Announcement and Call for Papers USENIX

6th USENIX Workshop on Hot Topics in Security (HotSec '11)

Sponsored by USENIX, the Advanced Computing Systems Association

http://www.usenix.org/hotsec11

August 9, 2011 **San Francisco, CA**

HotSec '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 12, 2011, 11:59 p.m. PDT*
Notification of acceptance: *June 14, 2011*
Electronic files of final papers due: *July 5, 2011*

Workshop Organizers

Program Chair

Patrick McDaniel, *Pennsylvania State University*

Program Committee

Matt Blaze, *University of Pennsylvania*
Dan Boneh, *Stanford University*
Sandy Clark, *University of Pennsylvania*
Steve Gribble, *University of Washington*
Richard Kemmerer, *University of California, Santa Barbara*
Sam King, *University of Illinois at Urbana-Champaign*
Wenke Lee, *Georgia Institute of Technology*
Fabian Monrose, *University of North Carolina*
Steve Myers, *Indiana University*
Andrew Patrick, *Carleton University*
Vern Paxson, *University of California, Berkeley*
Niels Provos, *Google*
Moheeb Abu Rajab, *Google*
Margo Seltzer, *Harvard University*
Alex C. Snoeren, *University of California, San Diego*
Patrick Traynor, *Georgia Institute of Technology*
Steve Zdancewic, *University of Pennsylvania*

Overview

Position papers are solicited for the 6th USENIX Workshop on Hot Topics in Security (HotSec '11). HotSec is renewing its focus by placing singular emphasis on new ideas and problems. Works reflecting incremental ideas or well understood problems will not be accepted. Cross-discipline papers identifying new security problems or exploring approaches not previously applied to security will be given special consideration. All submissions should propose new directions of research, advocate non-traditional approaches, report on noteworthy experience in an emerging area, or generate lively discussion around an important topic.

HotSec takes a broad view of security and privacy and encompasses research on topics including but not limited to large-scale threats, network security, hardware security, software security, physical security, programming languages, applied cryptography, privacy, human-computer interaction, emerging computing environment, sociology, and economics.

Workshop Format

Each session will be focused by topic area and will include three 15-minute talks, followed by a highly interactive 45-minute discussion of the papers and problems and solutions in the thematic area. Participants are strongly encouraged to participate in the discussions.

Submissions

Submissions must be 4–6 pages including figures, tables, and references. In order to promote discussion, the review process will heavily favor submissions that are forward-looking and open-ended, as opposed to those that summarize more mature work on the verge of conference publication.

All submissions must be anonymized.

Text should be formatted in two columns on 8.5" x 11" paper using 10 point type on 12 point leading ("single-spaced"), with the text block being no more than 6.5" wide by 9" deep. Pages should be numbered, and figures and tables should be legible in black and white without requiring magnification. Submissions must be in PDF and must be submitted via the Web submission form on the HotSec '11 Call for Papers Web site, http://www.usenix.org/hotsec11/cfp. Papers not meeting these criteria will be rejected without review, and no deadline extensions will be granted for reformatting.

Authors will be notified of acceptance by June 14, 2011. Authors of accepted papers will produce a final PDF by July 5, 2011. All papers will be available online to registered attendees before the workshop. If your accepted paper should not be published prior to the event, please notify production@usenix.org. The papers will be available online to everyone beginning on the day of the workshop, August 9, 2011.

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. Questions? Contact your program chair, hotsec11chair@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 HotSec '11 Web site; rejected submissions will be permanently treated as confidential.