Guest Editorial: Introduction to the Special Section on Emerging Security Trends for Biomedical Computations, Devices, and Infrastructures

Mehran Mozaffari-Kermani, Reza Azarderakhsh, Kui Ren, and Jean-Luc Beuchat

Unlike the traditional usage models for embedded systems security, nowadays, emerging computing systems are embedded in every aspect of human lives. One of the emerging usage models in which security is vital is deeply-embedded computing systems in human bodies, e.g., implantable and wearable medical devices. In addition to the security threats to traditional embedded systems, emerging deeply-embedded computing systems exhibit a larger attack surface, prone to more serious or life-threatening attacks. Biomedical deeply-embedded systems (deployed in human body, with computer programs sending and receiving medical data and performing data mining for the decisions) are currently getting developed with rapid rate and tremendous success. Moreover, the security/privacy issues in every aspect of bioinformatics (algorithmic, statistical, and the like) including secure and private big data analytics, acquisition, and storage, privacy-preserving data mining for biomedicine, secure machine-learning of bioinformatics, and security of hardware and software systems used for biological databases are emerging given their unique constraints. Many of the systems for such computations will need to be transparently integrated into sensitive environments – the consequent size and energy constraints imposed on any security solutions are extreme. Thus, unique challenges arise due to the sensitivity of computation processing, need for security in implementations, and assurance "gaps."

This special section contains four papers chosen after an extensive review process. The first paper, "Emerging Security Mechanisms for Medical Cyber Physical Systems" by O. Kocabas, T. Soyata, and M.K. Aktas is motivated by the importance of Medical Cyber Physical Systems (MCPS) security. The paper depicts the general architecture of an MCPS consisting of four layers: data acquisition, data aggregation, cloud processing, and action. Due to the differences in hardware and communication capabilities of each layer, different encryption schemes are used to guarantee data privacy within that layer. Such emerging encryption schemes enable exciting new features such as secure sharing and secure computation, whose overhead need to be considered closely.

The second paper "Authentication of Medicines Using Nuclear Quadrupole Resonance Spectroscopy" by C. Chen, F. Zhang, J. Barras, K. Althoefer, S. Bhunia, and S. Mandal focuses on a chemometric passport-based approach to improve the security of the pharmaceutical supply chain. The method is based on applying nuclear quadrupole resonance (NQR) spectroscopy to authenticate the contents of medicine packets. The paper describes several advanced NQR techniques, including two-dimensional measurements, polarization enhancement, and spin density imaging, that further improve the security of the authentication approach.

The third paper "Private Data Analytics on Biomedical Sensing Data via Distributed Computation" by Y. Gong, Y. Fang, and Y. Guo proposes and experimentally studies a scheme that keeps the training samples private while enabling accurate construction of predictive models, considering logistic regression models which are widely used for predicting dichotomous outcomes in healthcare. Experimental results based on real datasets show that the scheme is highly efficient and scalable to a large number of mobile health users.

The fourth paper "Security Assessment of Cyberphysical Digital Microfluidic Biochips" by SK. Subidh Ali, M. Ibrahim, O. Sinanoglu, K. Chakrabarty, and R. Karri provides the first assessment of the security vulnerabilities of digital microfluidic biochips (DMFBs). Two practical result-manipulation attacks are shown on a DMFB platform performing enzymatic glucose assay on serum. Then, the authors identify denial-of-service attacks, where the attacker can disrupt the assay operation by tampering either with the droplet-routing algorithm or with the actuation sequence.

Finally, the guest editors would like to express their thanks to the authors of all submitted papers and the referees for their outstanding review in a timely manner. This special section would not have been possible without the support of Prof. Xu, *TCBB*'s editor-in-chief, who stood behind our effort on this special section. They would also like to thank Ms. Joyce Arnold, *TCBB*'s Peer Review Support Specialist, for her help throughout this project.

Mehran Mozaffari-Kermani
Reza Azarderakhsh
Kui Ren
Jean-Luc Beuchat
Guest Editors

- *M. Mozaffari-Kermani is with the Department of Electrical and Microelectronic Engineering, Rochester Institute of Technology, Rochester, NY 14623. E-mail: m.mozaffari@rit.edu.*
- *R. Azarderakhsh is with the Department of Computer Engineering, Rochester Institute of Technology, Rochester, NY 14623. E-mail: rxaeec@rit.edu.*
- *K. Ren is with the Department of Computer Science and Engineering, State University of New York at Buffalo (SUNY Buffalo), Buffalo, NY 14260. E-mail: kuiren@buffalo.edu.*
- *J.-L. Beuchat is with ELCA Informatique SA, Switzerland. E-mail: jeanluc.beuchat@gmail.com.*

