Journal of Hardware and Systems Security (2020) 4:11–12
https://doi.org/10.1007/s41635-020-00091-0

Special Issue: 2019 PAINE Conference—Physical Assurance and Inspection of Electronics

Navid Asadi[1] · Mark Tehranipoor[2]

Published online: 11 February 2020

Physical inspection of electronics has grown significantly over the past decade and is becoming a major focus for the chip designers, original equipment manufacturers, and system developers. The complex long life of the electronic devices coupled with their diverse applications is making them increasingly vulnerable to various forms of threats and inspection. Large industry and government efforts have been put in place across the globe to address related supply chain security problems to offer solutions, training, and services. The number of programs introduced by US government has increased over the years to analyze and develop relevant solutions. Although much focus is given to digital domain, physical assurance and inspection of electronics as well as physical fingerprinting based on analog parameters are rapidly providing opportunities for unique countermeasures.

Submissions to this HaSS special issue are received from the 2019 Physical Assurance and Inspection of Electronics (PAINE) conference. PAINE 2019 was chaired by guest editors, and selected papers are from leading experts around the world.

The paper "Fluorescent X-ray Scan Image Quality Prediction" by Peter Weichman and Eugene M. Lavely summarizes approaches to image quality prediction in support of an effort under the IARPA RAVEN program to demonstrate a nondestructive, tabletop X-ray microscope for high-resolution 3D imaging of integrated circuits (ICs). The fluorescent X-rays are generated by scanning an electron beam along an appropriately patterned target layer placed in front of the sample and are then detected after passing through the sample by a high-resolution (in both solid angle and energy) backside sensor array. The images are created by way of a model-based tomographic inversion algorithm, with image resolution depending critically on the electron beam scan density and diversity of sample orientations. They derive image quality metrics that quantify the image point spread function and noise sensitivity for any proposed experiment design. Application of these metrics will guide final system design when physical data are not yet available.

The paper "Evaluation of Low-Cost Thermal Laser Stimulation for Data Extraction and Key Readout" by Thilo Krachenfels et al. evaluates the use of a cheap commercial laser fault injection station retrofitted with a suitable amplifier and light source to enable thermal laser stimulation (TLS). They demonstrate TLS attacks are possible at a hardware cost of around 100,000 dollars. This constitutes a reduction of the resources required by the attacker by a factor of at least five. In addition, they showcase two actual attacks: data extraction from the SRAM memory of a low-power microcontroller and decryption key extraction from a 20-nm technology FPGA device. The strengths and weaknesses of this low-cost approach are then discussed in comparison with the conventional failure analysis equipment approach. This work demonstrates that TLS backside attacks are available at a much lower cost than previously expected.

The paper "Decomposition Workflow for Integrated Circuit Verification and Validation" by Adam Kimura et al. reviews a developed integrated circuit (IC) decomposition workflow that can be leveraged for extracting design files and performing advanced verification and validation techniques on fabricated chips. In this work, a commercial 130-nm microcontroller is delayered and imaged to recreate the full design stack-up. Using MicroNet's Pix2Net, the features for each layer are extracted allowing a GDSII file to be generated and design netlists for target components to be recovered. The full decomposition process is executed on both the read-only memory (ROM) array and universal serial communications interface (USCI) of the microcontroller to recover the layout GDSII and circuit netlist. Once the netlists for each

✉ Navid Asadi
nasadi@ece.ufl.edu

✉ Mark Tehranipoor
tehranipoor@ece.ufl.edu

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

[2] Department of ECE, University of Florida, Gainesville, FL, USA

of the modified designs are extracted, formal verification techniques are applied to each netlist, thus illuminating the errors originally inserted into the layout. The extracted netlists are then converted into register transfer level (RTL) representations and simulated with the original design verification test bench.

The paper "Deep Neural Network–Based Detection and Verification of Microelectronic Images" by Md Reza et al. discusses two specific problems in this challenging area of microelectronic device inspection: (i) electronic component detection and (ii) electronic component verification. First, a technique for locating integrated circuits (ICs) on printed circuit boards (PCBs) is introduced. Finding the small and cluttered nature of electronic components is a significant challenge. Second, the problem of component verification is considered, given a pair of IC images. Authors have tried to determine if they are the same part or not, ignoring variations caused both by imaging conditions and by expected manufacturing variations across legitimate instances of the same part.

The paper "Analysis of Dynamic Laser Injection and Quiescent Photon Emissions on an Embedded Processor" by Karim Amin et al. discuss a new laser fault injection methodology which combines quiescent photon emissions with backside dynamic laser pulse profiling in time and space. Empirical results illustrate the impact of the laser on multiple-instruction fault injections and controlled instruction replacement faults. Unlike previous research, quiescent photon emissions combined with laser fault injection provides fine-tuning of faulty instructions in addition to reverse engineering within each clock cycle. This paper is critical to help understanding how to design more secure and trustworthy hardware, including countermeasures to thwart attacks.

We hope you enjoy this special issue, and we would like to thank all authors and reviewers for their efforts to produce the exceptional papers. We would also thank the HaSS editors and staff for their help and support in publishing this special issue.

Navid Asadi and Mark Tehranipoor
Guest Editors