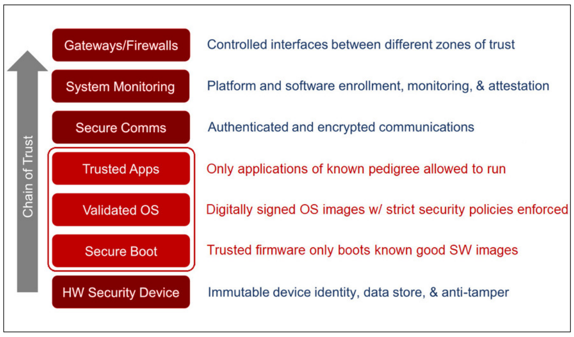
Marco
Zollinger

Marco
Reifler

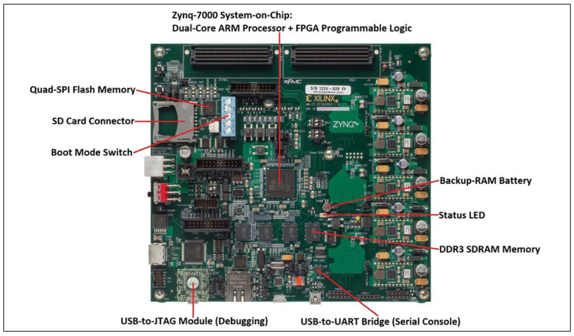
Students	Marco Zollinger, Marco Reifler
Examiner	Prof. Stefan Richter
Subject Area	System Software
Project Partner	ABB Schweiz AG, Turgi, AG

Secure Boot on Embedded Systems

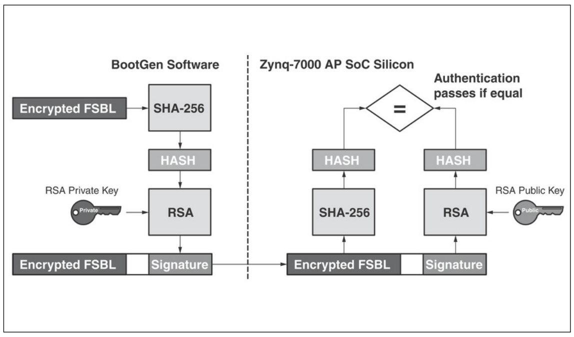
Implementing Secure Boot with Chain of Trust and Encryption on a Zynq-7000 System on Chip


Chain of Trust
Gateways/Firewalls
Controlled interfaces between different zones of trust
System Monitoring
Platform and software enrollment, monitoring, & attestation
Secure Comms
Authenticated and encrypted communications
Trusted Apps
Only applications of known pedigree allowed to run
Validated OS
Digitally signed OS images w/ strict security policies enforced
Secure Boot
Trusted firmware only boots known good SW images
HW Security Device
Immutable device identity, data store, & anti-tamper

Security Aspects Covered in This Project Highlighted
Xilinx Cybersecurity Presentation 2019 at CERN (modified)


Zynq-7000 System-on-Chip:
Dual-Core ARM Processor + FPGA Programmable Logic
Quad-SPI Flash Memory
SD Card Connector
Boot Mode Switch
Backup-RAM Battery
Status LED
DDR3 SDRAM Memory
USB-to-JTAG Module (Debugging)
USB-to-UART Bridge (Serial Console)

ZC702 Evaluation Board with Relevant Hardware Annotated
Xilinx User Guide 850 (modified)



Signature and Authentication Procedure
Xilinx White Paper 468

Introduction: While the demand for Internet of Things solutions has been skyrocketing for the past few years, security often has not been given enough attention. This is particularly alarming because this technology is not only used for smart light bulbs or temperature sensors, but also in industrial settings to control heavy machinery or critical infrastructure, where a failure could lead to injury or loss of life. This trend is probably caused by the pursuit of higher efficiency and flexibility which can be achieved with intelligent algorithms and by communicating over the internet. This results in exposing these devices to attacks by malicious actors trying to gain control. Additionally, the often highly specialized algorithms implemented in these devices are the result of considerable development investments. They represent an asset to the company that must be protected from industrial espionage attempts to maintain a competitive advantage. The aim of this project is therefore to prevent tampering with the system such as running unauthorized software or extracting intellectual property or cryptographic keys from the device.

Approach: Secure Boot is a technology where every step of the boot process checks the previous one for its authenticity using a cryptographic signature and only proceeds if the check succeeded. The first step of this so-called chain of trust is the hardware root of trust which is firmly integrated into the chip. To also ensure confidentiality of the sensitive software algorithms, the boot image is encrypted, with the decryption key again being safely stored within the chip. The embedded processor used for this project is the Zynq-7000 system on chip by Xilinx, which combines a dual-core ARM processor with programmable logic. Xilinx provides extensive documentation on using Secure Boot with their chips, which was studied and implemented on the ZC702 Evaluation Kit. We took on the roles of an attacker and a defender, then using an iterative approach the boot sequence was secured step-by-step. For every iteration a potential attack vector of the current system was shown and then a new security feature implemented as countermeasure in the next iteration. This process was repeated with the goal of the final boot sequence being as secure as possible within the given constraints.

Result: The final iteration comprises completely encrypted and authenticated bootloader and operating system partitions which the processor will only boot if they have a valid signature by the equipment manufacturer. Through use of asymmetric cryptography for authentication, only a hash of the public key needs to be stored on the chip, the secret key is never exposed. The symmetric encryption key is saved in on-chip volatile memory, which can be cleared if a tamper attempt is detected. The JTAG debugging interfaces have been disabled, as they would have provided adversaries with easy access to system internals. In the future, a mechanism could be developed to reenable the JTAG interfaces after a password has been entered by an authorized service technician. Further possible improvements are advanced tamper detection algorithms, measured boot for operation in a network or the upgrade to another chip with even more security features. If third party software needs to be run on the system, the use of a hypervisor and the ARM TrustZone features may be advised to limit privileges.