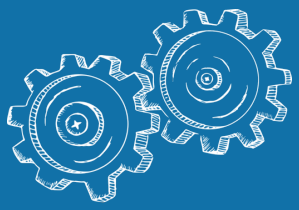

Building Secure CPUs/Compilers

Advisor: **Pascal Nasahl, Robert Schilling, Stefan Steinegger**

Motivation

CPUs typically do not offer a lot of protection once potential attackers find software bugs like buffer overflows and thus can tamper with pointer addresses or memory contents. The story is similar in case of embedded devices where side-channel attacks or fault attacks can be used to extract sesitive information or to take over the control of the program flow.

One major research focus of the SESYS group is the design of security extensions deeply embedded into computer architectures. Here, we are using a combination of hardware and software features to protect against concrete attacks. Typically, we are integrating and analyzing the countermeasures using an open-source RISC-V platform. In the past, we developed several countermeasures:

1. Hardware based control-flow protection unit [1].
2. RAM Encryption and Authentication Scheme [2].
3. Secure Memory Access Scheme with Pointer Encoding [3].

If you are interested in extending computer architectures, designing cryptographic hardware accelerators or integrating security features into a compiler, just talk to us. We can arrange several, individual master projects or theses.

Goals and Tasks

- Contact us for discussing possible topics and scope.
- Read literature to acquire the necessary background.
- Design/Implement/Attack/Protect/Verify.
- Write/Present your Master project/thesis.

Literature

- M. Werner et al.
  Sponge-based control-flow protection for iot devices
- M. Werner et al.
  Transparent memory encryption and authentication
- R. Schilling et al.
  Pointing in the right direction-securing memory accesses in a faulty world

Schedule

- Reading related work and first steps
- Intermediate presentation or poster
- Implementing, experiments, …
- Writing thesis
- Final presentation

Recommended if you're studying

☒ CS ☒ ICE ☒ SEM

Prerequisites

- Interest in hardware design
- Interest in cryptography
- Interest in implementation security

Advisor / Contact

pascal.nasahl@iaik.tugraz.at