Bachelor and Master Project / Bachelor- und Masterarbeit

Secure RISC-V Processor: Design and Implementation

Introduction: RISC-V is an open-source instruction set architecture (ISA) using reduced instruction set computer principles. This instruction set is considered an abstract model describing computer components. For instance, certain instructions of RISC-V lead to the implementation and realization of a specific Central Processing Unit (CPU). Recently several vendors have started using RISC-V. The number of products using the RISC-V CPU core is expected to be 62.4 billion by 2025. Therefore, investigating the security aspects of RISC-V together with developing a threat model is in high demand.
This project will illustrate the vulnerabilities of the control flow of RISC-V against current attacks. Then, it will show how to develop a hardware root of trust and use it as an essential countermeasure to protect RISC-V control flow. This project aims to develop a secure RISC-V processor by deploying the principles of "Security by Design".

Research Objectives: The work plan contains four steps as follow:

1) Studying and reviewing the possible well-known attack scenarios on RISC-V.
2) Studying current countermeasures to RISC-V..
3) Devising a hardware root of trust and use it as a source of trust for the processor.
4) Implementing the designed RISC-V and compare it with the state-of-art RISC-V cores, from the security and efficiency perspectives .

Applications of the research results:
Jupiter project.

Prerequisites/Requirements: Students should have good background in processor design or 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.