WOOT '27: 21st USENIX WOOT Conference on Offensive Technologies

August 9–10, 2027, Denver, CO, USA

Sponsored by USENIX, the Advanced Computing Systems Association

The 21st USENIX WOOT Conference on Offensive Technologies (WOOT '27) will take place on August 9–10, 2027, and is co-located with the 36th USENIX Security Symposium in Denver, CO, USA.

Important Dates

Cycle 1

- Paper submission deadline: Thursday, December 17, 2026, 11:59 pm AoE
- Notification to authors: Tuesday, February 2, 2027

Cycle 2

- Paper submission deadline: Tuesday, March 2, 2027, 11:59 pm AoE
- Notification to authors: Thursday, April 15, 2027

Both Cycles

- Artifact submission deadline: Thursday, May 6, 2027
- Artifact discussion period starts: Monday, May 10, 2027
- Artifact decisions announced: Friday, June 4, 2027
- Final paper deadline: Tuesday, June 8, 2027

Overview

The USENIX WOOT Conference on Offensive Technologies brings together both academics and practitioners in the field of offensive security research. Occurring annually since 2007, when it was first founded as the Workshop on Offensive Technologies, WOOT has become the top venue for collaboration between academia, independent hackers, and industry participants on offensive research. As offensive security has changed over the years to become a large-scale operation managed by well-capitalized actors, WOOT has consistently attracted a range of high-quality, peer-reviewed work from academia and industry on novel attacks, state-of-the-art tools, and offensive techniques.

WOOT '27 welcomes submissions from academia, independent researchers, students, hackers, and industry. Papers that have been formally reviewed and accepted will be presented during the WOOT conference and published in the formal proceedings. Authors are also expected to plan to publish research artifacts (such as source code and data sets) wherever possible; see further details below.

By submitting a paper, you agree that if the paper is accepted, at least one of the authors will register to attend the conference 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 conference registration fee will pose a hardship for the presenter of an accepted paper, please contact conference@usenix.org.

Paper Submission Requirements

We welcome submissions from researchers of all backgrounds, including academics, independent researchers, and industry practitioners. Submissions should be complete, formal research papers, and should not have significant editorial problems. The contribution needs to be well motivated, clearly exposed, and compared to the state of the art. All paper submissions should be at most 13 pages, excluding the bibliography and any clearly marked appendices. Submissions should be double-blind, i.e., anonymized and avoid obvious self-references. Acceptance of final papers may be subject to shepherd approval.

Papers should be typeset on U.S. letter-sized pages in two-column format in 10-point Times Roman type on 12-point (single-spaced) leading, in a text block 7" x 9" deep. Authors should use USENIX's LaTeX template and style files (https://www.usenix.org/conferences/author-resources/paper-templates) when preparing the paper for submission. Failure to adhere to the page limit and formatting requirements can be grounds for rejection.

Resubmissions Between Cycles

Papers rejected in Cycle 1 may not be resubmitted in Cycle 2 unless they have undergone substantial revisions. Changes limited to writing, presentation, or minor technical improvements are not sufficient.

In exceptional cases, the program co-chairs may explicitly invite authors to submit a major revision in Cycle 2. Such invitations will be communicated as part of the Cycle 1 decisions and will identify the main issues that must be addressed. An invitation for major revision does not guarantee acceptance.

Topics

Submissions should reflect the state of the art in offensive computer security technology, exposing poorly understood mechanisms, presenting novel attacks, highlighting the limitations of published attacks and defenses, or surveying the state of offensive operations at scale. WOOT '27 accepts papers in both an academic security context and more applied work that informs the field about the state of security practice in offensive techniques. The goal for these submissions is to produce published works that will guide future work in the field. Submissions will be peer-reviewed and shepherded as appropriate.

Submission topics include, but are not limited to, practical attacks on and offensive research into:

- Hardware, including embedded devices, physical attacks, cyber-physical systems, the "Internet of Things," and software-based exploitation of hardware vulnerabilities
- Web security, as well as browser and general client-side security (such as runtimes, JITs, and sandboxing)
- Machine learning, LLMs, AI agents, and other artificial intelligence topics with significant security implications
- Operating system and hypervisor security
- Application security
- Network and distributed systems, including virtualization and the cloud
- Wireless and applied protocol security
- Mobile device security
- Malware design, implementation, and analysis, including (de)obfuscation and sandboxing
- Mitigations, their weaknesses, and how they can be (automatically) bypassed
- Innovative approaches for software security testing, such as fuzzing for novel targets
- Security of decentralized finance, smart contracts, and blockchain
- Practical attacks on deployed cryptographic systems
- Offensive applications of formal methods and program analysis (such as solvers and symbolic execution)

"Systematization of Knowledge" (SoK) papers that evaluate, systematize, and contextualize existing knowledge are also encouraged. Suitable papers include survey papers that provide useful perspectives on major research areas, papers that support or challenge long-held beliefs with compelling evidence, or papers that provide an extensive and realistic evaluation of competing approaches to solving specific problems. Such papers should be clearly labeled as SoK in their title.

