Zurich University
of Applied Sciences

School of Engineering

InES Institute of Embedded Systems

Secure Boot for System on Chip

Although many embedded devices lack the required security, manufacturers slowly start to realize the need to secure their products. The company Enclustra wished to have a reference design to help developers starting secure development on their Mercury platform. Following the Platform Security Architecture (PSA) framework from ARM three different use-cases defined by Enclustra have been analyzed. To implement these use-cases, different security features of the Xilinx Zynq Ultrascale&#43; MPSoC were investigated and implemented.

The outcome is a modular reference design, where different security features can be added, depending on the individual use-case. The base is a PetaLinux project to boot the Zynq Ultrascale&#43; with an encrypted and authenticated image. It uses the cryptography hardware and key handling implemented by Xilinx. In addition to the base project, features like multiboot or tamper detection can be added as modules to the reference design. The Linux Crypto-API has been analyzed to use the cryptography hardware of the Zynq Ultrascale&#43; in Linux on the FPGA. Code examples for different algorithms have been created to simplify the implementation of the Linux Crypto-API. To isolate critical applications, ARM implements the TrustZone concept in their processor architectures. This concept was evaluated and implemented on the Xilinx evaluation kit ZCU102, with OP-TEE as Secure-OS. This enables a user to isolate critical applications or data and therefore, protect them even if parts of the system are compromised.

Finally, the thesis shows that the Zynq Ultrascale&#43; is built for secure product development. Not only cryptography features but also features for maintainability, reliability and secure execution of code are implemented. The reference design is a solid base to get started, using all these features.

Diplomierende
Thierry Delafontaine
Tobias Vögeli

Dozierende
Matthias Rosenthal
Andreas Rüst

Used Hardware: Mercury XU5 on a Mercury+PE1 board from Enclustra

The Zynq Ultrascale+ from Xilinx is an SoC (System on Chip) with programmable logic and multiple processors on a single chip.