36th USENIX Security Symposium

August 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.