Announcement and Draft Call for Papers USENIX

1st USENIX Workshop on Health Security and Privacy (HealthSec '10)

Sponsored by USENIX, the Advanced Computing Systems Association

http://www.usenix.org/healthsec10

August 10, 2010 **Washington, DC**

HealthSec '10 will be co-located with the 19th USENIX Security Symposium, which will take place August 11–13, 2010.

Important Dates

Paper submissions due: *April 9, 2010, 11:59 p.m. PDT*
Notification of acceptance: *May 28, 2010*
Papers available online for attendees (see below): *July 28, 2010*

Workshop Organizers

Program Chairs

Kevin Fu, *University of Massachusetts Amherst*
Tadayoshi Kohno, *University of Washington*
Avi Rubin, *Johns Hopkins University*

Program Committee

Ben Adida, *Harvard University*
Denise Anthony, *Dartmouth College*
Steven Bellovin, *Columbia University*
Melissa Chase, *Microsoft Research*
Kay Connelly, *Indiana University*
Carl A. Gunter, *University of Illinois*
Paul L. Jones, *Food and Drug Administration*
David Kotz, *Dartmouth College*
William Maisel, *Harvard Medical School*
Umesh Shankar, *Google*
Latanya Sweeney, *Carnegie Mellon University*

Overview

There is an increasing trend toward moving medical information to digital systems. This trend has materialized in the form of medical information sharing—both within internal and federated medical systems and in cloud systems such as Google Health and Microsoft HealthVault. This trend has also materialized in the form of advanced medical care, ranging from next-generation medical devices in the home and in the operating room to remote robotic medical devices on the battlefield. The focus of this workshop will be on protecting the security and privacy of these next-generation medical and healthcare systems.

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. A fundamental goal of the workshop is to promote 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. Position papers will be selected for their potential to stimulate or catalyze further research and explorations of new directions, as well as for their potential to spark productive discussions at the workshop.

The format of the workshop will be short presentations by the authors of the position papers, followed by break-out discussion groups. We expect the workshop to be highly interactive. There will be no published proceedings, but authors of accepted position papers will be expected to make their papers available on their own Web sites by July 28, 2010, and to provide the program chairs with the URLs to the papers by July 28 as well.

Topics

Workshop topics are solicited in all areas relating to healthcare information security and privacy, including:

- Security and privacy models for healthcare information systems
- Industrial experiences in healthcare information systems
- Deployment of open systems for secure and private use of healthcare information technology
- Security and privacy threats against and countermeasures for existing and future medical devices
- Regulatory and policy issues of healthcare information systems
- Privacy of medical records
- Usability issues in healthcare information systems
- Threat models for healthcare information systems

Submissions

Submitted papers must be no longer than two 8.5" x 11" pages. Your paper 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 '10 Call for Papers Web site, http://www.usenix.org/healthsec10/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, http://www.usenix.org/events/submissionspolicy.html, for details. Questions? Contact your program chairs, healthsec10chairs@usenix.org, or the USENIX office, submissionspolicy@usenix.org.