Digital Object Identifier 10.1109/TETC.2015.2482778

Guest Editorial: Introduction to the Special Issue on Emerging Security Trends for Deeply-Embedded Computing Systems

UNLIKE traditional embedded systems, nowadays, emerging computing systems are embedded in every aspect of human lives. These deeply-embedded computing systems often perform extremely sensitive tasks, and in some cases, such as health-care IT, these are life-saving. Thus, 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 malicious attacks. These call for revisiting traditional security mechanisms not only because of the new facets of threats and more adverse effects of breaches, but also due to the resource limitations of these often-battery-powered and extremely-constrained computing systems. As such, new trends for providing security for deeply embedded systems are emerging; many of which abandoning use of cryptographic computations or making use of lightweight crypto-systems, feasible for these computing platforms. Indeed, there exists paramount potential for applying these emerging security approaches to sensitive applications such as health-care IT for implantable medical devices, big data analytics and machine learning in deeply embedded systems, smart buildings, and smart fabrics.

This special issue contains five papers chosen after an extensive review process from 25 submitted manuscripts. The accepted papers cover different critical security domains including advances in health information security, emerging reliable key generation, privacy protection of surveillance videos, side-channel attacks and countermeasures, and emerging social network security.

The first paper, ''Physiological information leakage: a new frontier in health information security'' by A. Mohsen-Nia, S. Sur-Kolay, A. Raghunathan, and N. Jha is motivated by the importance of information security in healthcare systems, owing to the increasing prevalence of medical devices and the growing use of wearable and mobile computing platforms for health and lifestyle monitoring. Compared to the previous work in the area of health information security, which focuses on attacks on the wireless communication channel of medical devices, or on health data stored in online databases, in this paper, the authors pursue an entirely different angle to health information security, motivated by the insight that the human body itself is a rich source (acoustic, visual, and electromagnetic) of data. The authors propose a new class of information security attacks that exploit physiological information leakage - various forms of information that naturally leak from the human body - to compromise privacy. As an example, they demonstrate attacks that exploit acoustic leakage from the heart and lungs. Next, the medical devices deployed within or on bodies also add to natural sources of physiological information leakage, thereby increasing opportunities for attackers. Unlike previous attacks on medical devices, which target the wireless communication to/from them, this work proposes privacy attacks that exploit information leaked by the very operation of these devices.

The next work ''An aging-resistant RO-PUF for reliable key generation'' by M. T. Rahman, F. Rahman, D. Forte, and M. Tehranipoor in on emerging improvements in Physically Unclonable Functions (PUFs) for aging-resistance. PUFs have emerged as a promising security primitive for low-cost authentication and cryptographic key generation. However, PUF stability with respect to temporal variations still limits its utility and widespread acceptance. Compared to this paper, previous techniques in the literature have focused on improving PUF robustness against voltage and temperature variations, but the issues associated with aging have been largely neglected. In this paper, the authors address aging in the popular ring oscillator (RO)-PUF. Their simulation results demonstrate that the aging-resistant RO-PUF (ARO-PUF) can produce unique, random, and more reliable keys. On average, only 3.8% bits of an ARO-PUF flip over a 10-year operational period because of aging, compared to 12.8% bit flip for a conventional RO-PUF. The proposed ARO-PUF eliminates the need for error correction by adding extra ROs. The result shows RO-PUF saves $\sim 32\times$ area overhead compared to a conventional RO-PUF with required error correction schemes for a reliable key.

The third paper ''Lossless ROI privacy protection of H.264/AVC compressed surveillance videos'' by L. T. Yang, X. Ma, W. Zeng, D. Zou, and H. Jin focuses on privacy of video surveillance systems especially in cloud-based systems. Region-of-Interest (ROI) privacy protection is more practical compared to the whole video encryption approaches. However, one common drawback of virtually all current ROI privacy protection methods is that the original compressed surveillance video recorded in the camera is permanently distorted by the privacy protection process, due to the quantization in the re-encoding process. Thus the integrity of the original compressed surveillance video captured by the camera is destroyed. This is unacceptable for some application scenarios such as video forensics for investigations and video authentication for law enforcement. In this paper,

the authors introduce a new paradigm for privacy protection in surveillance videos, referred to as lossless privacy region protection, which has the property that the distortion introduced by the protection of the privacy data can be completely removed from the protected videos by authorized users. They eventually demonstrate the concept of lossless privacy region protection through a proposed scheme applied on H.264/AVC compressed videos.

The next paper ''Can algorithm diversity in stream cipher implementation thwart (natural and) malicious faults?'' by X. Guo, C. Jin, C. Zhang, Chi, A. Papadimitriou, D. Hely, and R. Karri is motivated by the vulnerability of hardware implementations of stream and other ciphers to natural and malicious faults. Moreover, attackers can launch fault attacks on these implementations. Concurrent error detection (CED) is used as a countermeasure against natural and malicious faults. The authors propose algorithm diversity (AD) to detect natural and malicious faults in stream ciphers and compare AD to hardware, time, and information redundancies. Hardware redundancy has 100% hardware overhead, but is not secure against fault attacks. Time redundancy has lower hardware overhead, but is vulnerable to faults that are injected in both the computation and recomputation. Information redundancy techniques such as parity cannot detect an even number of faulty bits. Information redundancy techniques such as robust code has higher fault miss rate (FMR) with higher hardware overhead. If robust code is configured to have lower FMR than AD in certain attacker model, the hardware overhead is excessively high. Grain, Trivium, and Achterbahn have been assessed and it is concluded that one can apply AD to parallel stream cipher implementations and combine AD with implementation diversity.

