Mobile Information Systems

Hindawi

Special Issue on

Advances in Security and Privacy for Mobile Users in Intelligent Environments

CALL FOR PAPERS

Security and privacy are vital challenges for mobile users as they move around denser and more prevalent intelligent environments embedded with different connected smart objects that interact with each other and with mobile users in new ways. The focus of security and privacy is predominantly on protecting the use of personal smart tab and pad sized devices such as smart phones, tablets, and laptops by mobile users, in passive environments.

Mobile users often have to tell all about their context to providers to access their mobile information services; hence, mobile users have a lack of user-centred control of their information privacy. Some lower computation device forms such as eHealth wearables tend to support weaker security as these often use open network connections or ones with weaker security, leading to higher security risks such as eavesdropping. Not only can mobile users be tracked by remote service providers but as physical environments become more intelligent, these physical spaces increasingly contain more smart devices that can track users too. When multiple devices are networked as an Internet of Things, multienvironment context collusion can be used to identify and track individuals in a way that violates their privacy expectations. The mobile instrumented-self offers challenges because of the use of microelectromechanical system (MEMS) sensors such as accelerometers embedded in phones and wearables, hiding the computing yet imbuing them with the ability to acquire more fine-grained user context information. This is accompanied by a rise in information services to share this and in crowd-sensing data applications that can data-mine mobile users' information to identify individual users' unique behaviours.

This special issue seeks submissions offering research and development systems, applications, results, and experimental solutions that advance the state of the art of security and privacy solutions for mobile users in intelligent environments comprising ubiquitous computing devices connected into Internets of Things. We seek articles that advance security and privacy for mobile users beyond mere mobile phone device use. We especially welcome papers that tackle both security and privacy for smart mobile users in intelligent environments.

Potential topics include but are not limited to the following:

- User-centred authentication and authorisation for mobile users
- Identity management, access control, and privacy policies for mobile users
- Formal models for adversaries and threats in intelligent environments for mobile users
- Privacy enhancing technologies and protocols for mobile devices
- End-to-end security with low-power mobile computing devices including wearables
- Risk analysis and management for mobile users
- Mobile user-centred access control, consent, and privacy protection
- Establishing trust and reputation in intelligent environments for mobile users
- Privacy preserving data management and contextual integrity for mobile users
- Practical security approaches for intelligent mobile environments
- Security and privacy designs and systems for the instrument self and for crowd-sensing data protection
- Decentralised mechanisms, algorithms, and protocols for security and privacy management, in order to further stress the suitability of distributed and scalable solutions
- Experiences with privacy and security in intelligent mobile environment deployments and applications, for example, eHealth, smart transport, smart cities, ambient assisted living, and augmented human interaction

Authors can submit their manuscripts through the Manuscript Tracking System at http://mts.hindawi.com/submit/journals/misy/aspm/.

Lead Guest Editor
Stefan Poslad, Queen Mary University of London, London, UK
stefan.poslad@qmul.ac.uk

Guest Editors
Davy Preuveneers, KU Leuven, Leuven, Belgium
davy.preuveneers@cs.kuleuven.be

Habtamu Abie, Norwegian Computing Center/Norsk Regnesentral, Oslo, Norway
habtamu.abie@nr.no

Manuscript Due
Friday, 7 April 2017

First Round of Reviews
Friday, 30 June 2017

Publication Date
Friday, 25 August 2017