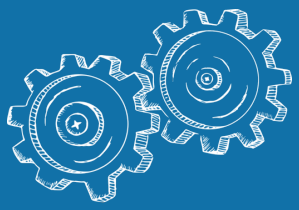

Memory Isolation & Shielded Execution

Advisor: **David Schrammel**

Motivation

Software bugs (like buffer overflows) or insufficient isolation of potentially malicious software can compromise the entire security of a system. Traditional process-based isolation is often too slow, or doesn't protect against malicious operating systems. Intel SGX allows execution of confidential code within untrusted environments. Other techniques (e.g., Software Fault Isolation) can execute untrusted software in an isolated environment. There also exist other techniques [1, 3, 4] to achieve a more fine-grained and more efficient isolation.

In the context of this work, you can explore how to leverage new hardware mechanisms to allow more efficient software sandboxing. You can also design your own proposed hardware changes, as an extension for the RISC-V ISA.

If you are interested in this topic area, or if you already have own ideas related to software- and system security, just contact us! We can arrange individual projects/theses based on your interests.

Goals and Tasks

- Contact us for discussing possible topics and scope.
- Get familiar with existing work.
- Design/Implement/Experiment
- Write/Present your project/thesis.

Literature

- S. Weiser et al.
  TIMBER-V: Tag-Isolated Memory Bringing Fine-grained Enclaves to RISC-V
- D. Lee et al.
  Keystone: An Open Framework for Architecting TEEs
- D. Schrammel et al.
  Donky: Domain Keys - Efficient In-Process Isolation for RISC-V and x86
- S. Narayan et al.
  Retrofitting Fine Grain Isolation in the Firefox Renderer

Courses & Deliverables

- ☑ **Introduction to Scientific Working**
  Short report on background
  Short presentation
- ☑ **Bachelor Project**
  Project code and documentation
- ☑ **Bachelor's Thesis**
  Project code
  Thesis
  Final presentation

Recommended if you're studying

☑ CS ☑ ICE ☑ SEM

Prerequisites

- Interest in the topic area

Advisor / Contact

david.schrammel@iaik.tugraz.at