Announcement and Call for Papers USENIX

4th USENIX Workshop on Hot Topics in Security (HotSec '09)

Sponsored by USENIX, the Advanced Computing Systems Association

http://www.usenix.org/hotsec09

August 11, 2009 **Montreal, Canada**

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

Important Dates

Position paper submissions due: *May 4, 2009, 11:59 p.m. PDT*
Notification of acceptance: *June 29, 2009*
Final files due: *July 20, 2009*

Workshop Organizers

Program Chair

Tadayoshi Kohno, *University of Washington*

Program Committee

Dan Boneh, *Stanford University*
Stephen Chong, *Harvard University*
George Danezis, *Microsoft Research*
Dirk Grunwald, *University of Colorado*
Jason Hong, *Carnegie Mellon University*
Christopher Kruegel, *University of California, Santa Barbara*
Wenke Lee, *Georgia Institute of Technology*
David Lie, *University of Toronto*
Patrick McDaniel, *Pennsylvania State University*
Michael Reiter, *University of North Carolina at Chapel Hill*

Overview

Security and privacy are important goals for today's and tomorrow's technologies. The challenge is to develop principled approaches for preserving our electronic security and privacy in the ever-changing landscape of new technologies and evolving threats. The 4th USENIX Workshop on Hot Topics in Security will bring together innovative practitioners and researchers in computer security and privacy, broadly defined, to tackle the challenging problems in this space.

We solicit position papers of six or fewer pages that propose new directions of research, advocate non-traditional approaches, report on noteworthy actual experience in an emerging area, or generate lively discussion around an important topic. While pragmatic and systems-oriented, 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, programming languages, applied cryptography, anonymity, human-computer interaction, sociology, economics, and law.

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. We expect that most accepted papers will fall into one or more of the following categories:

- Fundamentally new techniques, approaches, or perspectives for dealing with current security problems
- New major problems arising from new technologies that are now being developed or deployed
- Truly surprising results that cause rethinking of previous approaches

Further, while our goal is to solicit innovative ideas in their formative stages, we do expect submissions to be supported by some evidence of feasibility or preliminary quantitative results. We also expect that many position papers accepted for HotSec '09 will eventually evolve into finished, full papers presented at future conferences.

HotSec is fast becoming the premier venue for presenting innovative new ideas and directions in computer security and privacy, and we look forward to continuing that tradition.

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. Author names and affiliations should appear on the title page (reviewing is not blind). Pages should be numbered, and figures and tables should be legible in black and white without requiring magnification. Papers not meeting these criteria will be rejected without review, and no deadline extensions will be granted for reformatting.

Submissions must be in PDF and must be submitted via the Web submission form on the HotSec '09 Call for Papers Web site, http://www.usenix.org/hotsec09/cfp.

Authors will be notified of acceptance by June 29, 2009. Authors of accepted papers will produce a final PDF and the equivalent HTML by July 20, 2009. All papers will be available online to registered attendees prior to the workshop and will be available online to everyone starting on August 11. If your accepted paper should not be published prior to the event, please notify production@usenix.org.

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 chair, hotsec09chair@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 '09 Web site; rejected submissions will be permanently treated as confidential.