Transient Execution Emulator

Meltdown and Spectre Behind the Scenes

Felix Betke, Lennart Hein, Melina Hoffmann, Jan-Niklas Sohn

04-01-2022

Rheinische Friedrich-Wilhelms-Universität Bonn

Structure

- Topic
- Background
- Our task
- Our approach
- Backend
- Demo
- Conclusion

Topic

- Meltdown and Spectre mostly patched
- Difficult to experiment with
- Goal: Vulnerable CPU Emulator that runs on many systems

Background

CPU

- Frontend:
  - Fetches/Decodes instructions, maintains queue
  - Branch prediction
- Execution Engine:
  - Multiple sets of execution units
- Memory Subsystem:
  - Handles memory operations
  - Maintains L1 cache

Out-of-order execution

- Independent instruction streams
- Reservation stations
- Common Data Bus

Speculative execution

Meltdown

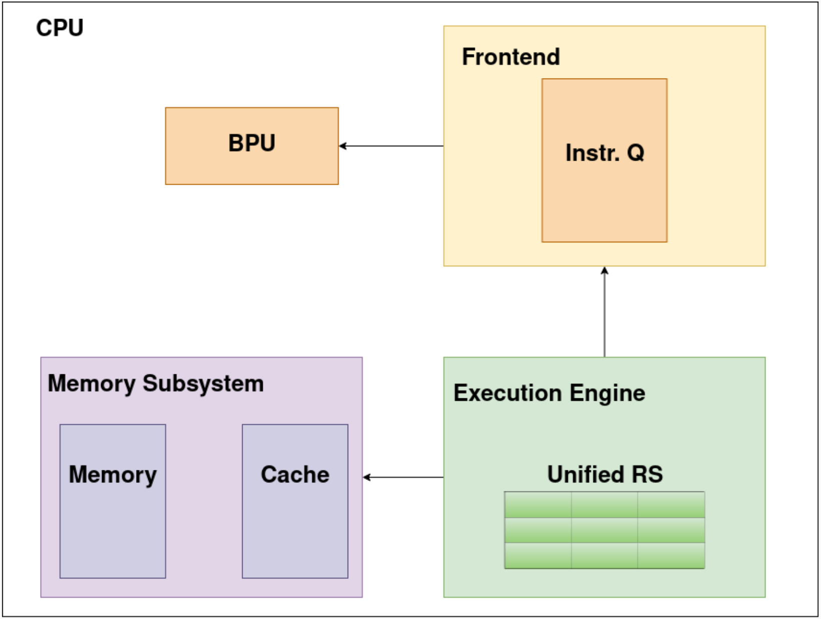
Spectre

Mitigations

Our task

Our approach

Our version


CPU
Frontend
BPU
Instr. Q
Memory Subsystem
Memory
Cache
Execution Engine
Unified RS

References

- Abbildung auf Folie 10 modifiziert von Abbildung 3.1 in:
  - Gruss, Daniel: „Transient-Execution Attacks“, 2020, URL: https://gruss.cc/files/habil.pdf (besucht am 15.01.2021)