Lehrstuhl für Sicherheit in der Informatik
Prof. Dr. Claudia Eckert

Fraunhofer AISEC

Working Student

Monitoring and Recovery of ARMv8-A based IoT Devices

In recent years a multitude of IoT devices have been deployed in remote or inaccessible locations. This poses additional risks for the security of those devices, as traditional monitoring and maintenance becomes unfeasible. Attacks on this device class are numerous and scale to thousands of devices. To address this, IoT devices have to be equipped with temper resistant management functionality. Fundamentally, this includes a secure monitoring mechanism, which can accurately describe the current system state to a central observer. This is then coupled with a mechanism to force the device into a pre-defined secure state, if the reported state deviates from it. Both these functionalities have to be resilient, even if the device is compromised by an attacker.

Task Description

The objective of this project is the implementation of a monitoring and recovery mechanism[1] for ARMv8-A based IoT devices. The security critical functionality should be enforced with hardware assisted security modules, such as ARM TrustZone or TCG-DICE. Existing solutions (e.g. OP-TEE) should be adapted for this use-case. The development targets the i.MX8-QM platform.

Prerequisites

- Experience in one or more:
  Embedded development, Yocto, ARM TrustZone and OP-TEE
- Basics in one of C/C++
- High motivation and ability to work independently
- Basic knowledge in cryptogaphic primitives, system- and network security

Contact

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

Albert Stark
Telefon: +49 89 322-9986-1038
E-Mail: albert.stark@aisec.fraunhofer.de

Fraunhofer Institute for Applied and Integrated Security (AISEC)
Secure Operating Systems (SOS)
Lichtenbergstraße 11, 85748 Garching (near Munich), Germany
https://www.aisec.fraunhofer.de

[1] https://www.microsoft.com/en-us/research/publication/cyber-resilient-platforms-overview/