In the Era of Cybersecurity: Cryptographic Hardware and Embedded Systems

Nicolas Sklavos

SCYTALE Group,
Computer Engineering & Informatics Department,
University of Patras, Hellas
e-mail: nsklavos@ceid.upatras.gr

***Short Abstract*:** Cybersecurity is a completely new concept, which has attracted the major interest of both academia and industry. New technologies, such as Internet of Things, have shown special interest for cybersecurity systems, in order to fruitful the special demands, of confidentially, authorization, and integrity, for sensitive and personal data. In the cybersecurity era, critical hardware based technologies are latest applied, in order to support efficiently crucial security applications and embedded devices. Filling the security gaps of present and future, for technologies such as IoT, 5G etc, are consider as targets of major importance. Security tokens, privacy services, approaches such as smart cards, and trusted platforms modules, are also focused. Systems' vulnerabilities, are well as security analysis and possible attacks, are considered of major importance, in the cybersecurity era. Cryptographic hardware and embedded systems, are proven powerful and trustworthy solutions in terms of implementation efficiency: timing, throughput, allocated resources, power, energy, always in balance with the security level, each time. Alternative hardware devices and frameworks, can be used alternatively, in order to achieve the best implementation parameters each time.

Keywords: *Cybersecurity, Cryptographic Hardware, Security, Embedder Systems, IoT*

Related References:

[1] N. Sklavos, R. Chaves, G. Di Natale, F. Regazzoni, *Hardware Security and Trust*, Springer, ISBN: 9783319443188, 2017.

[2] A. Kalapodi, N. Sklavos, I. D. Zaharakis, A. Kameas, "A Safe Traffic Network Design and Architecture, in the Context of IoT", proceedings of EUROMICRO Workshop on Machine Learning Driven Technologies and Architectures for Intelligent Internet of Things (ML-IoT), in conjunction with 21th EUROMICRO Conference on Digital System Design, Architectures, Methods, Tools (DSD'18), Prague, Czech Republic, August 29–31, 2018.

[3] E. Isa, N. Sklavos, "On the Detection of Hardware Trojans, in Hardware Security", Design Test Verification and EDA (DTVEDA'07) Workshop, Volos, Hellas, 6-7 July, 2017.

[4] N. Sklavos, I. D. Zaharakis, "Cryptography and Security in Internet of Things (IoTs): Models, Schemes, and Implementations", proceedings of 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS'16), Larnaca, Cyprus, November 21-23, 2016.

[5] N. Sklavos, R. Chaves, F. Regazzoni, "Wireless-SoC-Security: FPGA Based System-On-A-Chip Security Schemes for 4G & 5G", Tutorial, 11th HiPEAC Conference 2016 (HiPEAC'16), Prague, Czech Republic, January 18-20, 2016.

[6] J. Milosevic, N. Sklavos, K. Koutsikou, "Malware in IoT Hardware Devices", Workshop on Trustworthy Manufacturing and Utilization of Secure Devices (TRUDEVICE'16), Barcelona, Spain, November 14-16, 2016.

[7] N. Sklavos, "Cryptographic Algorithms on A Chip: Architectures, Designs and Implementation Platforms", proceedings of the 6th Design and Technology of Integrated Systems in Nano Era (DTIS'11), Greece, April 6-8, 2011.

Short CV

Dr. Nicolas Sklavos is Associate Professor, with Computer Engineering & Informatics Department (CEID), Polytechnic School, University of Patras, Hellas. He is Director of SCYTALE Group. His research interests include Cryptographic Engineering, Hardware Security, Cyber Security, Digital Systems Design, and IoT. He has participated to a number of European/National, Research and Development Projects. He is Evaluator/Reviewer of project calls, funded by the European Commission, or National Resources. He has participated to the organization of international scientific conferences, of IEEE/ACM/IFIP, serving several committee duties, as well as Editorial Board Member of Scientific Journals. He has authored and co-authored technical papers, books, chapters, reports etc, in the areas of his research. His published works has been cited in several papers of other authors, in technical literature. He is Senior Member of IEEE and Associated Member of HiPEAC.