Guest Editorial: Hardware/Software Cross-Layer Technologies for Trustworthy and Secure Computing

Shiyan Hu, *Senior Member, IEEE*, Yier Jin, *Member, IEEE*, Kenneth Heffner, and
Mark Tehranipoor, *Senior Member, IEEE*

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 the 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 complicate the problem of trusted system design and verification. Although 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.

Given the goal mentioned above, the special issue documents some recent progress in this emerging but challenging area. We note that the area is vast, covering a large scope of subjects ranging from embedded systems to modern computing systems. A full analysis to the entire research spectrum is far beyond the scope of a single special issue. Therefore, our goal is to provide a sampling of different topics in this emerging domain, highlight the diversity of research topics, and capture some research trends. With that goal in mind, this special issue provides six representative articles covering a wide range of topics encompassing new practices, challenges, and approaches towards cross-layer technologies for trustworthy and secure computing.

The first three articles provide a practical view on how hardware can play an active role in supporting cybersecurity. “A Lockdown Technique to Prevent Machine Learning on PUFs for Lightweight Authentication” by Meng-Day Yu, Matthias Hiller, Jeroen Delvaux, Richard Sowell, Srinivas Devadas, and Ingrid Verbauwhede presents a lightweight PUF-based authentication approach where the number of authentications is limited over a device’s lifetime. The second paper titled “Malicious Firmware Detection with Hardware Performance Counters” by Xueyang Wang, Charalambos Konstantinou, Michail Maniatakos, Ramesh Karri, Serena Lee, Patricia Robison, Paul Stergiou, and Steve Kim proposes a low-cost technique to detect firmware-level malicious modifications by measuring the number of low-level hardware events through hardware performance counters. In the third paper titled “Systemic Frequency Biases in Ring Oscillator PUFs on FPGAs”, Linus Feiten, Jonathan Oesterle, Tobias Martin, Matthias Sauer, and Bernd Becker suggest a method to overcome systemic ring oscillator (RO) frequency biases by predicting the average bias over FPGA devices. As a result, the generated PUF signatures will be more reliable, facilitating for high level applications.

The later two articles discuss how cross-layer solutions can help enhance the security and resiliency of hardware designs. The paper “Design and Validation for FPGA Trust under Hardware Trojan Attacks” by Sanchita Mal-Sarkar, Robert Karam, Seetharam Narasimhan, Anandaroop Ghosh, Aswin Krishna, and Swarup Bhunia presents a taxonomy of FPGA-specific hardware Trojan attacks based on activation and payload characteristics. A design method, called Adapted Triple Modular Redundancy (ATMR) is proposed to protect hardware Trojan insertions in FPGA devices. The article “A Game-Theoretic Approach for Testing for Hardware Trojans” by Charles A. Kamhoua, Hong Zhao, Manuel Rodriguez, and Kevin A. Kwiat develops a game-theory based approach for digital circuit testing by considering the decision-making process of attackers who may want to insert hardware Trojans in target designs.

Finally, this special issue also includes one paper introducing an emerging area that hardware-level vulnerability would lead to software breaches. The paper titled “Cross-VM Cache Attacks on AES” by Berk Gulmezoglu, Mehmet Sinan Inci, Gorka Irazoqui, Thomas Eisenbarth, and Berk Sunar applies cache side-channel attacks on a popular

- *S. Hu is with the Department of Electrical and Computer Engineering, Michigan Technological University, Houghton, MI 49931.
E-mail: shiyan@mtu.edu.*
- *Y. Jin is with the Department of Electrical and Computer Engineering, University of Central Florida, Orlando, FL 32816.
E-mail: yier.jin@eecs.ucf.edu.*
- *K. Heffner is with Honeywell, Phoenix, AZ 85034.
E-mail: kenneth.h.heffner@honeywell.com.*
- *M. Tehranipoor is with the Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL 32611.
E-mail: tehranipoor@ece.ufl.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/TMSCS.2016.2609298*

OpenSSL implementation of AES, suggesting a practical threat to public clouds.

The emerging area of hardware/software cross-layer technologies will enhance the security of modern computing systems and, at the same time, impose new threats to these systems. Developing a full set of all possible cross-layer technologies remains as an open goal. However, the area is vast, the challenges are real, and the benefits are significant. We hope that these six articles provide a high-level overview to the emerging topic and they will spur innovative ideas in this area to further secure our computing systems under various cyber attacks.

ACKNOWLEDGMENTS

This special issue resulted from the inputs and efforts of many individuals to whom we are thankful. The guest editors received several high quality articles, which were further strengthened through detailed comments and suggestions from a host of reviewers. They are grateful for their time and commitment. They thank the *IEEE Transactions on Multi-Scale Computing Systems* editor-in-chief Partha Pande for his continued support throughout this process. Finally, the editorial staff of the IEEE Computer Society deserves special thanks for their wonderful job in editing and organizing this issue.

