Theme Issue:

Security and Trust in Context-Aware Systems

Over the last several years, studies considering impacts of security and trust in personal and ubiquitous computing have become an independent research field within the Pervasive Computing area. One strand has concentrated on using context data to establish security or authentication, while a second strand considers trust in context and services provided by remote devices. A third strand, motivated by corporate applications, focuses on resilience of an instrumentation of distributed sources.

Research also considers the question how much information can be obfuscated to protect the privacy of a user without preventing the correct operation of a given application. Methodologically, new models for the specific attack scenarios, security threats and counter-effects in wireless sensor networks and context-aware mobile systems need to be developed.

Clearly, these strands intersect varied disciplines, including acquisition and classification of context, cryptography and fuzzy authentication, sensor networks, information theory and interface design.

The objective of this special issue is to provide a platform to bring together the above strands and emerging paradigms of research in this area and thereby provide further impetus to research on this class of problems.

We solicit original papers and tutorial surveys on the following list of indicative topics.

- Usability aspects of secure and privacy-preserving context-aware systems
- Mechanisms that improve a user's awareness of, and control over, privacy and security
- Agent-based methods and architectures for trust and security in Ubiquitous Computing
- Contextual reasoning methods for privacy and security in Ubiquitous Computing
- Ontology-based and knowledge-based methods and architectures
- Context-based mobile wireless authentication
- Context-based device pairing
- Securing context-aware applications
- Sensor-, context-, and location-based authentication
- Spontaneous secure context-based device interactions
- Autonomic and dependable computing
- Methods and techniques for self-configuration, self-healing, self-protecting systems
- Flexible and secure orchestration of ICT services
- Establishing and managing trust in cyber-physical systems
- Anonymous/pseudonymous context aware mobile computation
- Legal and social issues of security and privacy for mobile devices
- Perception of security and privacy in mobile computing
- Resilient cryptography
- Entropy of context based keys
- Fuzzy cryptography
- Security with noisy data

The above is not an exhaustive list but an indicative one.

Important Dates

Manuscript submission:	**28.02.2012**
First round of reviews:	31.03.2012
Submission of revisions:	21.04.2012
Acceptance notification:	21.05.2012
Final manuscript due:	**18.06.2012**
Publication date:	Summer 2012

Submission Process

Prospective authors should submit a pdf of their manuscript via EasyChair: https://www.easychair.org/account/signin.cgi?conf=stpuc2012. Formatting should follow the PUC-guidelines (see http://www.springer.com/computer/hci/journal/779 for more details). Submissions should not exceed 8000 words. Prior to submitting their papers for review, authors should make sure that they understand and agree to adhere to the over-length page charge policy presented in the PUC guidelines.

Guest Editors

René Mayrhofer,

Hedda R. Schmidtke

Stephan Sigg

Contact

SecurityAndTrust2012@easychair.org

Springer

http://www.springer.com/journal/779

Personal and Ubiquitous Computing
Editor-in-Chief:P. Thomas
ISSN: 1617-4909 (print version)
ISSN: 1617-4917 (electronic version)
Journal no. 779