Editorial

Ilia Polian*

Hardware-oriented security

https://doi.org/10.1515/itit-2019-0008

Security has ever since been a key requirement in design and operation of IT systems. The ongoing transition towards cyber-physical, intelligent and autonomous systems has had a dramatic impact on relevant security threats and applicable countermeasures. In the past, critical IT installations, e. g., compute centers of banks or insurances, were located in access-restricted buildings and operated only by authorized personnel. Today, critical IT systems are found in (airborne or ground-borne) vehicles, infrastructures or buildings that are accessible by the general public – which unfortunately includes potential attackers. These systems are constantly interacting with the environment (via sensors and actuators), with their users (via various interfaces) and are connected with other systems (via the Internet and other networks). They can contain a variety of sensitive information, e. g., operational parameters of a car engine, fabrication steps within an integrated production system, health information in a biomedical implant, or financial data in any system with a payment function. Therefore, the systems and the information that they are storing and processing are targets of malicious (cyber-)attacks and need to be protected against such attacks.

Traditionally, IT security techniques concentrated on software vulnerabilities (e. g., buffer overflows) or threats related to communication (e. g., wiretapping), and a number of effective protective techniques, typically based on cryptographic solutions, were developed. Hardware was considered a fixed and perfectly dependable part of the system that performed its task in a flawless and impeccable manner. This view is changing now. Attackers routinely have physical access to a system's hardware components and can use advanced side-channel analysis to derive protected information securely stored within the system, such as cryptographic keys. They could also induce physical disturbances upon a system (for instance, applying strong electromagnetic pulses) to manipulate its operation, e. g., jump over password verification. Even worse, modern hardware is very complex and is designed and manufactured in a sophisticated process distributed over many continents. It cannot be ruled out that hardware blocks have some unintended weaknesses; and it has even been speculated that a malicious party (a foundry or an intellectual property provider) might deliberately add insecure behavior to the system ("kill switches" or backdoors to leak protected information).

But hardware is not only one more security threat to care about. Hardware can (and even must) be a fundament and a "root of trust" of any critical electronic system. A number of basic security functions can be realized using hardware, and for some of them this is the only convincing option. Cryptographic secret keys must be generated by and/or stored in secure hardware primitives. Hardware must provide verifiable logical barriers between the high-security parts of the system where sensitive information is produced and processed, and other system parts that are less protected against attacks (secure isolation). A number of spectacular recent attacks, including Spectre and Meltdown, were based precisely on the inability of microprocessors to provide secure isolation that is effective under all circumstances. Finally, hardware provides the most natural options to counteract physical attacks: integrating sensors to detect tampering attempts; adding masking logic to reduce the exploitable correlation between sensitive data and physical observables; adding unique and unclonable fingerprints to assist in identification and authentication; and integrating real-time monitoring logic for identifying suspicious anomalous system behavior.

This special issue contains four articles spread over different sub-areas of the emerging scientific discipline of hardware-oriented security. Article "Modern random number generator design – Case study on a secured PLL-based TRNG" deals with hardware security primitives, and more specifically, true random number generators. TRNGs are used in secure applications for the generation of secret keys and other cryptographic data. The authors review modern expectations on TRNGs, including the requirements imposed by certification authorities. Then, they demonstrate these concepts on a specific instance of a TRNG designed for integration into application-specific integrated circuits.

The second article of this issue, "Evaluation of (Power) Side-Channels in Cryptographic Implementations", covers countermeasures against power side-channel analysis

***Corresponding author: Ilia Polian,** Pfaffenwaldring 47, University of Stuttgart, D-70569 Stuttgart, Germany, e-mail: ilia.polian@informatik.uni-stuttgart.de

on component level. The counteracted threat consists in an attacker being able to correlate the cryptographic circuit's power consumption with the secret information being processed, such as cryptographic keys. Modern cryptographic hardware implementations incorporate protective structures to prevent such information leakage. The article introduces a framework to quantify this leakage. The framework, which also provides statistical confidence of its assessment, can be used to validate the side-channel resistance of a given circuit; this is illustrated for a realization of a block cipher.

The third article, "Towards Memory Integrity and Authenticity of Multi-Processors System-on-Chip using PUFs", moves from component towards system and architecture level. It describes the concept of an architecture SEPUFSoC for multi-processor systems on chip (MPSoCs) which prevents code-injection attacks (an attacker replacing legitimate by malicious code in the system's memory). The code instructions are signed using another hardware primitive: a physical unclonable function (PUF), which can be understood as a unique fingerprint of every manufactured instance of a circuit. The authors describe the challenges in integrating the PUF into the system, the security properties achieved by SEPUFSoC (along with the assumptions under which these properties hold), possible attacks on it and necessary countermeasures. They also present an FPGA implementation of SEPUFSoC.

The final article of this special issue, "Security Validation of VP-based SoCs Using Dynamic Information Flow Tracking", establishes the connection between hardware-oriented security and formal verification. It deals with information flow tracking, a technique to validate isolation barriers of a system and to prevent uncontrolled propagation of sensitive information through the system. The article transfers the concept of information flow tracking onto embedded system level, making it applicable in early design steps. It specifically focuses on systems on chip realized using Virtual Prototypes, third-party intellectual-property blocks for which only the binary but not the source code is available.

Overall, the contributions in this special issue provide an overview of various research directions currently followed by the hardware-oriented security community. I would like to thank the authors of the articles, who prepared and revised their contributions within short time, and the anonymous reviewers of this issue for their helpful and constructive comments. My thanks also go to Stefan Conrad, Holger Kleeßen, Paul Molitor and the Associate Editor of this issue, Görschwin Fey, for their excellent and timely support. Last but not least, I am thanking you, the reader, for your interest in this emerging topic and wish you enjoyable and informative reading!

Bionotes

Prof. Dr. Ilia Polian
Pfaffenwaldring 47, University of Stuttgart,
D-70569 Stuttgart, Germany
ilia.polian@informatik.uni-stuttgart.de

Ilia Polian received his PhD degree and his habilitation from the University of Freiburg. After being a Professor in the University of Passau for eight years, he is now a Professor of Hardware-oriented Computer Science and the Director of the Institute of Computer Engineering and Computer Architecture at the University of Stuttgart. Prof. Polian co-authored ca. 200 publications and received two best paper awards. He is interested in hardware-oriented security, emerging technologies, and test methods.