



7th USENIX Workshop on Offensive Technologies (WOOT '13)

Sponsored by USENIX, the Advanced Computing Systems Association

August 13, 2013, Washington, D.C.

Important Dates

Submissions due: May 2, 2013, 11:59 p.m. EDT

Notification to authors: June 4, 2013

Final files due: July 2, 2013

Conference Organizers

Program Co-Chairs

Jon Oberheide, *Duo Security*

William Robertson, *Northeastern University*

Program Committee

Dave Aitel, *Immunity*

Michael Bailey, *University of Michigan*

Davide Balzarotti, *Institut Eurecom*

Dion Blazakis, *Trapbit*

Stephen Checkoway, *Johns Hopkins University*

Dino Dai Zovi, *Trail of Bits*

Mark Dowd, *Azimuth Security*

Manuel Egele, *Carnegie Mellon University*

Halvar Flake, *Google*

Chris Grier, *ICSI and University of California, Berkeley*

Felix "FX" Lindner, *Phenoelit*

Sean Heelan, *Persistence Labs*

Mario Heiderich, *Cure53*

Thorsten Holz, *Ruhr-University Bochum*

Karl Koscher, *University of Washington*

Christopher Kruegel, *University of California, Santa Barbara*

Wenke Lee, *Georgia Institute of Technology*

Timothy Leek, *MIT Lincoln Laboratory*

Charlie Miller, *Twitter*

Matt Miller, *Microsoft*

HD Moore, *Rapid7*

Collin Mulliner, *Northeastern University*

Alex Sotirov, *Trail of Bits*

Julien Vanegue, *Bloomberg*

Giovanni Vigna, *University of California, Santa Barbara*

Ralf-Philipp Weinmann, *Université du Luxembourg*

Overview

Progress in the field of computer security is driven by a symbiotic relationship between our understandings of attack and of defense. The USENIX Workshop on Offensive Technologies (WOOT) aims to bring together researchers and practitioners in systems security to present research advancing the understanding of attacks on operating systems, networks, and applications.

WOOT '13 will be held on August 13, 2013, in Washington, D.C. WOOT '13 will be co-located with the 22nd USENIX Security Symposium (USENIX Security '13), which will take place August 14–16, 2013. WOOT this year will feature a Best Paper Award and a Best Student Paper Award.

Topics

Computer security is unique among systems disciplines, in that practical details matter and concrete case studies keep the field grounded in practice. 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, either surveying previously poorly known areas or presenting entirely new attacks.

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 inform 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 '13, 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.

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 and 25 minutes each to present their ideas. Regardless of the talk length, we will allocate an extra 5 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. Eastern time on Thursday, May 2, 2013.

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 '13, 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 2 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 WOOT '13 Call for Papers Web site, www.usenix.org/conference/woot13/call-for-papers.

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 '13 Web site; rejected submissions will be permanently treated as confidential.

Policies and Contact Information

Simultaneous submission of the same work to multiple venues, submission of previously published work, 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 for details: www.usenix.org/conferences/submissions-policy.

Note: Work presented at industry conferences, such as BlackHat, is not considered to have been "previously published" for the purposes of WOOT '13. 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, woot13chairs@usenix.org, or the USENIX office, submissionspolicy@usenix.org.

