36th USENIX Security Symposium

April 11–13, Denver, CO, USA

Sponsored by USENIX, the Advanced Computing Systems Association

The USENIX Security Symposium brings together researchers, practitioners, and others interested in the latest advances in the security and privacy of computer systems and networks. The 36th USENIX Security Symposium will be held on August 11–13, 2027, in Denver, CO, USA.

Important Information (AoE)

Cycle 1

- Mandatory registration (fixed title, fixed authors, tentative non-blank abstract, and fixed topics) due: Tuesday, August 18, 2026
- Paper submissions due: Tuesday, August 25, 2026
- Submission artifacts due: Friday, August 28, 2026
- Early reject notification: Tuesday, October 6, 2026
- Rebuttal period: Thursday, November 5–12, 2026
- Notification to authors: Thursday, December 3, 2026
- Shepherded approval due: Tuesday, December 15, 2026
- Final papers due: Thursday, January 14, 2027

Cycle 2

- Mandatory registration (fixed title, fixed authors, tentative non-blank abstract, and fixed topics) due: Tuesday, January 19, 2027
- Paper submissions due: Tuesday, January 26, 2027
- Submission artifacts due: Friday, January 29, 2027
- Early reject notification: Tuesday, March 9, 2027
- Rebuttal period: Thursday, April 8–15, 2027
- Notification to authors: Thursday, May 6, 2027
- Shepherded approval due: Tuesday, May 18, 2027
- Final papers due: Thursday, June 3, 2027

Requirements

- Paper submissions can include up to 13 pages of body text
- Papers must include an "Open Science" Appendix on submission
- An Appendix discussing Ethics is recommended
- Overall length:
  - The initial submission can contain unlimited appendices and references
  - Final camera-ready papers can contain a maximum of 20 total pages
- Each author can submit at most seven papers per cycle

All papers accepted in either Cycle will appear in the proceedings of USENIX Security '27. All submissions must be made via the respective submission systems on the call for papers page.

Submitted papers should describe original, scientifically sound work produced by the co-authors. All submissions will be judged on originality, relevance, scientific rigor, correctness, and clarity. Submissions should be finished, complete papers.

Submissions must be in standard PDF format. Please ensure your submission is intelligible when printed/rendered in grayscale.

Summary of main changes from previous edition

1. Ethics appendix is no longer mandatory (but is strongly encouraged).
2. No Replication submissions.
3. Three-day grace period for artifact submissions.
4. USENIX Authorship policy. (https://www.usenix.org/conferences/authorship-policy)

Symposium Topics

Refereed paper submissions are solicited in all areas relating to systems research in security and privacy, and this topic list is not meant to be exhaustive. Papers without a clear application to security or privacy of computing systems will be considered out of scope and may be rejected without full review at the discretion of the chairs.

- System security
  - Operating 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
- Security and Privacy for Web, Mobile, and Emerging Technologies
  - Web
  - Mobile
  - IoT
  - VR/AR
  - Games
- Software security
  - Malware analysis
  - Forensics and diagnostics for security
  - Automated security analysis of source code and binaries
  - Program analysis
  - Fuzzing and vulnerability discovery
- Security of ML
  - Read the Submitting ML Work to USENIX Security page (https://www.usenix.org/conference/usenixsecurity27/submitting-ml-work-usenix-security) to prevent desk rejection.
  - USENIX Security is a systems security venue. ML-focused contributions must be relevant to the broader systems security community.
  - This topic is not meant for papers that propose/evaluate/improve ML-based techniques for a security task. Such papers should select the topic most closely related to the task.

