WOOT '17: 11th USENIX Workshop on Offensive Technologies

August 14–15, 2017 • Vancouver, BC, Canada

Sponsored by USENIX, the Advanced Computing Systems Association

WOOT '17 will be co-located with the 26th USENIX Security Symposium (USENIX Security '17) and take place August 14–15, 2017.

Important Dates

- Paper submissions due: **Wednesday, May 31, 2017, 8:59 p.m. PDT**
- Notification to authors: **Tuesday, June 27, 2017**
- Final papers files due: **Tuesday, July 25, 2017**

Workshop Organizers

Program Co-Chairs

William Enck, *North Carolina State University*
Collin Mulliner, *Square Inc.*

Program Committee

Lorenzo Cavallaro, *Royal Holloway University of London*
Sandy Clark, *University of Pennsylvania*
Erinn Clark, *FirstLook*
Scott Coull, *FireEye*
Lucas Davi, *University of Duisburg-Essen*
Razvan Deaconescu, *University POLITEHNICA of Bucharest*
Manuel Egele, *Boston University*
Mario Heiderich, *Cure53*
Alexandros Kapravelos, *North Carolina State University*
Zach Lanier, *Cylance*
Per Larsen, *University of California, Irvine, and Immunant*
Tarjei Mandt, *Azimuth Security*
Charlie Miller, *Uber ATC*
Adwait Nadkarni, *North Carolina State University*
Ben Nell
Christin Pöpper, *New York University*
Kapil Singh, *IBM T. J. Watson Research Center*
Julien Vanegue, *Bloomberg LP and Cornell University*
Ralf-Philipp Weinmann, *Comsecuris*
Georg Wicherski, *CrowdStrike*
Glenn Wurster, *BlackBerry*
Yves Younan, *Cisco Talos*

Overview

The USENIX Workshop on Offensive Technologies (WOOT) aims to present a broad picture of offense and its contributions, bringing together researchers and practitioners in all areas of computer security. Offensive security has changed from a hobby to an industry. No longer an exercise for isolated enthusiasts, offensive security is today a large-scale operation managed by organized, capitalized actors. Meanwhile, the landscape has shifted: software used by millions is built by startups less than a year old, delivered on mobile phones and surveilled by national signals intelligence agencies.

In the field's infancy, offensive security research was conducted separately by industry, independent hackers, or in academia. Collaboration between these groups could be difficult. Since 2007, the USENIX Workshop on Offensive Technologies (WOOT) has aimed to bring those communities together.

WOOT '17 will feature a Best Paper Award and a Best Student Paper Award.

Symposium Topics

Computer security exposes the differences between the actual mechanisms of everyday trusted technologies and their models used by developers, architects, academic researchers, owners, operators, and end users. While being inherently focused on practice, security also poses questions such as "what kind of computations trusted systems are and aren't capable of?," which harken back to fundamentals of computability. State-of-the-art offense explores these questions pragmatically, gathering material for generalizations that lead to better models and more trustworthy systems.

WOOT provides a forum for high-quality, peer-reviewed work discussing tools and techniques for attack. Submissions should reflect the state of the art in offensive computer security technology, exposing poorly understood mechanisms, presenting novel attacks, or surveying the state of offensive operations at scale.

WOOT '17 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:

- Vulnerability research
- Offensive applications of formal methods (solvers, symbolic execution)
- Practical attacks on deployed cryptographic systems and kleptography
- Offensive aspects of mobile security (including location, payments, and RF)
- Attacks on content protection and DRM
- Hardware attacks and attacks on the "Internet of Things"
- Internet-scale network reconnaissance
- Application security (web frameworks, distributed databases, multi-factor authentication)
- Malware design, implementation and analysis
- Vulnerabilities in browser and client-side security (runtimes, JITs, sandboxing)
- Mass surveillance and attacks against privacy

Workshop Format

The presenters will be authors of accepted papers. There will also be a keynote speaker and a selection of invited speakers.

Regular Submission

WOOT '17 welcomes submissions without restrictions of formatting (see below) or origin. Submissions from academia, independent researchers, students, hackers, and industry are welcome. Did you just give a cool talk in the hot Miami sun at Infiltrate? Got something interesting planned for Black Hat later this year? This is exactly the type of work we'd like to see at WOOT '17. Please submit—it will also give you a chance to have your work reviewed and to receive suggestions and comments from some of the best researchers in the world. More formal academic offensive security papers are also very welcome.

Systemization of Knowledge

Continuing the tradition of past years, WOOT '17 will be accepting "Systematization of Knowledge" (SoK) papers. The goal of an SoK paper is to encourage work that evaluates, systematizes, and contextualizes existing knowledge. These papers will prove highly valuable to our community but would not be accepted as refereed papers because they lack novel research contributions. 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. Be sure to select "Systematization of Knowledge paper" in the submissions system to distinguish it from other paper submissions.

All accepted papers will be available online to registered attendees prior to the workshop and will be available online to everyone beginning on the first day of the workshop, August 14, 2017. If your paper should not be published prior to the event, please notify production@usenix.org.

Submission

Papers must be received by 8:59 p.m. PDT on Wednesday, May 31, 2017.

What to Submit

Submissions should be in PDF format. Apart from this, there is no mandatory formatting requirement. Even though the submission format is open, the program committee will have to evaluate the submissions, and the guidelines below will help the program committee to evaluate the quality and originality of the submission.

Papers should be succinct but thorough in presenting the work. The contribution needs to be well motivated, clearly exposed, and compared to the state of the art. Typical research papers are 4–10 pages long (not counting bibliography and appendix). Shorter, more focused papers are encouraged and will be reviewed like any other paper. Papers whose lengths are incommensurate with their contributions will be rejected.

The submission should be formatted in 2 columns, using 10-point Times Roman type on 12-point leading, in a text block of 6.5" by 9". Please number the pages. If possible, use the USENIX Templates for Conference Papers at https://www.usenix.org/conferences/author-resources/paper-templates when preparing your paper for submission.

Authors of accepted papers will have to provide a paper for the proceedings following the above guidelines. A shepherd may be assigned to ensure the quality of the proceedings version of the paper (but not to write the paper for the author).

All submissions will be electronic and must be in PDF. Submissions are single-blind; author names and affiliations should appear on the title page. Submit papers using the Web form, which will be available here soon.

Submissions accompanied by non-disclosure agreement forms will not be considered. Accepted submissions will be treated as confidential prior to publication on the WOOT '17 Web site; rejected submissions will be permanently treated as confidential.

Policies and Contact Information

Simultaneous submission of the same work to multiple competing venues, submission of previously published work without substantial novel contributions, or plagiarism constitutes dishonesty or fraud. 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.

Note: Work presented at industry conferences, such as Black Hat, is not considered to have been "previously published" for the purposes of WOOT '17. We strongly encourage the submission of such work to WOOT '17, particularly work that is well suited to a more formal and complete treatment in a published, peer-reviewed setting. In your submission, please do note any previous presentations of the work.

Authors uncertain whether their submission meets USENIX's guidelines should contact the program co-chairs, woot17chairs@usenix.org, or the USENIX office, submissionspolicy@usenix.org.

Registration for Authors

One author per paper will receive a discount on registration. If the registration fee poses a significant hardship for the presenting author, contact conference@usenix.org.