CALL FOR PAPERS
IEEE Transactions on Dependable and Secure Computing

Special Issue/Section:
Emerging Embedded and Cyber Physical System Security Challenges and Innovations

IEEE Transactions on Dependable and Secure Computing seeks original manuscripts for a Special Issue/Section on **Emerging Embedded and Cyber Physical System Security Trends** scheduled to appear late in 2016**.**

Deeply-embedded systems (deployed in human body, with computer programs sending and receiving sensitive data and performing data mining for the decisions) are increasingly popular, but the security and privacy issues are not fully understood and studied. For example, issues relating to the confidentiality / integrity / availability / privacy of implantable and wearable medical devices, secure and private big data analytics, acquisition, and storage, privacy-preserving data mining, secure machine-learning, cyber physical systems security, and security of hardware and software systems used for databases (with diverse societal contexts) are critical, and can be challenging to address due to their unique constraints and usage model. Existing systems for such computations would need to be transparently integrated into sensitive environments – the consequent size and energy constraints imposed on any security solutions are demanding. Thus, unique challenges arise due to the sensitivity of computation processing, need for security in implementations, and assurance "gaps."

The focus of this special issue will be on novel security and forensic methods for deeply-embedded systems and cyber physical systems, and emerging cryptographic solutions applicable to extremely-constrained, sensitive infrastructures, and advancements in feasible security measures for evolving interdisciplinary research trends such as computing for: cyber-physical embedded systems used for therapeutic and diagnosis purposes, and smart fabrics/homes/grids. Topics of interest include, but are not limited to:

- Advances in Health-care IT and cyber-physical medical systems security and privacy
- Security and privacy in IoT applications
- Green cryptography for deeply-embedded data security
- Smart building security and spatial/temporal privacy preservation
- Privacy in cyber physical systems
- Secure and trustable cyber-physical systems
- Emerging cryptographic computing schemes for embedded security
- Novel anonymous sensitive data handling and restricted computing methods in cyber physical systems
- Novel deeply-embedded computing reliability methods

Submitted articles must not have been previously published or currently submitted for journal publication elsewhere. As an author, you are responsible for understanding and adhering to our submission guidelines. You can access them at the IEEE Computer Society web site, www.computer.org. Please thoroughly read these before submitting your manuscript.
Papers should be submitted directly to the manuscript central at:
https://mc.manuscriptcentral.com/tdsc-cs.

Please note the following important dates:
Full Paper Regular Submission Due: February 15, 2016
Notification of Results: April 15, 2016
Revisions Due: July 15, 2016
Notifications of Final Acceptance: August 30, 2016
Submissions of Final Revised Papers: September 30, 2016

Guest Editors

Kim-Kwang Raymond Choo	**Mehran Mozaffari Kermani**	**Reza Azarderakhsh**	**Manimaran Govindarasu**
University of South Australia	RIT	RIT	Iowa State University
Adelaide, Australia	Rochester, NY	Rochester, NY	Ames, Iowa
Raymond.Choo@unisa.edu.au	m.mozaffari@rit.edu	rxaeec@rit.edu	gmani@iastate.edu