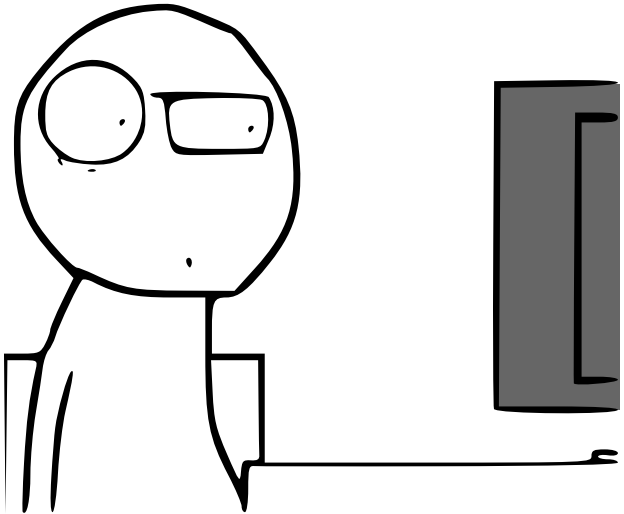
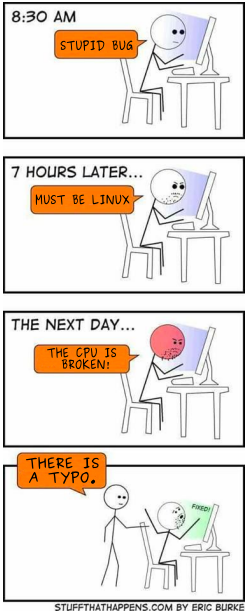
From Random Timings to Data Leakage

Michael Schwarz

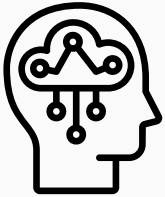
December 2022

CISPA Helmholtz Center for Information Security



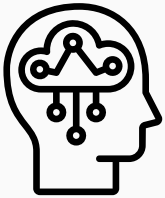

8:30 AM
STUPID BUG
7 HOURS LATER...
MUST BE LINUX
THE NEXT DAY...
THE CPU IS BROKEN!
THERE IS A TYPO.
FIXED!
STUFFTHATHAPPENS.COM BY ERIC BURKE

In-Order Execution



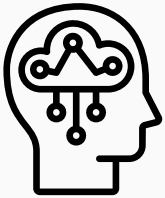
- Mental model of CPU is simple

In-Order Execution



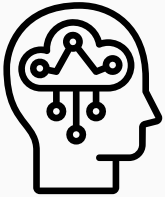
- Mental model of CPU is simple
- Instructions are executed in program order

In-Order Execution

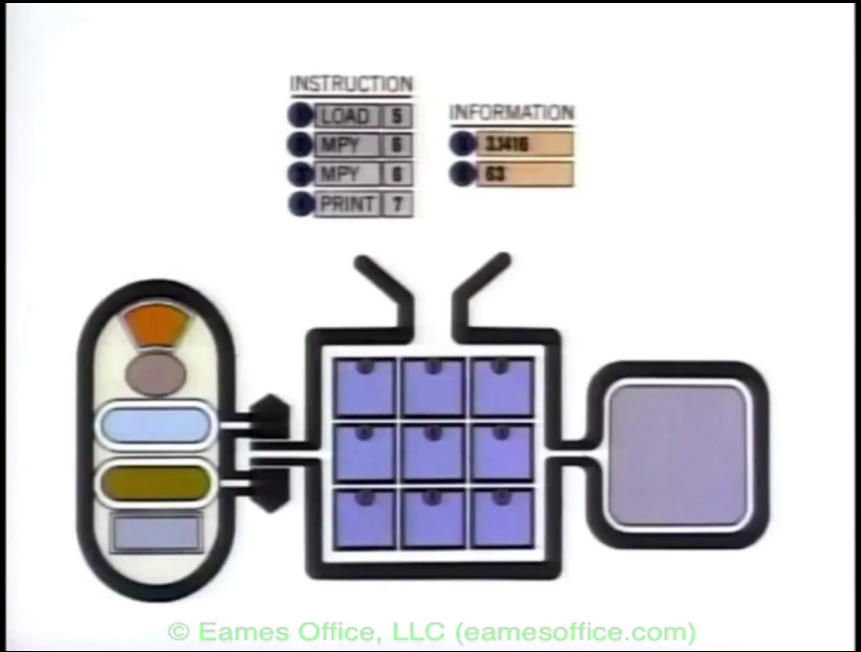


- Mental model of CPU is simple
- Instructions are executed in program order
- Pipeline stalls when stages are not ready

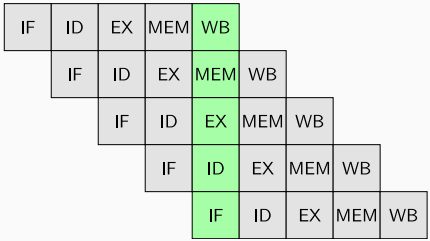
In-Order Execution



- Mental model of CPU is simple
- Instructions are executed in program order
- Pipeline stalls when stages are not ready
- If data is not cached, we need to wait

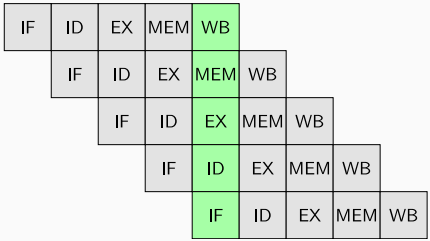


In-Order Execution



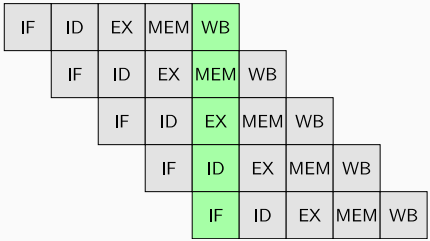
- Instructions are...

In-Order Execution



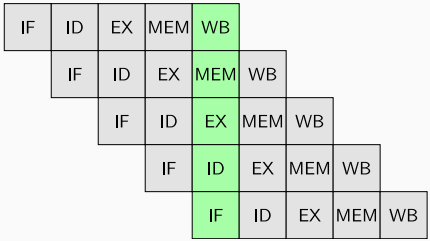
- Instructions are...
  - fetched (`IF`) from the L1 Instruction Cache

In-Order Execution



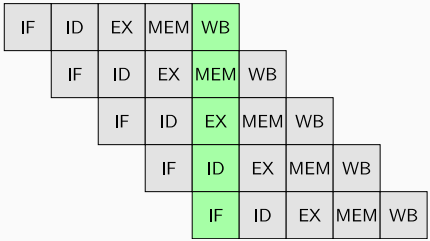
- Instructions are...
  - fetched (`IF`) from the L1 Instruction Cache
  - decoded (`ID`)

In-Order Execution



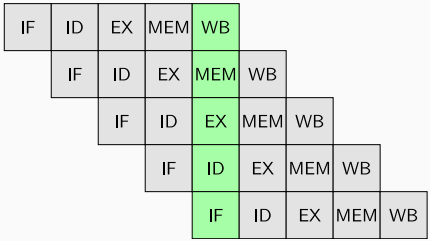
- Instructions are...
  - fetched (`IF`) from the L1 Instruction Cache
  - decoded (`ID`)
  - executed (`EX`) by execution units

In-Order Execution



- Instructions are...
  - fetched (`IF`) from the L1 Instruction Cache
  - decoded (`ID`)
  - executed (`EX`) by execution units
- Memory access is performed (`MEM`)

In-Order Execution



- Instructions are...
  - fetched (`IF`) from the L1 Instruction Cache
  - decoded (`ID`)
  - executed (`EX`) by execution units
- Memory access is performed (`MEM`)
- Architectural register file is updated (`WB`)

Measuring Time

```
x = y + 1
```

Measuring Time

```
start = ⏱
  x = y + 1
end = ⏱
```

Measuring Time

```
start = ⏱
  x = y + 1
end = ⏱
Δ = end - start
```

Measuring Time

```
start = ⏱
  x = y + 1
end = ⏱
Δ = end - start
```

1. run: Δ = 302

Measuring Time

```
start = ⏱
  x = y + 1
end = ⏱
Δ = end - start
```

1. run: $\Delta = 302$
2. run: $\Delta = 54$

Measuring Time

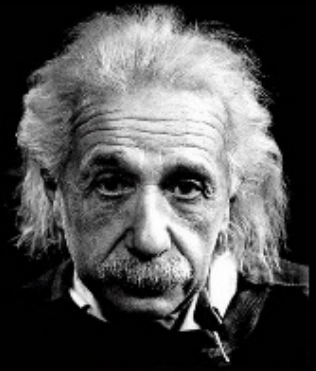
```
start = ⏱
  x = y + 1
end = ⏱
Δ = end - start
```

1. run: $\Delta = 302$
2. run: $\Delta = 54$

Determinism?

Same code with **different** execution time **without** changes

Insanity: doing the same thing over and over again and expecting different results.



Albert Einstein

Measuring Time

```
start = ⏱

end = ⏱
```

Measuring Time

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

```
start = ⏱
```

```
end = ⏱
Δ = end - start
```

Measuring Time

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

```
start = ⏱
```

1. run: Δ = 12

```
end = ⏱
Δ = end - start
```

Measuring Time

```
start = ⏱
```

```
end = ⏱
```

```
Δ = end - start
```

1. run: $\Delta = 12$
2. run: $\Delta = 12$

Measuring Time

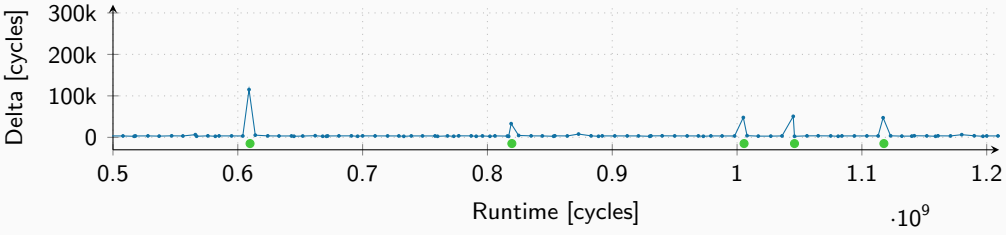
CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

```
start = ⏱
```

```
end = ⏱
```

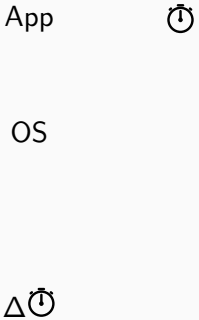
```
Δ = end - start
```

1. run: Δ = 12
2. run: Δ = 12

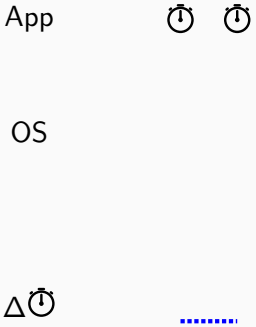



I HAVE NO
IDEA WHAT
I'M DOING

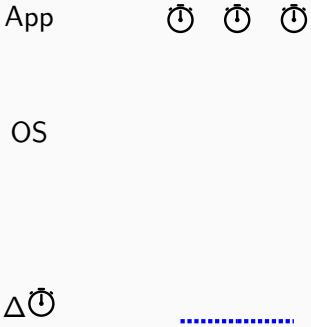
Interrupts!



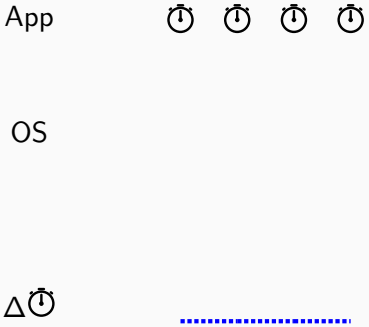
Interrupts!



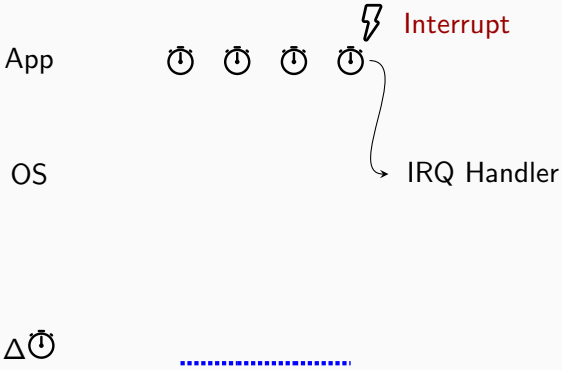
Interrupts!



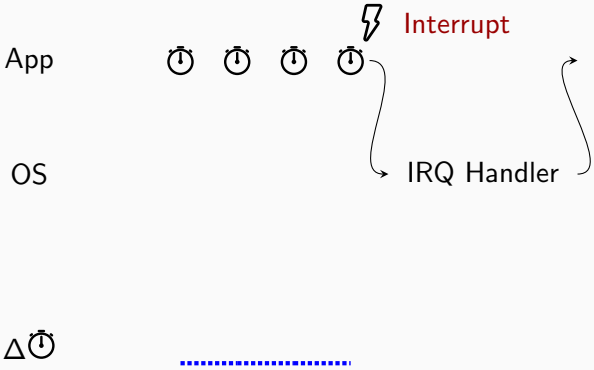
Interrupts!



