Athina Petropulu, Konstantinos I. Diamantaras,
Zhu Han, Dusit (Tao) Niyato, and Saman Zonouz

Contactless Monitoring of Critical Infrastructure

Industrial control systems (ICSs) manage and monitor critical civil or military infrastructure, such as water treatment facilities, power plants, electricity grids, transportation systems, oil and gas refineries, and health care. Because they are so important, ICSs are becoming attractive targets for malicious attacks that could lead to catastrophic failures with substantive impacts. Among such attacks was the BlackEnergy worm [1], which was used in 2015 against the Ukrainian electricity grid, resulting in widespread power outages, and the Stuxnet malware [2], which was used in 2010 and physically damaged 20% of the Iranian centrifuges controlled by programmable logic controllers (PLCs). New security concerns arise as the public adopts Internet of Things (IoT) devices, resulting in household electronics becoming computers that can be targets for malware. Over the last few years, Internet-connected appliances, home routers, webcams, and printers were used to launch distributed denial-of-service (DDoS) attacks, often without their owners' knowledge. The largest DDoS attack to target IoT devices was in 2016, when a botnet malware family named *Mirai* was launched [3]. IoT devices are attractive targets for malware because they lack cryptographic encryption and strong default authentication.

One important type of ICS attack occurs without physical contact by using side-channel information such as electromagnetic emanations, power dissipation, sound, and temperature. Typically, side-channel attacks (SCAs) attempt to perform cryptanalysis based on the time-series processing of side-channel signals by using statistical or machine-learning methods. Since SCAs can pose a serious authentication threat, both the academic community and industry have recently recognized the importance of side-channel analysis. Side-channel signals can also be used for attack detection, by recognizing anomalous execution of code running on a device.

Because they are so important, ICSs are becoming attractive targets for malicious attacks that could lead to catastrophic failures with substantive impacts.

This special issue of *IEEE Signal Processing Magazine* includes three articles on the emerging area of protecting embedded devices by monitoring code execution information that leaks through side channels. Specifically, the articles review the basics of extracting and processing side-channel signals, fingerprinting normal code operation during an initial phase, and detecting anomalies in those signals introduced by malware during runtime.

In the first article, "Side-Channel-Based Code-Execution Monitoring Systems," Han et al. provide a comprehensive discussion of using side-channel analysis to detect anomalies in embedded devices, such as PLCs and the IoT, during code execution. The anomalies occur when malware infects the device. In this article, the main steps of constructing an execution monitoring system, namely, profiling and deployment, are discussed in detail. During profiling, the program to be monitored is first analyzed and its structure is extracted. Then, side-channel signals that are correlated to that structure are collected, preprocessed, and a profiling model is established. During the deployment phase, the model is used to monitor the execution and/or report unknown code execution based on the real-time side-channel signals. The article provides the basic background on program analysis and on signal modeling tools such as the hidden Markov model, machine learning, and principal component analysis. Experimental results on electromagnetic emanation and power consumption side-channel signals are presented, where the hidden Markov model and recurrent neural networks are used for profiling. It also provides a literature review of modeling approaches and discusses strengths and limitations.

In "Protecting Water Infrastructure From Cyber and Physical Threats," Bakalos et al. study problems related to both physical attacks and cyberattacks on water infrastructure. A new attack-detection framework is introduced that is based on multimodal data fusion and adaptive

Digital Object Identifier 10.1109/MSP.2018.2890357
Date of publication: 26 February 2019

deep learning. In particular, fusion of data such as visual surveillance, channel state information from Wi-Fi signals for detecting a human presence, and ICS sensor data are considered. The authors show that the proposed approach is able to adapt and respond to the dynamic characteristics of sophisticated attackers. An evaluation is conducted using a data set from an actual water infrastructure environment, which consists of red, green, blue, and thermal camera streams; data from Wi-Fi reflectance-based detection; and ICS data.

In "A New Way to Detect Cyberattacks," Riley et al. leverage the analog side channels in IoT processors to detect intrusions. The goal is to defend against cyberattacks by detecting deviations in the code running on their processors from known firmware based on radio-frequency (RF) emissions produced during code execution. The article describes the process of positioning a wide-bandwidth RF probe over the processor of the device under test (DuT) and then implementing classifiers to identify the code running on the device and detect, identify, and isolate register contents based on signatures learned during DuT characterization. The proposed techniques enable reduction in feature dimensions, which improves the speed and accuracy of detecting differences due to intrusions.

In general, detecting runtime software execution changes as compared to firmware based on side-channel signals is a challenging problem due to several reasons. In addition to noise and interference, differences in input data cause the firmware to execute different sequences of code blocks, and detecting deviations requires knowledge of the control flow structure. Pipelining of instructions, implemented to increase instruction throughput also affects the runtime side-channel signals. Another challenge is introduced by out-of-order execution, which is an approach used in high-performance microprocessors, via which the processor executes the instructions in an order of availability of data or operands instead of original order of the instructions in the program. By doing so the processor avoids being idle while data is retrieved for the next instruction in the program. The signal processing community is uniquely qualified to address such a challenging detection problem.

