Microarchitectural Attacks

Project #1 - Hardware Security 2025

Project Goal

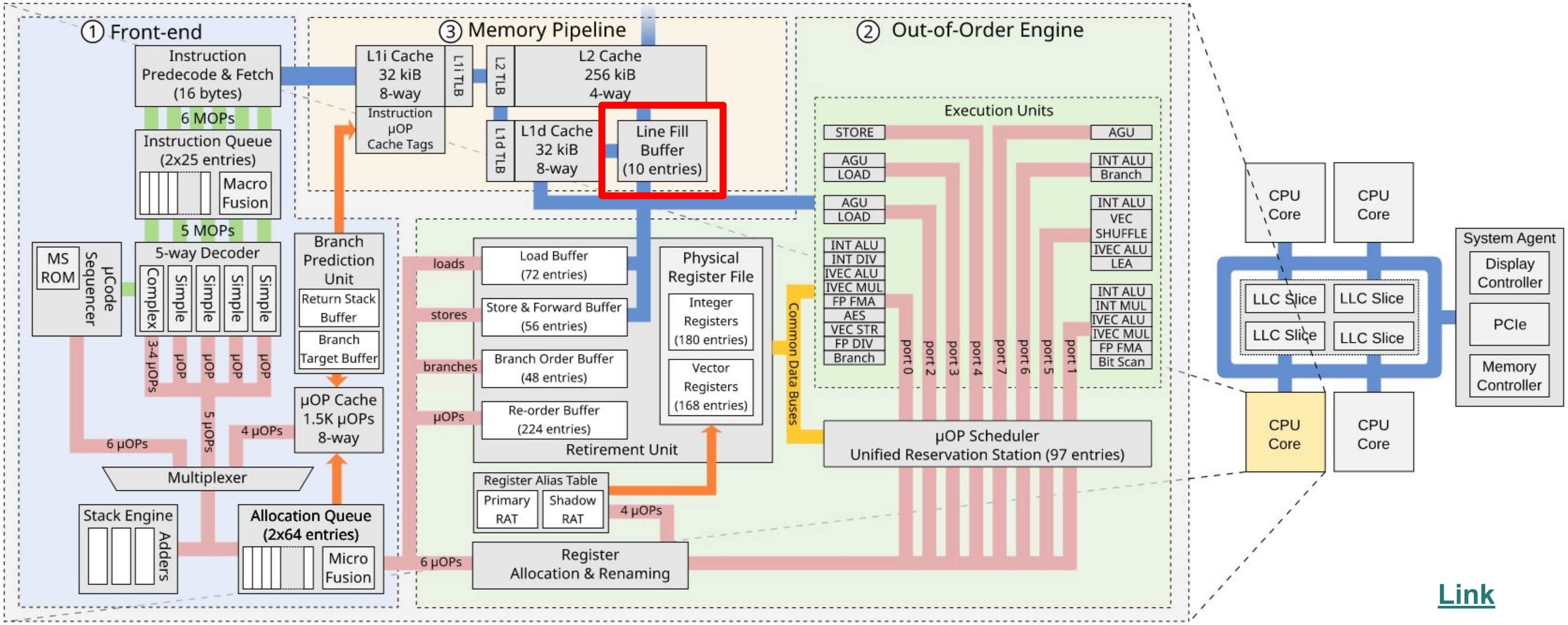
- Understand in depth how **three** internal CPU components work

- Understand how certain microarchitectural design decisions can lead these components to leak sensitive information.

- Understand how an attacker can leak this information through side-channels compromising the entire system

