Remote attacks on Internet of Things (IoT) devices are prevalent and usually have a high impact. They scale very well, since many devices use the same software stack. These attacks can render devices useless or misuse them for other purposes. At the same time, there is a need for connectivity even on tiny microcontroller-based devices. These devices usually run a microkernel instead of a full featured Linux OS with many security features built-in. Nevertheless, being connected to the internet, they require mechanisms for secure communication as well. Therefore, in scope of this work, a platform for secure IP-based communication between Cortex-M33 based microcontrollers shall be implemented. This platform shall be extended with security mechanisms provided by the devices. This includes the following tasks:

- Evaluating suitable development platforms
- Setting up a development environment for Cortex-M33 microcontrollers
- Implementing IP-based connectivity for the devices
- Implementing security mechanisms (TrustZone, cryptographic library, key storage)

Prerequisites

- High motivation and ability to work independently
- Good Programming skills in C
- Experience in embedded SW development
- At least basic knowledge of cryptographic Primitives

Contact

Simon Ott  
Telefon: +49 89 322-9986-143  
E-Mail: simon.ott@aisec.fraunhofer.de

Dr. rer. nat. Julian Horsch  
Telefon: +49 89 322-9986-118  
E-Mail: julian.horsch@aisec.fraunhofer.de

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

Advisors

Georg Sigl  
Simon Ott + Julian Horsch (Fraunhofer AISEC)