Guest Editorial Security-by-Design for Electronic Systems

IN A RECENT Special Section published in IEEE TRANSACTIONS ON CONSUMER ELECTRONICS we introduced smart electronics [1]. We presented a set of papers which were selected after rigorous review with a scope of artificial intelligence (AI) or machine learning (ML) approaches used for various levels of system abstractions, from device-level to system-level. In one school of thought energy-smart, security-smart, and response-smart are 3 dimensions of smart electronic systems.

Security-by-Design (SbD) [2] has been proposed as a novel paradigm for the design of smart electronics. The current Special Section has been presented with an intention to bring SbD principle to the attention of readers and new upcoming researchers. In the existing trend, the cybersecurity solution is mostly an afterthought. In other words, the system design is done first then cybersecurity solutions are retrofitted. SbD instead promotes cybersecurity as a design habit tightly integrated right from the first step of design flow as a proactive task. SbD has seven fundamental principles: (1) cybersecurity is proactive not reactive, (2) cybersecurity is a default, (3) cybersecurity is embedded into the design, (4) cybersecurity is full functionality - positive-sum, not zero-sum, (5) cybersecurity is end-to-end to provide lifecycle protection, (6) cybersecurity needs to be visible and transparency, and (7) cybersecurity solutions should respect have for users.

Most of the cybersecurity solutions have been heavily relying on software-based approaches. However, hardware-based solutions as well as hardware-assisted solutions are critical to meet the principle of SbD. Hardware-Assisted Security (HAS) is cybersecurity provided by the hardware for the information being processed by an electronic system, for hardware itself, and/or for the electronic system. In HAS, additional hardware components can used for cybersecurity, hardware design modification is performed and/or electronics-system design modification can be performed. Hardware-Assisted Security (HAS) is thus a subset of SbD.

Physical Unclonable Function (PUF) is a cybersecurity hardware primitive that relies on nanoelectronics manufacturing process variations for robust cybersecurity of electronic devices as well as large Cyber-Physical Systems (CPS) [3]. In last decade tons of research has been presented in the existing literature to explore its use in various electronic devices and systems. The following two papers of this special section deals with the PUF.

Digital Object Identifier 10.1109/TCE.2022.3147005

[A1] focuses on the design of robust PUFs and demonstrate its use in smart grids. Specifically, strong PUFs have been explored for LFSR-based key generation and cybersecurity in smart grids.

The use of PUF in a specific application domain is the scope of [A2]. It presents a low-cost, yet robust cybersecurity framework using PUFs. Specifically, arbiter PUF design and corresponding protocols have been presents for cybersecurity of Internet-of-Medical-Things (IoMT) devices in smart healthcare framework. An example of automatic noninvasive glucose reading and insulin delivery with integrated cybersecurity has been demonstrated.

Blockchain is a specific digital ledger technology (DLT) which has been getting lots of attention due to its success in the cryptocurrency domain. The research in blockchain is evolving in multiple fronts. Blockchain is being explored as a cybersecurity solution for data as well as CPS. Research is also performed to make blockchain more secure. This Special Section presents two papers that explore use of blockchain to make CPS more secure, thus SbD solutions for the complex systems.

[A3] presents the idea of blockchain to ensure authenticity of electronics. Due to the global nature of electronics supply chains their originality is often compromised, and fake electronics are present everywhere, which has two types of major issues: loss of revenue of the original manufacturer and compromising of the system in which the fake electronics are deployed. This paper proposes mitigation of this key problem through use of blockchain based supply chain.

[A4] presents custom hardware for efficient smart contract execution. Smart contract implementation in a public blockchain ensures that the contract terms cannot be changed due to its immutability. This paper proposes an on-die hardware module that can communicates with the smart contract for its functionalities.

SbD principles are further demonstrated in other accepted papers in which devices are made cyber attack proof by integrated cybersecurity features right at the device level with an intention to make systems in which these are deployed resilient to cyberattacks.

[A5] demonstrates a method for robust security in IoMT devices. This paper presents design of cryptographic modules which are energy-efficient to run in the IoMT-devices at the same time not susceptible to the physical attacks on cryptographic hardware which can make good guess of cryptographic keys without defeating the cryptography itself rather than analyzing physical signal like power traces.

[A6] advocates making each component of electronic system cybersecure. This paper presents methodology to design to Fortified Network-on-Chips to secure the data and resources against different kinds of hardware trojans. Hardware trojans can be built into the NoC of a consumer electronics to have a backdoor entry so that electronics which can be exploited when needed.

The guest editors sincerely believe that this Special Issue will be a good reading for researchers in the areas of cybersecurity and electronic systems around the globe. The guest editors would like to thank all the contributing authors for their excellent contributions and the reviewers for their help in reviewing the manuscripts throughout the multiple revisions to have a rigorous selection of the works.

