
- Masterthesis -

Realization of a multi-context Trust Anchor on Reconfigurable Hardware

CASED

In CASED (Center for Advanced Security Research Darmstadt) collaborate the Technische Universität Darmstadt, Fraunhofer Institute for Secure Information Technology and the University of Applied Sciences Darmstadt in the fast developing field of IT Security. In a unique cooperation, which combines different areas of expertise from these renowned institutions, progressive IT security solutions are researched, developed and implemented into industrial economy: CASED brings together computer scientists, engineers, physicists, legal experts and business economists. Read more on www.cased.de.

Motivation

The TCG Mobile Phone Work Group has specified in its TCG Mobile Reference Architecture a new concept to enable trust into future mobile devices. This concept introduces a hardware-based, multi-context trust anchor especially for mobile devices. This trust anchor is called a Mobile Trusted Module (MTM) and has properties and features comparable to a Trusted Platform Module. The main goal of this thesis is to realize such trust anchor facing the requirements of embedded systems.

Tasks

- Analysis and reflection of TCG Mobile Trusted Module Specification regarding the specific requirements of embedded systems on reconfigurable hardware
- Design and concept of a multi-context-enabled trust-anchor
- Prototypical implementation of significant hardware- and software components and required roots-of-trusts on a Xilinx-Virtex5 FPGA

Requirements

- Very good knowledge in VHDL, C/C++ and embedded systems
- Knowledge on Trusted Computing and IT security would be helpful

Date of entry

- Immediately

Contact

Hr. Michael Kasper

e-Mail: michael.kasper@sit.fraunhofer.de

CASED - Center for Advanced Security Research Darmstadt
Mornwegstraße 32, 4th floor, Room 4.2.17, 64293 Darmstadt