In summary, this special issue provides material that highlights the important issues and challenges in the emerging area of contactless monitoring of critical infrastructure. The editors hope the issue will generate interest among the signal processing community for further research in addressing those challenges.

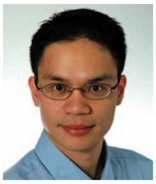
Meet the guest editors

Athina Petropulu (athinap@rutgers.edu) received her undergraduate degree from the National Technical University of Athens, Greece, and her M.Sc. and Ph.D. degrees in electrical and computer engineering from Northeastern University, Boston, Massachusetts, in 1988 and 1991, respectively, She is a distinguished professor in the Electrical and Computer Engineering Department at Rutgers University, New Brunswick, New Jersey. She is a Fellow of the IEEE and the American Association for the Advancement of Science and is currently a member-at-large of the IEEE Signal Processing Board of Governors. She is the recipient of the 2005 IEEE Signal Processing Magazine Best Paper Award and the 2012 IEEE Signal Processing Society Meritorious Service Award for "exemplary service in technical leadership capacities." She was an IEEE Distinguished Lecturer for the IEEE Signal Processing Society for 2017–2018. Her research interests include statistical signal processing, wireless communications, signal processing in networking, physical layer security, and radar signal processing.

Konstantinos I. Diamantaras (kdiamant@it.teithe.gr) received his diploma degree from the National Technical University of Athens, Greece, and his Ph.D. degree in electrical engineering from Princeton University, New Jersey, in 1992. Since 1998, he has been with the Department of Information Technology, Technological Educational Institute of Thessaloniki, Greece, where he is currently a professor. He is the recipient of the 1996 IEEE Signal Processing Society Best Paper Award, and he has been the chair of the Machine Learning for Signal Processing (MLSP) Technical Committee (TC) of the IEEE Signal Processing Society as well as a member of the MLSP and Signal Processing Theory and Methods TCs. He has been an associate editor of *IEEE Transactions on Signal Processing*, *IEEE Signal Processing Letters*, and *IEEE Transactions on Neural Networks*. He is currently an associate editor of *Journal of Signal Processing Systems*.

Zhu Han (zhan2@uh.edu) received his B.S. degree in electronic engineering from Tsinghua University, Beijing, China, in 1997, and his M.S. and Ph.D. degrees in electrical and computer engineering from the University of Maryland, College Park, in 1999 and 2003, respectively. From 2000 to 2002, he was an R&D engineer of JDSU, Germantown, Maryland. From 2003 to 2006, he was a research associate at the University of Maryland. From 2006 to 2008, he was an assistant professor at Boise State University, Idaho. Currently, he is a John and Rebecca Moores Professor in the Electrical and Computer Engineering Department as well as in the Computer Science Department at the University of Houston, Texas. His research interests include wireless resource allocation and management, wireless communications and networking, game theory, big data analysis, security, and smart grid. He received a National Science Foundation Career Award in 2010, the Fred W. Ellersick Prize of the IEEE Communication Society in 2011, the EURASIP Best Paper Award for *Journal on Advances in Signal Processing* in 2015, the IEEE

Leonard G. Abraham Prize in the field of Communications Systems (Best Paper Award in *IEEE Journal on Selected Areas in Communications*) in 2016, and several best paper awards in IEEE conferences. Currently, he is an IEEE Communications Society Distinguished Lecturer. He is a Fellow of the IEEE.



Dusit (Tao) Niyato (dniyato@ntu.edu.sg) received his B.Eng. degree from King Mongkuts Institute of Technology Ladkrabang, Thailand, in 1999 and his Ph.D. degree in electrical and computer engineering from the University of Manitoba, Canada, in 2008. He is currently a professor in the School of Computer Science and Engineering at Nanyang Technological University, Singapore. His research interests are in the area of energy harvesting for wireless communication, Internet of Things, and sensor networks. He is a Fellow of the IEEE.

Saman Zonouz (saman.zonouz@rutgers.edu) received his B.Sc. degree in computer engineering from the Sharif University of Technology, Tehran, Iran, and his Ph.D. degree in computer science, specifically, intrusion resilience architectures for the cyberphysical infrastructures, from the University of Illinois at Urbana–Champaign in 2006 and 2011, respectively. He is an associate professor in the Electrical and Computer Engineering Department at Rutgers University, New Brunswick, New Jersey, and the director of the 4N6 Cyber Security and Forensics Laboratory. He serves on the editorial board of *IEEE Transactions on Smart Grid* and was invited to cochair the National Science Foundation's CPS Principal Investigators Meeting in 2017.

References

[1] J. Nazario. (2007). BlackEnergy DDoS bot analysis. Arbor Networks. Burlington, MA. [Online]. Available: http://atlas-public.ec2.arbor.net/docs/BlackEnergy+DDoS+Bot+Analysis.pdf

[2] J. P. Farwell and R. Rohozinski, "Stuxnet and the future of cyber war," *Survival*, pp. 23–40, 2011.

[3] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," *Comput.*, vol. 50, no. 7, pp. 80–84, 2017.