Karlsruhe Institute of Technology

Institute of Computer Engineering
Chair of Embedded Systems

Machine Learning for Hardware Security

Yigit Oguz
2309297

Department of Informatics

Responsible Supervisor:
Sajjad Hussain

Abstract

English version of the Kurzfassung. Try to stay within 500 words (single page).

Contents

1. Introduction

Low-cost, high-volume electric devices have been increasingly popular in recent years. Hardware producers frequently outsource numerous elements of their design or manufacturing processes to keep up with the expanding demand for those devices and the globalization of hardware production. Untrusted entities engage in all phases of the life cycle of an electronic device or integrated circuit in this paradigm, either directly or indirectly. Insertion of hardware Trojans has become a serious concern in hardware production as a result of these conditions.

A hardware Trojan is defined as a malicious, intentional modification of a circuit design that results in undesired behavior when the circuit is deployed [6]. When an integrated circuit gets "infected" by a hardware Trojan, it may encounter changes in functionality or specification, leak sensitive information, or have reduced or unreliable performance. A Trojan consists of two main parts: trigger and payload [4]. A Trojan trigger is an optional element in the circuit that monitors numerous signals or a sequence of events. On the other hand, a Trojan payload listens to both the signals from the Trojan-free circuit and the trigger's output. The payload is activated to conduct malicious activity if the trigger detects an expected event or situation. In most cases, the trigger activates under hard-to-satisfy and rare situations, so the payload stays passive. In these situations, the integrated circuit functions like a Trojan-free circuit. Because of that, it is difficult to detect a hardware Trojan after it is inserted.

To deal with hardware Trojans, Trojan detection is used. Trojan detection's goal is to validate existing designs and fabricated integrated circuits without the need of additional circuitry. Hardware Trojan detection has two main approaches: the destructive and the non-destructive type.

The destructive approach is used after the fabrication process and checks the physically inserted hardware Trojans by reverse engineering. As the name suggests, after the destructive approach the the integrated circuit becomes unusable. Additionally the destructive approach only yields information for a single integrated circuit sample so they are not considered a viable option for Trojan detection.

The non-destructive approaches are further classified into three types: the IP-verification, the logic testing and the side-channel analysis type. Side-channel signal analysis approaches detect hardware Trojans by measuring circuit parameters, such

as delay [4], power [2] and leakage power [1], temperature [3], and radiation [5]. The logic testing applies test vectors to activate Trojans and compares the outputs with the expected results. On the other hand, the IP-verification method analyzes the hardware design written in a hardware description language and has the advantage of being able to detect hardware Trojans early.
As the machine learning expands it's reach to other fields, it's impact continues to grow more. One of these fields is the hardware security, where the machine learning can be used for both malicious and benevolent purposes. In the following sections, the basics of machine learning methods as well as their usage in hardware Trojan detection are presented.

2. Background

3. Machine Learning for Hardware Security

4. Summary

Bibliography

[1] Jim Aarestad et al. "Detecting Trojans Through Leakage Current Analysis Using Multiple Supply Pads". In: *IEEE Transactions on information forensics and security* 5.4 (2010), pp. 893–904.

[2] Dakshi Agrawal et al. "Trojan detection using IC fingerprinting". In: *2007 IEEE Symposium on Security and Privacy (SP'07)*. IEEE. 2007, pp. 296–310.

[3] Domenic Forte, Chongxi Bao, and Ankur Srivastava. "Temperature tracking: An innovative run-time approach for hardware Trojan detection". In: *2013 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*. IEEE. 2013, pp. 532–539.

[4] Yier Jin and Yiorgos Makris. "Hardware Trojan detection using path delay fingerprint". In: *2008 IEEE International workshop on hardware-oriented security and trust*. IEEE. 2008, pp. 51–57.

[5] Franco Stellari et al. "Verification of untrusted chips using trusted layout and emission measurements". In: *2014 IEEE international symposium on hardware-oriented security and trust (HOST)*. IEEE. 2014, pp. 19–24.

[6] Mohammad Tehranipoor and Cliff Wang. *Introduction to hardware security and trust*. Springer Science & Business Media, 2011.