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

UNIVERSITÄT **BONN**

Structure

- Topic

- Background

- Our task

- Our approach

- Backend

- Demo

- Conclusion

- Meltdown and Spectre mostly patched

- Difficult to experiment with

- Goal: Vulnerable CPU Emulator that runs on many systems

Background

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

- Independent instruction streams

- Reservation stations

- Common Data Bus

Speculative execution

Mitigations

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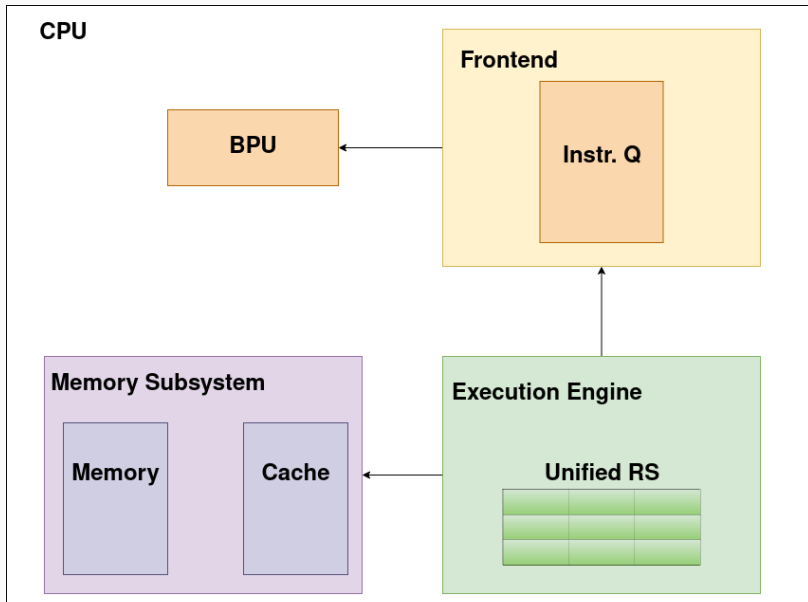
- Abbildung auf Folie 10 modifiziert von Abbildung 3.1 in:
  - Gruss, Daniel: „Transient-Execution Attacks", 2020, URL: https://gruss.cc/files/habil.pdf (besucht am 15.01.2021)