Topic Relevance

We reserve the right to desk reject papers that fall outside the scope of WOOT or for which the program committee cannot secure adequate expert reviewers. Papers with no clear contributions to applied security will be considered out of scope.

The list of topics above is necessarily incomplete and imprecise. In its ongoing effort to adjust scope, the WOOT Steering Committee has identified a list of topics that are explicitly excluded. Papers whose core contributions are on the following topics are likely to be desk rejected for reasons of scope:

- Papers with contributions primarily in another field: machine learning, AI, etc.
- Machine learning and AI papers that only show problems that have been solved before without these methods, meaning that they do not advance the state of security research.
- Papers with focus on theoretical cryptography but without implementation or evaluation on real systems.
- Papers with focus on mathematical proof without implementation or evaluation.
- Papers without any security or privacy contribution.

The chairs reserve the right to desk reject papers where the topic, contributions, or substance of the paper are not sufficiently clear, particularly those containing incoherent or unintelligible text, hallucinated or fabricated references, unsupported claims, or falsified results.

Ethical Considerations and Vulnerability Disclosure

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

Where relevant, papers should include a clear statement about why the benefits of the research outweigh the potential harms and how the authors have taken measures and followed best practices to ensure safety and minimize the potential harms caused by their research. This includes, but is not limited to, considering the impact of your research on deployed systems, understanding the costs your research imposes on others, safely and appropriately collecting data, and following responsible disclosure. Authors may wish to consult the USENIX Security '26 Ethics Guidelines (https://www.usenix.org/conference/usenixsecurity26/call-for-papers#ethics). This discussion may appear in a dedicated "Ethical Considerations" section or elsewhere in the paper.

When disclosure is necessary, authors should include a statement within their submission and/or final paper about the steps taken to ensure responsible disclosure. In particular, 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). Authors are expected to prioritize protecting users, which typically requires disclosing the vulnerability to affected vendors and other stakeholders and avoiding lengthy disclosure windows. Note that authors should avoid including CVE identifiers or other information in their submissions which would de-anonymize their submissions. Please contact the program co-chairs at woot27chairs@usenix.org with any questions or concerns.

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 2027 IEEE S&P Financial Conflicts Policy (https://www.ieee-security.org/TC/SP2027/financial-con.html) for examples.

Conflicts of Interest

Program committee members who have conflicts of interest with a paper, including program co-chairs, will be excluded from the review, discussion, and evaluation of that paper where possible. During the submission process, we will ask authors to identify members of the program committee with whom they share a conflict of interest. This should include (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 academic advisor or advisee of an author at any time in the past, (3) anyone the author has collaborated with or published with within 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.

Open Science and Artifact Evaluation

Authors are expected to document the artifacts they intend to publish at the time of submitting their paper and provide justification for cases where they cannot do so (e.g., licensing restrictions). Authors of accepted papers will also be expected to submit supporting artifacts (e.g., source code allowing research to be reproduced, measurement/evaluation data, scripts, and tests) to be reviewed by the Artifact Evaluation Committee (AEC). We expect these artifacts to be made publicly available. Exceptions may be granted by the chairs on a case-by-case basis.

The Call for Artifacts will be available online soon.

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.

Submission Instructions

All submissions must be made online through the respective HotCRP submission systems, which are linked from the WOOT '27 Call for Papers web page. We will not accept submissions via any other method.

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 academic venues that are under review at the same time as their submission to the conference. These citations to simultaneously submitted papers should be anonymized; non-anonymous versions of these citations should, however, be emailed to the program co-chairs at woot27chairs@usenix.org. Simultaneous submission of the same work to multiple academic 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 (https://www.usenix.org/conferences/author-resources/submissions-policy) for details.

Note that work presented by the authors at industry conferences, such as Black Hat, is not considered to have been "previously published" for the purposes of WOOT '27. We strongly encourage the submission of such work to WOOT '27, particularly work that is well suited to a more formal and complete treatment in a published, peer-reviewed setting. In your submission, please note any previous or planned presentations of the work.

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, or that do not have a clear application to offensive security may be rejected without review. Papers accompanied by nondisclosure agreement forms will not be considered. Accepted submissions will be treated as confidential prior to publication on the WOOT '27 website; rejected submissions will be permanently treated as confidential.

As part of USENIX's open access policy, all papers will be available online before the conference. If your accepted paper should not be published prior to the event, please notify production@usenix.org after you submit your final accepted paper. 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 (https://www.usenix.org/sites/default/files/consent_author_proceedings.pdf) for the complete terms of publication.

