Journal of Hardware and Systems Security (2018) 2:287–288
https://doi.org/10.1007/s41635-018-0059-9

EDITORIAL

Guest Editorial: Hardware Reverse Engineering and Obfuscation

Domenic Forte[1] · **Yousef Iskander**[2]

Received: 13 November 2018 / Accepted: 26 November 2018 / Published online: 4 December 2018

Reverse engineering (RE) of electronics is a double-edged sword for industry, government, and society. On the one hand, globalization of integrated circuit (IC) and printed circuit board (PCB) industries have resulted in well-documented concerns, such as counterfeiting, piracy, and hardware Trojan insertion. For such instances, RE represents a fool-proof approach for validating the performance, quality, authenticity, and integrity of electronics. Similarly, many of the critical systems and infrastructures in use today are decades old. Since redesigning them or their underlying components from scratch is too time-consuming and expensive, RE can be applied to reproduce them. On the other hand, RE is responsible for as many threats as solutions. For example, RE can be used to generate unauthorized copies and tampered clones, find weaknesses, and develop attacks, etc. To address these issues, a suite of anti-reverse engineering and anti-counterfeit solutions have been proposed, including hardware obfuscation, gate camouflaging, intellectual property (IP) encryption, DARPA Supply Chain Hardware Integrity for Electronics Defense (SHIELD), tamper-resistant devices and enclosures, and more.

This exciting HaSS special issue focuses on the advances in reverse engineering and anti-reverse engineering. The aim is to provide an authoritative reference of the current state-of-the-art in attacks and countermeasures for ICs, PCBs, and other critical electronic system hardware. Submissions to the special issue were received from leading experts around the world for a global perspective. Articles that were selected include three from Germany and one each from Spain, the UK, and the USA. Several of these were presented at the first IEEE International Workshop on Physical Attacks and Inspection on Electronics (PAINE) in June 2018.

In "Large-Area Automated Layout Extraction Methodology for Full-IC Reverse Engineering," Quijada et al. discuss the state-of-the-art in chip delayering, image acquisition by scanning electron microscope (SEM), and netlist extraction. They propose the "GDS-X" tool that stitches images within routing layers and between vertical layers based on Kruskal's algorithm and other customized optimization steps. Image segmentation and conversion to polygons are performed by machine learning. Finally, they discuss practical challenges such as error correction. Their overall approach reduces the time required to complete RE while minimizing errors. The methodology is validated on 30-mm^2 core die IC fabricated in a 180-nm 6-metal CMOS technology exceeding 500k gates.

In "Detecting Hardware Trojans Inserted by Untrusted Foundry using Physical Inspection and Advanced Image Processing," Vashistha et al. discuss the limitations of nondestructive and full-blown RE methods for hardware Trojan detection. As an alternative, they propose "Trojan Scanner" where changes made to active and lower metal layers from a known authentic design are detected using rapid backside SEM imaging and Structural SIMilarity (SSIM). SEM parameters such as beam voltage, field of view, dwelling time, and resolution are optimized to balance imaging time and detection accuracy. Their approach is demonstrated using a 400 μm $\times$ 400 μm region of a smart card fabricated in a 130-nm technology.

In ''Hardware Security Implications of Reliability, Remanence and Recovery in Embedded Memory," Dr. Sergei Skorobogatov describes the challenges associated with secure data erasure upon tamper detection. A new power glitching technique is introduced that reduces data remanence in embedded SRAM by a thousand times at virtually zero cost. It is also shown that a similar technique has an adverse effect

✉ Domenic Forte
dforte@ece.ufl.edu

Yousef Iskander
yiskande@cisco.com

[1] Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL 32611-6200, USA

[2] Cisco Systems, Inc., Advanced Security Research - S&TO, Knoxville, TN, USA

on secure erase in Flash/EEPROM. Experimental results are provided using microcontrollers from Freescale, Texas Instruments (TI), Microchip, and Atmel.

"Assessment of a Chip Backside Protection" by Amini et al. scrutinizes existing protection IC structures and underscores why they cannot prevent attacks initiated from the backside (i.e., silicon substrate). The authors then propose, realize, and evaluate a countermeasure concept, whereby the IC backside is protected by an optically active layer. This layer is opaque to infrared light, thereby blocking the transistor emissions occurring through the backside that are critical to an attacker. Since the layer can also reflect light, detectors within the chip can monitor whether it has been removed/damaged (i.e., detect an attack). Several interesting future research directions are also highlighted.

"The Past, Present, and Future of Physical Security Enclosures: From Battery-Backed Monitoring to PUF-Based Inherent Security and Beyond" is a position paper by Johannes Obermaier and Vincent Immler on tamper-resistant enclosures. They assess several commercial battery-backed enclosures and argue that alternatives based on physical unclonable functions (PUFs) would provide a higher level of security without the need for battery power. Nevertheless, since details on security enclosures are often undisclosed, they encourage the community to develop and publish more inexpensive and battery-free solutions.

In the last article, "Exploring RFC 7748 for Hardware Implementation: CURVE25519 and CURVE448 with Side-Channel Protection," Pascal Sasdrich and Tim Güneysu investigate side-channel-resistant implementations of two recently recommended ECC curves suitable for resource-constrained devices. They demonstrate that both can be efficiently mapped to modern FPGAs without significant loss in security and throughput. Experimental results show that, with high confidence, scalar- and base-point-dependable leakage cannot be detected even with 1 million power measurements.

We sincerely hope that you enjoy this special issue, and we would like to thank all authors and reviewers for their tremendous efforts in producing these high-quality articles. We also take this opportunity to thank the HaSS editors and administrative staff for their assistance in delivering this special issue.

Domenic Forte and Yousef Iskander
Guest Editors
Journal of Hardware and Systems Security (HaSS)