

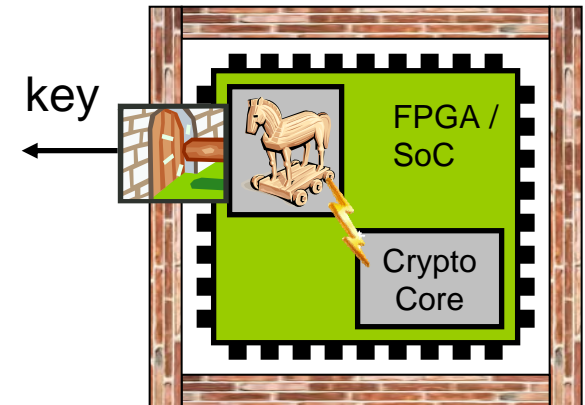
Hardware Trojans on FPGAs

Motivation

A Trojan horse is a software (according to Wikipedia) that appears to perform a desirable function for the user prior to run or install, but steals information or harms the system. The idea of Trojan horses however also applies to hardware modules of System on Chips. They can be used to extract secret information and to reveal the secret of the system.

Project description

- Goals
 - Design of a Hardware Trojan
 - Exploiting the System Monitor in Vertex-6 FPGAs to extract secret key information
 - Open a back-door (or side channel) to reveal the secret
- Tasks
 - Literature research about Hardware Trojans.
 - Design of a System on a Chip with a Trojan Module
 - Exploit side-channel information using the Xilinx Virtex System Monitor.



Literature

- Lang Lin, Markus Kasper, Tim Güneysu, Christof Paar, and Wayne Burleson, „Trojan Side-Channels: Lightweight Hardware Trojans through Side-Channel Engineering“, CHES 2009.

Deliverables

- Project files (.zip, cleaned)
- Documentation (inline)
- Readme (getting started)
- Presentation (10 .ppt slides)

Project schedule

- Start Immediately
- Month 1 Reading, planning, preparing
- Month 2 FPGA programming
- Month 3 Final deliverables

Master Project

Studies: INF SEW TEL

Prerequisites

- HDL, FPGAs, Side-Channel Attacks

Advisor / contact

Michael.Hutter@iaik.tugraz.at