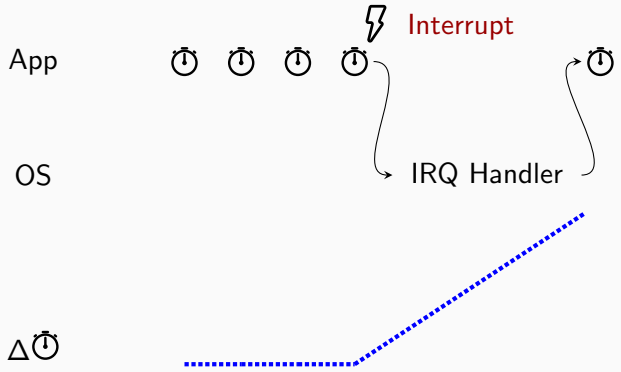
Interrupts!



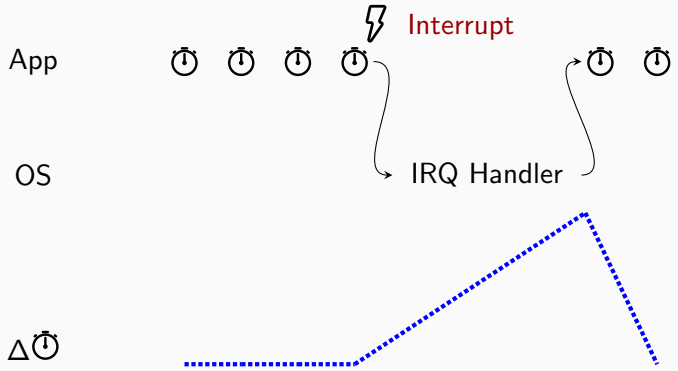
Interrupts!



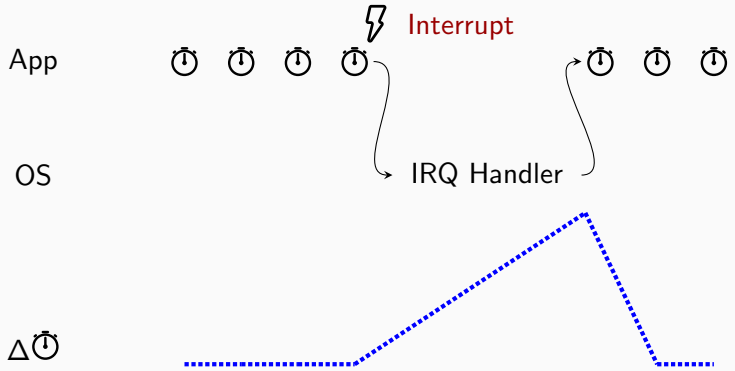
Interrupts!



Interrupts!



Interrupts!




Why?
Why?
Why?
Oh, that's why.

Interrupt-timing Attacks

```
int now = rdtsc();
while (true) {
  int last = now;
  now = rdtsc();
  if ((now - last) > threshold) {
    reportEvent(now, now - last);
  }
}
```

Interrupt-timing Attacks

```
int now = rdtsc();
while (true) {
  int last = now;
  now = rdtsc();
  if ((now - last) > threshold) {
    reportEvent(now, now - last);
  }
}
```

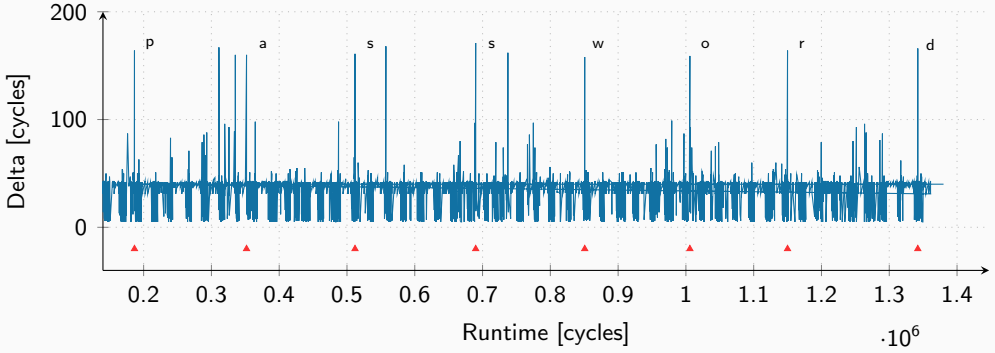
- Continuously acquire high-resolution timestamp

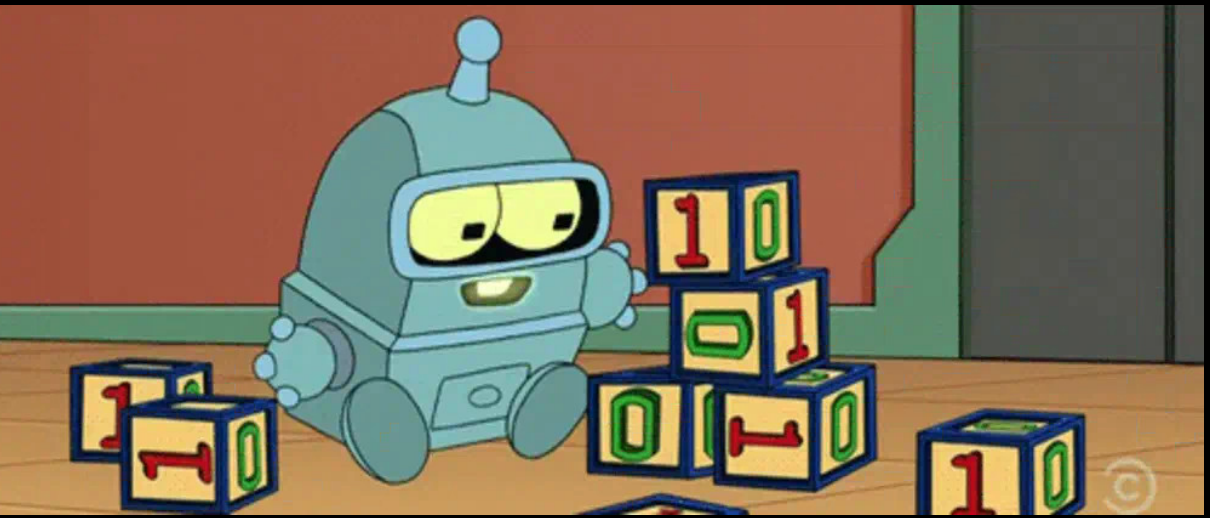
Interrupt-timing Attacks

```
int now = rdtsc();
while (true) {
  int last = now;
  now = rdtsc();
  if ((now - last) > threshold) {
    reportEvent(now, now - last);
  }
}
```

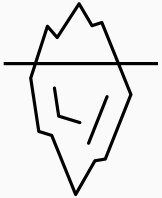
- Continuously acquire high-resolution timestamp
- Interrupt $\rightarrow$ large difference between timestamps

Interrupt-timing Attacks




1 0
0 1
0 1 0
1 0
1 0

Is that everything?



- Explains last experiment...
- ...but what about the simple calculation?
- Noise?

Data Location

- Memory operations have different runtimes

Data Location

- Memory operations have different runtimes
- Depends where the data is located

Data Location

- Memory operations have different runtimes
- Depends where the data is located
  - → Loading from cache: fast

Data Location

- Memory operations have different runtimes
- Depends where the data is located
  - → Loading from cache: fast
  - → Loading from memory: slow

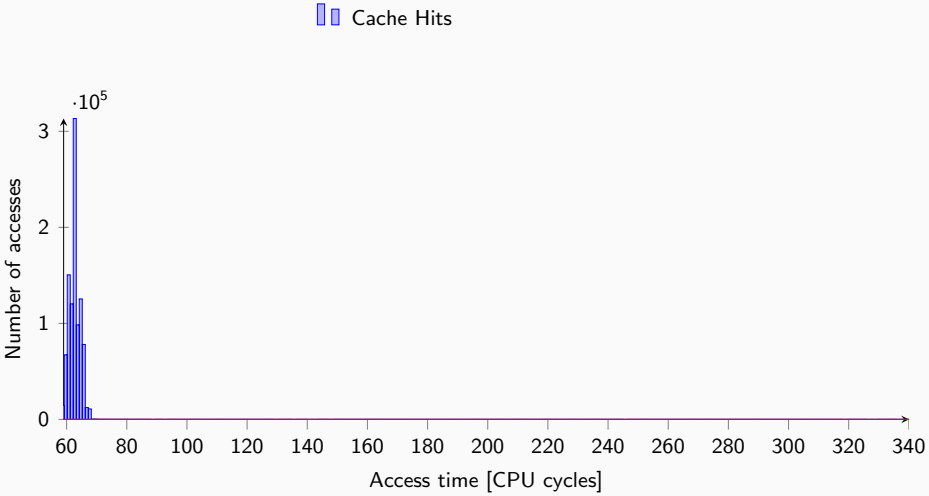
Data Location

- Memory operations have different runtimes
- Depends where the data is located
  - → Loading from cache: fast
  - → Loading from memory: slow
  - → Loading from disk: extremely slow

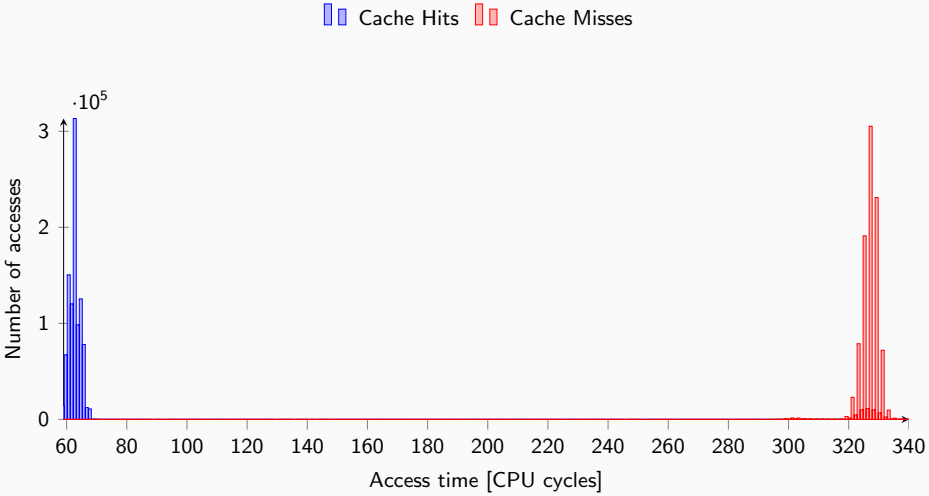
Data Location

- Memory operations have different runtimes
- Depends where the data is located
  - → Loading from cache: fast
  - → Loading from memory: slow
  - → Loading from disk: extremely slow
- Can also be measured

