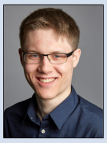


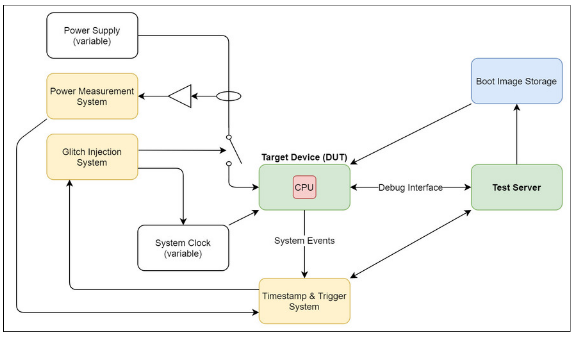
Marco
Zollinger

Marco
Reifler

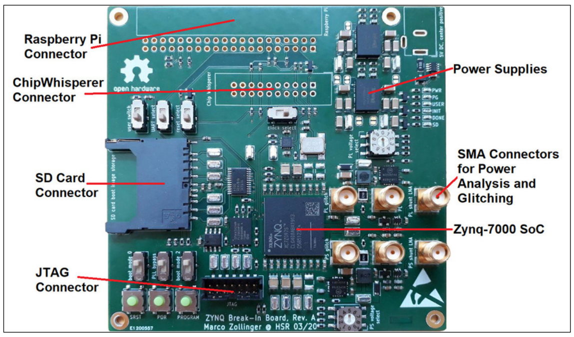
Graduate Candidates	Marco Zollinger, Marco Reifler
Examiner	Prof. Stefan Richter
Co-Examiner	Dr. Ettore Ferranti, ABB Schweiz AG, Baden, AG
Subject Area	Security

Embedded Secure Boot Test Suite

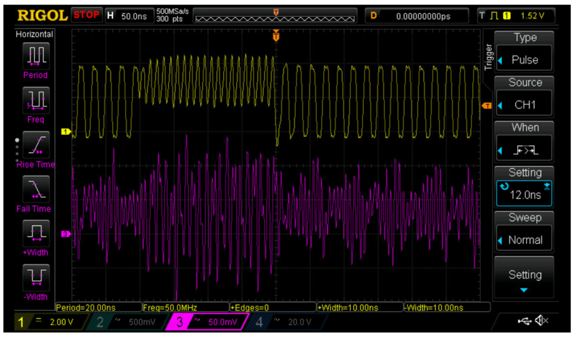
A Generalized Approach in Assessing the Physical Security of Embedded Secure Boot



System Block Diagram of Experimentation Hardware Design
Own presentment



Custom-Designed Experimentation Board for the Zynq-7000 SoC
Own presentment



Clock Glitching Oscilloscope Screenshot
Top: Clock signal with glitches, Bottom: CPU power consumption
Own presentment

Introduction: This bachelor thesis is a follow-up to our last student research project "Secure Boot on Embedded Systems". There, we implemented a secure boot process on the Xilinx Zynq-7000 system-on-chip according to the recommendations of the manufacturer. After an analysis of the available security options, we settled on both encrypting and authenticating the boot image to ensure its authenticity and confidentiality. There was however no time left for an in-depth security analysis of the chip itself. The secure boot process is based on a chain of trust, where every stage relies on the security of the previous one. The first step in this chain, the root of trust (ROT), is therefore the most important one. If it is compromised the rest of the secure boot process cannot be trusted. In most cases, the ROT is a piece of proprietary hardware or firmware deeply embedded into the chip, is confidential and cannot be read out by the user. This requires users to put a lot of trust in the manufacturer and the chip, because its security cannot be verified independently.

Approach: The goal of this project was to provide a test suite to analyze the root of trust (ROT) firmware security in different processors and systems-on-chip. Software vulnerabilities in user code can be fixed with security patches, but this is usually not possible with ROT firmware images. They are burned into the chip during production and cannot be altered afterwards. Because of their high execution privileges and immutability, vulnerabilities in ROT firmware images can be very dangerous. However, the firmware memory locations in the chip are usually read-protected and the code cannot be extracted and reverse engineered by the user for security auditing. Glitching may provide a means to temporarily manipulate the chip and override this read-out protection, or to coerce it to accept unauthenticated software images, if physical access to the device is possible. If the code cannot be extracted black-box fuzzing methods can still be applied to test the interfaces for security vulnerabilities without knowing anything about the inner workings of the firmware.

Result: A generalized hardware system design has been elaborated from the requirements to support experiments with physical attacks like power analysis and voltage glitching or clock glitching. These experiments can be difficult to perform on off-the-shelf development boards without extensive modifications. The generalized design can be adapted and implemented for different target processors or systems-on-chip. For this project, the process has been demonstrated by developing a custom board with the Zynq-7000 system-on-chip. The result is an experimentation board that provides interfaces specifically engineered for security testing and allows for a clean laboratory setup with high reliability and repeatability. To support the experiments, a test suite has been elaborated. It consists of code analysis guidelines and procedures and scripts to support power analysis, fault injection and fuzzing attacks. Instruction skipping and manipulation of the control flow of user code running on the target platform through clock glitching have been successfully demonstrated. Further research is needed to confirm that the root of trust firmware is also susceptible to such manipulations or if there are countermeasures in place.

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

FHO Fachhochschule Ostschweiz