Announcement and Call for Papers **USENIX**

3rd USENIX Workshop on Offensive Technologies (WOOT ’09)

Sponsored by USENIX, the Advanced Computing Systems Association

http://www.usenix.org/woot09

August 10, 2009

Montreal, Canada

WOOT ’09 will be co-located with the 18th USENIX Security Symposium (USENIX Security ’09), which will take place August 10–14, 2009.

Important Dates

Submissions due: *May 28, 2009, 11:59 p.m. PDT*
Notification to authors: *June 29, 2009*
Electronic files due: *July 14, 2009*

Workshop Organizers

Program Co-Chairs

Dan Boneh, *Stanford University*
Alexander Sotirov, *Independent Security Consultant*

Program Committee

Dave Aitel, *Immunity*
Pedram Amini, *TippingPoint*
David Brumley, *Carnegie Mellon University*
Martin Casado, *Nicira*
David Dagon, *Georgia Institute of Technology*
Chris Eagle, *Naval Postgraduate School*
Halvar Flake, *Zynamics*
Tal Garfinkel, *Stanford University and VMware*
Alex Halderman, *University of Michigan*
Trent Jaeger, *Pennsylvania State University*
Charlie Miller, *Independent Security Evaluators*
Matt Miller, *Microsoft*
Tim Newsham, *iSEC Partners*
Jon Oberheide, *University of Michigan*
Dug Song, *Zattoo*
Michal Zalewski, *Google*

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 attendees will be authors of accepted position papers/presentations as well as invited guests. Each author 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 starting on August 10, 2009. If your accepted paper should not be published prior to the event, please notify production@usenix.org.

Submission Instructions

Papers must be received by 11:59 p.m. Pacific time on Thursday, May 28, 2009. This is a hard deadline—no extensions will be given. Submissions should contain six or fewer two-column pages, excluding references, 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. 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 submission form on the WOOT ’09 Call for Papers Web site, http://www.usenix.org/woot09/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 to a more formal and complete treatment in a published, 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, or plagiarism constitutes 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. In some cases, program committees may share information about submitted papers with other conference chairs and journal editors to ensure the integrity of papers under consideration. If a violation of these principles is found, sanctions may include, but are not limited to, barring the authors from submitting to or participating in USENIX conferences for a set period, contacting the authors’ institutions, and publicizing the details of the case.

Authors uncertain whether their submission meets USENIX’s guidelines should contact the program chairs, woot09chairs@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 ’09 Web site; rejected submissions will be permanently treated as confidential.