Forschungspraxis

**Trusted Channels for IoT Devices (AISEC)**

Remote Attestation is the process of assessing the trustworthiness of a remote computing platform through verifying the integrity of its software stack. Arm Trusted Firmware-M provides the Initial Attestation Service (IAS) to enable attestation on resource-constraint Arm Cortex-M microcontrollers. However, executing a remote attestation protocol without binding it to the device’s communication channel opens up the possibility of Man-in-the-Middle (MitM) attacks: In such a scenario, an attacker uses a rogue device to fetch attestation evidence from a good device and establish communication to an IoT hub or other IoT devices. Therefore, the scope of this work is to design and implement a channel binding mechanism for common IoT protocols such as Constraint Application Protocol (CoAP) to augment the communication channel with an attestation mechanism. This includes the following tasks:

- Survey of existing IoT protocols and attestation mechanisms
- Design of a channel binding mechanism, e.g., for CoAP with OSCORE/EDHOC
- Implement a Proof-of-Concept for the solution
- Evaluate the solution

**Prerequisites**

- High motivation and ability to work independently
- Good Programming skills in C
- At least basic knowledge of cryptographic primitives
- Preferably knowledge about embedded systems and Arm Cortex-M processors

**Contact**

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

**Advisors**

Georg Sigl  
Simon Ott (Fraunhofer AISEC)