M2MSec'14	October 29, 2014
with IEEE CNS 2014	San Francisco, CA, USA

First International Workshop on Security and Privacy in Machine-to-Machine Communications (M2MSec'14)

Call for Papers

Machine to machine (M2M) communications refer to technologies that enable devices to interact with each other over both wireless and wired communication network without any human intervention. By 2020, there will be 12.5 billion M2M devices globally, up from 1.3 billion devices today. M2M communication technology involves the usage of a wide range of smart devices such as sensors, actuators, RFIDs, microcontrollers equipped with RF transceivers. Those smart devices capture data and events that are then transmitted through a communication network (wireless, wired or hybrid) to a back-end application server that processed the received data into meaningful information. M2M communication systems have existed in different forms and been utilized in applications such as e-health, smart energy, automobile, and RFID. While M2M communication systems bring new exciting opportunities, security remains of the greatest concern in the development and deployment of M2M systems, balanced with the need to protect the privacy and rights of individuals.

Aspects of M2M communications can be found in other research areas such as wireless sensor networks (WSN) and cyber-physical systems (CPS). The differences are that M2M does not require the communicating devices to be limited in terms of energy or computational capabilities, nor does M2M require an explicit feedback loop between the physical and cyber entities. The goal of this workshop is to provide a venue for researchers in the communication and network security aspects related to Internet of Things (IoT) and pervasive/ubiquitous computing to share and exchange ideas, experiences, and lessons learned.

The First International Workshop on Security and Privacy in Machine-to-Machine Communications (M2MSec'14) aims to foster innovative research and discuss about security and privacy challenges, solutions, implementations, and standardizations in emerging M2M communication systems. M2MSec'14 takes place on October 29, 2014 in San Francisco, USA in conjunction with IEEE Conference on Communications and Network Security (CNS'14). Papers from academic researchers, industry practitioners, and government institutions offering novel research contributions in all theoretical and practical aspects of security and privacy in M2M communications are solicited for submission to M2MSec'14.

The scope of this workshop covers all aspects of security and privacy in M2M communications and particular topics of interest include, but are not limited to:

- Threat and vulnerability analysis in M2M communications
- Attacks and countermeasures in M2M communications
- System architecture for security and privacy in M2M communications
- Physical layer security in M2M communications
- Cross layer design for security and privacy in M2M communications
- Security and privacy in smart grid, RFID, near field communications (NFC), bluetooth, wireless sensor networks, body area networks, e-health, vehicular ad-hoc networks

- Lightweight cryptographic primitives and protocols
- Trust and assurance in M2M communications
- Hardware security module and platform for M2M communications
- Identity and credential management in M2M communications
- Standardization for M2M communications
- Cloud computing and M2M communications
- Device-to-Device (D2D) networks such as LTE-direct
- Pervasive sensing Networks, including mobile crowdsourcing, participatory sensing
- Novel attacks resulting in IoT environments
- Data mining, cleaning and analysis techniques for IoT
- Real world deployment and experiences
- Prototype IoT systems and applications

General Co-chairs

Prof. Daniel W. Engels, Southern Methodist University, USA
Prof. Guang Gong, University of Waterloo, Canada
Prof. Jie Wu, Temple University, USA

Technical Program Co-chairs

Dr. Xinxin Fan, University of Waterloo, Canada
Dr. Katrin Reitsma, Motorola Solutions, USA
Dr. Chiu Chiang Tan, Temple University, USA

Submissions Instruction

The workshop solicits original papers of up to 6 pages. For instructions on the manuscript layout, please visit `http://cns2014.ieee-cns.org/content/submission-instructions-1`. To submit, go to `http://edas.info/N16587`, then select the appropriate workshop. Each accepted paper must be presented by one registered author. A paper submitted to this workshop must not be in parallel submission to any other journal, magazine, conference, or workshop with proceedings. Submissions not meeting these guidelines risk rejection without consideration of their merits. Accepted and presented papers will be published in the IEEE CNS 2014 Conference Proceedings and submitted to IEEE Xplore®.

Important Dates

Workshop papers submission:	June 1, 2014
Workshop papers notification of acceptance:	July 1, 2014
Workshop papers camera ready:	July 11, 2014