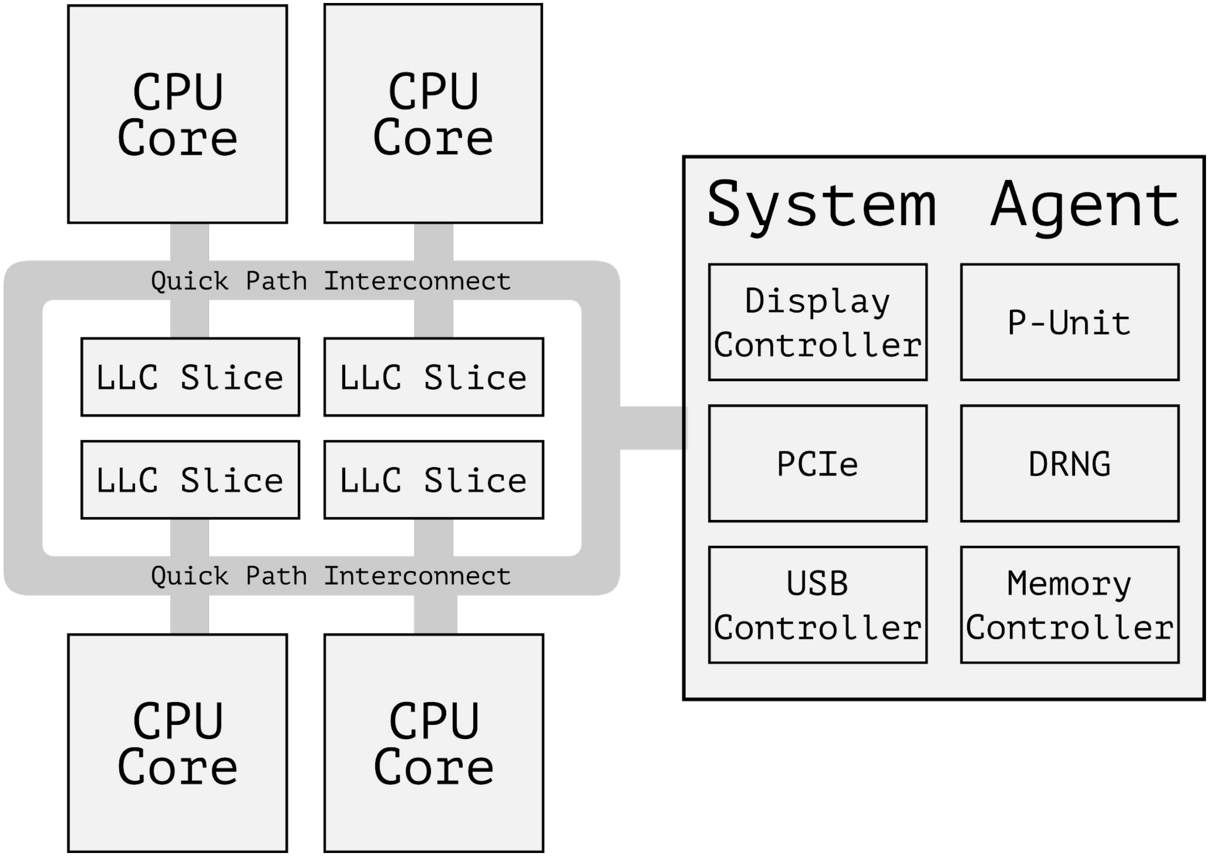
Background

RIDL: Rogue In-Flight Data Load



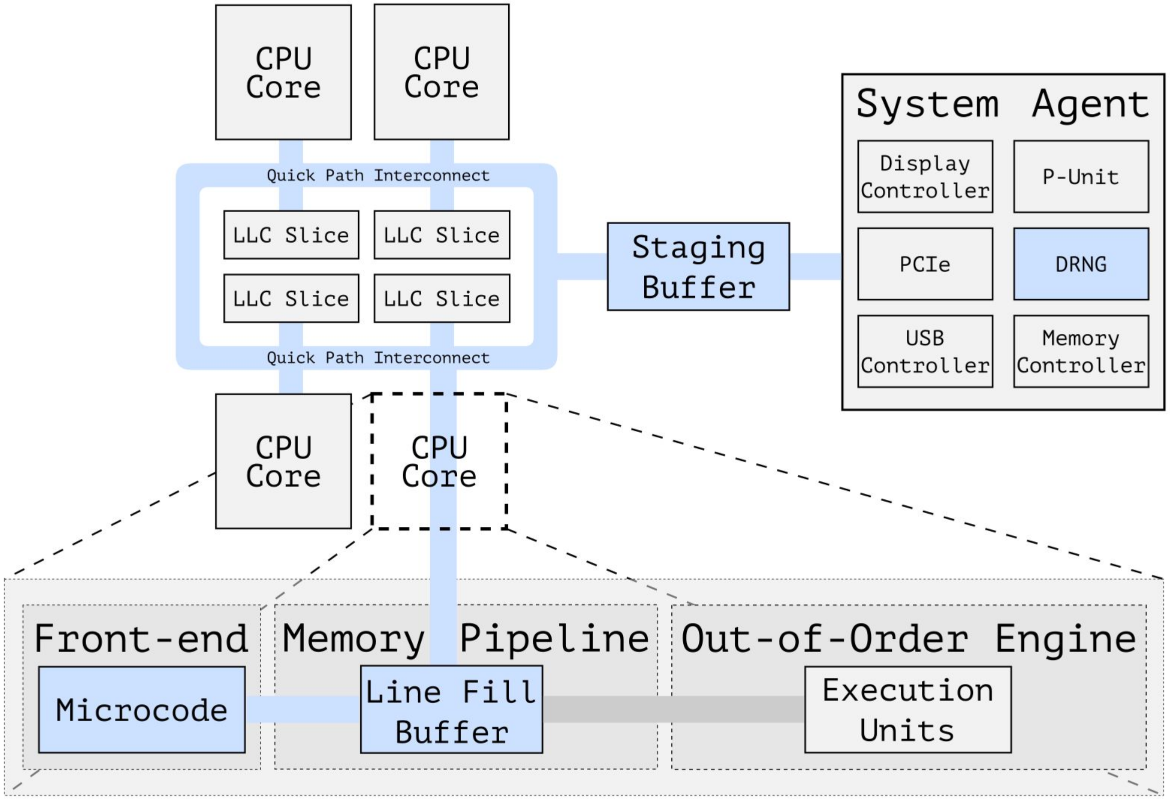
Link

Background


CPU Core
CPU Core
Quick Path Interconnect
LLC Slice
LLC Slice
LLC Slice
LLC Slice
Quick Path Interconnect
CPU Core
CPU Core
System Agent
Display Controller
P-Unit
PCIe
DRNG
USB Controller
Memory Controller