Caching Speeds-up Memory Accesses

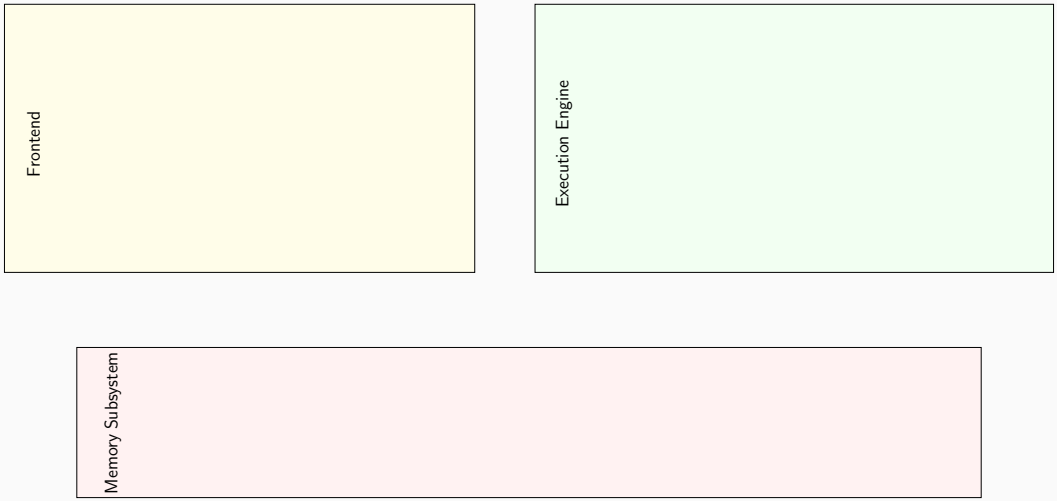


Caching Speeds-up Memory Accesses

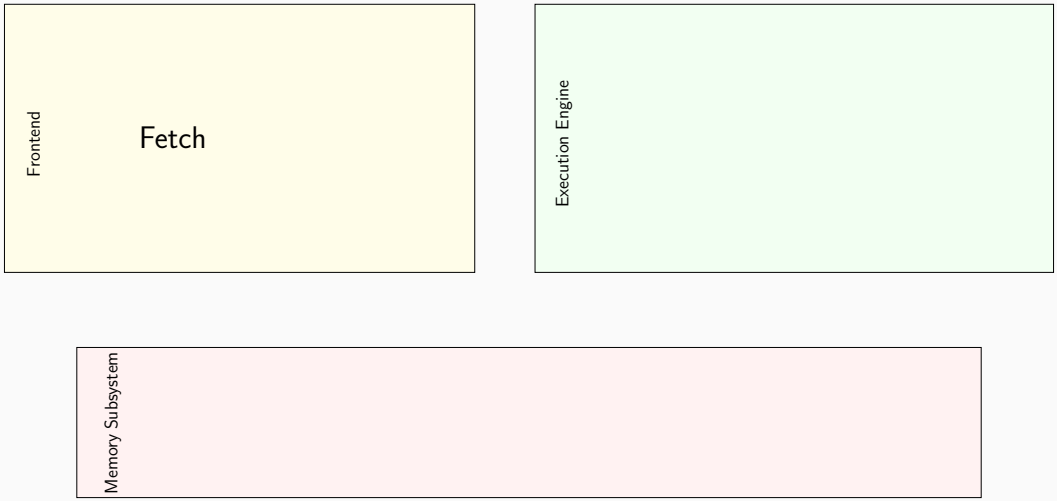



IS MY MENTAL MODEL OF THE CPU WRONG?
NO, IT MUST BE THE MEASUREMENTS THAT ARE WRONG
imgflip.com

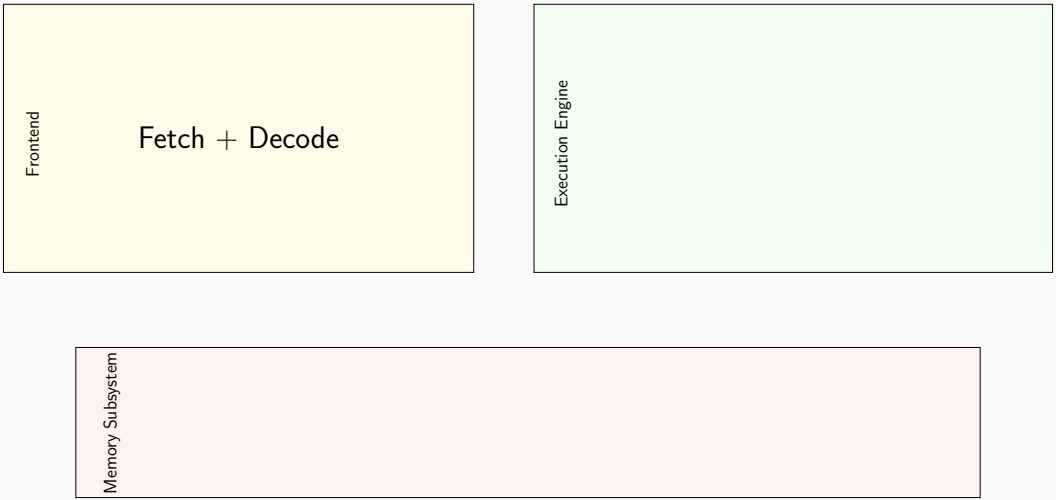
Reality: (Simplified) Modern CPU



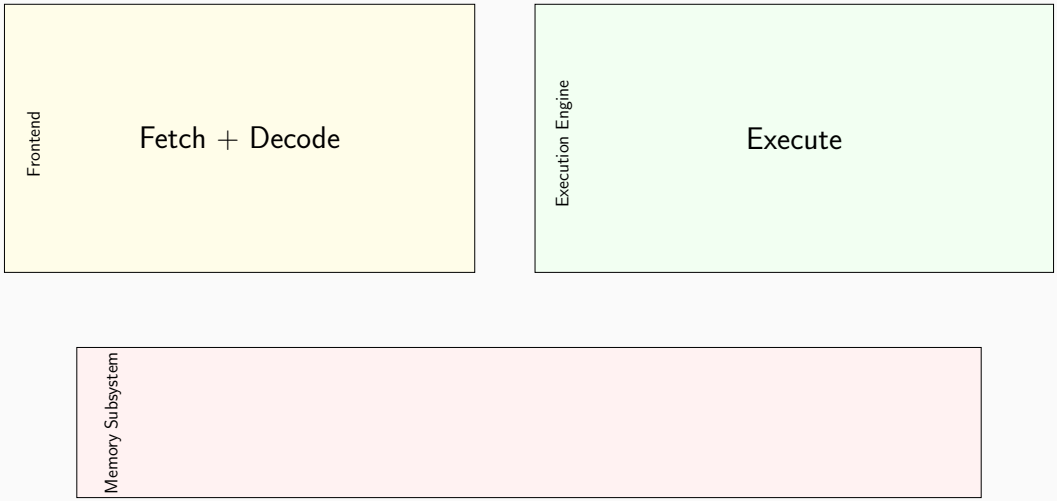
Reality: (Simplified) Modern CPU



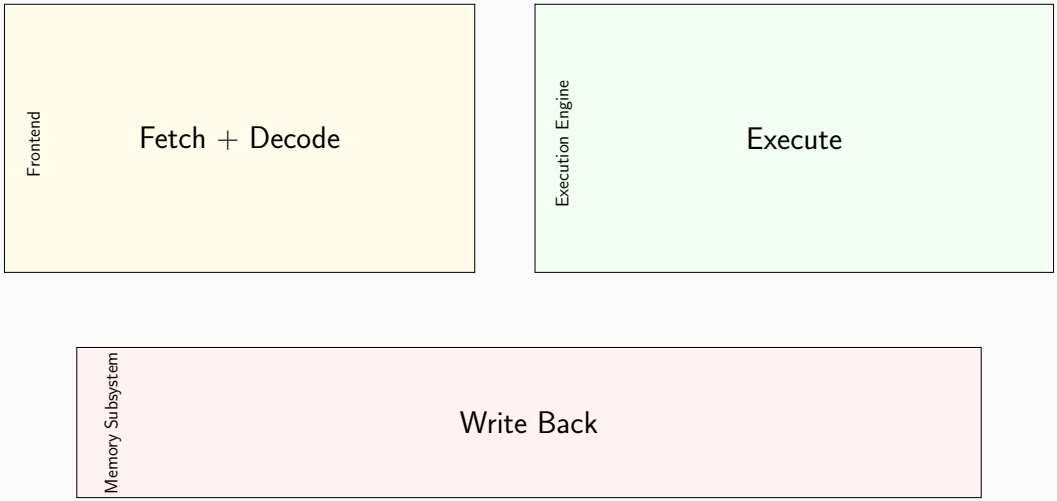
Reality: (Simplified) Modern CPU



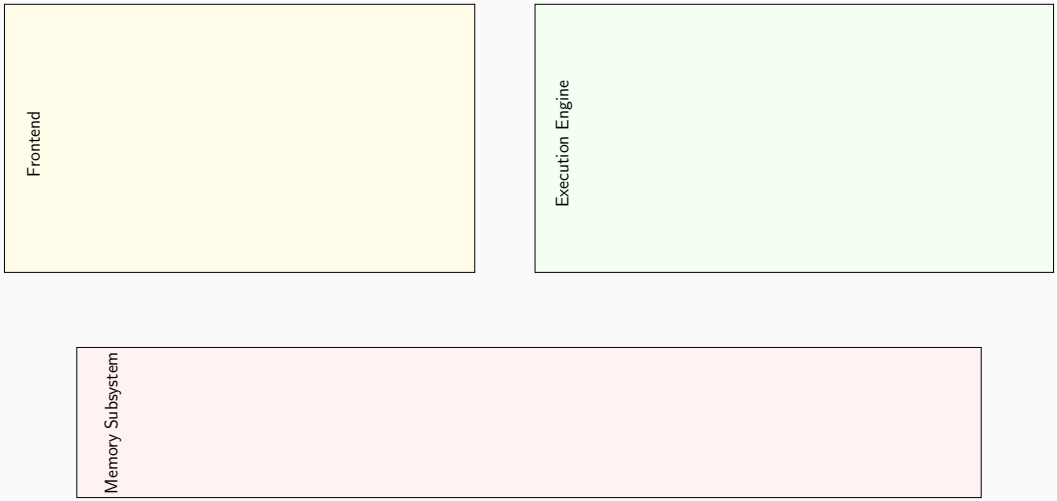
Reality: (Simplified) Modern CPU



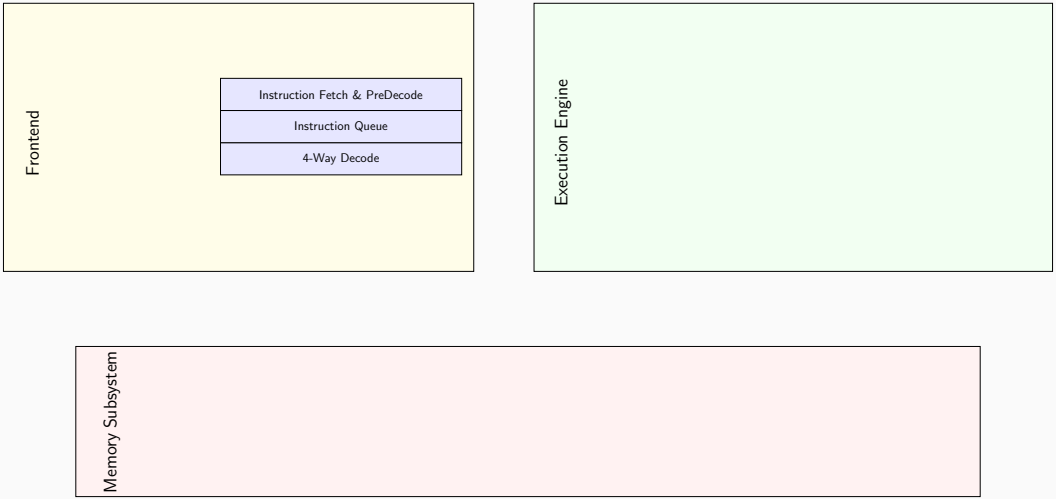
Reality: (Simplified) Modern CPU



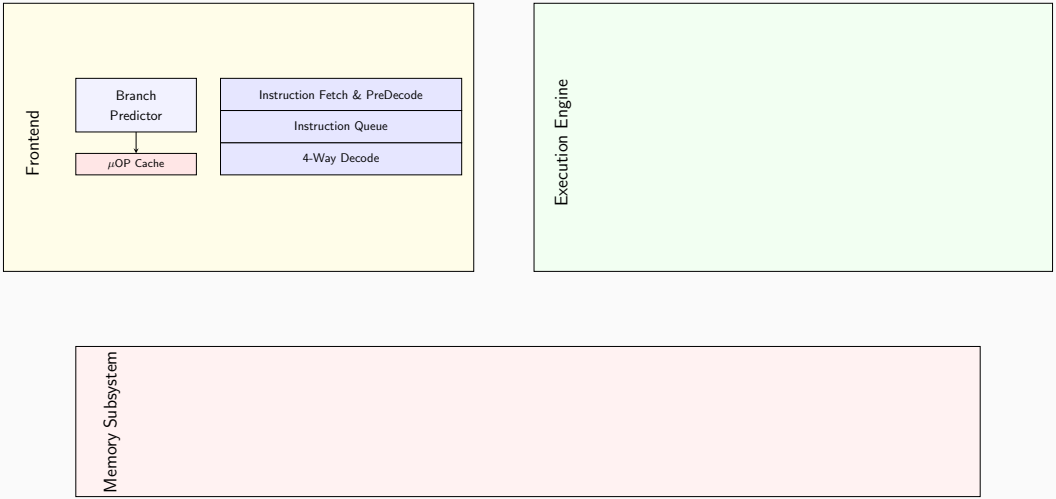
Reality: (Simplified) Modern CPU



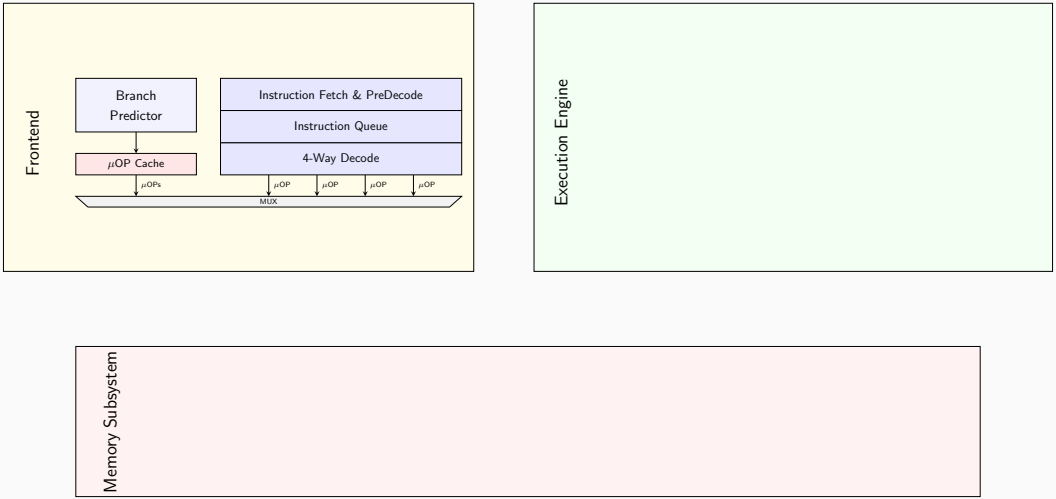
Reality: (Simplified) Modern CPU



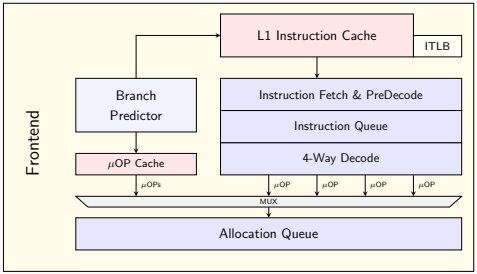
Reality: (Simplified) Modern CPU

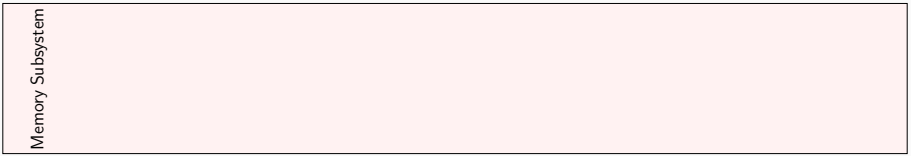


Reality: (Simplified) Modern CPU

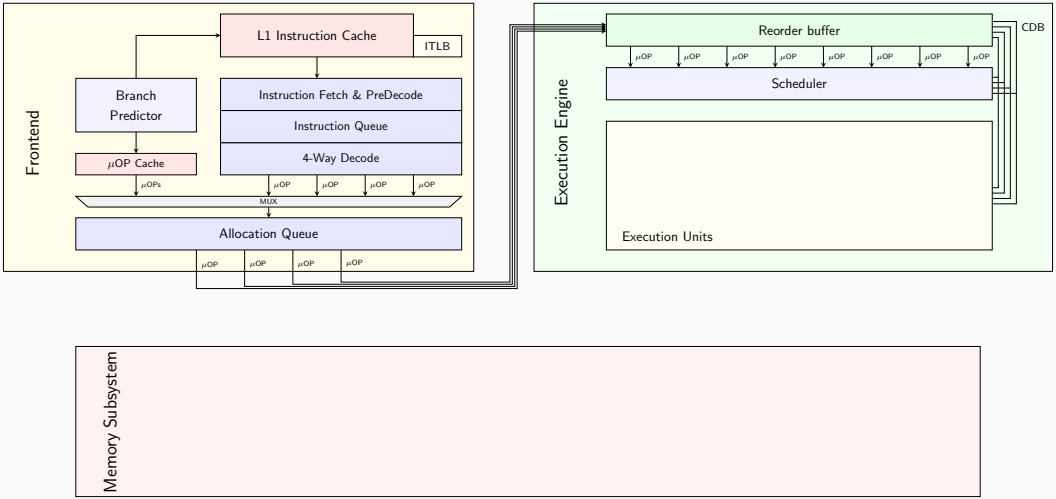


