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

Fraunhofer AISEC

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

Implementation of Remote Attestation Tools and a Crypto Provider in Rust or Java

Motivation and Task Description

Remote Attestation is the process of assessing the trustworthiness of a remote computing platform through verifying the integrity of its software stack. Several hardware-based technologies enable remote attestation, such as Trusted Platform Modules (TPMs) or Confidential Computing (CC) technologies (e.g., AMD SEV, Intel SGX).

In previous projects, a generic attestation framework has been implemented as a Proof of Concept (PoC) in Go. Now we are looking for one or more students for implementing and extending this framework in either Rust or Go, for usage in different computing environments.

Requirements

- High motivation and ability to work independently
- Good programming skills in either Rust or 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