Background

CrossTalk: Speculative Data Leaks Across Cores Are Real

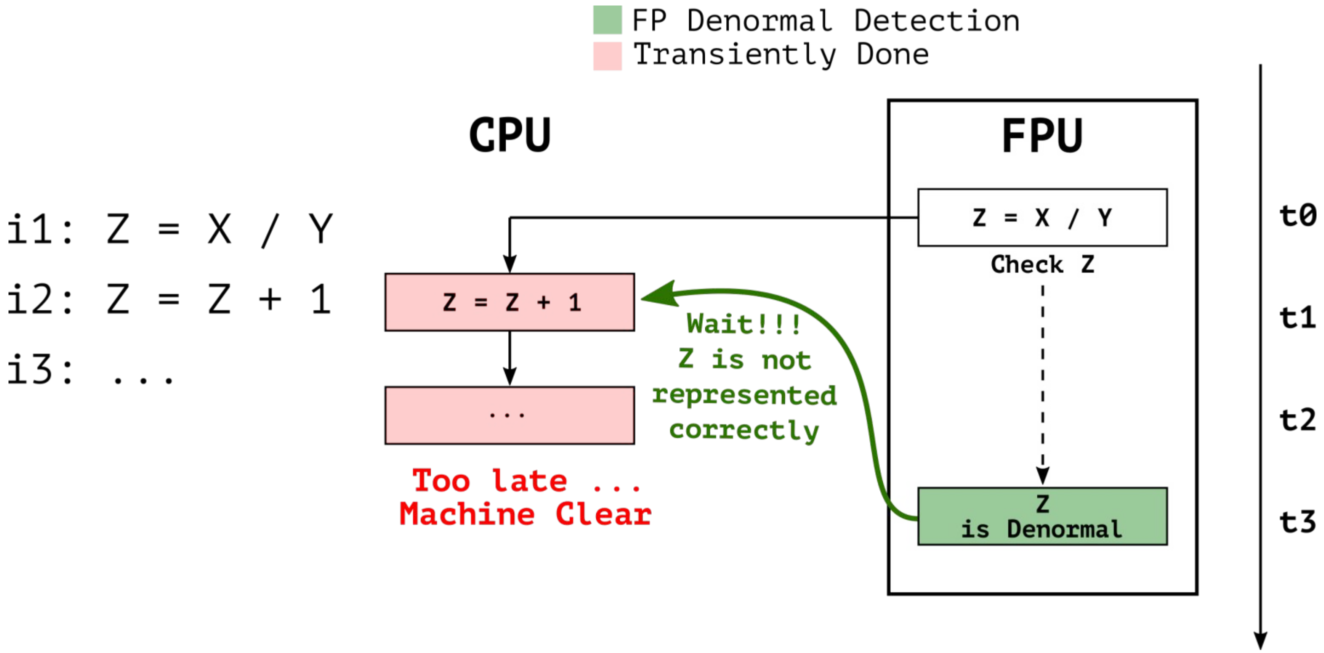


Link

Background

Rage Against The Machine Clear:

A Systematic Analysis of Machine Clears and Their Implications for Transient Execution Attacks



🟩 FP Denormal Detection
🟥 Transiently Done

```
i1: Z = X / Y
i2: Z = Z + 1
i3: ...
```

Link

The HWSec root password

X = subnormal(rdrand())

Y = subnormal(rdrand())

WEEK 1

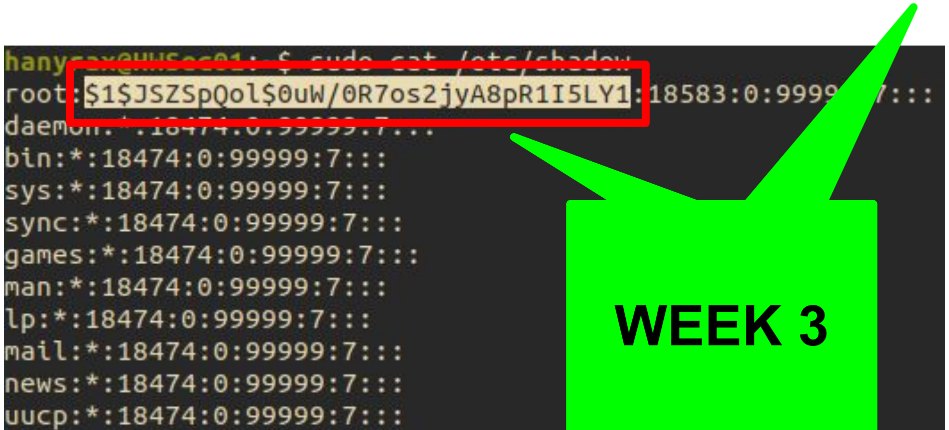
WEEK 2

$$Z = X / Y$$

Z_{tra} = 0x2a19f2c24d8932c7

Z_{arc} = 0xffff128770ce1baf

$$\text{root\_password} = \text{2a19f2c24d8932c7}\underbrace{\text{*****}}_{\text{Crackable (Lower case \& numbers)}}$$



```
hanyrax@HWSec01:~$ sudo cat /etc/shadow
root:$1$JSZSpQol$0uW/0R7os2jyA8pR1I5LY1:18583:0:99999:7:::
daemon:*:18474:0:99999:7:::
bin:*:18474:0:99999:7:::
sys:*:18474:0:99999:7:::
sync:*:18474:0:99999:7:::
games:*:18474:0:99999:7:::
man:*:18474:0:99999:7:::
lp:*:18474:0:99999:7:::
mail:*:18474:0:99999:7:::
news:*:18474:0:99999:7:::
uucp:*:18474:0:99999:7:::
```

WEEK 3

Deadlines

- Fri, November **28nd** @ 23:59
- Fri, December **5th** @ 23:59
- Fri, December **12th** @ 23:59

Important: Weekly discussions are not graded, but you need to upload your solution on Canvas each week to access the next week's tasks (you can optimize stuff later)

Demo Day

Optionally - present your solution live!

- Deadline: December **17th**
- Short presentation: tell us what’s unique about your approach
- Have fun with it!
- Quiz, Borrel & Prizes

Questions?