Guest Editorial: Special Section on Embedded System Security

EMBEDDED computing systems are continuously adopted in a wide range of application areas. These systems are responsible for a large number of safety and security-critical applications as well as for the management of critical information. The advent of the Internet of Things introduces a large number of security issues: the Internet can be used to attack embedded systems and embedded systems can be used to attack the Internet. Furthermore, embedded systems are vulnerable to many attacks not relevant to servers because they are physically accessible. Cyber-physical systems create new classes of risks resulting from their interaction between cyberspace and the physical world. Inadvertent threats due to bugs, improper system use, etc. can also have effects that are indistinguishable from malicious attacks.

This Special Section addresses embedded systems security and, particularly, security topics that are unique to embedded systems.

The letter, *Design and Operation of Secure Cyber-Physical Systems*, addresses the problem of design and operation of cyber-physical systems in a reliable and secure fashion under the constraint of limited resources. The authors describe a framework that enables one to design cyber-physical systems taking into account both the operational requirements at the process level and the security requirements of the communication infrastructure of the systems, which may come under attack. This holistic approach enables the development of related cyber-physical systems through analysis of tradeoffs among process performance, system security and scheduling in systems with limited resources.

The letter, *NoC-Based Protection for SoC Time-Driven Attacks*, addresses time-driven attacks in Systems-on-Chips, where attackers use timing information leaked through cache misses to extract secret data. As cache misses are routed through the Network-on-Chip, the authors propose the use of random arbitration and adaptive routing at Network-on-Chip routers, in order to overcome such attacks while avoiding introduction of additional attacks, such as denial-of-service.

Automotive embedded systems have a strong need for security while featuring tight constraints on system performance and cost. The letter, *Security-Aware Modeling and Efficient Mapping for CAN-Based Real-Time Distributed Automotive Systems*, proposes a method to define path-based security constraints that minimizes security risk directly, together with a heuristic algorithm to find efficient solutions to the problem statement. Experiments on an industrial automotive CAN-based system show that the proposed approach achieves comparable solution quality as previously proposed MILP-based approach at better efficiency.

Acknowledgment

The Guest Editors would like to thank the reviewers for their careful evaluation and insightful comments, which contributed in a significant way to the quality of these letters.

Thomas Eisenbarth, *Guest Editor*
Worcester Polytechnic Institute
Department of Electrical and Computer Engineering
Worcester, MA 01602 USA
E-mail: teisenbarth@wpi.edu

Yunsi Fei, *Guest Editor*
Northeastern University
Department of Electrical and Computer Engineering
Boston, MA 02115 USA
E-mail: yfei@ece.neu.edu

Dimitrios Serpanos, *Guest Editor*
Qatar Computing Research Institute
Doha, Qatar
E-mail: dserpanos@qcri.org.qa

Digital Object Identifier 10.1109/LES.2015.2404940

Thomas Eisenbarth received the doctoral degree from Ruhr-Universität Bochum, Bochum, Germany, where he worked as a Member of the Horst Goertz Institute for IT Security.

He is currently an Assistant Professor at the Department of Electrical and Computer Engineering at WPI. His research interests are in applied cryptography and physical attacks. Before joining WPI, he spent two years at the Center for Cryptology and Information Security (CCIS) at Florida Atlantic University.

Yunsi Fei (M’04) received the B.S. and M.S. degrees in electronic engineering from Tsinghua University, Beijing, China, in 1997 and 1999, respectively, and the Ph.D. degree in electrical engineering from Princeton University, Princeton, NJ, USA, in 2004.

She was a Faculty Member at University of Connecticut until September 2011, when she joined the faculty of Northeastern University. She is currently an Associate Professor of the Electrical and Computer Engineering Department at Northeastern University. Her research interests include hardware-oriented security and trust, side-channel attacks analysis and countermeasures, energy-efficient embedded system design, and optimization, computer architecture, and adaptive networking for underwater sensor networks, etc. Her research has been primarily supported by NSF and ONR.

Dr. Fei currently serves as an Associate Editor for the *ACM Transaction on Embedded Computing Systems*, the IEEE EMBEDDED SYSTEM LETTER, and the *Journal of Low Power Electronics*. She was a recipient of NSF CAREER Award.

Dimitrios Serpanos received the Ph.D. degree in computer science from Princeton University, Princeton, NJ, USA, in 1990, and the Dipl. degree in computer engineering from the University of Patras, Panepistimioupoli , Greece, in 1985.

His research interests include architecture of embedded computing systems, cybersecurity, industrial control systems, and parallel and distributed systems. He has published extensively in books, journals, and conferences, and holds two U.S. patents and six inventions.

Dr. Serpanos has served as an Associate Editor of *ACM TECS*, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, and the *Journal of Internet Engineering*, as well as General Chair and TPC Chair in several conferences and workshops. He is a Member of ACM and NYAS.