Announcement and Call for Papers USENIX

3rd USENIX Workshop on Health Security and Privacy (HealthSec '12)

Sponsored by USENIX, the Advanced Computing Systems Association

http://www.usenix.org/healthsec12

August 6–7, 2012 **Bellevue, WA**

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

Important Dates

Paper submissions due: *April 10, 2012, 11:59 p.m. PDT*
Notification of acceptance: *May 22, 2012*
Electronic files of final papers due: *June 25, 2012*

Workshop Organizers

Program Co-Chairs

Carl Gunter, *University of Illinois at Urbana-Champaign*
Zachary Peterson, *Naval Postgraduate School*

Program Committee

Elisa Bertino, *Purdue University*
Anupam Datta, *Carnegie Mellon University*
Matthew Green, *Johns Hopkins University*
Insup Lee, *University of Pennsylvania*
Ruby Lee, *Princeton University*
Bradley Malin, *Vanderbilt University*
Helen Nissenbaum, *New York University*
Nathanael Paul, *University of Tennessee and Oak Ridge National Laboratory*
Raj Rajagopalan, *HP*
Elaine Shi, *University of California, Berkeley, and Xerox PARC*
Jacob Sorber, *Dartmouth College*
XiaoFeng Wang, *Indiana University at Bloomington*

Steering Committee

Bed Adida, *Mozilla*
Kevin Fu, *University of Massachusetts Amherst*
Tadayoshi Kohno, *University of Washington*
Avi Rubin, *Johns Hopkins University*
Margo Seltzer, *Harvard School of Engineering and Applied Sciences and Oracle*
Umesh Shankar, *Google*

Overview

There is a rapidly moving trend, fueled by both the public and the private sector, toward electronic healthcare systems and devices. These new systems show great potential to improve the administration of healthcare and, ultimately, patient health. However, due to a host of technical shortfalls and a complicated regulatory environment, threats to patient safety, privacy, and security loom large. The focus of this workshop will be on the development of new techniques and policies to ensure the privacy and security of next-generation healthcare systems and devices.

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.

For the first time, the HealthSec Program Committee is soliciting previously unpublished, full-length technical papers that concern privacy and security threats, models, architectures, and protections for health information technologies. We will also select shorter position papers that show potential to stimulate or catalyze further research and explore new directions—surprising results and thought-provoking ideas will be strongly favored. Lastly, we hope to repeat last year's lively rump session, open to anyone with work in progress or preliminary results.

We plan to expand this year's workshop to two days, allowing for more time to discuss a wider array of thought-provoking ideas and topics. The format of the workshop will be short presentations by the authors of position papers and longer presentations by authors with full-length papers. Paper presentation will be augmented by break-out discussion groups, expert panels, and a keynote address. The papers will be published on the USENIX Web site.

Topics

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

- Access control and consent management systems
- Techniques for analyzing and securing audit logs
- Architectures for large-scale health information systems and health information exchange
- Medical devices and body area networks
- Mobile devices and their use with health and fitness devices
- Home and assisted living monitoring systems
- Threat models: formal descriptions and analysis
- Privacy enhancing technologies such as de-identification and differential privacy for electronic health records generally or specific types of data such as images or genomic data
- Usability and human factors
- Regulatory and policy issues
- Authentication and identification techniques
- Cryptographic protocols

Submissions

Submitted full-length papers must be no longer than ten (10) 8.5" x 11" pages. Submitted position papers should be no longer than two (2) 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 '12 Call for Papers Web site, http://www.usenix.org/healthsec12/cfp.

Papers accompanied by nondisclosure agreement forms will not be considered. 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, healthsec12chairs@usenix.org, or the USENIX office, submissionspolicy@usenix.org.

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 first day of the workshop, August 6, 2012.