- Privacy of ML
    - Read the Submitting ML Work to USENIX Security page (https://www.usenix.org/conference/usenixsecurity27/submitting-ml-work-usenix-security) to prevent desk rejection.
    - USENIX Security is a systems security venue. ML-focused contributions must be relevant to the broader systems security community.
    - This topic is not meant for papers that propose/evaluate/improve ML-based techniques for a privacy task. Such papers should select the topic most closely related to the task.
- Privacy and Anonymity
    - Privacy metrics
    - Anonymity
    - Privacy-preserving computation
    - Privacy attacks
    - Surveillance and censorship
- Human Aspects
    - Usable security and privacy
    - Security and privacy policy and/or ethics
    - Security education and training
    - Understanding and protecting users from online harms (e.g., harassment, abuse, mis/disinformation, etc.)
- Security Measurement Studies
    - Measurements of fraud, malware, spam, or cybercrime
    - Measurements of human behavior and 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
- 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

Systematization of Knowledge

USENIX Security solicits the submission of Systematization of Knowledge (SoK) papers.

SoK papers go beyond simply summarizing previous research (as 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 major research area.

For examples, please see the list of SoK papers at https://oaklandsok.github.io.

These submissions must have their title prefixed with "SoK: ".

Submission Policies and Instructions

Formatting Requirements & Page Limit

Submissions must be in PDF format, typeset using the USENIX Security template and style files (https://www.usenix.org/sites/default/files/usenixsecurity2027_latex_templates.zip): 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. The main body of the submission must not exceed 13 pages excluding References and any appendices.

At submission time, there is no limit on the length of the bibliography and optional appendices, but reviewers are not required to read any optional appendices. Papers must be self-contained without the optional appendices.

Authors must meet page limits through the modification of content alone. Any attempts to remove whitespace (e.g., negative vspaces, savetrees, titlesec, removing author blocks, etc.) or change the formatting defaults (e.g., fonts) are forbidden and may result in rejection.

Once accepted, papers must be reformatted to fit in 20 pages, including any "Ethical Considerations" or "Open Science" appendices, the bibliography, and any additional optional appendices.

Ethical Considerations

Papers in-scope for USENIX Security frequently, if not always, have both ethical considerations and implications that should be addressed prior to conducting research. Reviewers will be asked to evaluate the ethics of both the research and the implications of all submissions. At the co-chairs' and PC's discretion, papers may be rejected on ethical grounds. Our expectation however is that the common case, involving established research approaches, will be straightforward and require limited ethical analysis and that substantive efforts (both on the part of submitters and the PC) will be reserved for cases involving new and/or substantive risk of harm.

Authors are strongly encouraged to include a well-labeled section in the Appendix (e.g., "Ethics", "Ethical Considerations", etc.) that discusses the ethical considerations and implications of their work. We may work with authors throughout the review process, and authors who do not include an adequate discussion of ethics may be asked to provide additional information.

We encourage the authors to consult the Ethics Guidelines (https://www.usenix.org/conference/usenixsecurity26/call-for-papers#ethics) from USENIX Security 2026 for examples of ethics sections, analysis frameworks, and resources to consider when conducting security research.

Open Science Policy

The bedrock of scientific progress is standing on the shoulders of giants, and to do this USENIX Security '27's principle is that research results should be accessible and, if possible, empirical studies should be reproducible.

We encourage all authors to release all artifacts (source code, datasets, models, benchmarks, scripts, etc.) needed to evaluate the paper's core contributions, to the extent possible while maintaining data confidentiality and industry protections. Therefore, all USENIX Security '27 submissions must include an Open Science Appendix describing the artifacts and how to access them or an explicit description of why artifacts cannot be provided.

To preserve double-blind review, artifacts must be shared through anonymous links with no tracking mechanisms. Authors are solely responsible for ensuring no identifying

information is exposed (e.g., usernames, organization names, commit history). For source code repositories, we recommend https://anonymous.4open.science, using the conference ID "SEC27" to apply the current cycle's expiration deadline. Check any expiration times carefully: files must remain accessible for the entire evaluation period, until the shepherd approval deadline.

Anonymous URLs should be included in the paper's Open Science Appendix. After the submission deadline, URLs are final, but a 3-day grace period is provided to anonymize and upload artifacts. During this period, the paper itself cannot be modified. Once the grace period ends, artifacts are considered frozen and must not be updated.

