Fraunhofer AISEC

Announcement: Research Assistant (HiWi)
In cooperation with Fraunhofer AISEC, Garching

Microcontroller Programming with Rust and TrustZone

Motivation and Topic

At the department of Secure Operating Systems of Fraunhofer AISEC, we push new ideas for the development of system software, which includes software that runs directly on top of a processor or microcontroller. We want to explore new research approaches for creating secure system software by combining the safety guarentees of hardware-based isolation mechanisms like ARM TrustZone together with Rust - a modern programming language, designed with strong focus on security and performance comparable to C/C++. A possible demonstrator case can be, e.g., a secure key storage implemented on an ARM-Cortex M33 microcontroller. Possible tasks for students can include one or more of the following – depending on interest and skills:

- Bare-metal programming with TrustZone-M in Rust
- Evaluate new Rust-based research operating systems, e.g.,
  - TockOS (https://www.tockos.org/)
  - DroneOS (https://www.drone-os.com/)
- Explore and evaluate different OS architectures (Microkernel, Unikernel, Exokernel)
- Develop new programming patterns to securely setup isolation domains

The monthly working time for research assistants is 40 hours but can be de-/increased on request.

Requirements

- Experience or at least interest in learning the Rust programming language.
- Some basic knowledge of the C programming language might be a plus.
- First experiences with programming a microcontroller.
- Experience or at least interest in learning about ARM's TrustZone technology.
- Self-driven and goal-oriented work ethic.
- Fluency in German or English.

Contact

Oliver Braunsdorf
Mail: oliver.braunsdorf@aisec.fraunhofer.de
Phone: +49-89-3229986-161
Fraunhofer Research Institute AISEC
Secure Operating Systems Department
Lichtenbergstraße 11, 85748 Garching (bei München)