Personal and Ubiquitous Computing
Special Issue on
Security and Privacy for Smart Cities

Call For Papers

A Smart City is a cutting-edge concept to integrate multiple information and communication technologies (ICT) solutions in a secure fashion to manage the city's assets, in particular the urban areas using ubiquitous computing technologies to improve the quality of life of residents. Smart city technologies, which can be seen as a fusion of information systems and social systems, are deployed for the management of various city infrastructures such as traffic, waste, electricity, sewage, air pollution and water quality, monitoring fire and crime, conserving renewable resources, coordinating urban policies and programs for urban planners etc. Within this paradigm, every device and service is linked to an information network through the Internet. These devices are not limited to traditional static sensors along the road or RFID tags, but any personal wearable device such as a smart phone, a smart watch or smart glasses can also be a ubiquitous point to collect data and get information from a central administrator. It is obvious that this innovative concept provides a two-way communication platform between citizens and government anytime anywhere and for any services.

Despite the huge advantages of smart cities, serious stability, reliability and privacy problems can occur if they are not considered in the design and development stages of smart city projects. For example, a ubiquitous network within the smart city can be corrupted and fall under the control of malicious agents. Also, sensitive data can be captured by hackers. Such circumstances may result into serious disruption. On the other side, privacy is another issue that has to be addressed carefully. No one wants to be traced for his daily activity or personal habits. Since personal devices are pervasive, location privacy becomes especially important.

This special issue intends to gather cutting-edge results on security and privacy issues in the flourishing domain of smart cities. The aim of the proposed Special Issue is to promote research and reflect the most recent advances of technologies in security and privacy of smart cities, with emphasis on the following aspects, but certainly without limitation to them:

- Cryptographic solutions for smart cities
- Authentication in smart cities
- Access control in smart cities
- Security model for smart cities
- Cyber-physical security in smart cities
- Key management in smart cities
- Anti-social event detection in smart cities assisted by big data analysis
- Cloud-assisted secure applications for smart cities
- Secure Internet of Things (IoT) applications for smart cities
- Lightweight security for wearable devices in smart cities
- Location and trajectory privacy for personal devices in smart cities
- New business processes and models involving cybersecurity in smart cities
- Physical security threats and solutions to endpoints in smart city devices
- Privacy Enhanced Technologies (PET) for smart cities
- Privacy preserving data collection and disclosure in smart cities
- Secure big data analysis for smart cities
- System model and architecture for secure smart city technologies
- Secure outsourcing for pervasive devices in smart cities

Important Dates:

Submission deadline: September 1, 2016

First-round notification: October 15, 2106

Final notification: January 20, 2017

Submission Instructions:

Submission should be emailed to the leading guest editor Joseph Liu, with the header "Submission: Special Issue on Security and Privacy for Smart Cities".

Guest Editors

Joseph Liu – Monash University, Australia (joseph.liu@monash.edu)

Raymond Choo – University of South Australia, Australia (Raymond.Choo@unisa.edu.au)

Xinyi Huang – Fujian Normal University, China (xyhuang81@gmail.com)

Man Ho Au - Hong Kong Polytechnic University, Hong Kong (csallen@comp.polyu.edu.hk)