FERNANDO PESCADOR
Centro de Investigación en Tecnologías Software y Sistemas Multimedia para la Sostenibilidad
Universidad Politécnica de Madrid
28040 Madrid, Spain
E-mail: fernando.pescador@upm.es

SARAJU P. MOHANTY
Department of Computer Science and Engineering
University of North Texas
Denton, TX 76203 USA
E-mail: saraju.mohanty@unt.edu

APPENDIX: RELATED ARTICLES

[A1] V. C. Patil and S. Kundu, "Realizing robust, lightweight strong PUFs for securing smart grids," *IEEE Trans. Consum. Electron.*, vol. 68, no. 1, pp. 5–13, Feb. 2022.

[A2] A. M. Joshi, P. Jain, and S. P. Mohanty, "iGLU 3.0: A secure noninvasive glucometer and automatic insulin delivery system in IoMT," *IEEE Trans. Consum. Electron.*, vol. 68, no. 1, pp. 14–22, Feb. 2022.

[A3] N. Vashistha, M. M. Hossain, M. R. Shahriar, F. Farahmandi, F. Rahman, and M. Tehranipoor, "eChain: A blockchain-enabled ecosystem for electronic device authenticity verification," *IEEE Trans. Consum. Electron.*, vol. 68, no. 1, pp. 23–37, Feb. 2022.

[A4] M. N. Islam and S. Kundu, "Remote device management via smart contracts" *IEEE Trans. Consum. Electron.*, vol. 68, no. 1, pp. 38–46, Feb. 2022.

[A5] A. Degada and H. Thapliyal, "2-phase adiabatic logic for low-energy and CPA-resistant implantable medical devices," *IEEE Trans. Consum. Electron.*, vol. 68, no. 1, pp. 47–56, Feb. 2022.

[A6] M. JYV, A. Swain, K. Mahapatra, and S. Mohanty, "Fortified-NoC: A robust approach for trojan-resilient network-on-chips to fortify multicore based consumer electronics," *IEEE Trans. Consum. Electron.*, vol. 68, no. 1, pp. 57–68, Feb. 2022.

REFERENCES

[1] F. Pescador and S. P. Mohanty, "Machine learning for smart electronic systems," *IEEE Trans. Consum. Electron.*, vol. 67, no. 4, pp. 224–225, Nov. 2021.

[2] A. Cavoukian, "Understanding how to implement privacy by design, one step at a time," *IEEE Consum. Electron. Mag.*, vol. 9, no. 2, pp. 78–82, Mar. 2020, doi: 10.1109/MCE.2019.2953739.

[3] S. Joshi, S. P. Mohanty, and E. Kougianos, "Everything you wanted to know about PUFs," *IEEE Potentials*, vol. 36, no. 6, pp. 38–46, Nov./Dec. 2017, doi: 10.1109/MPOT.2015.2490261.

Fernando Pescador (Senior Member, IEEE) received the Ph.D. degree from the Universidad Politécnica de Madrid, Madrid, Spain, in 2011, where he has been an Associate Professor since 1995 and the Assistant Vicerrector for Digital Transformation since 2021. He has been with the Electronics and Microelectronics Design Group (GDEM) since 1999 and the Software Technologies and Multimedia Systems for Sustainability (CITSEM) Research Center since 2013. He has published more than 30 papers in JCR journals. His research interests are real-time video coding, multiprocessor architectures for video coding, and digital video broadcasting. He received the Best Paper Award from the 2011 IEEE International Symposium on Consumer Electronics and the IEEE Consumer Electronics Society Chester Sall Award for the third-place best paper in the IEEE TRANSACTIONS ON CONSUMER ELECTRONICS in 2014. From 2017-2021, he was the Editor-in-Chief of the IEEE TRANSACTIONS ON CONSUMER ELECTRONICS.

Saraju P. Mohanty (Senior Member, IEEE) received the bachelor's degree (Hons.) in electrical engineering from the Orissa University of Agriculture and Technology, Bhubaneswar, in 1995, the master's degree in systems science and automation from the Indian Institute of Science, Bengaluru, in 1999, and the Ph.D. degree in computer science and engineering from the University of South Florida, Tampa, in 2003. He is a Professor with the University of North Texas. His research is in "Smart Electronic Systems" which has been funded by National Science Foundation, Semiconductor Research Corporation, U.S. Air Force, IUSSTF, and Mission Innovation. He has authored 400 research articles, four books, and invented seven granted/pending patents. His Google Scholar H-index is 45 and i10-index is 180 with 8500 citations. He is a recipient of 13 best paper awards, the Fulbright Specialist Award in 2020, the IEEE Consumer Electronics Society Outstanding Service Award in 2020, the IEEE-CS-TCVLSI Distinguished Leadership Award in 2018, and the PROSE Award for Best Textbook in Physical Sciences and Mathematics category in 2016. He has delivered 15 keynotes and served on 13 panels at various international conferences. He was the Editor-in-Chief of the *IEEE Consumer Electronics Magazine* from 2016 to 2021 and currently serves on the editorial board of several journals.