Announcement and Call for Papers www.usenix.org/woot25/cfp

WOOT '25: 19th USENIX WOOT Conference on Offensive Technologies

August 11–12, 2025, Seattle, WA, USA

Sponsored by USENIX, the Advanced Computing Systems Association

The **19th USENIX WOOT Conference on Offensive Technologies(WOOT '25)** will be co-located with the 34th USENIX Security Symposium and will take place August 11–12, 2025, at the Seattle Convention Center in Seattle, WA, USA.

Important Dates

- Up-and-coming track paper submissions due: **Tuesday, March 4, 2025, 11:59 pm AoE**
- Academic track paper submissions due: **Tuesday, March 11, 2025, 11:59 pm AoE**
- Notification to authors: **Thursday, April 10, 2025**
- Up-and-coming track final papers due: **Thursday, May 29, 2025**
- Academic track final papers due: **Thursday, June 5, 2025**

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. In 2025, it is co-located with USENIX Security (in Seattle) and will take place on August 11–12, 2025, just before USENIX Security.

WOOT '25 welcomes submissions from academia, independent researchers, students, hackers, and industry. Two different submission tracks are available—an academic "classic" track for those intending to submit complete formal academic papers and an "up-and-coming" track for new or non-academic researchers who may be less familiar with academic procedures and may desire assistance writing a paper or just additional feedback and reviews.

Papers that have been formally reviewed and accepted will be presented during the WOOT conference and published in the formal proceedings. By submitting a paper, you agree that at least one of the authors will register for and attend the conference to present it. Authors are also expected to plan to publish research artifacts (such as source code and data sets) wherever possible; see further details below.

Up-and-Coming Track

Paper submissions due: March 4, 2025, 11:59 pm AoE
Notification to authors: April 10, 2025
Final papers due: May 29, 2025, 11:59 pm AoE

Are you planning to give a cool talk on cutting-edge offensive security research at Black Hat, DEF CON, or another non-academic venue in 2025? Been working on amazing new academic offensive research but not quite confident enough about writing a complete formal academic paper on it? Or do you have existing work that you think deserves publication in a more formal and complete form? Consider submitting to WOOT '25!

The "up-and-coming" track is intended for early researchers, or researchers with non-academic backgrounds, and aims to provide more detailed feedback—typically including one-to-one assistance from a "shepherd"—to help researchers transform their research into a complete paper that will be part of the scientific record. Just as with the "classic" academic track, all these papers will go through the peer-review process, and accepted papers will be published in WOOT's formal conference proceedings; however, the timeline for this track provides more flexibility for early reviewer feedback and shepherd engagement. To ensure that we can meet the deadlines for this process, we expect researchers to respond to feedback quickly and be willing and able to submit an updated, complete paper (with the assistance of a shepherd, if needed) within weeks of receiving feedback. Acceptance of final papers may be subject to shepherd approval.

Rev. 02/18/25

We expect submissions to this track to describe finished research and provide as much detail as possible. Submissions should be in the form of a draft paper, but can also be in any reasonable form (e.g., plain text, Markdown, Word, or LaTeX). The peer review process is double-blind, so submissions should be anonymous; i.e., you should avoid any mention of author/group names and avoid obvious indications of who the authors are (e.g., references to previous work should be in the third person).

Authors of accepted papers are expected to continue to work with their shepherds (where relevant) to improve their papers. We expect final papers (after shepherd approval) to adhere to the same requirements as the academic track (see below), and thus be in the form of a full paper (up to 13 pages, plus a bibliography and appendices). Note that WOOT also expects the submission of "artifacts"—such as source code, documentation, and supporting data—to accompany an accepted paper.

Please contact the chairs at woot25chairs@usenix.org with any questions related to these requirements.

