usenix
THE ADVANCED
COMPUTING SYSTEMS
ASSOCIATION

8th USENIX Workshop on Offensive Technologies (WOOT '14)

Sponsored by USENIX, the Advanced Computing Systems Association

August 19, 2014, San Diego, CA

WOOT '14 will be co-located with the 23rd USENIX Security Symposium (USENIX Security '14), which will be held August 20–22, 2014.

Important Dates

Submissions due: *May 27, 2014, 11:59 p.m. PDT* ***Deadline extended!***
Notification to authors: *June 24, 2014*
Final paper files due: *July 22, 2014*

Workshop Organizers

Program Co-Chairs

Sergey Bratus, *Dartmouth College*
Felix "FX" Lindner, *Recurity Labs*

Program Committee

TBA

Overview

Practical defense springs from offense (paraphrasing John Lambert's Offense and defense aren't peers. Defense is offense's child). Nowadays, offense is no longer a product of relatively isolated artisans or a few exploit-development schools of thought; it is a matter of continuous large-scale operations. 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.

The 8th USENIX Workshop on Offensive Technologies (WOOT '14) will be held on August 19, 2014, in San Diego, CA. WOOT '14 will be co-located with the 23rd USENIX Security Symposium (USENIX Security '14), which will take place August 20–22, 2014. WOOT will feature a Best Paper Award and a Best Student Paper Award.

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 papers 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 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 (software auditing, reverse engineering)
- Penetration testing
- Exploit techniques and automation
- Network-based attacks (routing, DNS, IDS/IPS/firewall evasion)
- Reconnaissance (scanning, software, and hardware fingerprinting)
- Malware design and implementation (rootkits, viruses, bots, worms)
- Denial-of-service attacks
- Web and database security
- Weaknesses in deployed systems (VoIP, telephony, wireless, games)
- Practical cryptanalysis (hardware, DRM, etc.)

Industry Abstracts

For WOOT '14, we will be accepting short abstracts from those working in industry. Abstract submissions serve as an opportunity for industry researchers to present current and emerging work on system exploitation that will help to drive forward the field of computer security. Did you just give a cool talk in the hot Miami sun at Infiltrate? Got something interesting planned for BlackHat later this year? This is exactly the type of work we'd like to see at WOOT. 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. Be sure to select Industry Abstract in the submissions system to distinguish your abstract from other paper submissions.

Systematization of Knowledge and Invited Talks

Continuing the tradition of past years, WOOT will be accepting "Systematization of Knowledge" (SoK) papers and invited talk 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.

Workshop Format

The presenters will be authors of accepted papers as well as a keynote speaker and a selection of invited speakers. This year we ask presenters to choose how much time they would like to present their papers to keep the workshop fast paced. Presenters can request between 10 to 25 minutes each to present their ideas. Regardless of the talk length, we will allocate an extra five minutes for questions per presentation.

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

Submissions

Papers must be received by 11:59 p.m. Pacific time on Thursday, May 22, 2014.

Research Papers

There is no arbitrary minimum or maximum length imposed on research papers. Rather, reviewers will be instructed to weigh the contribution of a paper relative to its length. Papers should be succinct but thorough in presenting the work. Typical research papers are 4–10 pages long, but papers can be shorter if the contribution is smaller. While we will review papers longer than 10 pages, the contributions must warrant the extra length. 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 paper guideline lengths outlined above exclude bibliography and well-marked appendices. The submission must 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. There is no limit on the length of the appendices, but reviewers are not required to read them.

Industry Abstracts

For WOOT '14, we will also accept short abstracts from industry researchers. Submissions in this category will be evaluated on the basis of novelty and potential interest to the security research community at large. Abstracts will be posted alongside other accepted papers on the workshop Web site, and abstract authors will be expected to present a talk. Abstract submissions should be no longer than two single-spaced pages.

General Guidelines

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 and abstracts using the Web form on the Call for Papers Web site, www.usenix.org/woot14/cfp.

Submissions accompanied by non-disclosure agreement forms will not be considered. Accepted submissions will be treated as confidential prior to publication on the USENIX WOOT '14 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, www.usenix.org/conferences/submissions-policy, for details, .

Note: Work presented at industry conferences, such as BlackHat, is not considered to have been "previously published" for the purposes of WOOT '14. We strongly encourage the submission of such work to WOOT, 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, woot14chairs@usenix.org, or the USENIX office, submissionspolicy@usenix.org.

Rev. 5/20/14