Reality: (Simplified) Modern CPU

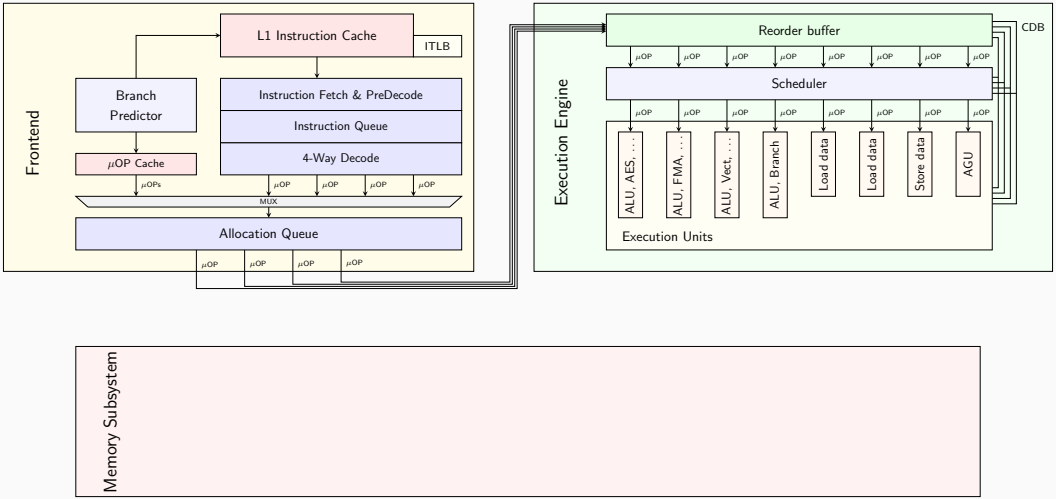




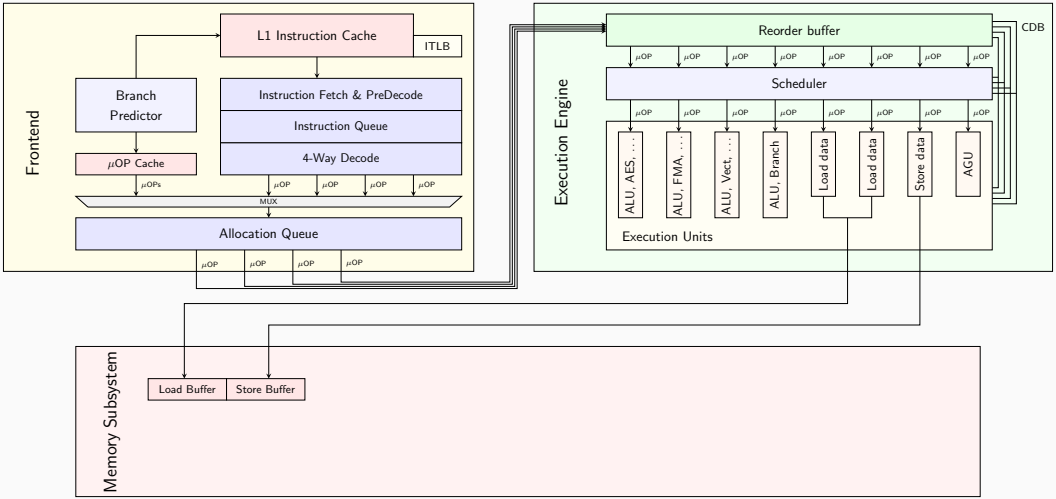
Reality: (Simplified) Modern CPU



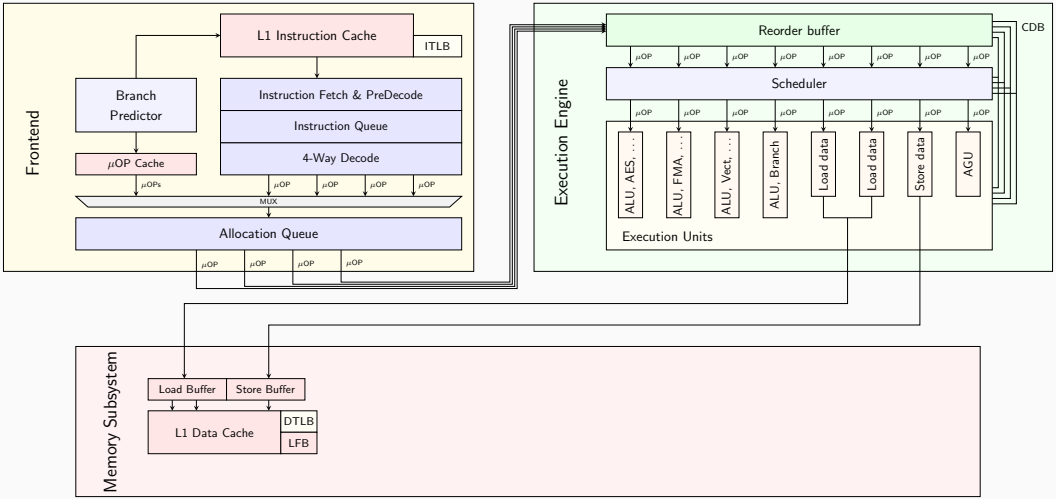
Reality: (Simplified) Modern CPU



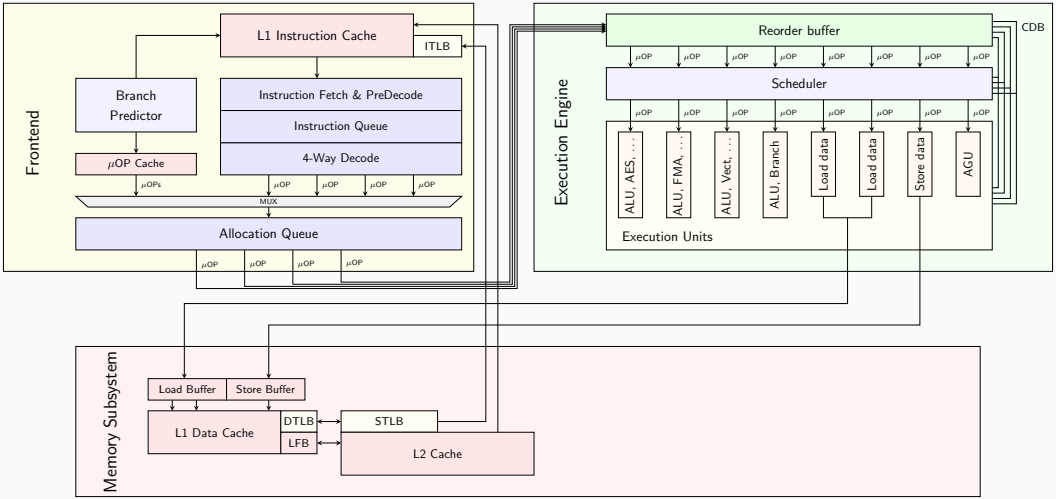
Reality: (Simplified) Modern CPU



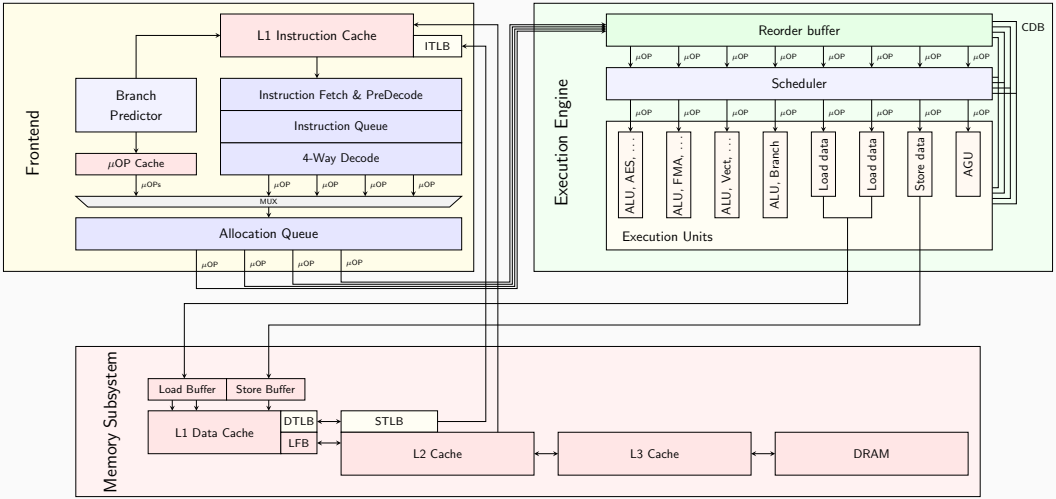
Reality: (Simplified) Modern CPU



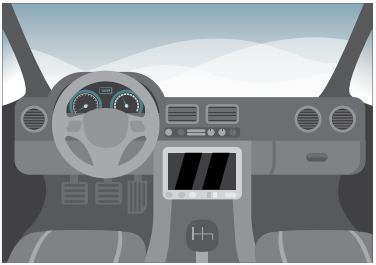
Reality: (Simplified) Modern CPU



Reality: (Simplified) Modern CPU



Intermezzo: CPU Architecture



- Cars all have the same interface (= architecture)

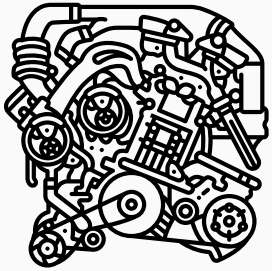
→ Steering wheel, pedals, gear stick, ...

- Some have special extensions

→ Air conditioning, cruise control, ...

- Driving skills are “compatible” with all cars

Intermezzo: CPU Microarchitecture



- Cars are implemented differently (= microarchitecture)

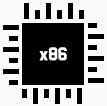
→ engine, fuel, motor control, ...