Academic "Classic" Track

Paper submissions due: March 11, 2025, 11:59 pm AoE
Notification to authors: April 10, 2025
Final papers due: June 5, 2025, 11:59 pm AoE

The academic track is aimed at researchers who are already familiar with the academic review process and plan to submit a complete formal academic paper. Of course, we welcome submissions to this track from anyone—not just academics. Papers should be succinct but thorough in presenting the work. Submissions should be finished, complete 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 leading (single-spaced), in a text block 7" x 9" deep. Authors should use USENIX's LaTeX template and style files (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.

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 '25 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, and other artificial intelligence topics
- Operating system and hypervisor security
- Application security
- Network and distributed systems, including virtualization and the cloud
- Wireless and applied protocol 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 (such as solvers and symbolic execution)

"Systemization 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.

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 benefit of the research outweighs the 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 '25 Ethics Guidelines available at www.usenix.org/conference/usenixsecurity25/ethics-guidelines.

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. When disclosure is necessary, authors should include a statement within their submission and/or final paper about steps taken to fulfill the goal of disclosure. 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 woot25chairs@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 2023 IEEE S&P Financial Conflicts Policy (www.ieee-security.org/TC/SP2023/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 or published 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, Artifact Evaluation, and Demos

Authors are expected to document the artifacts they expect to eventually 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).

At least one author of each accepted paper is also expected to attend and participate in the poster/demo session.

Submission Instructions

All submissions should be made online via HotCRP, linked from the 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 woot25chairs@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 (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 '25. We strongly encourage the submission of such work to WOOT '25, 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 '25 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 (www.usenix.org/sites/default/files/consent_author_proceedings.pdf)for the complete terms of publication.

If the conference registration fee will pose a hardship for the presenter of an accepted paper, please contact conference@usenix.org.

Any other questions related to the submission process may be sent to the program co-chairs at woot25chairs@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

Jiska Classen, *Hasso Plattner Institute*
Alyssa Milburn, *Intel*

Program Committee

Shevek
Ange Albertini, *Google*
Daniele Antonioli, *EURECOM*
Jakob Bleier, *TU Wien*
Jake Corina, *Apple*
Adrian Dabrowski, *University of Applied Sciences FH Campus Wien*
Sanjay Devnani, *Google*
Barış Ege, *Keysight Technologies*
Andrew Fasano, *Independent*
Christine Fossaceca, *Microsoft*
Aurélien Francillon, *EURECOM*
Fabs Freyer, *Apple*
Pietro Frigo, *Qualcomm*
Florian Hantke, *CISPA Helmholtz Center for Information Security*
Sean Heelan
Xiali Hei, *University of Louisiana at Lafayette*
Maggie Jauregui, *Intel Corporation*
Martin Johns, *Technische Universität Braunschweig*
Yongdae Kim, *Korea Advanced Institute of Science and Technology (KAIST)*
David Klein, *Technische Universität Braunschweig*

Daniel Klischies, *Ruhr University Bochum*
Karl Koscher, *NVIDIA*
Zion Leonahenahe Basque, *Arizona State University*
Xiang Li, *Nankai University*
Federico Maggi, *Amazon Web Services*
Dominik Maier, *Google*
Thaís Moreira Hamasaki, *Intel Corporation*
Marius Muench, *University of Birmingham*
Cristofaro Mune, *Raelize*
Matthias Neugschwandtner, *Oracle Labs*
Colin O'Flynn, *Dalhousie University*
Fabio Pagani, *Binarly*
Mathias Payer, *EPFL*
Vera Rimmer, *DistriNet, KU Leuven*
Felix Rohrbach, *Technische Universität Darmstadt*
Thomas Roth, *hextree.io*
Tarini Saka, *Ruhr University Bochum*
Henning Seidler, *Technische Universität Berlin*
Natalie Silvanovich, *Google*
Asia Slowinska, *Vrije Universiteit Amsterdam*
Carlotta Tagliaro, *TU Wien*
Sam L. Thomas, *Binarly*
Dave (Jing) Tian, *Purdue University*
Yingchen Wang, *University of California, Berkeley*
Yuval Yarom, *Ruhr University Bochum*
Kyle Zeng, *Arizona State University*
Andrew D. Zonenberg, *IOActive*

Steering Committee

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*