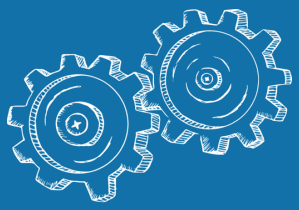


Transient Execution Attacks in Various Programming Languages

Advisor: **Martin Schwarzl**

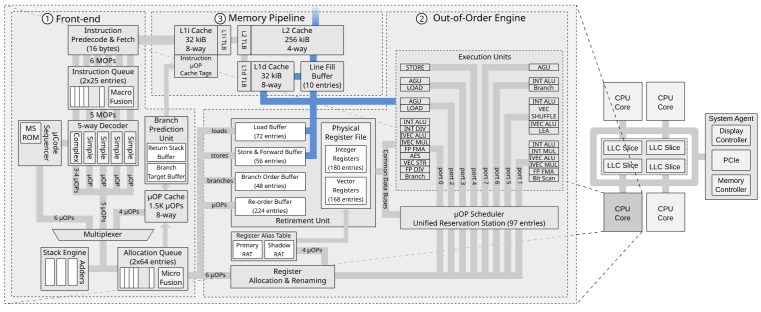
Motivation

Speculative execution and out-of-order executions are crucial components of every processor. Since the discovery of Meltdown [2] and Spectre [1] various further attacks have been found.

So far all of the exploits have been demonstrated in native code languages(C/C++) and JavaScript. The aim of this thesis is to verify whether further compiled,interpreted and just-in-time compiled programming languages are also susceptible to transient execution attacks i.e. Haskell,Java,C#,Rust,Go or Python.

Goals and Tasks

- Get familiar with existing transient execution attacks
- Implement variants of those attacks in different programming languages
- Check real-world software for Spectre gadgets
- Perform and evaluate experiments



The Intel x86 Skylake microarchitecture (diagram by Stephan van Schaik)

Literature

- P. Kocher et al.
  Spectre Attacks: Exploiting Speculative Execution
  S&P
- M. Lipp et al.
  Meltdown: Reading Kernel Memory from User Space
  USENIX Security Symposium

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

- C/C++
- Basic assembly programming (any of x86/ARM/RISC-V)
- Prior knowledge of CPU architecture is useful, but not essential!

Advisor / Contact

martin.schwarzl@iaik.tugraz.at