Working Student/Research Internship/IDP *March 14, 2019*

Security Features of NXP i.MX Application Processors

The NXP i.MX6/i.MX7/i.MX8 application processors are widely used in automotive, industrial automation, and robotics. The chips are equipped with a large variety of built-in security features, including but not limited to:

- ARM TrustZone providing secure execution environment
- Cryptographic Acceleration and Assurance Module (CAAM) with hardware-accelerated cryptographic functions and true random number generation
- Watchdog timers
- Secure boot / high assurance boot (HAB)
- Physical tamper protection
- Unique Manufacturing Protection Private Key

Physical tamper protection, for instance, can detect opening or damaging of the device's envelope by constantly measuring signal on dedicated pins. The deviation of the signal indicates the tamper event, in which case the device master key is automatically erased.

Task Description

The goal of this project is to explore the key security features of one of the i.MX families and facilitate the use and development by consolidating and extending available documentation, creating understandable code examples and/or usable APIs where appropriate, and provide discussion on security of the available mechanisms and measures. Examples of the features considered for prototypical implementation may include:

- Tamper detection
- Implementation of secure boot and encrypted boot with OPTEE OS for the TrustZone environment
- Use of the TrustZone Watchdog
- Secure network communication and use of CAAM from OPTEE
- Use of the Manufacturing Protection Key for device authentication
- Use of secure real-time clock

Prerequisites

- At least basic knowledge in cryptography, system- and network security
- Basic knowledge in signal processing and electrical/electronic engineering
- Good C programming skills
- Preferably: Embedded development / Yocto experience

Contact

Mykolai Protsenko, Dr.-Ing.
Telefon: +49 89 322-9986-192
E-Mail: mykolai.protsenko@aisec.fraunhofer.de

Fraunhofer AISEC
Parkring 4, 85748 Garching (near Munich)
https://www.aisec.fraunhofer.de