Announcement and Call for Papers USENIX

4th USENIX Workshop on Offensive Technologies (WOOT '10)

Sponsored by USENIX, the Advanced Computing Systems Association

http://www.usenix.org/woot10

August 9, 2010 **Washington, DC**

WOOT '10 will co-located with the 19th USENIX Security Symposium (USENIX Security '10), which will take place August 11–13, 2010.

Important Dates

Submissions deadline extended: *May 31, 2010, 11:59 p.m. PDT*
Notification to authors: June 25, 2010
Electronic files due: *July 12, 2010*

Workshop Organizers

Program Co-Chairs

Charlie Miller, *Independent Security Evaluators*
Hovav Shacham, *University of California, San Diego*

Program Committee

Dave Aitel, *Immunity*
Pedram Amini, *TippingPoint*
Dan Boneh, *Stanford University*
David Brumley, *Carnegie Mellon University*
Mark Dowd, *Azimuth Security*
Chris Eagle, *Naval Postgraduate School*
Halvar Flake, *Zynamics*
Tal Garfinkel, *VMware*
Collin Jackson, *Carnegie Mellon University*
Christian Kreibich, *International Computer Science Institute*
Christopher Kruegel, *University of California, Santa Barbara*
Neel Mehta, *Google*
Matt Miller, *Microsoft*
HD Moore, *Rapid7*
Vern Paxson, *International Computer Science Institute and University of California, Berkeley*
William Robertson, *University of California, Berkeley*

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 aims to bring together researchers and practitioners in system security to present research advancing the understanding of attacks on operating systems, networks, and applications.

Instructions for Authors

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.

We are interested in work that could be presented at more traditional, academic security forums, as well as more applied work that informs the field about the state of security practice in offensive techniques.

A significant goal is producing published artifacts that will inform future work in the field. Submissions will be peer-reviewed and shepherded as appropriate.

Submission topics include:

- 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.)

Workshop Format

The presenters will be authors of accepted position papers/presentations 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 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 9, 2010.

If your accepted 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 Friday, May 28, 2010. This is a hard deadline—no extensions will be given. Submissions should contain eight or fewer two-column pages, excluding references and appendices titled as such, using 10 point type on 12 point (single-spaced) leading, with the text block being no more than 6.5" wide by 9" deep. 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 either PDF (preferred) or PostScript. Author names and affiliations should appear on the title page. Submit papers using the Web form on the WOOT '10 Call for Papers Web site, http://www.usenix.org/woot10/cfp.

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 types of work we'd like to see at WOOT. We would like WOOT to serve as a "best-of" event, bringing work presented at industry conferences to a new audience working in academic computer security. It will also give you a chance to have your work reviewed along with suggestions and comments from some of the best researchers in the world.

Invited talk submissions: We encourage authors of papers that have already been published or accepted for publication at security conferences or workshops with proceedings (and thus are ineligible for submission to WOOT '10 as research papers) but that will be of interest to academic and industry researchers to submit invited talk proposals for those papers. We intend to feature a substantial number of such invited talks at WOOT '10, again in the hope that WOOT will serve as a "best-of" conference for recent research. Be sure to select "invited talk proposal" in the submission system, to distinguish them from research paper submissions.

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.

(Work presented at industry conferences, such as Black Hat, is not considered to have been "previously published" for the purposes of WOOT '10. 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, woot10chairs@usenix.org, or the USENIX office, submissionspolicy@usenix.org.

Papers accompanied by nondisclosure agreement forms will not be considered. Accepted submissions will be treated as confidential prior to publication on the USENIX WOOT '10 Web site; rejected submissions will be permanently treated as confidential.

Rev. 5/28/10