Hardware-Centric Boot-Time Integrity and Authenticity Checking for PSoCs

Programmable System-on-Chips (PSoCs) have several advantages over other processing platforms through the availability of hardware acceleration in the form of Field Programmable Gate Arrays (FPGAs) that are tightly coupled with integrated General Purpose Processors (GPPs). However, PSoCs are designed to be processor-centric, i.e., configuration of hardware and software is controlled by the processor at boot-time which is a potential **security** threat. Therefore, **cryptographic** algorithms are used to carry out file encryption and authentication. A common way is to store the cryptographic keys on chip. As a consequence, the root of trust and the entire boot process depends on the confidentiality of this embedded keys. The goal of this thesis is to investigate a novel **hardware-centric secure boot process** for PSoCs to ensure integrity and authentication and if possible without storing sensitive data on the chip. The main tasks within this thesis are:

- Acquiring a general understanding of the Xilinx Zynq boot process.
- Implementing custom boot routines with integrity and authenticity checks on Xilinx Zynq PSoC.
- Evaluation of boot routines in terms of security and resource costs.

Prerequisites:	Programming Skills in C/C++ and VHDL, interest in PSoC design and security
Type of Work:	Theory (15%), Conception (35%), Implementation (50%)
Supervisors:	Franz-Josef Streit (franz-josef.streit@fau.de) and Stefan Wildermann (stefan.wildermann@fau.de)

Lehrstuhl für Informatik 12
Hardware-Software-Co-Design
Cauerstraße 11
91058 Erlangen

FRIEDRICH-ALEXANDER
UNIVERSITÄT
ERLANGEN-NÜRNBERG
TECHNISCHE FAKULTÄT