- Same car ("architecture") with different engines

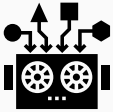
→ stronger or more efficient "microarchitecture"

- Drivers don't need to now anything about internals

No thorough Description



Intel manual
(full architecture)



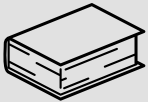
Intel optimization manual
(microarchitecture parts)

4778 pages

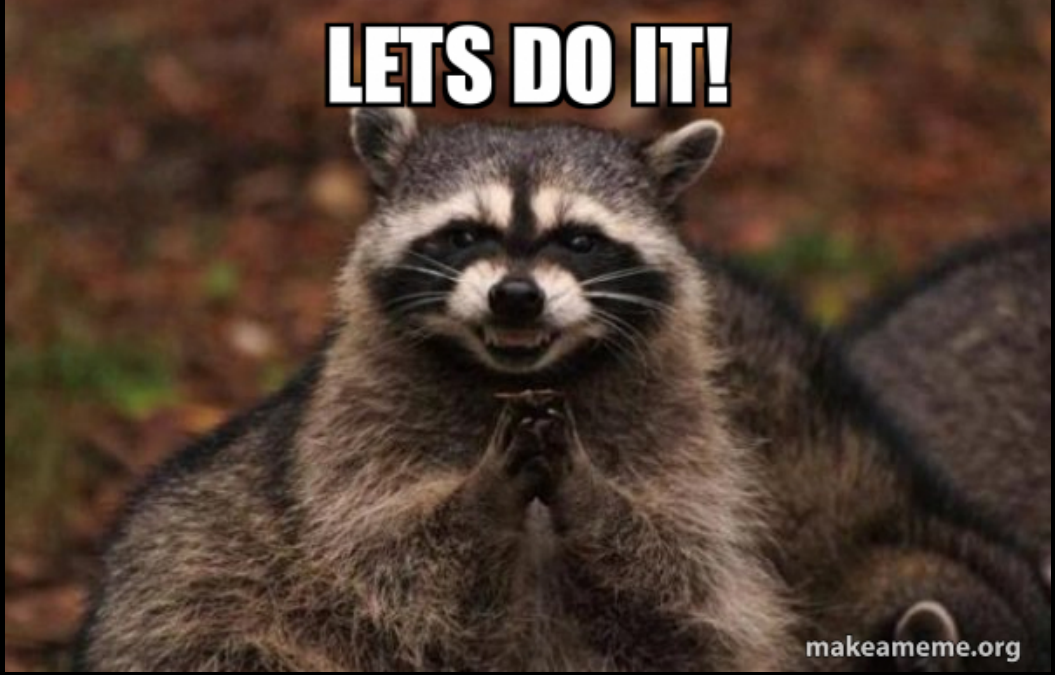
868 pages

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

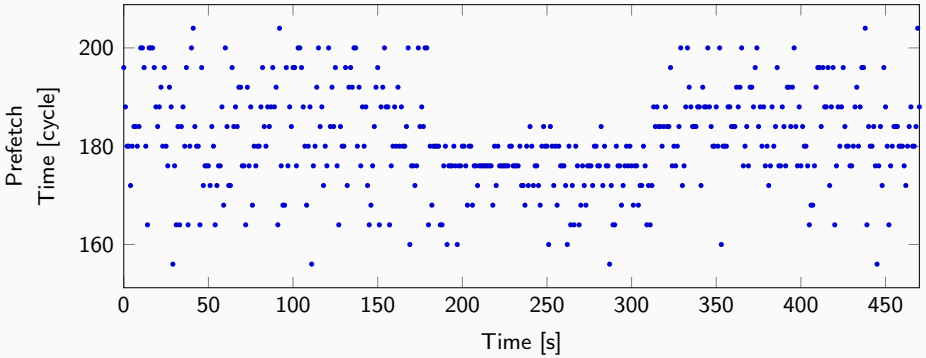
The `prefetch` Instruction



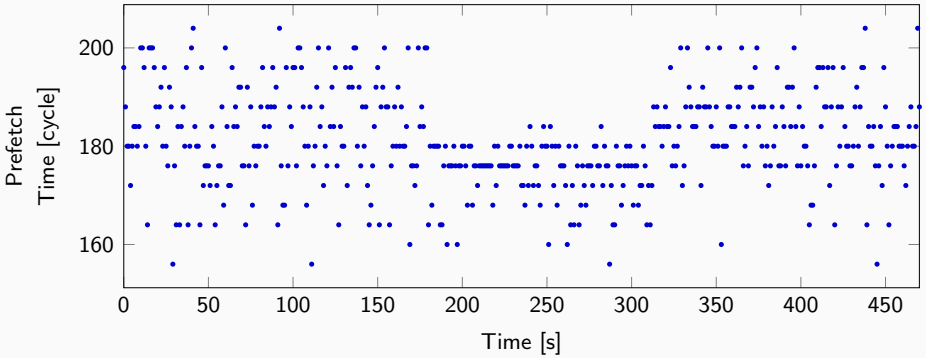
Use of software prefetch should be limited to memory addresses that are managed or owned within the application context. Prefetching to addresses that are not mapped to physical pages can experience non-deterministic performance penalty.


LETS DO IT!
makeameme.org

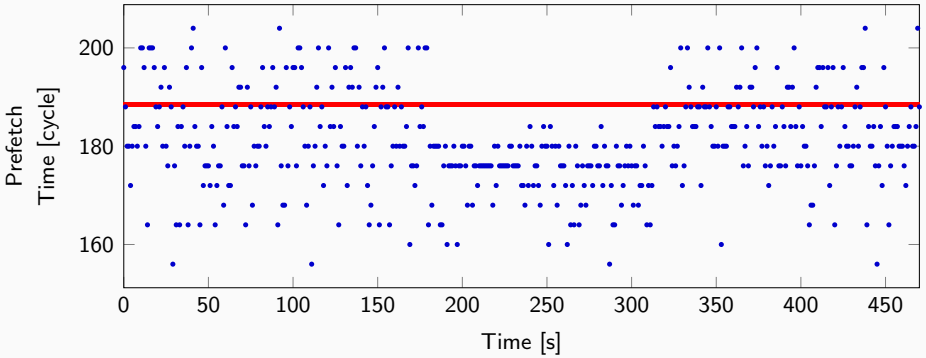
Prefetch Timings on the Operating System



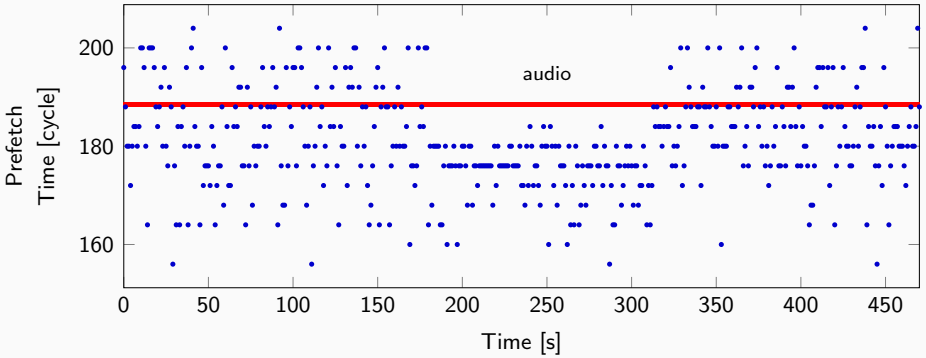
Prefetch Timings on the Operating System

