Announcement and Call for Papers

7th USENIX Workshop on Hot Topics in Security (HotSec ’12)

Sponsored by USENIX, the Advanced Computing Systems Association
http://www.usenix.org/hotsec12

August 7, 2012

HotSec ’12 will be co-located with the 21st USENIX Security Symposium (USENIX Security ’12), which will take place August 8–10, 2012.

Important Dates
Submissions due: May 7, 2012, 11:59 p.m. EDT
Notification of acceptance: June 14, 2012
Electronic files of final papers due: July 5, 2012

Workshop Organizers
Program Chair
Patrick Traynor, Georgia Institute of Technology

Program Committee
Bill Aiello, University of British Columbia
Matt Blaze, University of Pennsylvania
Dan Boneh, Stanford University
Kevin Butler, University of Oregon
Srdjan Capkun, ETH Zurich
Will Enck, North Carolina State University
Nick Feamster, Georgia Institute of Technology
Ian Goldberg, University of Waterloo
Sam King, University of Illinois at Urbana-Champaign
Wenke Lee, Georgia Institute of Technology
Morley Mao, University of Michigan
Jon McCune, Carnegie Mellon University
Patrick McDaniel, Pennsylvania State University
David Molnar, Microsoft Research
Fabian Monrose, University of North Carolina
Steven Myers, Indiana University
Vern Paxson, University of California, Berkeley
Niels Provos, Google
Jennifer Rexford, Princeton University

Overview
Position papers are solicited for the 7th USENIX Workshop on Hot Topics in Security (HotSec ’12). HotSec places its 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.

Reviews
HotSec ’12 will be attempting to add transparency to the reviewing process and will publish a summary review with each of the accepted papers. A summary review will not be published for papers that are not accepted. This short (<1 page) statement will note the reasons why each paper was accepted and concerns expressed by the PC. Reviews will be posted next to the final papers on the HotSec ’12 Web site, and the authors will have an opportunity to rebut any issues both before they are made public and in the presentation of their work (a video or audio recording of which will also be included on the HotSec Web site). Taken as a whole, these materials are designed to provide the community with valuable context that is traditionally lost after a PC meeting.

Workshop Format
Attendance will be limited to 35–50 participants, with preference given to the authors of accepted position papers/presentations. Sessions will be focused by topic area and 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 no longer than 6 pages, including figures, tables, and references. 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 ’12 Call for Papers Web site, http://www.usenix.org/hotsec12/cfp.

All submissions must be anonymized. Papers not meeting these criteria will be rejected without review, and no deadline extensions will be granted for reformating.

Authors will be notified of acceptance by June 14, 2012. Authors of accepted papers will produce a final PDF by July 5, 2012. 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 7, 2012.

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, hotsec12chair@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 ’12 Web site; rejected submissions will be permanently treated as confidential.

Rev. 1/31/12