CALL FOR PAPERS

ACM Transactions on Embedded Computing Systems
Special Issue on "Embedded Device Forensics and Security: State of the Art Advances"

Embedded devices such as smart mobile devices and smart cards are an increasingly ubiquitous technology used throughout the daily lives of people worldwide. Ensuring the security of embedded devices, particularly those found in cyber-physical systems, is a challenging task as such devices are typically produced under cost constraints and in large volumes. Embedded devices generally operate with limited power energy budget and work in a mobile (and potentially hostile) environment. Testing and debugging of embedded devices, such as those used in industrial software systems and cyber-physical systems, can be difficult in practice as reproducing observed bugs can be challenging in environments where bug reports are often incomplete, systems are tightly coupled with their operating environment, are poorly observable, embedded devices are resource constrained and offer limited support for advanced debugging mechanisms.

This special issue will focus on cutting edge research on the topic of embedded device security and forensics, with a particular emphasis on novel techniques to secure embedded devices (including those found in cyber-physical systems) as well as obtaining evidential data from embedded devices in crimes that make use of sophisticated and secure technologies (e.g. the use of strong encryption to secure both data-at-rest and data-in-transit). Topics of interest include:

- Advanced security features for embedded devices and cyber-physical systems (e.g. computationally efficient anonymity and authentication schemes such as cancellable biometrics)
- Cryptanalysis, side channel attacks, fault injection attacks, memory-based attacks and other attacks targeting embedded devices and cyber-physical systems
- Forensic and anti-forensic techniques for embedded devices and cyber-physical systems
- Ontology of bug reproduction productivity tools for embedded devices and cyber-physical systems
- Vulnerability and bug detection and mitigation techniques for embedded devices and cyber-physical systems

High quality survey (e.g. survey of debugging and bug reproduction state of the advances on embedded devices used on industrial software platforms) and position papers on the above topics are also welcome.

Submissions must be based on formal, experimental, or other scholarly approaches to problems in software engineering research, providing an evaluation of the research that is appropriate to and commensurate with the research claims.

IMPORTANT DATES

- Submission deadline: 31 December 2015
- Authors' notification: 28 February 2016
- Revisions due: 30 April 2016
- Final decision: 30 June 2016
- Camera ready version due: 31 July 2016
- Tentative publication date: Late 2016

Please contact the Guest Editors for further questions.

Guest Editors

Dr Kim-Kwang Raymond Choo University of South Australia, AU
Google Scholar: http://scholar.google.com.au/citations?user=rRBNI6AAAAAJ&hl=en
Email: raymond.choo@unisa.edu.au

Associate Professor Yunsi Fei Northeastern University, USA
Google Scholar: http://scholar.google.com.au/citations?user=Ja64KW4AAAAJ&hl=en
Email: yfei@ece.neu.edu

Professor Yang Xiang Deakin University, AU
Google Scholar: http://scholar.google.com.au/citations?user=7ymTWY4AAAAJ&hl=en
Email: yang.xiang@deakin.edu.au

Research Professor Yu Yu Shanghai Jiao Tong University, PRC
Google Scholar: http://scholar.google.co.uk/citations?user=lpRkCB4AAAAJ&hl=en
Email: yuyu@yuyu.hk