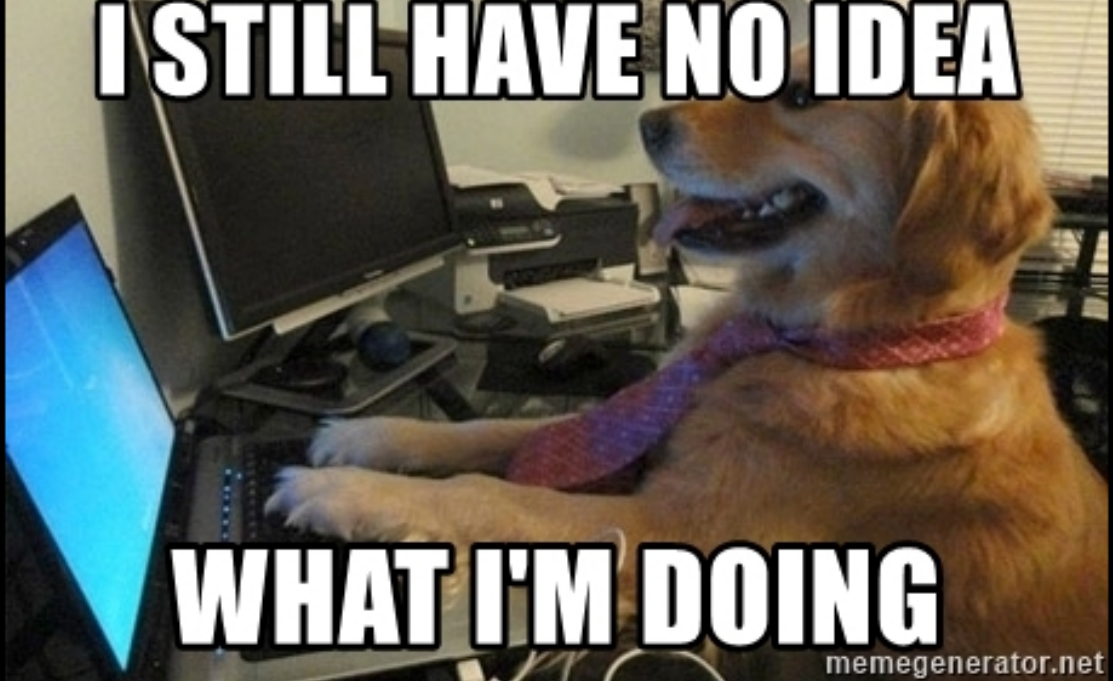


Prefetch Timings on the Operating System



Prefetch Timings on the Operating System




I STILL HAVE NO IDEA
WHAT I'M DOING
memegenerator.net

Systematic Approach

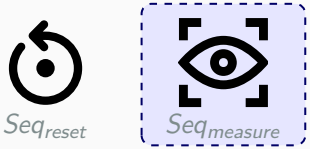
Reset instruction

Instruction to measure

Instruction with possible side effect

Testing A Sequence Triple

Testing A Sequence Triple



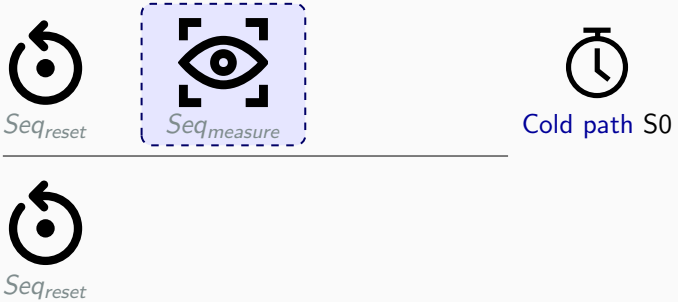
Testing A Sequence Triple

Seq_{reset}

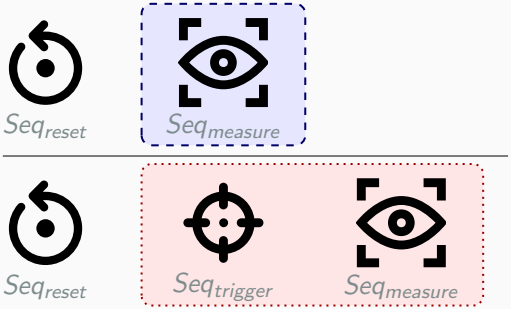
$Seq_{measure}$

Cold path S0

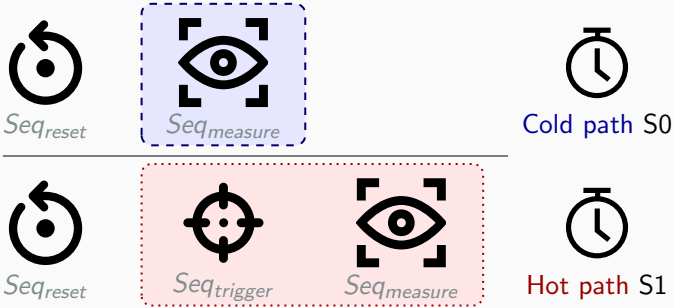
Testing A Sequence Triple



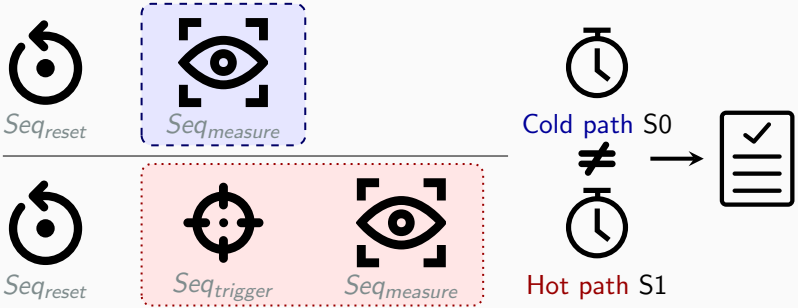
Testing A Sequence Triple



Testing A Sequence Triple

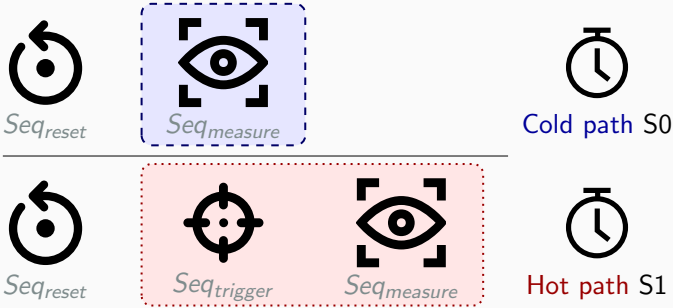


Testing A Sequence Triple



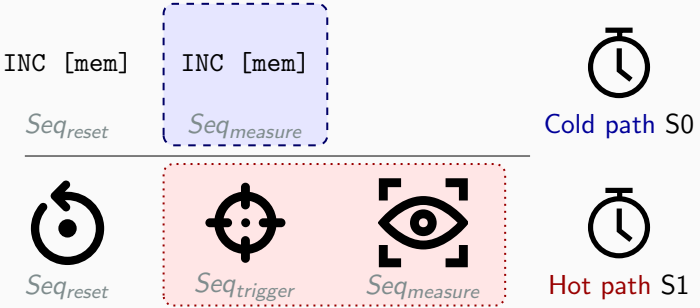
Testing A Sequence Triple

Example 1: $Seq_{measure} = Seq_{trigger} = Seq_{reset}$ = `INC [mem]`



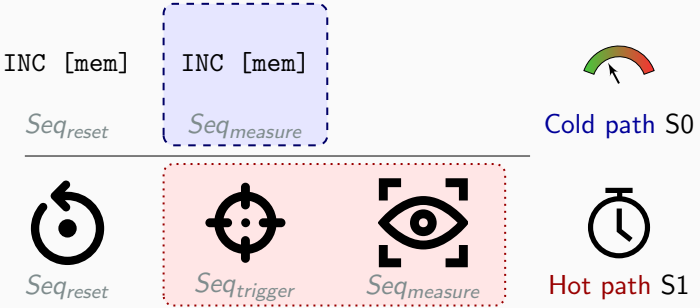
Testing A Sequence Triple

Example 1: $Seq_{measure} = Seq_{trigger} = Seq_{reset} =$ `INC [mem]`



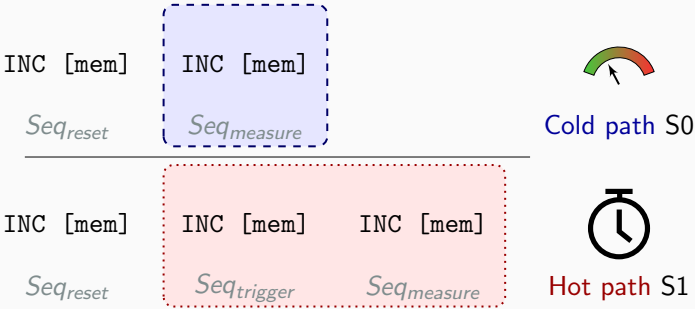
Testing A Sequence Triple

Example 1: $Seq_{measure} = Seq_{trigger} = Seq_{reset} =$ `INC [mem]`



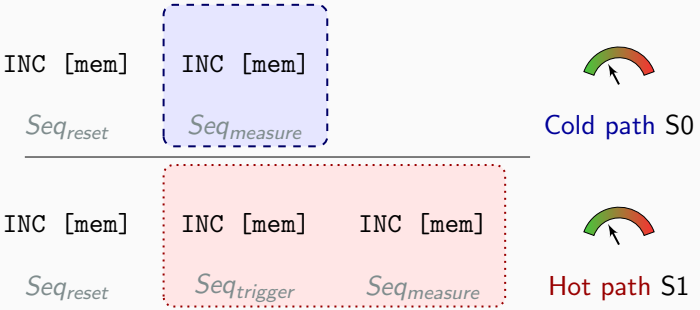
Testing A Sequence Triple

Example 1: $Seq_{measure} = Seq_{trigger} = Seq_{reset} = \texttt{INC [mem]}$



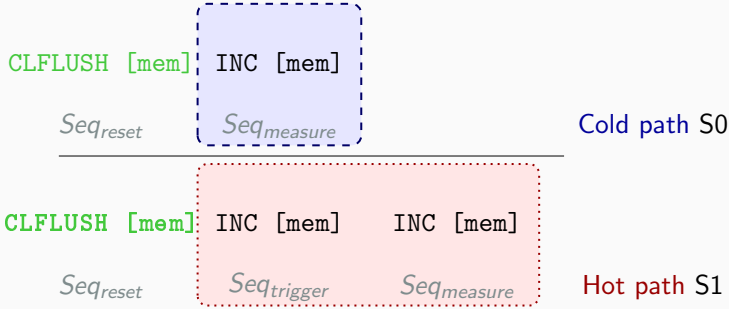
Testing A Sequence Triple

Example 1: $Seq_{measure} = Seq_{trigger} = Seq_{reset} =$ `INC [mem]`



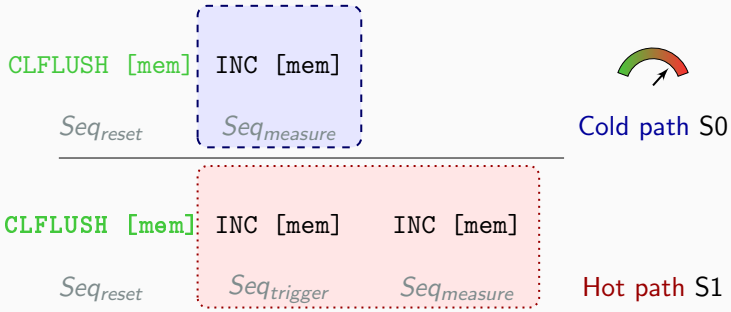
Testing A Sequence Triple

Example 2: $Seq_{measure} = Seq_{trigger} =$ `INC [mem]`;
$Seq_{reset} =$ `CLFLUSH [mem]`



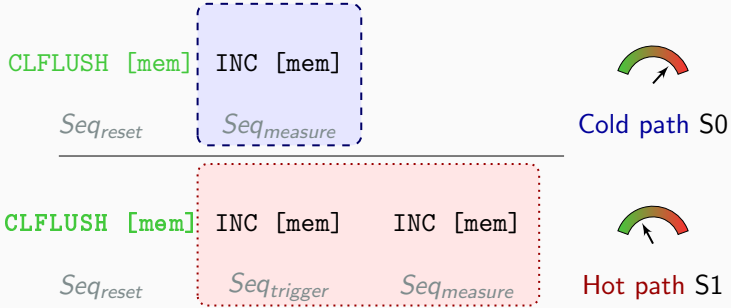
Testing A Sequence Triple

Example 2: $Seq_{measure} = Seq_{trigger} = \texttt{INC [mem]};$
$Seq_{reset} = \texttt{CLFLUSH [mem]}$



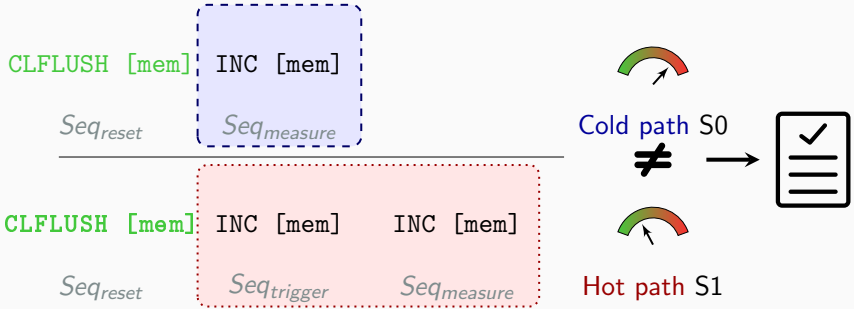
Testing A Sequence Triple

Example 2: $Seq_{measure} = Seq_{trigger} =$ `INC [mem]`;
$Seq_{reset} =$ `CLFLUSH [mem]`



Testing A Sequence Triple

Example 2: $Seq_{measure} = Seq_{trigger} =$ `INC [mem]`;
$Seq_{reset} =$ `CLFLUSH [mem]`



Recap: Measuring Time

```
start = ⏱
  x = y + 1
end = ⏱
Δ = end - start
```

Recap: Measuring Time

```
start = ⏱
  x = y + 1
end = ⏱
Δ = end - start
```

1. run: Δ = 302 $\rightarrow$ cache miss
2. run: Δ = 54 $\rightarrow$ cache hit

Recap: Measuring Time

```
clflush [y]
start = ⏱
  x = y + 1
end = ⏱
Δ = end - start
```

1. run: Δ = 302 $\rightarrow$ cache miss
2. run: Δ = 302 $\rightarrow$ cache miss

Recap: Measuring Time

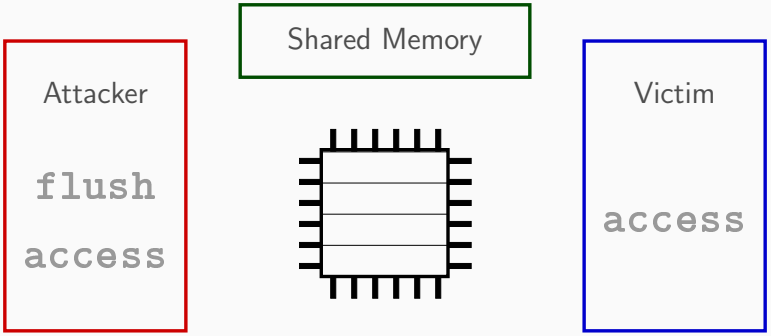
```
clflush [y]
start = ⏱
  x = y + 1
end = ⏱
Δ = end - start
```

1. run: Δ = 302 $\rightarrow$ cache miss
2. run: Δ = 302 $\rightarrow$ cache miss

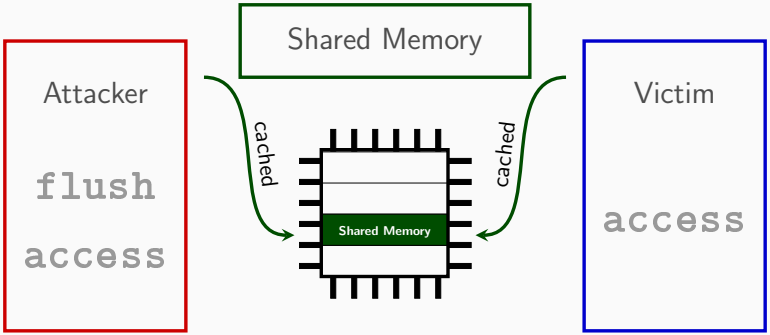
Determinism!

