recorded 15-to-20-minute video presentations, which will be published on the USENIX Security website. Preparation of posters and uploaded videos will not be mandatory.

### Submission Policies and Instructions

USENIX Security '25 submissions deadlines are as follows:

Cycle 1 Deadline: **Wednesday, September 4, 2024, 11:59 pm AoE**

Cycle 2 Deadline: **Wednesday, January 22, 2025, 11:59 pm AoE**

All papers that are accepted by the end of the second submission cycle (January–June 2025) will appear in the proceedings for USENIX Security '25. All submissions should be made online via their respective submission systems on the Call for Papers page. We do not accept email submissions.

Submitted papers should describe original, scientifically sound work produced by the co-authors. All submissions will be judged on originality, relevance, correctness, and clarity. Submissions should be finished, complete papers. We may desk-reject papers that have severe editorial problems (broken references, egregious spelling or grammar errors, missing figures, etc.), are submitted in violation of the Submission Instructions outlined below, are outside of the scope of the symposium, or are deemed clearly of insufficient quality to appear in the program.

#### Summary of main changes from previous editions

- Ethics considerations and compliance with the open science policy must be discussed in the paper. An extra page is provided just for these topics. Artifacts are expected to be available by the camera-ready deadline.

#### Paper Format

Submissions must be in PDF format. Please make sure your submission can be opened using Adobe Reader. Please make sure your submission, and all embedded figures, are intelligible when printed in grayscale.

Submissions 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. Authors must use USENIX's templates and style files when preparing the paper for submission. Failure to adhere to the page limit and formatting requirements can be grounds for rejection.

Initial paper submissions (i.e., all papers except those that have been revised after receiving an "Invited for Major Revision" decision at USENIX Security '25 or "Accept Conditional on Major Revision" at USENIX Security '24) should consist of at most 13 typeset pages for the main body of the paper, one additional page for discussing ethics considerations and compliance with the open science policy, and a bibliography and well-marked appendices. At submission time, there is no limit on the length of the bibliography and appendices but reviewers are not required to read any 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. The paper should be self-contained without appendices.

To accommodate additional material requested by reviewers, the revisions for papers that previously received an “Accept Conditional on Major Revision” decision can use up to 14 typeset pages for the main body of the paper, excluding the one page for discussing ethics considerations and compliance with the open science policy, the bibliography, and well-marked appendices.

Once accepted, the final version should be no longer than 20 pages, including the bibliography and any appendices.

### Anonymous Submission

The review process will be anonymous. 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. Anonymous references are only allowed in the (unusual) case that a third-person reference is infeasible, and after approval of the chairs.
- 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 suggest the authors' identities (e.g., the website should not contain the authors' names or affiliations).
- Authors should carefully check any submitted prior reviews for identifying details.

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.

### Simultaneous Submission and Plagiarism

Simultaneous submission of the same work to multiple venues, submission of previously published work, and plagiarism constitute dishonesty or fraud. 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 [sec25chairs@usenix.org](mailto:sec25chairs@usenix.org). Failure to point out and explain overlap with published or simultaneously submitted papers 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 <https://www.usenix.org/conferences/author-resources/submissions-policy> for details.

Papers that have received a decision of “Invited for Major Revision” from USENIX Security are still considered to be under review until accepted or rejected by the reviewers; authors must formally withdraw their paper if they wish to submit to another venue. See the USENIX Security '25 Reviewing Model page at <https://www.usenix.org/conference/usenixsecurity25/>

reviewing-model for details. Submissions that were rejected from the last cycle of USENIX Security '24 may not be resubmitted until the second cycle of USENIX Security '25.

All submitted papers are considered to be under review for USENIX Security '25 until authors are notified of a decision by the program committee or the program co-chairs approve a request for withdrawal.

### Ethics

Reviewers will be asked to evaluate the ethics of all submissions. All submissions are hence required to have an ethics considerations section in the main body of the paper, or in the extra page offered for “ethics considerations and compliance with the open science policy” (see the Paper Format section above), or both. In some cases, the ethics discussion may be short; in other cases, the ethics consideration may be long. Regardless of length, from reading the main body of the paper and the extra “ethics considerations and compliance with the open science policy” page, it should be clear to reviewers that the authors made sound and responsible ethical decisions.

Authors should be prepared to answer these questions in the conference submission portal:

- “I attest that I read the ethics considerations discussions in the conference call for papers, the detailed submissions instructions, and the guidelines for ethics document.”
- “I attest that the research team considered the ethics of this research, that the authors believe the research was done ethically, and that the team's next-step plans (e.g., after publication) are ethical.”
- “I attest that the submission has a clearly-marked section on ethical considerations in the body of the paper and/or in the extra ‘ethics considerations and compliance with the open science policy’ page.”

In addition to reading the Call for Papers and the Submission Policies and Instructions sections, authors are also expected to read the Ethics Guidelines page (<https://www.usenix.org/conference/usenixsecurity25/ethics-guidelines>).

### Open Science Policy

Non-compliance with the new open science policy can lead to severe repercussions, including the rejection of the non-compliant paper or, in the case of egregious violations such as not following through with promised artifact sharing, barring the authors from submitting to future conference cycles.

### Reviews from Prior Submissions

For papers that were previously submitted to and rejected from a conference (including USENIX Security), authors may, but are not required to, submit a separate PDF document containing the prior reviews along with a description of how those reviews were addressed in the current version of the paper.

Reviewers will submit their initial reviews prior to becoming aware of previous reviews and summaries of changes to avoid being biased in formulating their own opinions; once their initial reviews are submitted, however, reviewers will be given the opportunity to update their thoughts based on the submission history of the paper.

