

Hardware Trojans - Design, Implementation and Detection



TECHNISCHE
UNIVERSITÄT
DARMSTADT



CASED

Master-/Diploma-Thesis

CASED

In CASED (Center for Advanced Security Research Darmstadt), the Technische Universität Darmstadt, Fraunhofer Institute for Secure Information Technology and the University of Applied Sciences Darmstadt collaborate in the rapidly developing field of IT security.

Read more on www.cased.de.

Motivation

Hardware Trojans are an upcoming threat for manufacturers of integrated circuits. As customers demand lower prices for everyday technology, electronic devices are fabricated outside of the company where they are produced. An adversary can then insert malicious code in hardware which unknowingly can be activated by its operator. One goal of this thesis is to implement different types of Hardware Trojans that can be added to existing designs. Additionally it should be evaluated if there are methodologies that reveal the existence of a Hardware Trojans on an FPGAs. New ideas for Hardware Trojans can also be implemented and tested. This thesis offers the opportunity to gain in-depth knowledge in VHDL and FPGA implementations. Industry-relevant experience in HW/SW-Codesign can also be acquired.

Task

- ▶ Survey about State of the Art implementations
- ▶ Concept and implementation of different covert channels
- ▶ Demonstration of the information leakage with a common crypto module (e.g. AES)
- ▶ Finding evidence for the existence of a Trojan.
- ▶ Feasibility study for device identification purposes

Requirements

- ▶ creative, autonomous and analytical mentality
- ▶ Knowledge of programming FPGAs: VHDL or Verilog
- ▶ interest and some knowledge of cryptography
- ▶ (optional) knowledge in placement and routing methodologies for FPGAs
- ▶ Language of the thesis should be english, but german is also possible

Date of Entry

As of now.