No randomness or non-determinism – just behavior we did not understand

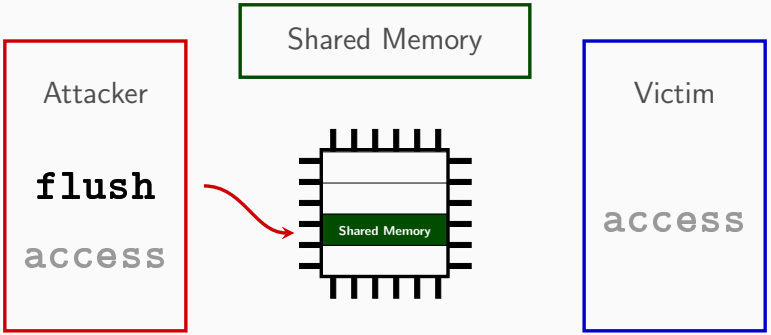
Flush+Reload



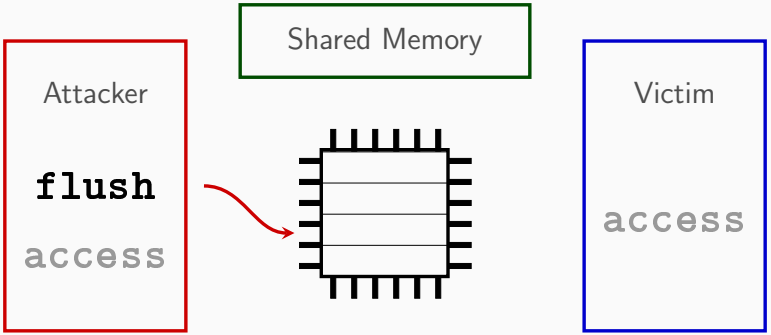
Flush+Reload



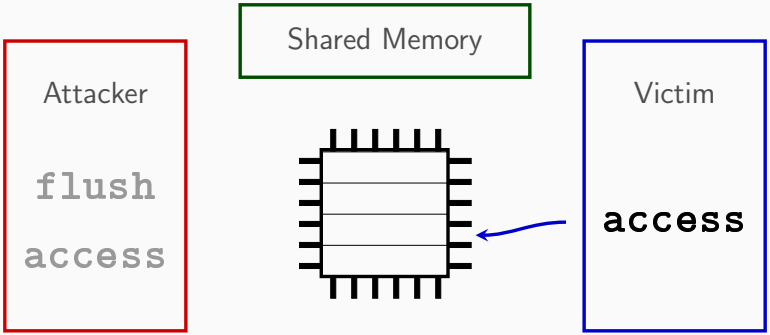
Flush+Reload



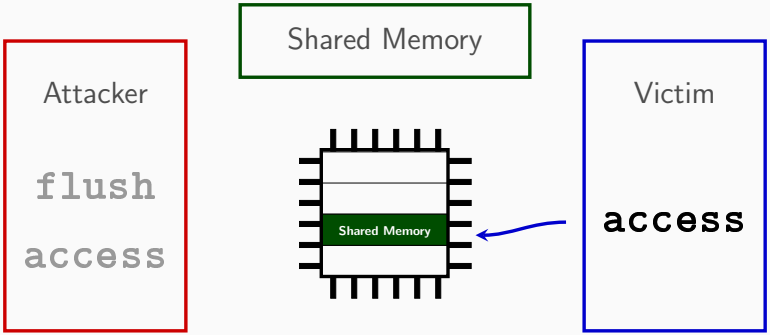
Flush+Reload



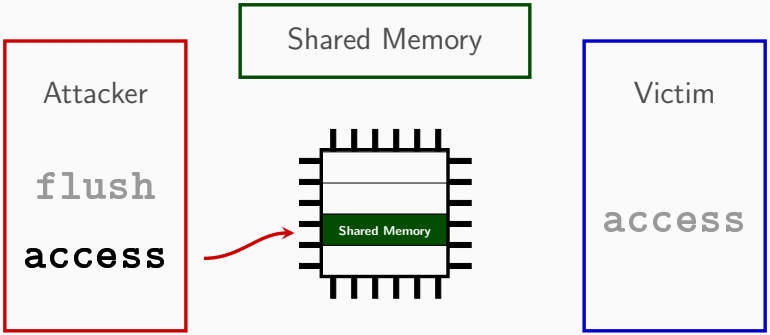
Flush+Reload



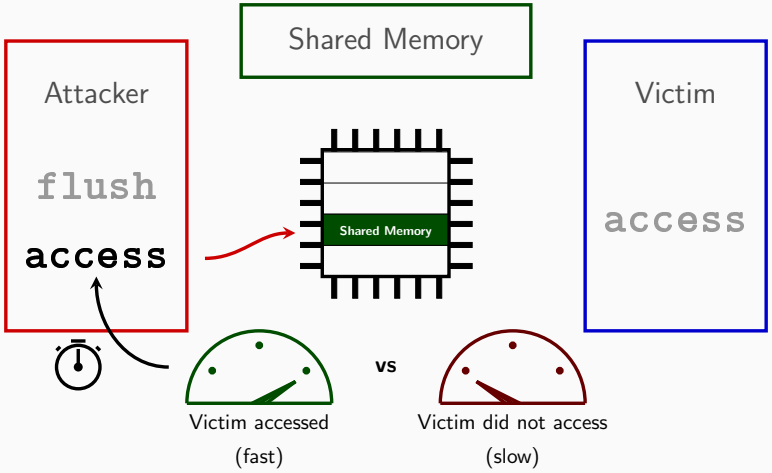
Flush+Reload



Flush+Reload



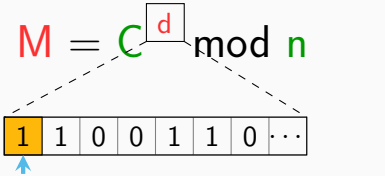
Flush+Reload



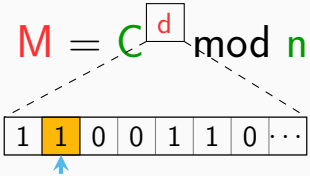
Flush+Reload on Square-and-Multiply

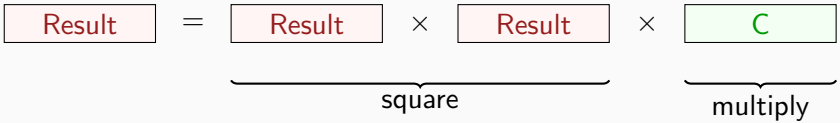
$$M = C^{d} \bmod n$$

Flush+Reload on Square-and-Multiply

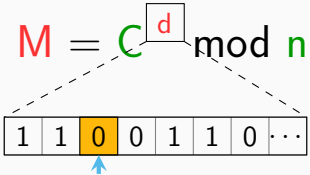


Flush+Reload on Square-and-Multiply





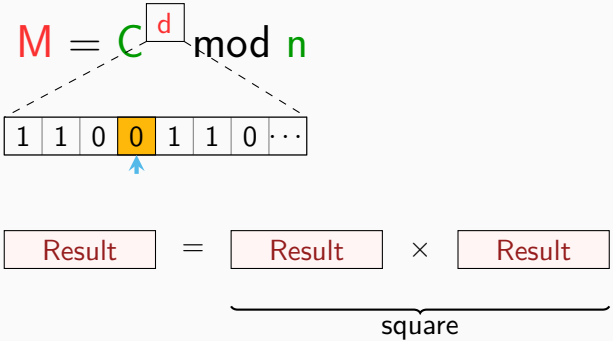
Flush+Reload on Square-and-Multiply



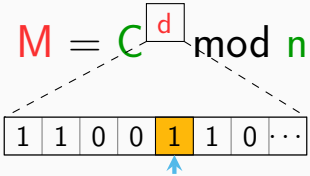
Result = Result × Result

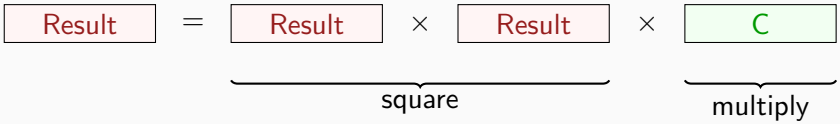
square

Flush+Reload on Square-and-Multiply

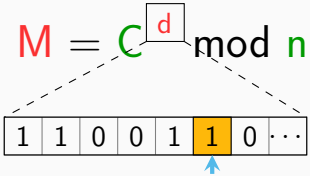


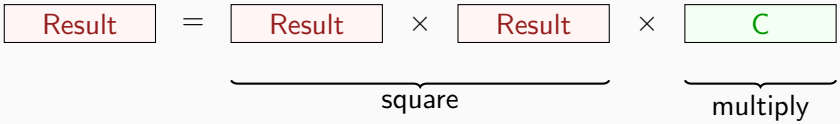
Flush+Reload on Square-and-Multiply



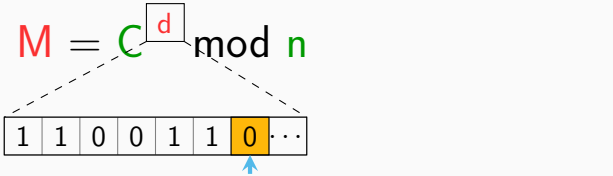


Flush+Reload on Square-and-Multiply





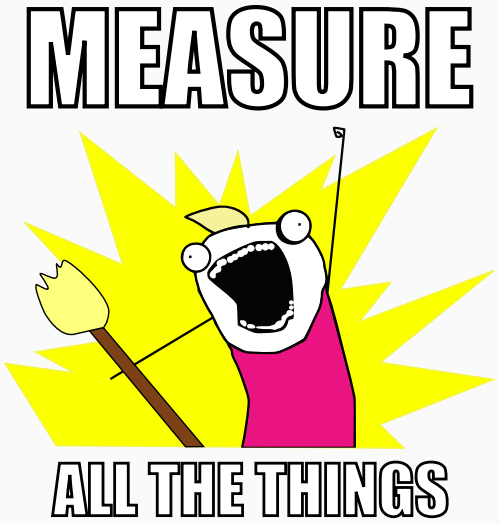
Flush+Reload on Square-and-Multiply



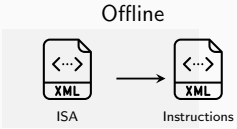
Motivation

Problem

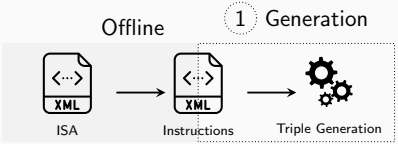
Finding side channels is a **complex** and **time-consuming** process


MEASURE
ALL THE THINGS

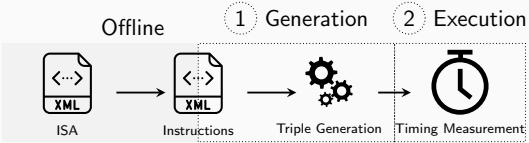
Osiris – Fuzzing x86 CPUs for Side Channels



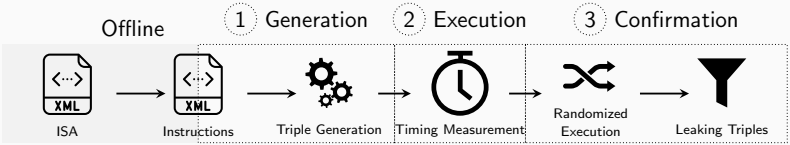
Osiris – Fuzzing x86 CPUs for Side Channels



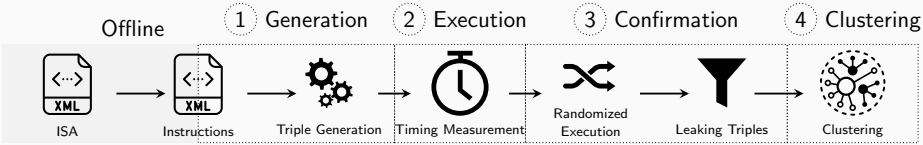
Osiris – Fuzzing x86 CPUs for Side Channels



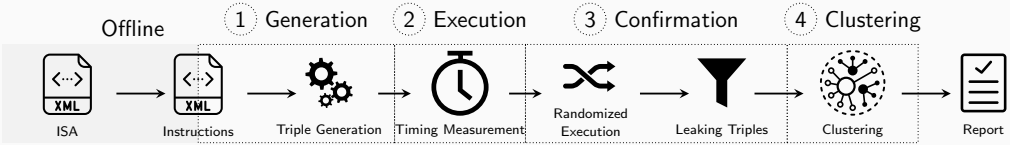
Osiris – Fuzzing x86 CPUs for Side Channels



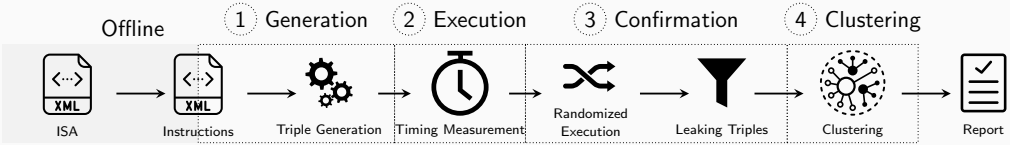
Osiris – Fuzzing x86 CPUs for Side Channels



Osiris – Fuzzing x86 CPUs for Side Channels



Osiris – Fuzzing x86 CPUs for Side Channels

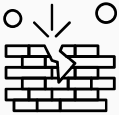


- Fuzzed on 5 different CPUs
- AMD and Intel

Osiris Results

~4 days per CPU

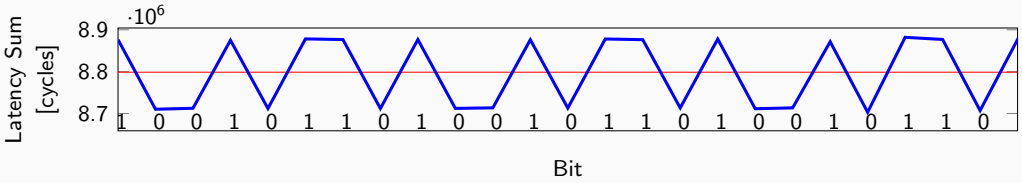
2 side channels rediscovered



4 new side channels

2 new attacks

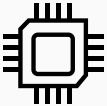
Cross-VM Interference



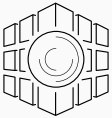
- Random-number generator `RDRAND`
- VM in the cloud (e.g., AWS) sees usage of other VMs

