Chair of IT Security
Prof. Dr. Claudia Eckert

Student Assistant (m/f/)*

Formal Verification of TPM Functions

Trusted Platform Modules (TPMs) are cryptoprocessors that are widely used in modern systems. They are responsible for security-critical functionalities such as storing cryptographic keys and using them for cryptographic operations or serving as a root of trust to assess platform integrity. It is therefore crucial that the software that runs inside TPMs adheres to the TPM specification and does not suffer from vulnerabilities that allow a potential attacker to compromise the security guarantees that TPMs are meant to offer.

Task Description

The goal of this work is to establish formal guarantees of the correctness of a TPM implementation. Representative functionality from the TPM 2.0 reference implementation shall be formally verified against (the most) relevant parts of the TPM 2.0 specification. Suitable tooling might include the Verified Software Toolchain or RefinedC.

Requirements

- Interest in writing high-assurance, formally verified software
- Fundamentals of low-level systems programming (from IN0009)
- Fundamentals of functional verification (from IN0003)
- Proficiency with a proof assistant such as Isabelle/HOL or Coq is not mandatory but may be necessary to obtain as part of the project

Contact

Please send your application with current CV and transcript of records to:

Patrick Herter
Secure Operating Systems
Mail: patrick.herter@aisec.fraunhofer.de
Phone: +49 89 322 9986-1058

Johannes Wiesböck
Secure Operating Systems
Mail:
johannes.wiesboeck@aisec.fraunhofer.de
Phone: +49 89 322 9986-1046

Fraunhofer Institute for Applied and Integrated Security (AISEC)
Lichtenbergstr. 11, 85748 Garching near Munich

Publication Date: 09.09.2024