Any other questions related to the submission process may be sent to the program co-chairs at woot27chairs@usenix.org; please reach out as soon as possible, since it may not be possible to answer late questions prior to the submission deadlines.

Conference Organizers

Program Co-Chairs

Antonio Bianchi, *Purdue University*
Marion Marschalek, *Hack & Cheese Security Consulting LLC and Dartmouth College*

Program Committee

Syed Ghazanfar Abbas, *Purdue University*
Ange Albertini, *Google*
Hussain Almohri, *Kuwait University*
Marco Balduzzi, *Arctic Wolf Networks*
Sébastien Bardin, *CEA & Université Paris-Saclay*
Dana Baril, *Microsoft*
Hadjer Benkraouda, *Purdue University*
Nathaniel Bennett, *Brigham Young University*
Alessandro Bertani, *Durham University*
Tim Blazytko, *Independent Security Consultant*
J Peter Brady, *Dartmouth College*
Thomas Brandstetter, *Limes Security and University of Applied Sciences St. Poelten*
Sergey Bratus, *Dartmouth College*
Hongkai Chen, *Arizona State University*
Sourag Cherupattamoolayil, *Purdue University*
Jiska Classen, *Hasso Plattner Institute, University of Potsdam*
Daniele Cono D'Elia, *Sapienza University of Rome*
Suweera De Souza, *Crowdstrike*
Stephanie Domas, *Mozilla*
Diane Dubois, *Google*
Fabien Duchene
Tim Ebringer, *Microsoft*
Sebastian Eckl, *LMU Munich*
Aurélien Francillon, *EURECOM*
Yanick Fratantonio, *Google*
Dhiman Goswami, *George Mason University*
Carolin Groß, *DB InfraGO AG*
Adhip Gupta, *Meta*
Florian Hantke, *Northeastern University*
Sean Heelan
Flora Herzner, *European Space Agency*
Trammell Hudson, *Lower Layer Labs*
Abdullah Imran, *Purdue University*

Seth Jenkins, *Google Project Zero*
Jiwon Kim, *Purdue University*
Sungwoo Kim, *Purdue University*
Yongdae Kim, *KAIST*
Veronica Kovah, *Dark Mentor LLC*
Xeno Kovah, *Dark Mentor LLC*
Philippe Laulheret, *Cisco Talos*
Zeyu Lei, *Palo Alto Networks*
Caroline Leman, *Synacktiv*
Kun Liu, *Tulane University*
Siyu Liu, *Palo Alto Networks*
Eleonora Losiouk, *University of Padua*
Aravind Machiry, *Purdue University*
Maria Markstedter, *Azeria Labs*
Michal Melewski, *JumpTrading*
Falcon Darkstar Momot, *Aiven*
Thaís Moreira Hamasaki, *Independent*
Marius Muench, *University of Birmingham*
Cristofaro Mune, *Raelize*
Sai Vinod Nagabhairava, *Meta Platforms*
Yuhong Nan, *Sun Yat-sen University*
Antonio Nappa, *Fuzzsociety*
Rishab Nithyanand, *University of Iowa*
Fabio Pagani, *Binarly*
Jeman Park, *Kyung Hee University*
Akshata Krishnamoorthy Rao, *Palo Alto Networks*
Matthew Revelle, *Montana State University*
Felix Rohrbach, *CISPA*
Tommaso Sacchetti, *EURECOM*
Brendan Saltaformaggio, *Georgia Institute of Technology*
Amit Kumar Sikder, *Iowa State University*
Natalie Silvanovich, *Google*
Zihao Su, *University of California, Santa Barbara*
Carlotta Tagliaro, *AIT Austrian Institute of Technology*
Dave (Jing) Tian, *Purdue University*
Saastha Vasan, *University of California, Santa Barbara*
Patrick Ventuzelo, *Fuzzinglabs*
Junpeng Wan, *Purdue University*
Mengxiao Wang, *Texas A&M University*
Morgan Whitlow, *The BlackHoodie Institute*
Jianliang Wu, *Simon Fraser University/Shandong University*
Zhiyuan Zhang, *Max Planck Institute for Security and Privacy*
Jiacheng Zhong, *University of California, Santa Barbara*
Weidong Zhu, *Florida International University*
Andrew D. Zonenberg, *IOActive*

Steering Committee

Jiska Classen, *Hasso Plattner Institute*
Adam Doupé, *Arizona State University*
Aurélien Francillon, *EURECOM*
Yanick Fratantonio, *Google*
Casey Henderson-Ross, *USENIX Association*
Martina Lindorfer, *TU Wien*
Clémentine Maurice, *CNRS*
Alyssa Milburn, *Intel*
Collin Mulliner, *Cruise*
Colin O'Flynn, *NewAE Technology and Dalhousie University*
Mathias Payer, *EPFL*
Sara Rampazzi, *University of Florida*
Yuval Yarom, *Ruhr University Bochum*