Chair of IT Security
Prof. Dr. Claudia Eckert

Fraunhofer AISEC

Announcement: Research Assistant (HiWi) in Cooperation with Fraunhofer AISEC, Garching

Implementing a Secure Attestation Protocol in Rust

IDSCP is a secure transport protocol which builds on top of TLS to ensure confidentiality, integrity and authenticity of the communication channel is. Beyond those basic security goals, it additionally provides establishment of mutual trust in the software stack running on the communication peers. This is done by utilizing a *Trusted Platform Module (TPM)* and algorithms for *Remote Attestation*. The protocol ensures that data is only transmitted, if the receiving peer can prove to be running on a system with a valid software stack (incl. bootloader, hypervisor, OS, applications).

At Fraunhofer AISEC we develop a library for IDSCP using *Rust* – a modern, security-focused programming language. For exchange of control messages we are using Google's *Protobuf* message format.

Task Description

For this student job, you will be fully included into the development process of the IDSCP Rust library. Because the software architecture is highly modular, there are different tasks which you may contribute to – depending on your interest and skills, e.g.,

- Development of the libraries core components (e.g. the protocol's state machine, message formats, API design)
- Design and/or implementation of new features and security extensions
- Interaction of Rust software with Trusted Platform Modules (TPM)

Requirements

For this job you should bring initial experience with Rust and Google's Protobuf – or strong interest in learning it. You enjoy a self-driven work ethic, have fun experimenting and contribute new ideas from your learnings.

Contact

Oliver Braunsdorf
Fraunhofer Institute for Applied and Integrated Security AISEC
Lichtenbergstraße 11, 85748 Garching
Mail: oliver.braunsdorf@aisec.fraunhofer.de
Phone: +49-89-3229986-161