
In conjunction with ICCCN 2016
Waikoloa, Hawaii, USA
August 4, 2016

Mobile wireless devices, such as wireless sensors, smart tags, smart pads, tablets, PDAs, and smart phones, have become pervasive and attract significant interest from academia, industry, and standard organizations. With the latest cloud computing technology, those mobile wireless devices will play a more and more important role in computing and communication. When those devices become pervasive, security, privacy and trust become critical components for the acceptance of applications built on those devices. Moreover, several favorable characteristics of mobile and wireless devices, including portability, mobility, and sensitivity, further impose the challenge of security and privacy in those systems.

Despite recent advances, many research issues still remain in the design of secure, privacy-preserving, or trust architectures, protocols, algorithms, services, and applications on mobile and wireless systems. For example, when mobile devices have more storage space, high bandwidth, and super sensing capacity, more sensitive information will be stored in those devices. On the other hand, operating systems running on those devices are not as powerful and reliable as those on traditional computers. Both OS layer and higher-layer protocol models are expected to enhance the security and preserve the privacy of those devices. With more mobile devices being used in social networks and traditional web-based systems, novel trust models are essential for new applications. New cryptographic algorithms, key distribution schemes and access control policies are also encouraged by considering the special characteristics of mobile and wireless devices. Other issues such as malware, cyber threat, intrusion detection, attack modeling, security analysis, identity management and anonymity also need to be revisited in mobile and wireless systems.

This workshop aims to bring together the technologists and researchers who share interest in the area of security, privacy and trust in mobile and wireless systems, as well as explore new venues of collaboration. The main purpose is to promote discussions of research and relevant activities in the models and designs of secure, privacy-preserving, or trust architectures, protocols, algorithms, services, and applications, as well as analysis on cyber threat in mobile and wireless systems. It also aims at increasing the synergy between academia and industry professionals working in this area. We plan to seek papers that address theoretical, experimental research, and work in progress for security, privacy and trust related issues in the context of mobile and wireless systems that include, but are not limited to, the following:

- Cryptography for Mobile and Wireless Systems
- Cryptography for Cloud Computing, Fog/Edge Computing
- Wireless Local Area Networks
- Wireless Sensor Networks
- Wireless Mesh Networks
- Wireless Ad-hoc Networks
- Vehicular Networks
- Body-area Networks
- Cellular Networks (3G, 4G, ...)
- WiMAX Networks
- Machine to Machine (M2M) Networks
- Software Defined Networks (SDN)
- Social Networks
- Smart Grid
- RFID-based Systems
- Mobile Cloud
- Cyber-Physical Systems (CPS)
- Internet of Things
- Location-based Service Systems
- Mobile Healthcare Systems
- Smart Building Systems
- Big Data

Instructions for Authors

Authors are invited to submit manuscripts reporting original unpublished research and recent developments in the topics related to the workshop. Submissions should include a title, abstract, keywords, author(s) and affiliation(s) with postal and e-mail address(es) of the corresponding author. Submitted manuscripts must be formatted in standard IEEE camera-ready format (double-column, 10 pt font) and must be submitted via EasyChair (http://www.easychair.org/) as PDF files (formatted for 8.5x11-inch paper). The manuscripts should be no longer than 6 pages. Two additional pages are permitted if the authors are willing to pay an over-length charge at the time of publication (manuscripts should not exceed 6 pages). Submitted papers cannot have been previously published in or be under consideration for publication in another journal or conference. The workshop Program Committee reserves the right to not review papers that either exceed the length specification or have been submitted or published elsewhere. Submissions must include a title, abstract, keywords, author(s) and affiliation(s) with postal and e-mail address(es). All authors of a paper must be registered in the RIGHT order via EasyChair at the SUBMISSION TIME and cannot be changed after the submission due time at EasyChair. The paper title and author name list order cannot be changed during the final camera-ready submission.

Review and Publication of Manuscripts

Submitted papers will be reviewed by the workshop Program Committee and judged on originality, technical correctness, relevance, and quality of presentation and the comments will be provided to the authors. Workshop papers will be in the same proceedings of the main conference papers. An accepted paper must be presented at the ICCCN 2016 venue by one of the authors registered at the full registration rate. If any accepted paper is not registered, the paper will be removed from the workshop program and the proceedings. Each workshop registration covers up to two workshop papers by an author. Accepted and registered papers will be published in proceedings that will be available through Xplore. Papers that are not presented at the ICCCN 2016 venue by one of the registered co-authors will not appear in Xplore. Outstanding papers will be invited to extend to full version for a journal (SG(E)-indexed), currently under contacting and targeting publication in early 2017.