Announcement and Call for Papers USENIX

First USENIX Workshop on Offensive Technologies (WOOT '07)

Sponsored by USENIX, the Advanced Computing Systems Association

http://www.usenix.org/woot07

August 6, 2007 **Boston, MA, USA**

WOOT '07 will be co-located with the 16th USENIX Security Symposium (Security '07), which will take place August 6–10, 2007.

Important Dates

Submissions due: *June 14, 2007, 11:59 p.m. PDT*
Notification of acceptance: *July 7, 2007*
Electronic files due: *July 31, 2007*

Workshop Organizers

Program Chairs

Dan Boneh, *Stanford University*
Tal Garfinkel, *Stanford University*
Dug Song, *Arbor Networks*

Program Committee

Martin Casado, *Stanford University*
Chris Eagle, *Naval Postgraduate School*
Halvar Flake, *SABRE Security*
Greg Hoglund, *HBGary*
Nate Lawson, *Root Labs*
David Litchfield, *NGSSoftware*
Patrick McDaniel, *Pennsylvania State University*
Tim Newsham, *Information Security Partners, LLC*
Vern Paxson, *International Computer Science Institute and Lawrence Berkeley National Laboratory*
Niels Provos, *Google*
Thomas Ptacek, *Matasano Security*
Peter Szor, *Symantec*
Giovanni Vigna, *University of California, Santa Barbara*

Overview

Progress in the field of computer security is driven by a symbiotic relationship between our understanding 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 for 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 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

Attendance will be by invitation only, with preference given to the authors of accepted position papers/presentations. A limited number of grants are available to assist presenters who might otherwise be unable to

attend the workshop. Each author will have 25 minutes to present his or her idea.

Paper files will be available on the USENIX Web site to participants, and will be made generally accessible after the workshop.

Submission Instructions

Papers must be received by 11:59 p.m. PDT on Thursday, June 14, 2007. This is a hard deadline—no extensions will be given. Submissions should contain six or fewer two-column pages, excluding references, using 10-point fonts, standard spacing, and 1-inch margins. Please number pages. All submissions will be electronic and must be in either PDF format (preferred) or PostScript. Author names and affiliations should appear on the title page. Submit papers using the Web form, which will be available available soon on the WOOT '07 Call for Papers Web site, http://www.usenix.org/woot07/cfp.

Given the unique focus of this workshop, we expect that work that has been presented previously in an unpublished form (e.g., Black Hat presentations), but that is well-suited for a more formal and complete treatment in a peer-reviewed setting, will be submitted to WOOT, and we encourage such submissions with adequate citation of previous presentations.

Simultaneous submission of the same work to multiple venues, submission of previously published work, and plagarism constitute dishonesty or fraud. USENIX, like other scientific and technical conferences and journals, prohibits these practices and may, on the recommendation of a program chair, take action against authors who have committed them.

Authors uncertain whether their submission meets USENIX's guidelines should contact the workshop organizers at woot07chairs@usenix.org or the USENIX office, submissionspolicy@usenix.org.