Announcement and Call for Papers USENIX

First Workshop on Hot Topics in Security (HotSec '06)

Sponsored by USENIX, the Advanced Computing Systems Association

http://www.usenix.org/hotsec06

July 31, 2006 **Vancouver, B.C., Canada**

HotSec '06 will be co-located with the 15th USENIX Security Symposium (Security '06), which will take place July 31–August 4, 2006.

Important Dates

Position paper submissions due: *April 20, 2006, 11:59 p.m. PDT (extended deadline)*
Notification of acceptance: *May 15, 2006*
Final files due: *June 30, 2006 (extended deadline)*

Workshop Organizers

Matt Blaze, *University of Pennsylvania*
Virgil Gligor, *University of Maryland*
Angelos D. Keromytis, *Columbia University*
Paul van Oorschot, *Carleton University*
Niels Provos, *Google Inc.*
Dan Wallach, *Rice University*

Overview

Position papers are solicited for the First Workshop on Hot Topics in Security (HotSec '06).

HotSec is intended as a forum for lively discussion of aggressively innovative and potentially disruptive ideas in all aspects of systems security. Surprising results and thought-provoking ideas will be strongly favored; complete papers with polished results in well-explored research areas are discouraged. Papers will be selected for their potential to stimulate discussion in the workshop.

HotSec '06 will be a one-day event, Monday, July 31, 2006, co-located with the 15th USENIX Security Symposium in Vancouver, B.C., Canada.

Workshop Format

Attendance will be by invitation only, limited to 35–40 participants, with preference given to the authors of accepted position papers/presentations.

Each author will have 10–15 minutes to present his or her idea, followed by 15–20 minutes of discussion with the workshop participants.

Instructions for Authors

The goal of the workshop is to stimulate discussion of and thinking about aggressive ideas and issues in systems security.

Position papers are expected to fit into one of the following categories:

- Fundamentally new techniques for and approaches to 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

While our goal is to solicit ideas that are not completely worked out, we expect submissions to be supported by some evidence of feasibility or preliminary quantitative results.

Possible topics of interest include but are not limited to:

- Secure operation, management, and event response of/for ultra–large-scale systems
- Designing secure large-scale systems and networks
- Self-organizing and self-protecting systems
- Security assurance for non-expert users
- Balancing security and privacy/anonymity
- Interactions between security technology and public policy

Submission Instructions

Submitted position papers must be no longer than five (5) single-spaced 8.5" x 11" pages, including figures, tables, and references. Author names and affiliations should appear on the title page.

Submissions must be in PDF format and must be submitted via the Web submission form, which will be

available soon on the HotSec '06 Call for Papers Web site, http://www.usenix.org/hotsec06/cfp.

Authors will be notified of acceptance by May 15, 2006. Authors of accepted papers will produce a final PDF and the equivalent HTML by June 30, 2006. All papers will be available online to participants prior to the workshop, will be published in the Proceedings of HotSec '06 (CD-ROM), and will be generally available online after the workshop.

Simultaneous submission of the same work to multiple venues, submission of previously published work, and plagiarism 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. 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.

Note, however, that we expect that many position papers accepted for HotSec '06 will eventually morph into finished, full papers presented at future conferences.

Authors uncertain whether their submission meets USENIX's guidelines should contact the workshop organizers at hotsec06org@usenix.org or the USENIX office, submissionspolicy@usenix.org.