IEEE

Design&Test

Call for Contributions

Special Issue on
Cyber-Physical Systems Security and Privacy

The research relating to cyber-physical systems (CPS) has recently drawn the attention of academia, industry, and the government because of its wide impact to society, economy, and environment. While still lacking in formal definition, cyber-physical systems are largely referred to as the next generation of engineered systems with the integration of communication, computation, and control to achieve the goals of stability, performance, robustness, and efficiency for physical systems.

While ongoing research work focuses on achieving these goals, security within CPS is largely ignored. As cyber-physical systems are being widely integrated in various critical infrastructures, however, any security breaches to these systems could have catastrophic consequences. For example, if a vehicle-to-vehicle communication network is compromised, accidents would occur when wrong distance information is transmitted. In fact, the emergence of autonomous cars has further deteriorated the problem since passengers have to trust all decisions made by the vehicles. Applications of CPS institute at different levels of integration, ranging from nation-wide power grids, to medium scale, such as the smart home, and small scale, e.g. ubiquitous health care systems including implantable medical devices.

Besides security concerns, CPS privacy is a serious issue. Cyber-physical systems are often distributed broadly across wide geographic areas and typically collect huge amounts of information for data analysis and decision making. The collection of information helps the system make smart decisions through sophisticated machine learning algorithms. Data breach, however, could potentially happen in any part of the system, including the stages of data collection, data transmission, data operation, and data storage. Again, most of the current CPS design methodologies do not consider data protection, leaving the collected data in jeopardy. Moreover, discussions and surveys on geographic implications on CPS security/privacy are also encouraged. **Topics of interest include, but are not limited to:**

(1) Security and privacy implications of CPS

(2) System, network and platform level approaches to CPS security

(3) control theory and mathematical foundations for CPS security

(4) Economics and game theory approaches to CPS security and privacy

(5) Physics-based approaches to CPS security and privacy

(6) Domain specific approaches to CPS security

(7) Geographical and societal impact of CPS

Submission Guidelines can be found at: http://ieee-ceda.org/publications/d-t/paper-submission

Please choose special session category "CPS-Security" while submitting the manuscript to the ScholarOne Manuscripts website (https://mc.manuscriptcentral.com/dandt).

Paper Submission and Review Schedule:

Submission Deadline:	1 June 2016
First Round of Reviews:	15 July 2016
Revisions Due:	15 Aug 2016
Notification of Final Acceptance:	15 Sep 2016
Camera Ready Due:	30 Sep 2016

Guest Editor Contacts

Ramesh Karri, rkarri@nyu.edu
Michail Maniatakos, michail.maniatakos@nyu.edu
Alvaro Cardenas, alvaro.cardenas@utdallas.edu
Jorge Cuellar, jorge.cuellar@siemens.com