November 13, 2009
Hyatt Recency Hotel
Chicago, IL, USA

Important Dates

Submissions	**June 12 , 2009**
Notification of acceptance	August 16, 2009
Final papers due	August 25, 2009
Workshop	13 November 2009

(immediately following the 16th ACM CCS)

SPIMACS - An ACM CCS Workshop http://www.infosecon.net/SPIMACS

Security and Privacy in Medical and Home-Care Systems (SPIMACS)

The defined domain of the home includes a wide range of devices from powerful broadband-connected desktop machines to embedded sensors for specialized applications. There are unique dimensions to security when computing occurs in the home: the importance of location privacy when location is equivalent to identification; unique usability targets including children and elders; a complete lack of IT staff and possible support; requirements for strong authentication in the home with the potential requirement for strong anonymity outside the home; and mobility requirements that ranging from constantly at rest to always in motion. Examples of unique security challenges include defense against traffic analysis with medium latency requirements for physical security or some cases of medical monitoring, or sensor networks that need to be managed (and be made trustworthy) by naïve users.

These challenges are compounded when the technology in the home is for the purpose of monitoring for medical purposes. Vulnerable populations can be made more independent by the adoption of ubicomp, AI, social technologies, and digital, networked living assistance. But ill-considered systems can create new risks. Medical monitoring and home monitoring of vulnerable populations create unique security and privacy risks in design and application.

SPIMACS (pronounced *spy-max)* seeks to bring together the computer and social scientists that will be require to address the challenges of securing the intimate digital spaces of the most vulnerable. Therefore the scope of this workshop includes but is not uniquely limited to:

- usable security
- usable privacy technologies
- home-based wireless network security
- security in specialized application for the home, e.g. medical or physical security monitoring
- authentication in the home environment
- security and anonymization of home-centric data on the network
- usable security for unique populations, e.g. elders, children, or the ill
- privacy and security evaluation mechanisms for home environments
- security in home-based sensor networks
- privacy-aware medical devices
- privacy-enhanced medical search
- analyses of in-home and medical systems
- attacks on medical devices
- threat analyses or attacks on medical or home data

We invite talks emphasizing unique security challenges, innovative technologies, and reconsidered threat models. We also invite papers which analyze the use of technologies at home, the challenges of design targeted at a population with cognitive decline, design for the disable with a focus on medical and home support when these projects have a primary or at least significant focus on privacy and security. Papers explaining the data constraints and controls on data from policy, ethical or legal perspectives are also welcome. Please see http://www.infosecon.net/SPIMACS for details.