Emerging Embedded and Cyber Physical System Security Challenges and Innovations

Kim-Kwang Raymond Choo, *Senior Member, IEEE*, Mehran Mozaffari Kermani, *Senior Member, IEEE*, Reza Azarderakhsh, and Manimaran Govindarasu, *Fellow, IEEE*

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."

This special issue is dedicated to the identification of techniques designed for embedded systems and cyber-physical systems, such as emerging cryptographic solutions applicable to extremely-constrained, sensitive infrastructures. We received 35 submissions for this special issue, of which 4 have been accepted (acceptance rate ~11.45 percent). Each paper went through a rigorous peer review process, in addition to multiple follow-up rounds with the authors. A summary of the papers is provided below.

In "*On Emerging Family of Elliptic Curves to Secure Internet of Things: ECC Comes of Age*", a team of researchers from Canada, China, Kingdom of Saudi Arabia, Singapore and Luxembourg defined a family of lightweight elliptic curves designed for resource-constrained devices, prior to presenting the design of a scalable, regular, and highly-optimized ECC library for MICAz and Tmote Sky sensor nodes.

- *K.-K.R. Choo is with the University of Texas at San Antonio, San Antonio, TX 78248. E-mail: raymond.choo@fulbrightmail.org.*
- *M.M. Kermani is with Rochester Institute of Technology, Rochester, NY 14623. E-mail: m.mozaffari@rit.edu.*
- *R. Azarderakhsh is with Florida Atlantic University, Boca Raton, FL 33431. E-mail: razarderakhsh@fau.edu.*
- *M. Govindarasu is with Iowa State University, Ames, IA 50011. E-mail: gmani@iastate.edu.*

For information on obtaining reprints of this article, please send e-mail to: reprints@ieee.org, and reference the Digital Object Identifier below.
Digital Object Identifier no. 10.1109/TDSC.2017.2664183

In "*Towards a Reliable Detection of Covert Timing Channels over Real-Time Network Traffic*", the authors from University of Nebraska-Lincoln presented a way of detecting covert timing channels over real-time network traffic. Specifically, the authors leveraged three different non-parametric statistical tests to generate statistical test scores that differ between overt and covert traffic inter-packet delays.

In "*SMA: A System-Level Mutual Authentication for Protecting Electronic Hardware and Firmware*", researchers from Auburn University and University of Florida studied the supply chain vulnerabilities for electronic systems. They presented a system-level mutual authentication approach that allows the hardware to authenticate the firmware and the firmware to verify the identity of the hardware, using two secure protocols, TIDP and TIDS, proposed in the paper.

In "*Don't fool me!: Detection, Characterisation and Diagnosis of Spoofed and Masked Events in Wireless Sensor Networks*", the authors from Imperial College London presented a wavelet transform-based approach designed to detect malicious data injections in wireless sensor networks. The approach allows one to distinguish malicious interference due to faulty behaviours.

Despite the significant amount of efforts devoted to addressing embedded and cyber physical system security, there are a number of challenges that remain to be addressed. Potential topics for future research would include:

- Advances in Health-care IT and cyber-physical medical systems security and privacy
- 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