We expect all submitted artifacts to be available publicly on paper acceptance, however we acknowledge that some artifacts cannot be shared publicly e.g., due to licensing restrictions, adversarial risk, or harm to study subjects. Artifacts help the PC to review the paper, therefore, if at all possible, submit the artifacts and note in the Open Science Appendix those which will not be made public. If submission of artifacts is not possible (e.g., due to NDA or legal constraints), the Open Science Appendix must explain such omissions explicitly.

Artifacts will be treated with the same strict confidentiality as the manuscript. Access is restricted to assigned PC members for evaluation purposes only.

For all submitted artifacts that can be made public, paper acceptance is conditional on their public availability. Camera-ready paper versions will include an Open Science Appendix that includes a non-anonymous, stable artifact link. Artifact availability will be re-verified by the Artifact Evaluation Committee.

Authors of accepted papers are additionally encouraged to optionally register their artifacts to be checked for functionality and reproducibility by the Artifact Evaluation Committee.

Anonymous Submission

Papers must be submitted for anonymous review: no author names or affiliations may appear on the title page and authors must not reveal 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.

For provided artifacts, neither the link in the paper nor the website itself may suggest the authors' identities nor track reviewers accessing them.

Papers that are not properly anonymized may be rejected without review or during the review process.

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. While the PC will not go out of its way to attempt to deanonymize papers, authors should take care to avoid timing of publicity or public announcements of work, and avoid other behaviors that appear to intentionally aim to inform reviewers of their identity.

Use of AI

The use of AI tools to assist in preparing submissions is permitted, and human authors are ultimately responsible for all submitted content and results, ensuring their accuracy, originality, and integrity. Works submitted should constitute self-respecting work that respects the importance of scientific inquiry and integrity and respects the time and energy of reviewers.

Upon submitting to USENIX Security '27, authors acknowledge that they have reviewed all content that was generated by AI as if they had written it themselves, including text, code, experimental data, and references.

Any violation to this policy which results in fabrications or hallucinations, including non-existing references or incorrect authors, invented claims, and falsified results is considered academic misconduct and might lead to the paper being desk rejected or other sanctions.

Authors are encouraged to evaluate their submissions using the same open-source tools that we will use (https://github.com/gianlucasb/hallucinator).

Submission Limit

Each author can submit at most seven papers per cycle to USENIX Security 2027. Checking will happen right after paper submission (abstracts may be withdrawn). If an author submits more than seven papers, the chairs will retain the seven papers with the lowest submission numbers.

Submission Instructions and Procedures

Registration and additional requirements for submissions

All papers intended to be submitted must be registered with the fixed title, the fixed full list of authors including their ORCIDs, a tentative abstract, and fixed topics one week before the submission deadline. Any papers not registered at that time or those missing requirements will not be considered for review.

By submission time, all authors are required to (1) set up or update their HotCRP profile to include their ORCID (https://orcid.org/) and (2) confirm the submission terms within HotCRP. In exceptional cases of unavailability of a co-author, contact the co-chairs with an explanation of why the requirements cannot be fulfilled. In all other cases, papers for which at least one author fails to comply with the requirements will not be considered for review.

Conflicts of Interest

To maintain the integrity of the peer review process, we all need to prevent submissions from being evaluated by reviewers who have a conflict of interest. During the submission process, we ask authors to 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 or within the past two years (including secondary affiliations and consulting work)
- who was the advisor or advisee of an author at any time in the past
- with whom the author has collaborated with (includes work in progress) or published in the current year or the two years preceding it
- who is a co-PI or sub-award on grants or funding
- who is affiliated with a party that provides research funding to an author
- with whom you have a close personal relationship

The chairs will contact authors if more information is necessary. Authors should be prepared to explain conflicts.

Note that adversarial or illegitimate conflicts are strictly prohibited. The chairs retain the right to remove conflicts (e.g., because reviewers are potential competitors).

All authors should update their HotCRP profiles to include the names of recent collaborators to help identify missed 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).

Submission Confidentiality

The program committee and external reviewers are required to treat all submissions as confidential. All papers must only be read for the purposes of evaluation for publication. 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.

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. 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.

