Announcement and Call for Papers www.usenix.org/woot19/cfp

WOOT '19: 13th USENIX Workshop on Offensive Technologies

August 12–13, 2019, Santa Clara, CA, USA

Sponsored by USENIX, the Advanced Computing Systems Association

usenix THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

The 13th USENIX Workshop on Offensive Technologies (WOOT '19) will be co-located with the 28th USENIX Security Symposium and will take place at the Hyatt Regency Santa Clara in Santa Clara, CA, USA

Important Dates

- Paper submissions due: **Wednesday, May 29, 2019**
- Notification to authors: **Tuesday, June 25, 2019**
- Final papers due: **Tuesday, July 23, 2019**

Conference Organizers

Program Co-Chairs

Alex Gantman, *Qualcomm*
Clémentine Maurice, *CNRS, IRISA*

Program Committee

David Adrian, *Censys*
Johanna Amann, *International Computer Science Institute (ICSI)*
Jean-Philippe Aumasson, *Teserakt AG*
Andrea Barisani, *F-Secure and Inverse Path*
Liang Chen, *Tencent Keen Security Lab*
Lucas Davi, *University of Duisburg-Essen*
Brendan Dolan-Gavitt, *New York University*
Thomas Dullien, *Optimyze*
Jiahong Fang, *Tencent Keen Security Lab*
Yanick Fratantonio, *EURECOM*
Mariano Graziano, *Cisco Talos*
Daniel Gruss, *Graz University of Technology*
Christophe Hauser, *University of Southern California*
Lin Huang, *360 Technology*
Yongdae Kim, *Korea Advanced Institute of Science and Technology (KAIST)*
Marina Krotofil, *admeritia GmbH*
Pierre Laperdrix, *Stony Brook University*
Maria Azeria Markstedter, *Azeria Labs*
Marion Marschalek, *Intel*
Veelasha Moonsamy, *Radboud University Nijmegen*
Cristina Nita-Rotaru, *Northeastern University*
Yossi Oren, *Ben Gurion University of the Negev*
Mathias Payer, *École Polytechnique Fédérale de Lausanne (EPFL)*
Paul Pearce, *Georgia Institute of Technology*
Natalie Silvanovich, *Google*
Window Snyder, *Intel*
Sam Thomas, *CNRS, IRISA*
Gabrielle Viala, *Quarkslab*
Lenx Tao Wei, *Baidu*
Lukas Weichselbaum, *Google*
Hao Xu, *PwnZen InfoTech*
Yuval Yarom, *University of Adelaide and Data61*
Sarah Zennou, *Airbus*

Steering Committee

Michael Bailey, *University of Illinois, Urbana-Champaign*
Dan Boneh, *Stanford University*
Aurélien Francillon, *EURECOM*
Casey Henderson, *USENIX Association*
Collin Mulliner, *Cruise Automation*
Niels Provos, *Google*

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.

Workshop 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 are and aren't trusted systems 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 '19 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, attacks on and offensive research into:

- Hardware, including software-based exploitation of hardware vulnerabilities
- Virtualization and the cloud
- Network and distributed systems
- Operating systems
- Browser and general client-side security (runtimes, JITs, and sandboxing)
- Application security
- Internet of Things
- Machine Learning
- Privacy
- Cryptographic systems (practical attacks on deployed systems)
- Malware design, implementation, and analysis
- Offensive applications of formal methods (solvers, symbolic execution)

Workshop Format

The presenters will be authors of accepted papers. There will also be a keynote speaker and a selection of invited speakers. WOOT '19 will feature a Best Paper Award and a Best Student Paper Award.

Regular Submission

WOOT '19 welcomes submissions without restrictions of formatting (see below) or origin. Submissions from academia, independent researchers, students, hackers, and industry are welcome. Are you planning to give a cool talk at Black Hat in August? Got something interesting planned for other non-academic venues later this year? This is exactly the type of work we'd like to see at WOOT '19. 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 '19 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.

Submission Requirements

Papers must be received on Wednesday, May 29, 2019, AoE (Anywhere on Earth).

What to Submit

Submissions must be in PDF format. 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 at least 4 pages, and maximum 10 pages long (not counting bibliography and appendix). Yet, 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 7" x 9". Please number the pages. We encourage authors to use the USENIX Templates for Conference Papers (https://www.usenix.org/paper-templates).

Submissions are double blind: Submissions should be anonymized and avoid obvious self-references. Submit papers using the submission form, which will be linked from the Call for Papers web page.

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. 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. If your paper should not be published prior to the event, please notify production@usenix.org. Submissions accompanied by non-disclosure agreement forms will not be considered. Accepted submissions will be treated as confidential prior to publication on the WOOT '19 website; rejected submissions will be permanently treated as confidential.

Policies and Contact Information

Simultaneous submission of the same work to multiple competing academic 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 (https://www.usenix.org/submissionspolicy) for details.

Note: 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 '19. We strongly encourage the submission of such work to WOOT '19, 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, woot19chairs@usenix.org, or the USENIX office, submissionspolicy@usenix.org.

Vulnerability Disclosure

If the submission describes, or otherwise takes advantage of, newly identified vulnerabilities (e.g., software vulnerabilities in a given program or design weaknesses in a hardware system) the authors should disclose these vulnerabilities to the vendors/maintainers of affected software or hardware systems prior to the CFP deadline. 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.

Ethical Considerations

Submissions that describe experiments on human subjects, that analyze data derived from human subjects (even anonymized data), or that otherwise may put humans at risk should:

1. Disclose whether the research received an approval or waiver from each of the authors' institutional ethics review boards (e.g., an IRB).
2. Discuss steps taken to ensure that participants and others who might have been affected by an experiment were treated ethically and with respect.

If a paper raises significant ethical or legal concerns, including in its handling of personally identifiable information (PII) or other kinds of sensitive data, it might be rejected based on these concerns.

Registration for Authors

At least one author per paper has to register and and be on site to present the paper. 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.