Cyber-Physical Systems Security (CPSS)

Aims and Scope:

Due to the rapid developments in sensing, electronics, computing, and hardware fields, Information and Communication Technology (ICT) has become the backbone of any IT-infrastructure. Besides, the Internet-of-Things (IoT) has become a driver for various cyber-physical systems with board deployment domains. Due to the broad applications of IT and IoT infrastructures, new and sometimes hidden security vulnerabilities, are emerging. Unaddressed security vulnerabilities will create potential threats that if successfully exploited lead to security risks and assets damage.

The CPSS track at ICM-2020 deals with a broad spectrum of security attacks and countermeasures. It particularly highlights emerging techniques, methods, as well as recent applications where microelectronics go together with cyber-physical systems security. This includes new attack vectors, novel designs and materials, lightweight security primitives, nanotechnology, as well as the internet of things, automotive security, smart homes, pervasive and wearable devices, and industrial control systems security.

The track aims to facilitate the rapid growth of cyber-physical systems security research and development with particular emphasis on bridging electronics and security domains. The track will highlight new results from both the research and industry communities in the areas of electronics and cyber-physical systems security and serves as a discussion forum in order to share knowledge, experiences, and ideas concerning the theme of the track. The track aims to collect all security-related submissions to ICM-2020 in one place instead of scattered papers in different sessions across several conference tracks. We believe that a separate cybersecurity track should improve the organization and also the outlook of the ICM-20202.

Topics of Interest:

The cyber-physical systems security track is comprehensive and covers a broad spectrum of topics. The topics of interest include, but limited to:

- Physical attacks including side-channel and fault attacks
- Cryptography and cryptanalysis
- Biometric security
- Trusted platform modules (TPM)
- Efficient implementations for HW security
- Intellectual property protection and content protection
- Automative security
- Reverse engineering
- Security of wireless sensor networks

- Digital forensics and crime science
- Security Analysis of cyber-physical systems
- Machine learning applications in cybersecurity
- Security of reconfigurable and adaptive hardware
- Industrial systems security
- Cloud and big data security
- Computer network security

Review Process:

A rigorous review process will be conducted for all submissions to the track. The track co-chairs will invite security experts to the conferences and manage the review process as well. Therefore, full access to the conference submission system (EDAS) is required. However, the given access does not mean sending the author notifications or working separately from the ICM-2020 conference regulations. The EDAS system needs to be configured to reflect the possibility to submit to the cybersecurity track. Based on the number of the accepted papers, the track will be presented in multiple or a single session.

Deadlines:

The track will be totally in line with the decided ICM-2020 deadlines.

Track co-chairs:

- **Ali Ismail Awad, SMIEEE, PhD.** Dr. Ali Ismail Awad is currently an Associate Professor (Docent) with the Department of Computer Science, Electrical and Space Engineering, Luleå University of Technology, Luleå, Sweden, where he also serves as a Coordinator of the Master Programme in Information Security. He is a Visiting Researcher with the University of Plymouth, United Kingdom. He is also an Associate Professor with the Electrical Engineering Department, Faculty of Engineering, Al-Azhar University at Qena, Qena, Egypt. His research interests include information security, Internet-of-Things security, image analysis with applications in biometrics and medical imaging, and network security. He has edited or co-edited five books and authored or co-authored several journal articles and conference papers in these areas. He is an Editorial Board Member of the Future Generation Computer Systems journal, Computers & Security journal, Internet of Things; Engineering Cyber Physical Human Systems journal, and Health Information Science and Systems journal. Dr. Awad is currently an IEEE senior member.
  Email: ali.awad@ltu.se

- **Karim M. Abdellatif, PhD**. Dr. Karim Abdellatif received his B.S. (Honors) and M.S. in Electrical Engineering from Minia University, Egypt, in 2008 and 2010, respectively. He

obtained the Ph.D. from LIP6, University of Paris VI, in 2014. His Ph.D. presented efficient HW security implementations of authenticated encryption algorithms on FPGAs and ASIC. From 2014 to 2016, he worked as a HW security engineer at the Secure Architectures and Systems group, a joint team between the CEA-Leti and the Ecole Nationale Supérieure des Mines de St Etienne. He joined Morpho in 2017 as a HW security expert in order to evaluate smartcards against physical attacks (side channel and fault attacks). Currently, he is a HW security expert at Ledger and he evaluates hardware wallets against fault and side channel attacks.
Email: karim.abdellatif@ledger.fr

— **Houssem Maghrebi, PhD.** Dr. Houssem Maghrebi received the Engineering degree in communication from Ecole Supérieure des Communications de Tunis in 2008, the Master degree in digital telecommunications systems from Telecom ParisTech in 2009 and the Ph.D. degree in electronics and communications from Telecom ParisTech in 2012. His PhD thesis was about side-channel attacks against smartcards and the corresponding countermeasures. He joined Morpho in 2013 as an embedded security expert. Now, he is working for UL Identity Management and Security as a technical leader for smartcard security evaluation. His main specific research interests include cryptography, physical attacks (side-channel and fault analysis) and the different countermeasures to thwart these attacks.
Email: houssem.mag@gmail.com

— **Ahmed Shatnawi, PhD.** Currently an Assistant Professor in the Software Engineering and Network Engineering & Security departments at Jordan University of Science and technology with extensive experience in Software Engineering and information security. Dr. Shatnaw's research interests lie primarily in the intersection of software engineering, information security, Cryptography, and human-computer interaction. His especially interested in finding better ways to design software systems that are safe, secure, and reliable to use. He received my Ph.D. in Engineering from the University of Wisconsin Milwaukee in 2017 and my M.S. in Software Engineering from George Mason University in 2012. He received his B.S. degree from the Department of Computer Engineering of Jordan University of Science and Technology in Jan 2007.
Email: ahmedshatnawi@just.edu.jo