Chair of Security in Information Technology
TUM Department of Electrical and Computer Engineering
Technical University of Munich

Assistant (Student), Bachelor's Thesis

# Monitoring and Recovery of i.MX8-based IoT Devices (AISEC)

Many IoT use cases require deployment of embedded devices with considerable geographical spread, for instance in smart-city, smart-home, or automotive application domains. The spatial distribution of the devices makes their on-site maintenance a costly and time-consuming task. The large number of Internet-enabled IoT devices with homogeneous software stacks poses an attractive target for remote attacks. To address this problem, IoT platforms have to be enhanced with device-recovery
functionality along with a control and monitoring backend able to remotely obtain status information and update software of the IoT devices even in case those were taken over by an adversary.

Task Description
The objective of this project is the implementation of a monitoring and recovery mechanism1 for i.MX8 based IoT devices. For this purpose, the security critical communication with the backend and software recovery functionality have to be secured employing the ARM TrustZone execution environment and OP-TEE.

## Prerequisites

- At least a basic knowledge in cryptography, system- and network security
- High motivation and ability to work independently
- Good C/C++ programming skills
- Preferably experience in: Embedded developmentand Yocto, ARM TrustZone and OPTEE

## Contact

Mykolai Protsenko, Dr.-Ing.

Telefon: +49 89 322-9986-192
E-Mail: mykolai.protsenko@aisec.fraunhofer.de

Manuel Huber

Telefon: +49 89 322-9986-165
E-Mail: manuel.huber@aisec.fraunhofer.de

Fraunhofer Institute for Applied and Integrated Security (AISEC)
Secure Operating Systems
Parkring 4, 85748 Garching (near Munich), Germany
https://www.aisec.fraunhofer.de

## Advisors

Georg Sigl
Mykolai Protsenko + Manuel Huber (Fraunhofer AISEC)