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/TCBB.2016.2518874

Mehran Mozaffari-Kermani (M'11) 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, ON, Canada, in 2007 and 2011, respectively. He joined the Advanced Micro Devices, Markham, ON, Canada, as a senior ASIC/layout designer, integrating sophisticated security/cryptographic capabilities into a single accelerated processing unit. In 2012, he joined the Department of Electrical Engineering, Princeton University, Princeton, NJ, as a Natural Sciences and Engineering Research Council of Canada (NSERC) postdoctoral research fellow. He is currently with the Department of Electrical and Microelectronic Engineering, Rochester Institute of Technology (RIT), Rochester, NY. He has been recognized as the featured faculty member in research with the School of Engineering, RIT, in 2014. His current research interests include emerging security/privacy measures for deeply embedded systems, cryptographic hardware systems, and low-power secure and efficient FPGA and ASIC designs. He received the NSERC postdoctoral research fellowship in 2011 and the Texas Instruments Faculty Award (Douglas Harvey) in 2014. He currently serves as an associate editor for the *IEEE Transactions on Circuits and Systems I, the IEEE Transactions on VLSI Systems,* and the *ACM Transactions on Embedded Computing Systems*. He also serves as the guest editor for the *IEEE Transactions on Dependable and Secure Computing* for the special issue on Emerging Embedded and Cyber Physical System Security Challenges and Innovations. He has served as the lead guest editor for the *IEEE Transactions on Emerging Topics in Computing* for the Special Issue on Emerging Security Trends for Deeply-Embedded Computing Systems in 2014 and 2015. He is a member of the IEEE.

Reza Azarderakhsh received the BSc degree in electrical and electronic engineering and the MSc degree in computer engineering from the Sharif University of Technology, Tehran, Iran, in 2002 and 2005, respectively, and the PhD degree in electrical and computer engineering from the University of Western Ontario, London, Canada, in 2011. He joined the Department of Electrical and Computer Engineering, University of Western Ontario, Canada, as a limited duties instructor, in September 2011. He has been an NSERC postdoctoral research fellow with the Center for Applied Cryptographic Research and the Department of Combinatorics and Optimization, University of Waterloo, Waterloo, ON, Canada. He is currently with the Department of Computer Engineering, Rochester Institute of Technology, Rochester, NY. His current research interests include finite field and its application, elliptic curve cryptography, and pairing-based cryptography. He received the prestigious Natural Sciences and Engineering Research Council of Canada (NSERC) Postdoctoral Research Fellowship in 2012. He currently serves as an associate editor for the *IEEE Transactions on Circuits and Systems I.* He also serves as the guest editor for the *IEEE Transactions on Dependable and Secure Computing* for the special issue on Emerging Embedded and Cyber Physical System Security Challenges and Innovations. He is a member of the IEEE.

Kui Ren received the PhD degree from Worcester Polytechnic Institute. He is an associate professor of computer science and engineering and the director in the Ubiquitous Security and Privacy Research Lab at State University of New York at Buffalo. His current research interest spans cloud & outsourcing security, wireless & wearable system security, and human-centered computing. His research has been supported by the US National Science Foundation (NSF), DoE, AFRL, MSR, and Amazon. He received the NSF CAREER Award in 2011, Sigma Xi/IIT Research Excellence Award in 2012, and UB SEAS senior researcher of the year in 2015. He has published 150 peer-reviewed journal and conference papers and received several Best Paper Awards including IEEE ICNP 2011. He currently serves/has served as an associate editor for the *IEEE Transactions on Mobile Computing*, *IEEE Transactions on Dependable and Secure Computing*, *IEEE Transactions on Information Forensics and Security*, *IEEE Wireless Communications*, *IEEE Internet of Things Journal*, *IEEE Transactions on Smart Grid*, and *Oxford The Computer Journal*. He is a fellow of the IEEE, a member of the ACM, a distinguished lecturer of the IEEE Vehicular Technology Society, and a past board member of Internet Privacy Task Force, State of Illinois.

Jean-Luc Beuchat received the MSc and PhD degrees in computer science from the Swiss Federal Institute of Technology, Lausanne, in 1997 and 2001, respectively. Before joining ELCA Informatique SA as a security expert, he was an associate professor in the Graduate School of Systems and Information Engineering, University of Tsukuba, Japan. His research interests are in the areas of cryptography, cybersecurity, computer arithmetic, and computer architecture. His work has been recognized with two best paper awards at CHES, the world's foremost conference in cryptographic hardware. He currently serves as an associate editor for the *IEEE Transactions on Computers*. He is a member of the IACR.