



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



Announcement: Student job (HiWi) in cooperation with Fraunhofer AISEC, Garching

# Attacks on Trusted Execution Environments

## Job Description

We currently have an opening for a research assistant position. The position includes familiarization in the Trusted Execution Environment (TEE) topic such as Intel SGX, ARM TrustZone and SEV as well as evaluation of attacks against TEEs. The monthly working time is 40 hours, but can be increased on request. Tasks include:

- Implementation of attacks against TEEs
- Comparison of different TEEs
- Evaluation of new attacks against TEEs

## Area of work

You will get in touch with the following topics:

- Trusted Execution Environments, such as Intel SGX, ARM TrustZone and AMD SEV
- Operating System basics
- Programming in C(++)
- Scripting in Bash/Python

Existing in-depth knowledge in any of the areas is not required. Generation of own ideas is desired and creative work is encouraged. If desired and applicable a follow-up thesis topic can be provided.

## Contact

Fraunhofer Institute for Applied and Integrated Security (AISEC)

Mathias Morbitzer

Email: [mathias.morbitzer@aisec.fraunhofer.de](mailto:mathias.morbitzer@aisec.fraunhofer.de)

Phone: +49 89 322-9986-164