Comparison With Related Work

Authors must relate their submission to all related work they are aware of in their paper, including their own work that is currently under submission (either at USENIX Security or another conference) or have already been accepted (but not yet published). Citations to simultaneously submitted papers should be anonymized; non-anonymous versions of these citations must, however, be emailed to the program co-chairs at sec27chairs@usenix.org. Failure to point out and explain overlap with published, accepted, or simultaneously submitted papers will be grounds for rejection.

Simultaneous Submission and Plagiarism

Simultaneous submission of the same work to multiple venues with archived proceedings, submission of previously published work, and plagiarism constitute dishonesty or fraud. This includes cases in which preliminary reviews from another venue indicate likely rejection but the paper is still considered under submission to the venue. USENIX, similar to 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 (https://www.usenix.org/conferences/author-resources/submissions-policy) for details.

All submitted papers are considered to be under review for USENIX Security '27 until authors are notified of a decision by the program committee or the program co-chairs approve a request for withdrawal.

Authorship

USENIX expects authors to adhere to high ethical standards and to ensure transparency and integrity in the publication of their work. Clear and consistent authorship practices support USENIX's core mission and are essential to maintaining confidence in the research record. See the USENIX Authorship Policy (https://www.usenix.org/conferences/authorship-policy) for complete information, including criteria for authorship, details about pseudonymous authorship, and the difference between contributors and authors.

Outcomes and Expectations

Review Process Outcomes

The reviewing process will result in one of the following three outcomes:

- Accepted: In this case, reviewers either see no need for any required edits—the paper could be published as is—or trust the authors to make any required edits.
- Accepted on Shepherd Approval: These papers offer sufficient contributions to be in the USENIX Security program, but the reviewers feel that some changes are needed. Reviewers expect that these changes are highly unlikely to reduce their enthusiasm regarding the paper being published. These can include text changes, clarifications, and explicit discussion of limitations.
- Rejected: This outcome indicates that the paper is not currently appropriate for publication at USENIX Security. Reviews for such papers will attempt to identify major changes that could move the paper toward a publishable state.

Papers rejected from either cycle of USENIX Security '26 may be submitted. Papers rejected from the first cycle of USENIX Security '27 may not be submitted to the second cycle of USENIX Security '27.

Desk Rejection

The chairs reserve the right to desk-reject papers for any reason they deem necessary, including, but not limited to: severe editorial issues, scope/fit issues, insufficient quality, fabricated references, failure to adhere to the CFP, etc.

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, if the paper is accepted, at least one of the authors will register to attend the Symposium at full price (i.e., not the student rate) and to present the paper; USENIX members at the Sustainer level and higher may apply their membership discounts to their registrations. If an author plans to present more than one paper, one full-price registration will still be required for each paper. If the 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. USENIX allows authors to retain ownership of the copyright in their work, 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 after the final paper deadline for the first reviewing cycle. Papers accepted during the second reviewing cycle will be published on the first day of the symposium.

Embargo Requests

Authors may request an embargo for their papers by the deadlines listed below. All embargoed papers will be released on the first day of the symposium, Wednesday, August 11, 2027.

- Cycle 1 deadline for embargo requests: Thursday, February 11, 2027
- Cycle 2 deadline for embargo requests: Thursday, July 1, 2027

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

Presentation of Papers

At this time, the exact format for the presentations at USENIX Security '27 has not been decided and will follow based on the experience of presenters and attendees of USENIX Security '26.

Contact Information

Specific questions about submissions may be sent to the program co-chairs at sec27chairs@usenix.org. The chairs will respond to individual questions about the registration process if contacted at least a week before the registration deadline and 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, sec27chairs@usenix.org, or the USENIX office, submissions-policy@usenix.org.

Symposium Organizers

Program Co-Chairs

Adam Doupé, *Arizona State University*
Andrei Sabelfeld, *Chalmers University of Technology*

Program Committee

TBA

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, *Max Planck Institute for Security and Privacy (MPI-SP)*
Tadayoshi Kohno, *Georgetown University*
Franziska Roesner, *University of Washington*
Kurt Thomas, *Google*
Patrick Traynor, *University of Florida*
Carmela Troncoso, *MPI-SP and EPFL*