Shiyan Hu
Yier Jin
Kenneth Heffner
Mark Tehranipoor
Guest Editors

Shiyan Hu received the PhD degree in computer engineering from Texas A&M University, in 2008. He is an associate professor with Michigan Technological University where he is a director of the Center for Cyber-Physical Systems and an associate director of the Institute of Computer and Cybersystems. He was a visiting professor with IBM Research, Austin, in 2010, and a visiting associate professor with Stanford University from 2015 to 2016. His research interests include cyber-physical systems, cybersecurity, computer-aided design of VLSI circuits, and embedded systems, where he has published more than 100 refereed papers. He is an ACM distinguished speaker, an IEEE Computer Society distinguished visitor, an invited participant for US National Academy of Engineering Frontiers of Engineering Symposium, a recipient of a National Science Foundation (NSF) CAREER Award, a recipient of the ACM SIGDA Richard Newton DAC Scholarship (as the faculty advisor), and a recipient of the JSPS Faculty Invitation Fellowship. He is the chair of the IEEE Technical Committee on Cyber-Physical Systems. He serves as an associate editor of the *IEEE Transactions on Computer-Aided Design*, the *IEEE Transactions on Industrial Informatics*, and the *IEEE Transactions on Circuits and Systems*. He is also a guest editor of seven IEEE/ACM Transactions such as the *IEEE Transactions on Computers* and the *IEEE Transactions on Computer-Aided Design*. He has served as a conference chair, track chair, and TPC member more than 70 times. He is a senior member of the IEEE.

Yier Jin received the BS and MS degrees in electrical engineering from Zhejiang University, China, in 2005 and 2007, respectively, and the PhD degree in electrical engineering from Yale University, in 2012. He is currently an assistant professor in the EECS Department, University of Central Florida. His research focuses on the areas of trusted embedded systems, trusted hardware intellectual property (IP) cores, and hardware-software co-protection on computer systems. He proposed various approaches in the area of hardware security, including the hardware Trojan detection methodology relying on local side-channel information, the post-deployment hardware trust assessment framework, and the proof-carrying hardware IP protection scheme. He is also interested in the security analysis on Internet of Things (IoT) and wearable devices with particular emphasis on information integrity and privacy protection in the IoT era. He was awarded the DoE Early CAREER Award in 2016 and is the best paper award recipient of DAC'15 and ASP-DAC'16. He is a member of the IEEE.

Kenneth Heffner received the PhD degree in chemistry from the University of South Florida, Tampa, Florida. He is currently an engineering fellow of Honeywell Aerospace, Clearwater, Florida, supporting Honeywell's Aerospace business units. He is the technology leader for Honeywell's new Systems Security Engineering business unit. His research includes sensors for inertial navigation systems, autonomous thin film instrumental analysis, high-density vertically-integrated microsystems, high-performance computing, and embedded secure microelectronics systems. He holds 16 US patents. He is also a certified Design for Six Sigma Black Belt for hardware design.

Mark Tehranipoor (S'02-M'04-SM'07) received the PhD degree from the University of Texas at Dallas, in 2004. He is currently the Intel Charles E. Young Preeminence Endowed professor in Cybersecurity, University of Florida. His current research projects include hardware security and trust, supply chain security, VLSI design, and test and reliability. He has published more than 300 journal articles and refereed conference papers and has given more than 150 invited talks and keynote addresses. He has published six books and 11 book chapters. He received several best paper awards as well as the 2008 IEEE Computer Society (CS) Meritorious Service Award, the 2012 IEEE CS Outstanding Contribution, the 2009 NSF CAREER Award, and the 2014 MURI award. He serves on the program committee of more than a dozen leading conferences and workshops. He served as program chair of the 2007 IEEE Defect-Based Testing (DBT) workshop, program chair of the 2008 IEEE Defect and Data Driven Testing (D3T) workshop, co-program chair of the 2008 International Symposium on Defect and Fault Tolerance in VLSI Systems (DFTS), general chair of D3T-2009 and DFTS-2009, and vice-general chair of NATW-2011. He co-founded the IEEE International Symposium on Hardware-Oriented Security and Trust (HOST) and served as HOST-2008 and HOST-2009 general chair. He is currently serving as an associate editor for the *Journal of Electronic Testing: Theory and Applications*, the *Journal of Low Power Electronics*, the *IEEE Transactions on Very Large Scale Integration Systems,* and the *ACM Transactions on Design Automation of Electronic Systems*. Prior to joining UF, he served as the founding director of CHASE and CSI centers, University of Connecticut. He is currently serving as co-director of the Florida Institute for Cybersecurity Research. He is a senior member of the IEEE, a Golden Core member of the IEEE, and a member of the ACM and the ACM SIGDA.