

Hiwi, IDP, Research Internship

Implementation of Security Mechanisms for ARM Embedded Devices

The NXP i.MX8 based embedded systems are widely used for various applications in automotive and industry. Its rich security architecture features ARM TrustZone technology, secure boot, cryptographic acceleration and assurance module. These building blocks can be utilized to design and implement advanced protection techniques for high-end embedded devices.

Task Description

In this project several security mechanisms are to be implemented or extended. This includes the following tasks:

- Implementation of a secure update mechanism, also under the assumption of a possibly compromised OS.
- Setup of reproducible and verifiable build environment based on Yocto toolchain.
- Setup of continuous integration and automated tests for the embedded systems.

Prerequisites

- High motivation and ability to work independently
- Experience in embedded software development
- Good system programming skills in C/C++
- Preferably experience in u-boot or bare-box bootloaders, ARM TrustZone, Yocto toolchain

Contact

Simon Ott

Telefon: +49 89 322-9986-143

E-Mail: simon.ott@aisec.fraunhofer.de

Mykolai Protsenko, Dr.-Ing.

Telefon: +49 89 322-9986-192

E-Mail: mykolai.protsenko@aisec.fraunhofer.de

Fraunhofer Institute for Applied and Integrated Security (AISEC)

Secure Operating Systems

Lichtenbergstraße 11, 85748 Garching (near Munich), Germany

<https://www.aisec.fraunhofer.de>

Date of publication: December 21, 2020