Announcement and Call for Papers USENIX

5th USENIX Workshop on Offensive Technologies (WOOT '11)

Sponsored by USENIX, the Advanced Computing Systems Association

http://www.usenix.org/woot11

August 8, 2011 **San Francisco, CA**

WOOT '11 will be co-located with the 20th USENIX Security Symposium (USENIX Security '11), which will take place August 8–12, 2011.

Important Dates

Submissions due: *May 8, 2011, 11:59 p.m. PDT*
Notification to authors: *June 6, 2011*
Final paper files due: *June 23, 2011*

Workshop Organizers

Program Co-Chairs

David Brumley, *Carnegie Mellon University*
Michal Zalewski, *Google*

Program Committee

Dave Aitel, *Immunity, Inc.*
Ivan Arce, *Core Security Technologies*
Dan Boneh, *Stanford University*
Stephen Checkoway, *University of California, San Diego*
Mark Dowd, *Azimuth Security*
Chris Evans, *Google*
Halvar Flake, *Zynamics*
Thorsten Holz, *Ruhr-University Bochum*
Collin Jackson, *Carnegie Mellon University*
Engin Kirda, *Northeastern University*
Amit Klein
Gordon "Fyodor" Lyon, *Nmap Project*
David Molnar, *Microsoft Research*
HD Moore, *Rapid7*
Shobha Venkataraman, *AT&T Labs—Research*
Giovanni Vigna, *University of California, Santa Barbara*

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 '11 will be held on August 8, 2011, in San Francisco, CA. WOOT '11 is co-located with the 20th USENIX Security Symposium (USENIX Security '11), which will take place August 10–12, 2011. 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.)

For industry researchers: Did you just give a cool talk at SOURCE Boston? Got something interesting planned for Black Hat or DEFCON? 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.

Systematization of Knowledge and Invited Talks

In addition to new work, WOOT will be accepting "Systematization of Knowledge" (SoK) papers and invited talk papers.

The goal of a SoK paper is to encourage work that evaluates, systematizes, and contextualizes existing knowledge. These papers will provide a high value 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.

Invited talk papers are papers previously published or accepted for publication at security conferences or workshops with proceedings (and thus are ineligible for submission to WOOT '11 as research papers), but that will be of interest to academic and industry researchers. This track is intended to help academics working in offensive computing broaden their exposure to industry, and vice versa.

Be sure to select "Systematization of Knowledge paper" or "invited talk proposal" in the submissions system to distinguish it from research paper submissions.

Workshop Format

The presenters will be authors of accepted papers, as well as invited guests. Each presenter will have 25 minutes to present his or her idea. A limited number of grants are available to assist presenters who might otherwise be unable to attend the workshop. 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, August 8, 2011. 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 Sunday, May 8, 2011. Paper submissions should be at most 8 typeset pages, excluding 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. All submissions will be electronic and must be in PDF.

Paper submissions are single-blind. Author names and affiliations should appear on the title page. Submit papers using the Web form on the WOOT '11 Call for Papers Web site, http://www.usenix.org/woot11/cfp.

Papers accompanied by nondisclosure agreement forms will not be considered. Accepted submissions will be treated as confidential prior to publication on the USENIX WOOT '11 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 at http://www.usenix.org/submissionspolicy 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 '11. 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, woot11chairs@usenix.org, or the USENIX office, submissionspolicy@usenix.org.