Prevention & Detection of Hardware Trojans in Wireless Cryptographic ICs: Silicon Demonstration

Georgios Volanis, C. Kapatsori, Yu Liu, and Yiorgos Makris
Department of Electrical Engineering, The University of Texas at Dallas, Richardson, TX 75080

I. Research Description

In this demonstration we present two mechanisms for real-time prevention and detection of hardware Trojans in a fabricated wireless cryptographic IC consisting of an Advanced Encryption Standard (AES) core and an Ultra-Wide-Band (UWB) transmitter. The two mechanisms, which are described below, are based on the concept of hardware dithering and invariant property for prevention and detection, respectively.

Hardware Trojan Operation: The hardware Trojan can leak the encryption key by modulating transmission power amplitude. With its impact carefully hidden in the specification margins allowed for process variations, the Trojan does not violate the transmission protocol or any circuit- or system-level specifications and cannot be detected by traditional tests. An adversary who knows its functionality, however, can retrieve the 128-bit AES key, which is leaked with every 128-bit ciphertext sent by the UWB transmitter [1].

Prevention through Hardware Dithering: Hardware dithering aims to occupy or render useless the margin introduced by process variation which allows Trojan insertion in ICs (Figure 1(a)). To this end, two tuning knobs operating on the power and frequency characteristics of the wireless cryptographic IC are added to the circuit forcing it into a random walk around its normal operating mode, thus limiting the range of Trojan operation and muddying the water for the adversary.

Concurrent Hardware Trojan Detection (CHTD): CHTD is a self-referencing approach and is based on an invariant property, which is continuously computed in hardware and evaluated by a programmable on-chip neural classifier (Figure 1(b)). The method which is performed in real-time along with the circuit operation targets hardware Trojans which are dormant during testing and are activated after deployment, and raises an alert when a hardware Trojan is activated.

II. Hardware Demonstration

As shown in Figure 2(a), our demonstration setup includes:

- Two custom-designed ICs fabricated in a 0.35um CMOS process, i.e. (i) a wireless cryptographic IC wherein the CHTD circuitry and the tunable components are also implemented, and (ii) an analog neural network experimentation platform for checking the invariant property Figure 2(b).
- A laptop that provides a user interface.
- A Tektronix MDO-4104 oscilloscope.
- Two antennas that enable communication over the air between the wireless cryptographic IC and the oscilloscope.

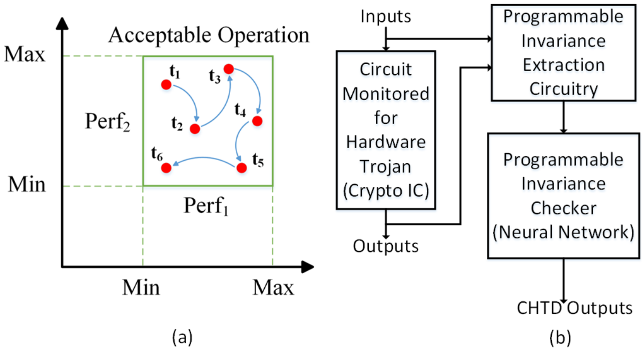
Max
Acceptable Operation
Perf$_2$
Min
t_1
t_2
t_3
t_4
t_5
t_6
Perf$_1$
Min
Max
(a)
Inputs
Circuit Monitored for Hardware Trojan (Crypto IC)
Outputs
Programmable Invariance Extraction Circuitry
Programmable Invariance Checker (Neural Network)
CHTD Outputs
(b)

Fig. 1: (a) Hardware dithering. and (b) CHTD.

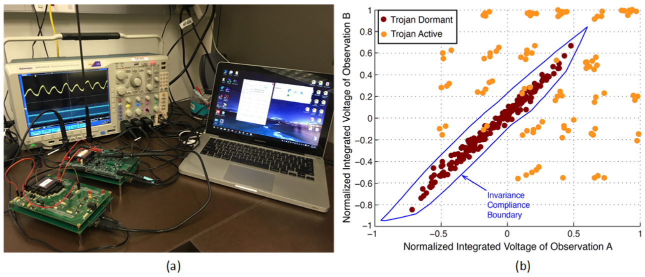

Fig. 2: (a) Hardware demonstration platform setup and (b) CHTD results for amplitude-based hardware Trojan.

III. Description of the Observables

In this demonstration, the audience is able to observe:

- Covert operation of the hardware Trojan (i.e., leakage of encryption key bits) with user-defined input for plaintext and encryption key (on oscilloscope).
- Alert raised by the programmable CHTD method on the analog neural network, which directly communicates with the wireless cryptographic IC, upon activation of previously dormant hardware Trojan.
- Hardware Trojan prevention through adjustment of the programmable tuning knobs.

References

[1] Y. Liu, and Y. Makris, “Hardware Trojans in Wireless Cryptographic ICs: Silicon Demonstration & Detection Evaluation,” Best Demo Award in *IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, 2016

[2] D. Maliuk, Y. Makris, “An Experimentation Platform for On-chip Integration of Analog Neural Networks: A Pathway to Trusted and Robust Analog/RF ICs,” in *IEEE Transactions on Neural Networks and Learning Systems*, vol. 26, no. 8, pp. 1721-1734, 2015