Bachelor and Master Project / Bachelor- und Masterarbeit

A New Design of Hardware Root of Trust: OpenTitan-based

Introduction: In any modern computing platform, the root of trust (RoT) usually is a combination of hardware and software prices that manages and controls the platform secrets and provides the cryptographic functions with required secret keys. RoT is not only a secure storage but also includes unique ID and certificates. Lately, several studies show the need for pure hardware RoT that exhibits a high security level and efficient performance compering with the traditional RoT. Following these studies, GOOGLE together with several industrial companies and research institutes announced OpenTitan as a first open source framework for building a silicon root of trust (RoT).
This project aims to show how to build a hardwired function as a key generation and integrate such a function into OpenTitan framework. The resulting Rot will be investigated and analyzed based on several security aspects.

Project Plan: The work plan contains three steps as follow:

1) Studying and review the recent RoT.
2) Deigning a hardwired function as a key generation.
3) Integrating the designed function into OpenTitan framework.
4) Implementing the resulting RoT on System-on-Chip (SoC) and check the complexity.

Applications of the research results:
Jupiter Project.

Prerequisites/Requirements: Students should have good background in security, and they should be interested in hardware-implementations.

Starting Date: To be agreed on with the interested party.

Interested students are kindly asked to contact:

- **Instructor and adviser**: Saleh Mulhem, mulhem@iti.uni-luebeck.de
- **Supervisor:** Prof. Dr-Ing, Mladen Berekovic.

Institut für Technische Informatik,
Gebäude 64, 2. Stock,
Universität zu Lübeck
Ratzeburger Allee 160,
23562 Lübeck.