### Rules for Revisions

For submissions that received “Invited for Major Revision” decisions during one of the USENIX Security '25 submission periods, authors who revise their papers must submit a separate PDF document that includes the verbatim revision criteria, a list of changes made to the paper, an explanation of how the



changes address the criteria, and a copy of the revised paper in which the changes from the original version are highlighted. Ideally, the highlighted version of the paper would be produced by latexdiff or a similar tool. However, if papers have gone through major changes that would make such a document unreadable, authors are free to provide another format that helps the shepherd to identify changes efficiently.

Papers that have received a decision of “Invited for Major Revision” from USENIX Security are still considered to be under review until accepted or rejected by the reviewers; authors must formally withdraw their paper if they wish to submit to another venue.

For resubmissions of “Major Revisions” from USENIX Security ’24, please look at USENIX Security ’24 Submission Policies and Instructions at <https://www.usenix.org/conference/usenix-security24/submission-policies-and-instructions> for requirements. Authors are encouraged but not required to adhere to the USENIX Security ’25 guidelines for discussing ethics considerations and compliance with open science guidelines.

### 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 13, 2025.

- Cycle 1 deadline for embargo requests: **Thursday, February 27, 2025**
- Cycle 2 deadline for embargo requests: **Thursday, July 10, 2025**

If your accepted paper should not be published prior to the event, please notify [production@usenix.org](mailto:production@usenix.org) after you submit your final paper.

### 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 (including secondary affiliations and consulting work), (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 affiliated with a party that funds your research, or (5) close personal relationships. For other forms of conflict, authors must contact the chairs and explain the perceived conflict. In addition to selecting program committee conflicts when submitting, we recommend that all authors ensure they have up-to-date Hot-CRP profiles listing all known conflicts.

Program committee members who have conflicts of interest with a paper, including program co-chairs, will be excluded from the evaluation and discussion of the paper.

Final versions of accepted submissions should include all sources of funding in an acknowledgments section. Authors should also disclose any affiliations, interests, or other facts that might be relevant to readers seeking to interpret the work and its implications. Authors may wish to consider the 2023 IEEE S&P Financial Conflicts Policy (<https://www.ieee-security.org/TC/SP2023/financial-con.html>) for example.

To prevent retroactive conflicts of interest, all authors must be declared at submission time.

### Confidentiality of Submissions

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 accompanied by nondisclosure agreement forms will not be considered.

### Reasons for Desk Rejection

Papers should not attempt to “squeeze space” by exploiting underspecified formatting criteria (e.g., columns) or through manipulating other document properties (e.g., page layout, spacing, fonts, figures and tables, headings). Papers that, in the chair’s assessment, make use of these techniques to receive an unfair advantage, will be rejected, even if they comply with the above specifications. We offer several examples (<https://www.usenix.org/sites/default/files/disallowed-squeezing-examples.pdf>) of observed techniques that have or could lead to rejection. Authors should seek to meet page limits through the modification of content alone. Any other techniques (whether appearing in these examples or not) may result in rejection.

Please make sure your paper successfully returns from the PDF checker (visible upon PDF submission) and that document properties, such as font size and margins, can be verified via PDF editing tools such as Adobe Acrobat. Papers where the chairs can not verify compliance with the CFP will be rejected.

During the paper submission, the authors need to select among the available topics the ones that are more appropriate for their work. A failure to select topics or a clear attempt at selecting inappropriate or misleading entries may be grounds for administrative rejection.

### 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 Meta 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. The USENIX Security Awards Committee—selected by the Program Chairs among the symposium Program Committee members—independently determines the prize, to be distributed by USENIX.

You may submit your USENIX Security ’25 paper submission for consideration for the Prize as part of the regular submission process.

### Contact Information

Specific questions about submissions may be sent to the program co-chairs at [sec25chairs@usenix.org](mailto:sec25chairs@usenix.org). The chairs will respond to individual questions about the submission process if contacted at least a week before the submission deadline.

Further questions? Contact your program co-chairs, [sec25chairs@usenix.org](mailto:sec25chairs@usenix.org), or the USENIX office, [submissionspolicy@usenix.org](mailto:submissionspolicy@usenix.org).

## **Symposium Organizers**

### **Program Co-Chairs**

Lujo Bauer, *Carnegie Mellon University*

Giancarlo Pellegrino, *CISPA Helmholtz Center for Information Security*

### **Program Vice Co-Chairs**

Giulia Fanti, *Carnegie Mellon University*

Marco Guarnieri, *IMDEA Software Institute*

Wouter Lueks, *CISPA Helmholtz Center for Information Security*

Olya Ohrimenko, *The University of Melbourne*

Cristina Onete, *Université de Limoges, XLIM, and CNRS 7252*

Brad Reaves, *North Carolina State University*

Nuno Santos, *INESC-ID and Instituto Superior Técnico, University of Lisbon*

Daniel Votipka, *Tufts University*

### **Program Committee**

TBA

### **Ethics Committee Chair**

Tadayoshi Kohno, *University of Washington*

### **Artifact Evaluation Committee Chair**

Aurore Fass, *CISPA Helmholtz Center for Information Security*

Phani Vadrevu, *Louisiana State University*

### **Steering Committee**

Michael Bailey, *Georgia Institute of Technology*

Kevin Butler, *University of Florida*

Joe Calandrino, *Federal Trade Commission*

Srdjan Capkun, *ETH Zurich*

William Enck, *North Carolina State University*

Rachel Greenstadt, *New York University*

Casey Henderson-Ross, *USENIX Association*

Nadia Heninger, *University of California, San Diego*

Thorsten Holz, *Ruhr-Universität Bochum*

Tadayoshi Kohno, *University of Washington*

Franziska Roesner, *University of Washington*

Kurt Thomas, *Google*

Patrick Traynor, *University of Florida*

Carmela Troncoso, *EPFL*