Announcement and Call for Papers USENIX

2nd USENIX Workshop on Health Security and Privacy (HealthSec '11)

Sponsored by USENIX, the Advanced Computing Systems Association

http://www.usenix.org/healthsec11

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

HealthSec '11 will be co-located with the 20th USENIX Security Symposium (USENIX Security '11), which will take place August 8–12, 2011.

Important Dates

Paper submissions due: *April 12, 2011, 11:59 p.m. UTC (7:59 p.m. EDT)*
Notification of acceptance: *May 24, 2011*
Papers online for attendees (see below): *June 20, 2011*

Workshop Organizers

Program Co-Chairs
Ben Adida, *Harvard University*
Umesh Shankar, *Google*

Program Committee
Steven Bellovin, *Columbia University*
Eric Corndorf, *Medtronic*
Kevin Fu, *University of Massachusetts Amherst*
Carl Gunter, *University of Illinois at Urbana-Champaign*
David Kotz, *Dartmouth College*
Ruby Lee, *Princeton University*
Arien Malec, *Direct Project, ONC*
Arvind Narayanan, *Stanford University*
Sean Nolan, *Microsoft*
Raj Rajagopalan, *HP*
Avi Rubin, *Johns Hopkins University*

Overview

Medical information is rapidly becoming digital. In the United States, the government is providing incentives for doctors to transition to electronic medical records. Tools such as Google Health and Microsoft HealthVault are giving individual patients the ability to manage their own health data. Medical devices and home-care coordination are driving an increase in digital health data sources, while the genomic revolution, with full sequencing achievable for a few thousand dollars and only minutes of processing, is providing a deluge of data we barely know how to manage. The focus of this workshop, HealthSec, is the exploration of security and privacy issues that arise from this exploding quantity of digital personal health information, in both the provider and the patient settings.

HealthSec is intended as a forum for lively discussion of aggressively innovative and potentially disruptive ideas on all aspects of medical and health security and privacy. We strongly encourage cross-disciplinary interactions between fields, including, but not limited to, technology, medicine, and policy. Surprising results and thought-provoking ideas will be strongly favored; complete papers with polished results in well-explored research areas are comparatively discouraged. We will select position papers that show potential to stimulate or catalyze further research and explorations of new directions, as well as extended abstracts that explore a specific issue a little more deeply, including preliminary results.

The workshop will combine posters and brief presentations by position paper authors, slightly longer talks by extended abstract authors, and panel discussions around 2 or 3 major topic areas. We expect the workshop to be highly interactive. There will be no published proceedings, but authors of accepted position papers and extended abstracts will be expected to make their papers available on their own Web sites before the workshop.

Topics

Workshop topics include all areas related to healthcare security and privacy, including:

- Security and privacy models for healthcare information systems
- Industry experience in securing healthcare information systems
- Design and deployment of patient-oriented systems for securely accessing and managing personal health data
- Security and privacy threats against existing and future medical devices—and countermeasures
- Regulatory and policy issues of healthcare information systems
- Privacy of medical information
- Usability issues, especially combined with security constraints
- Threat models for healthcare information systems

Please contact the program co-chairs, healthsec11chairs@usenix.org, if you have any questions.

Submissions

Submitted position papers must be no longer than two 8.5" x 11" pages. Submitted extended abstracts should be no longer than four 8.5" x 11" pages. All papers should be typeset in two-column format in 10 point type on 12 point (single-spaced) leading, with a text block no more than 6.5" wide by 9" deep. Submissions are single-blind; authors should include their names and affiliations as part of their submissions. Submissions must be in PDF format and must be submitted via the Web submission form on the HealthSec '11 Call for Papers Web site, http://www.usenix.org/healthsec11/cfp.

Papers accompanied by nondisclosure agreement forms will not be considered. Accepted submissions will be treated as confidential prior to publication on the authors' Web sites; rejected submissions will be permanently treated as confidential.

Submission of work containing plagiarism constitutes dishonesty or fraud. USENIX, like other scientific and technical conferences and journals, prohibits this practice and may take action against authors who have committed it. See the USENIX Conference Submissions Policy at http://www.usenix.org/submissionspolicy for details. Questions? Contact your program co-chairs, healthsec11chairs@usenix.org, or the USENIX office, submissionspolicy@usenix.org.