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

Fraunhofer AISEC

Announcement: Student Assistant in co-operation with Fraunhofer AISEC, Garching

Implementation of a Crypto Provider and Remote Attestation Tools in Java

Motivation and Task Description

Most modern computing platforms are equipped with Trusted Platform Modules (TPMs). They can be used for securing communication channels, such as Transport Layer Security (TLS), by protecting the private keys used for authentication. Furthermore, they can be utilized to establish trust in communication partners through providing cryptographic verification of the software stack running on the device.

In previous projects, a Proof of Concept (PoC) has been implemented in different programming languages (Rust, Go). Now, we are looking for one or more students for implementing a cryptographic provider to interact with the TPM, and tools for verifying software stacks, in the Java programming language.

Requirements

- High motivation and ability to work independently
- Good programming skills in Java
- At least basic knowledge of cryptographic primitives

Contact

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

Monika Huber
Telefon: +49 89 322-9986-148
E-Mail: monika.huber@aisec.fraunhofer.de

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