The final paper ''Data protection for online social networks and P-stability for graphs'' by V. Torra and T. Shafie is motivated by the fact that graphs can be used as a model for online social networks. In this framework, vertices represent individuals and edges relationships between individuals. In recent years, different approaches have been considered to offer data privacy to online social networks and for developing graph protection. Perturbative approaches are formally defined in terms of perturbation and modification of graphs. In this paper, the authors discuss the concept of P-stability on graphs and its relation to data privacy. The concept of P-stability is rooted in the number of graphs given a fixed degree sequence. In this paper, they also show that for any graph there exists a class of P-stable graphs. This result implies that there is a fully polynomial randomized approximation for graph masking for the graphs in the class. In order to further refine the classification of a given graph, the authors introduce the concept of natural class of a graph which is based on a class of scale-free networks.

Finally, we would like to express our thanks to the authors of all submitted papers and the referees for their outstanding review in a timely manner. This special issue would not have been possible without the support of Prof. Fabrizio Lombardi, the IEEE TETC Editor-in-Chief who stood behind our effort on this special issue on emerging security trends for deeply-embedded computing systems. We would also like to thank Ms. Alexandra Titta of the IEEE TETC for her help throughout this project.

MEHRAN MOZAFFARI KERMANI, *Guest Editor*
Rochester Institute of Technology

ERKAY SAVAS, *Guest Editor*
Sabancl University

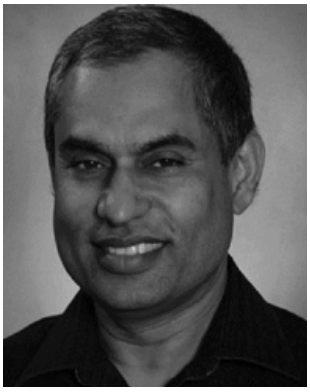
SHAMBHU J. UPADHYAYA, *Guest Editor*
State University of New York at Buffalo

MEHRAN MOZAFFARI-KERMANI (M'11) received the B.Sc. degree in electrical and computer engineering from the University of Tehran, Tehran, Iran, in 2005, and the M.E.Sc. and Ph.D. degrees from the Department of Electrical and Computer Engineering, University of Western Ontario, London, ON, Canada, in 2007 and 2011, respectively.

He joined 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, USA, as a Natural Sciences and Engineering Research Council of Canada (NSERC) Post-Doctoral Research Fellow. He was recognized as the Featured Faculty Member in research with the School of Engineering, Rochester Institute of Technology, Rochester, NY, USA, in 2014, where he is currently with the Department of Electrical and Microelectronic Engineering. 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.

Dr. Mozaffari-Kermani was a recipient of the NSERC Post-Doctoral Research Fellowship in 2011 and the Texas Instruments Faculty Award (Douglas Harvey) in 2014. He serves as an Associate Editor of the IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS I and the *ACM Transactions on Embedded Computing Systems*. He also serves as the Guest Editor of the IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING for the Special Issue of Emerging Embedded and Cyber Physical System Security Challenges and Innovations and the IEEE TRANSACTIONS ON COMPUTATIONAL BIOLOGY AND BIOINFORMATICS for the Special Issue of Emerging Security Trends for Biomedical Computations, Devices, and Infrastructures. He served as the Lead Guest Editor of the IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTING for the Special Issue of Emerging Security Trends for Deeply-Embedded Computing Systems in 2014 and 2015.

ERKAY SAVAS (M'00) received the B.S. and M.S. degrees in electrical engineering from the Electronics and Communications Engineering Department, Istanbul Technical University, in 1990 and 1994, respectively, and the Ph.D. degree from the Department of Electrical and Computer Engineering, Oregon State University, in 2000. He had worked for various companies and research institutions before he joined Sabanci University in 2002. His research interests include applied cryptography, data and communication security, privacy in biometrics, security and privacy in data mining applications, embedded systems security, and distributed systems. He is a member of ACM, the IEEE Computer Society, and the International Association of Cryptologic Research. He is an Associate Editor of the IEEE TRANSACTIONS ON COMPUTERS and the *Journal of Cryptographic Engineering*.



SHAMBHU J. UPADHYAYA has held visiting research faculty positions with the Center for Reliable and High Performance Computing, University of Illinois at Urbana–Champaign, Intel Corporation, Folsom, CA, the Air Force Research Laboratory, Rome, NY, and the Naval Research Laboratory, Washington, DC. His research has been supported by the National Science Foundation, the Rome Laboratory, the U.S. Air Force Office of Scientific Research, DARPA, the National Security Agency, IBM, Intel Corporation, and Harris Corporation. He is currently a Professor of Computer Science and Engineering with the State University of New York at Buffalo, where he also directs the Center of Excellence in Information Systems Assurance Research and Education, designated by the National Security Agency. He has authored or co-authored over 250 articles in refereed journals and conferences in his research areas. His research interests are information assurance, computer security, fault diagnosis, fault tolerant computing, and VLSI testing. He received the IBM Faculty Partnership Fellowship and the NRC Faculty Fellowships. He was an Associate Editor of the IEEE TRANSACTIONS ON COMPUTERS from 2001 to 2006, and is a member of the Editorial Board of the *International Journal on Reliability, Quality, and Safety Engineering* (World Scientific Publishers) and the *ICST Transactions on Security and Safety*. He was a Guest Co-Editor of the Special Issue on Secure Knowledge Management of the IEEE TRANSACTIONS ON SYSTEMS, MAN AND CYBERNETICS in 2006, and a Co-Editor of the book entitled *Annals of Emerging Research in Information Assurance, Security and Privacy Services* (Elsevier, 2009).