K.-K. R. Choo
M. M. Kermani
R. Azarderakhsh
M. Govindarasu
Guest Editors

Kim-Kwang Raymond Choo received the PhD degree in information security from the Queensland University of Technology, Australia, in 2006. He currently holds the Cloud Technology Endowed professorship at The University of Texas at San Antonio. He has served as the Special Issue guest editor of the *ACM Transactions on Embedded Computing Systems* (2017; DOI: 10.1145/3015662), the *ACM Transactions on Internet Technology* (2016; DOI: 10.1145/3013520), the *Digital Investigation* (2016; DOI: 10.1016/j.diin.2016.08.003), the *Future Generation Computer Systems* (2016; DOI: 10.1016/j.future.2016.04.017), the *IEEE Cloud* (2015; DOI: 10.1109/MCC.2015.84), the *IEEE Network* (2016; DOI: 10.1109/MNET.2016.7764272) the *Journal of Computer and System Sciences* (2017; DOI: 10.1016/j.jcss.2016.09.001), the *Multimedia Tools and Applications* (2017; DOI: 10.1007/s11042-016-4081-z), the *Pervasive and Mobile Computing* (2016; DOI: 10.1016/j.pmcj.2016.10.003), etc. He is a recipient of various awards including the ESORICS 2015 Best Paper Award, the Winning Team of the Germany's University of Erlangen-Nuremberg (FAU) Digital Forensics Research Challenge 2015, the 2014 Highly Commended Award by the Australia New Zealand Policing Advisory Agency, the Fulbright Scholarship in 2009, the 2008 Australia Day Achievement Medallion, and the British Computer Society's Wilkes Award in 2008. He is a fellow of the Australian Computer Society, and a senior member of the IEEE.

Mehran Mozaffari Kermani received the BSc degree in electrical and computer engineering from the University of Tehran, Tehran, Iran, in 2005, and the MESc and PhD degrees from the Department of Electrical and Computer Engineering, University of Western Ontario, London, Canada, in 2007 and 2011, respectively. He joined the Advanced Micro Devices as a senior ASIC/layout designer, integrating sophisticated security/cryptographic capabilities into accelerated processing. In 2012, he joined the Electrical Engineering Department, Princeton University, New Jersey, as an NSERC post-doctoral research fellow. Currently, he serves as an associate editor for the *IEEE Transactions on VLSI Systems*, the *ACM Transactions on Embedded Computing Systems*, and the *IEEE Transactions on Circuits and Systems I*. He was the lead guest editor for the *IEEE/ACM Transactions on Computational Biology and Bioinformatics* and the *IEEE Transactions on Emerging Topics in Computing for special issues on security*. He was a recipient of the prestigious Natural Sciences and Engineering Research Council of Canada Post-Doctoral Research Fellowship in 2011 and the Texas Instruments Faculty Award (Douglas Harvey) in 2014. He is a senior member of the IEEE.

Reza Azarderakhsh received the PhD degree in electrical and computer engineering from Western University, London, ON, Canada. After that he was a postdoctoral research fellow at Center for Applied Cryptographic Research and the Department of Combinatorics and Optimization, University of Waterloo, Canada, while he was the recipient of NSERC PDF award. After that he was with the Department of Computer Engineering at Rochester Institute of Technology, Rochester, New York, as an assistant professor. He is currently an I-SENSE fellow at Florida Atlantic University, Boca Raton, Florida. His current research interests include finite field arithmetic and its application, elliptic curve cryptography, pairing based cryptography, and post-quantum cryptography. He is serving as an associate editor of the *IEEE Transactions on Circuits and Systems – Part I* (TCAS-I).

Manimaran Govindarasu received the master's in computer technology from Indian Institute of Technology (IIT) Delhi, in 1994 and the PhD degree in computer science and engineering from Indian Institute of Technology Madras, India in 1998. He is currently a professor in the Department of Electrical and Computer Engineering at Iowa State University. His research expertise is in the areas of cyber-physical security of smart grid, cyber security, real-time systems, and QoS/overlay networks. He has published more than 150 peer-reviewed research publications in international journals and conferences. He is co-author of the text "*Resource Management in Real-Time Systems and Networks*", MIT Press, 2001. He has given tutorials in reputed conferences, including IEEE Infocom 2004, IEEE ComSoc TutorialsNow (2004). IEEE ISGT 2012. He serves in the editorial board of IEEE Trans. on Smart Grid, served as guest co-editor for several journal special issues (the *IEEE Power & Energy* - Jan. 2012, the *IEEE Network*, the *Journal Systems and Software*, the *Journal of High Speed Networks*), and served as workshops/symposium chair, technical program vice-chair, and session chair for several IEEE conferences. He serves as the chair of the Cyber Security Task Force at IEEE PES PSACE-CAMS and Chair of CAMS Subcommittee. He is a fellow of the IEEE.