Guest Editorial

Special Issue on Hardware-Assisted Security for Emerging Internet of Things

1. Hardware-Assisted Security (HAS) for Emerging IoT

We have recently seen Internet of Things (IoT) deployed to ensure smart systems (Cyber-Physical Systems or CPS) and smart system of systems (like smart cities) are possible using the right variety of connected sensors, and data analytics. The emerging Internet of Things (IoT), such as Internet of Medical Things (IoMT), Internet Agro Things (IoAT), and Industrial Internet of Things (IIoT) are being designed to make smart systems across various application domains. IoT computing has evolved to edge computing and fog computing based on the location of computing and intelligence. As a natural evolution, when implantable and/or wearable devices are connected to the IoT, users become part of the IoT as Human-in-the-Loop (HITL), thus leading to Internet-of-Everything (IoE). Cybersecurity solutions at different design phases of electronic systems which build emerging IoT/IoE has become critical. Device, circuit, and system level cybersecurity solutions for IoT/IoE are essential for robust CPS and smart component design. In the IoE framework, device, system, and data security are required, while location and data privacy are also important.

Adversarial attacks in the IoT/IoE can be remote or local using various software and hardware methods. At the same time, security solutions can be based on software, and/or hardware, or combinations of both. Software-based security solutions that rely on some form of encryption are not full-proof as breaking them is just a matter of time. Software-based solutions also need significant computational resources and energy. IoT devices may not always have the computational resources to run the necessary software security solutions. For example, an IoT sensor may not have the capabilities, and IoMT devices such as pacemakers and insulin pumps may not have the computational power given energy constraints. Thus, a paradigm shift to Hardware-Assisted Security (HAS) is needed to provide security solutions in IoT/IoMT/IoE framework. HAS provides hardware-based security for: (1) information being processed, (2) the hardware itself, and (3) the overall system. HAS may take on various forms including: (1) specialized hardware primitives used for security, (2) chip-level security-centric design modifications, and (3) system-level security monitors and design modifications. A key aspect of HAS is to integrate security into the system design flow and avoid retrofitting systems with security features after the IoT system is productized. This is the essence of new cybersecurity aware design paradigm called Secure-by-Design (SbD), which advocates the integration of the cybersecurity early in the design phase rather than as afterthoughts in which systems are designed first and then cybersecurity solutions are retrofitted.

With the above thoughts in consideration, we released call to receive worldwide submissions from researchers. We received many submissions and only manuscripts that were well received were accepted to appear in this Special Issue after a rigorous review process. In the next Section we briefly introduce the selected papers of this Special Issue.

2. Scanning the Special Issue

Embedded systems include various hardware and software building blocks including operating systems, firmware, device drivers, and application software. A simple compartmentalization of various components of embedded system as "trusted" and "untrusted" can help to define cybersecurity policies in the embedded systems. The paper titled "SCALPEL: Exploring the Limits of Tag-Enforced Compartmentalization" discusses a tool for automatic separation of policies for security enforcement.

Firmware is an important element of electronic devices whose functionalities depend on it and many such devices make use of it in IoT/IIoT/IoMT. Firmware can be exploited to breach the security of IoT-devices and consequently that of the overall cyber-physical systems (CPS), such as healthcare CPS and transportation CPS. The paper titled "A Modular End-to-End Framework for Secure Firmware Updates on Embedded Systems" introduces a HAS approach to secure firmware in IoT devices. The proposed method relies on a public PUF-based paradigm to provide robust cybersecurity for firmware updates.

Side-channel attacks represent a major cybersecurity vulnerability of embedded components of IoT. Side-channel attacks utilize power and/or timing analysis to physically exploit the system instead of breaking the encryption algorithms. The paper titled "EM-X-DL: Efficient Cross-Device Deep Learning Side-Channel Attack with Noisy EM Signatures" discusses a Deep Neural Network (DNN) based side-channel analysis method.

A method that uses the power signature of IoT devices for detecting anomalies has been introduced in the paper "Integrated Power Signature Generation Circuit for IoT Abnormality". The work demonstrates power signatures to differentiate operations such as WiFi connection and data sampling rate in IoT devices.

The work titled "Low-Overhead Hardware Supervision for Securing an IoT Bluetooth-Enabled Device: Monitoring Radio Frequency and Supply Voltage" presents a HAS method for Bluetooth cybersecurity which are omnipresent in IoT/IoMT. The key thrust of this solution is a supervisory component which can disable the power supply if abnormal behavior is observed.

The paper titled "Enhancing Privacy in PUF-Cash through Multiple Trusted Third Parties and Reinforcement Learning" introduces a method for anonymity assurance in e-cash transactions. Preserving anonymity while preventing counterfeiting is a challenging problem which this paper addresses. The idea is demonstrated in a hardware implementation of a e-cash system called PUF-cash.

PUF integrated design modification of electronic control units (ECUs) is outlined in the paper titled "Fortifying Vehicular Security Through Low Overhead Physically Unclonable Functions". Such ECUs along with the protocols can improve cybersecurity of Controller Area Network (CAN) leading to robust transportation CPS in smart transportation.

PUFs are demonstrated to be useful for providing robust cybersecurity in the paper "PUF based Secure and Lightweight Authentication and Key-Sharing Scheme for Wireless Sensor Network". PUF plays key role in the proposed authentication and key sharing scheme.

3. Acknowledgement

We would like to thank the EiC of ACM JETC for the opportunities to have this special issue on Hardware-Assisted Security (HAS) for emerging IoT which makes CPS leading to smart systems secure, including smart healthcare, smart transportation, and smart energy. We would like to sincerely thank all the reviewers for helping us in the review process of the submitted manuscript. All the authors who submitted their manuscripts for this Special Issue are hereby acknowledged without whom this would not have been possible. We would like to thank the the productions staffs for bringing this Special issue.

Saraju P. Mohanty, University of North Texas, saraju.mohanty@unt.edu
Jim Plusquellic, University of New Mexico, jplusq@unm.edu
Garrett S. Rose, University of Tennessee, Knoxville, garose@utk.edu
Wei Zhang, Hong Kong University of Science and Technology, wei.zhang@ust.hk
Maria K. Michael, University of Cyprus, mmichael@ucy.ac.cy

Guest Editors