CALL FOR PAPERS

IEEE Transactions on Multi-Scale Computing Systems

Special Issue/Section on Hardware/Software Cross-Layer Technologies for Trustworthy and Secure Computing

GUEST EDITORS:
Shiyan Hu, shiyan@mtu.edu, Michigan Technological University
Yier Jin, yier.jin@eecs.ucf.edu, University of Central Florida
Mark M. Tehranipoor, tehrani@engr.uconn.edu, University of Connecticut
Kenneth Heffner, kenneth.h.heffner@honeywell.com, Honeywell

TOPIC SUMMARY:

The increasing complexity of networked computing systems makes modern network systems vulnerable to various attacks against their resources, infrastructure, and operability. While the reasons for such attacks may be tied to complex sociological issues, the cause of our inadequate defense solutions lies in the single-layered approach used to address computer systems security. Current security approaches separate defense strategies into distinct realms, either hardware or software. Accordingly, cross-layer approaches for secure computing and circuit systems are entirely lacking. In addition, the wide usage of third-party IP cores and outsourcing fabrication/packaging services make it possible for malicious hardware modules to enter the design flow and, therefore, complicates the problem of trusted system design and verification. While hardware security has been under investigation for years, systematically understanding the security threats to hardware infrastructure from a cross-layer perspective is an emerging research topic. Therefore, this special issue intends to serve as a forum to present state-of-the-art security solutions crossing software and hardware layers towards trustworthy computing system development.

The topics of interest for this special issue include, but are not limited to:

- Cross-layer solutions for computing system protection
- Cross-layer hardware/software attacks and protections on computing systems
- Hardware-supported trustworthy computing system
- Topographic and data flow modeling for cyber physical system security.
- Non-redundancy-based methods for persistent threat prognostics.
- Security-enhanced hardware structure for system protection
- Hardware security primitives including PUFs and Public PUFs
- Software level attacks leveraging hardware vulnerabilities
- Trusted computing platforms for smart devices in cyber-physical systems
- Computer aided design (CAD) techniques for secure ICs and systems
- Interplay between security, trust and reliability of emerging nanotechnologies
- Countermeasures for backdoors and in the software-hardware interface
- Formal verification for computing system security

IMPORTANT DATES:

Open for submissions in ScholarOne Manuscripts:	September 1, 2015
Closed for submissions:	October 31, 2015
Results of first round reviews:	January 15, 2016
Submission of revised manuscripts:	February 15, 2016
Results of second round reviews:	March 15, 2016
Publication material due:	May 1, 2016

SUBMISSION GUIDELINES:

Prospective authors are invited to submit their manuscripts electronically after the "open for submissions" date, adhering to the *IEEE Transactions on Multi-Scale Computing Systems* guidelines (http://www.computer.org/portal/web/tmscs/author). Please submit your papers through the online system (https://mc.manuscriptcentral.com/tmscs-cs) and be sure to select the special issue or special section name. *Manuscripts should not be published or currently submitted for publication elsewhere.* Please submit only full papers intended for review, not abstracts, to the ScholarOne portal. If requested, abstracts should be sent by e-mail to the Guest Editors directly.