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

The Industrial Data Space Communication Protocol (IDSCP) is a TLS-based protocol, that employs **remote attestation** to ensure integrity, authenticity and trustworthiness of the communication peers. It is used to send user data together with custom data usage policies and other arbitrary metadata.

Task Description

The main task is to **implement a lightweight version of the IDSCP client in the Rust programming language**, that is efficient enough to be runnable on embedded linux devices. Within the scope of this re-implementation, an improved version of the protocol *IDSCP 2.0* will be designed to adapt to recent use cases. Therefore, the tasks that this job offers include one or more of the following tasks depending on your interest:

- Build a new code base from scratch in Rust, a modern security-focused programming language
- Contribute to protocol design decisions
- Establish a productive build and test environment (e.g. using Gitlab CI/CD)

Requirements

Applicants for this job should at least provide initial experience with the Rust programming language and it's ecosystem (`https://crates.io/`, cargo, etc.). Optionally helpful would be experiences with Google's Protobuf (`https://developers.google.com/protocol-buffers/`) as well as basic knowledge in applied cryptography and communication protocol design.

Contact

Oliver Braunsdorf
Fraunhofer Institute for Applied and Integrated Security AISEC
Parkring 4, 85748 Garching
Mail: oliver.braunsdorf@aisec.fraunhofer.de
Phone: +49-89-3229986-161