$\rightarrow$ Breaks VM isolation

RDRAND Covert Channel - Properties



AMD and Intel



VM and native

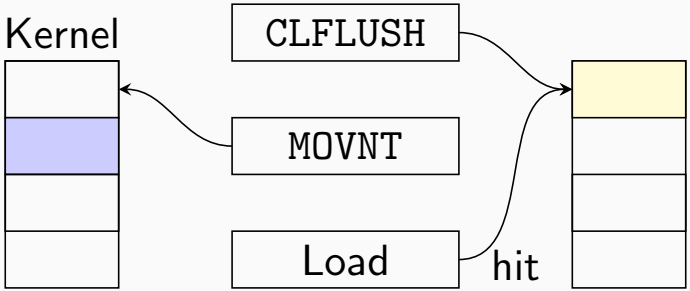
1000 bit/s

No memory

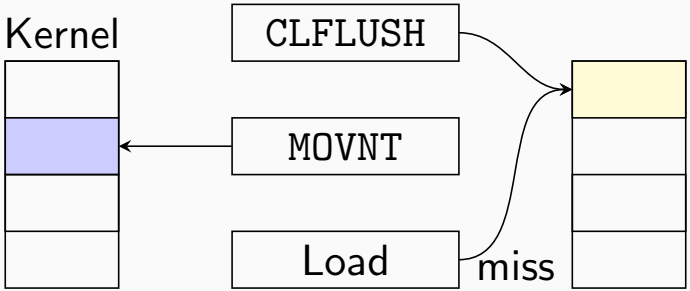
No detection

No mitigation

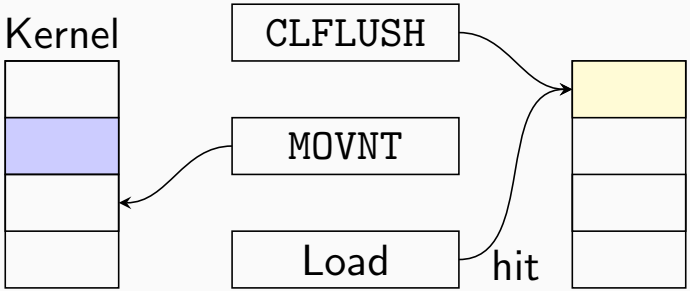
KASLR Break

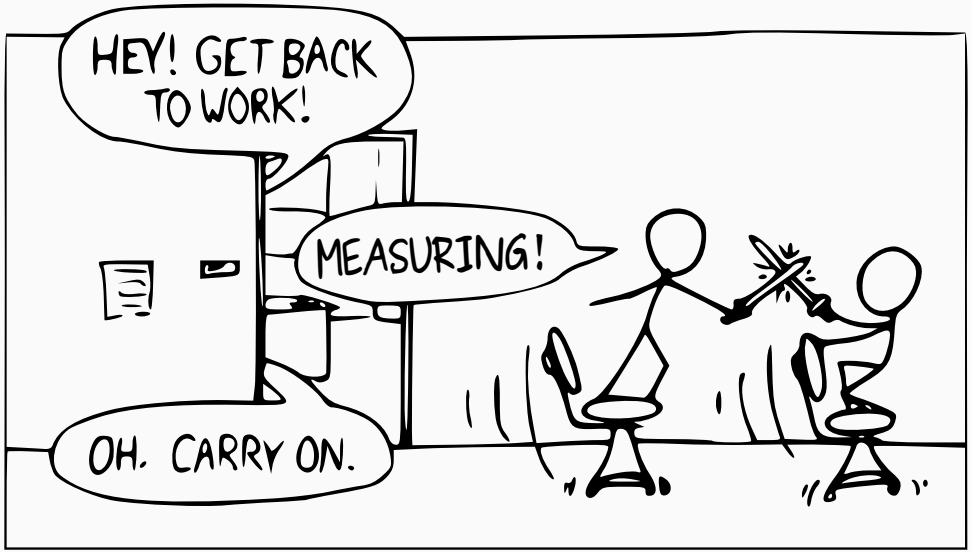


KASLR Break



KASLR Break




HEY! GET BACK TO WORK!
MEASURING!
OH. CARRY ON.

Continue Measuring

```
x = y + 1


start = ⏱
  x = y + 1
end = ⏱
Δ = end - start
```

Continue Measuring

```
x = y + 1
```

```
start = ⏱
  x = y + 1
end = ⏱
Δ = end - start
```

1. run: Δ = 54 $\rightarrow$ cache hit
2. run: Δ = 54 $\rightarrow$ cache hit

Continue Measuring


```
<crash>
x = y + 1 (never executed architecturally)
<restart>
start = ⏱
  x = y + 1
end = ⏱
Δ = end - start
```

1. run:
2. run:

Continue Measuring

```
<crash>
x = y + 1  (never executed architecturally)
<restart>
start = ⏱
  x = y + 1
end = ⏱
Δ = end - start
```

1. run: Δ = 54 $\rightarrow$ cache hit
2. run: Δ = 54 $\rightarrow$ cache hit

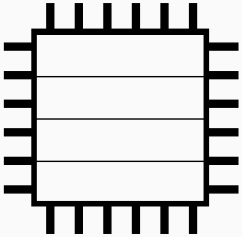
(Im)possible

Microarchitecture can do things impossible for the architecture

User Memory

	$\mathbb{A}$	$\mathbb{B}$
$\mathbb{C}$	$\mathbb{D}$	$\mathbb{E}$
$\mathbb{F}$	$\mathbb{G}$	$\mathbb{H}$
$\mathbb{I}$	$\mathbb{J}$	$\mathbb{K}$
$\mathbb{L}$	$\mathbb{M}$	$\mathbb{N}$
$\mathbb{O}$	$\mathbb{P}$	$\mathbb{Q}$
$\mathbb{R}$	$\mathbb{S}$	$\mathbb{T}$
$\mathbb{U}$	$\mathbb{V}$	$\mathbb{W}$
$\mathbb{X}$	$\mathbb{Y}$	$\mathbb{Z}$

```
char value = kernel[0]
```

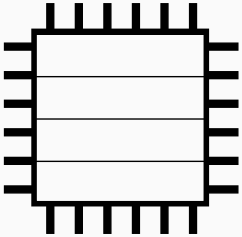


User Memory

	$\mathbb{A}$	$\mathbb{B}$
$\mathbb{C}$	$\mathbb{D}$	$\mathbb{E}$
$\mathbb{F}$	$\mathbb{G}$	$\mathbb{H}$
$\mathbb{I}$	$\mathbb{J}$	$\mathbb{K}$
$\mathbb{L}$	$\mathbb{M}$	$\mathbb{N}$
$\mathbb{O}$	$\mathbb{P}$	$\mathbb{Q}$
$\mathbb{R}$	$\mathbb{S}$	$\mathbb{T}$
$\mathbb{U}$	$\mathbb{V}$	$\mathbb{W}$
$\mathbb{X}$	$\mathbb{Y}$	$\mathbb{Z}$

```
char value = kernel[0]
```

Page fault (Exception)



User Memory

	𝔸	𝔹
ℂ	𝔻	𝔼
𝔽	𝔾	ℍ
𝕀	𝕁	𝕂
𝕃	𝕄	ℕ
𝕆	ℙ	ℚ
ℝ	𝕊	𝕋
𝕌	𝕍	𝕎
𝕏	𝕐	ℤ

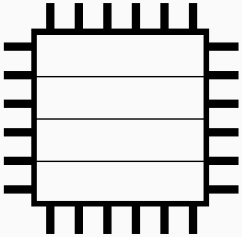
```
char value = kernel[0]
```

Page fault (Exception)

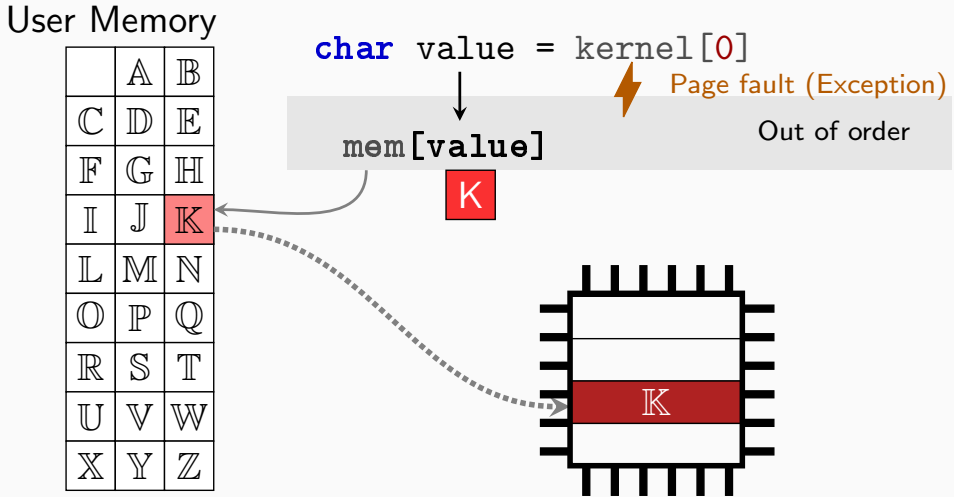
Out of order

```
mem[value]
```

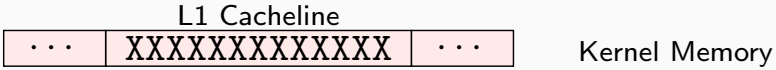
K



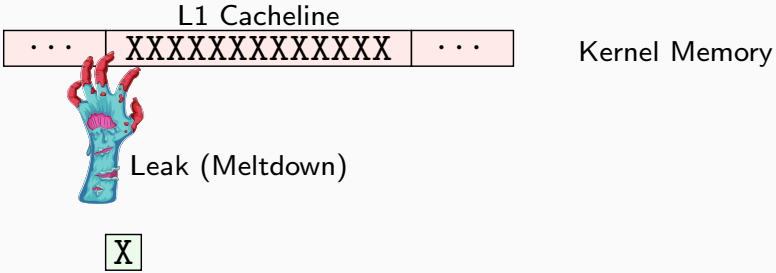
Meltdown


User Memory
char value = kernel[0]
Page fault (Exception)
Out of order
mem[value]
K
A
B
C
D
E
F
G
H
I
J
K
L
M
N
O
P
Q
R
S
T
U
V
W
X
Y
Z
K

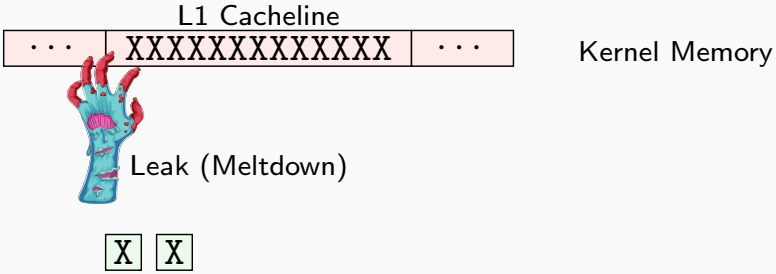
Meltdown Experiment



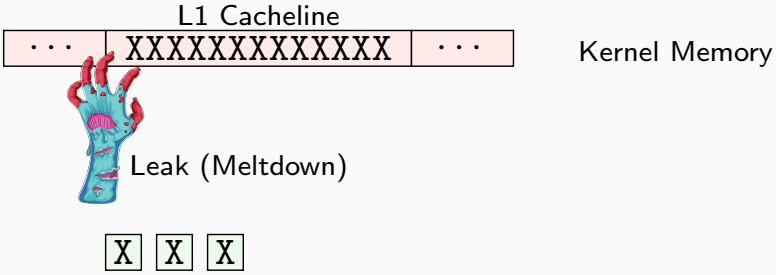
Meltdown Experiment



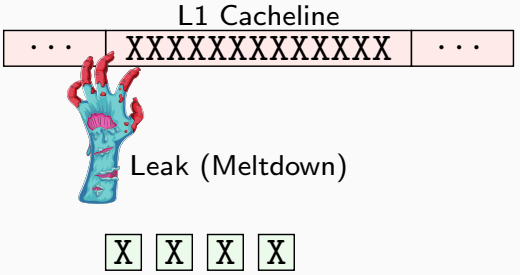
Meltdown Experiment



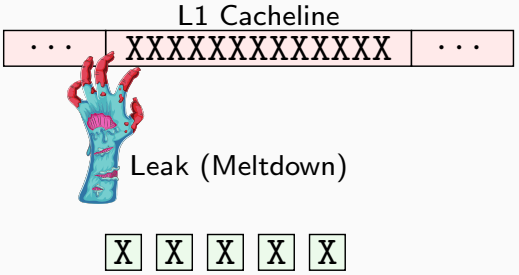
Meltdown Experiment



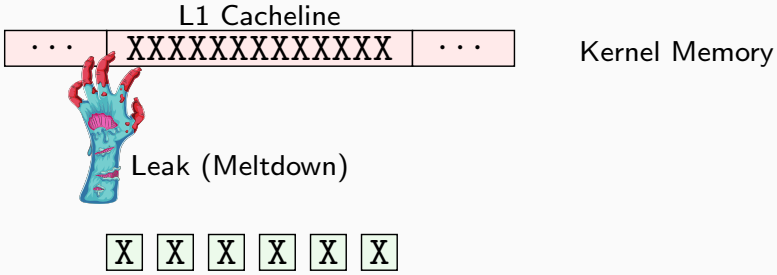
Meltdown Experiment



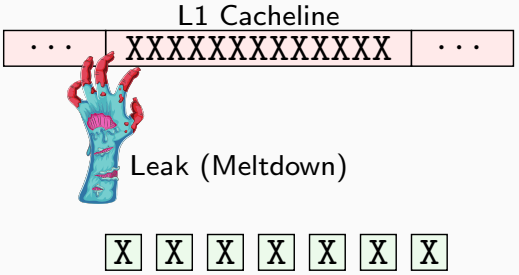
Meltdown Experiment



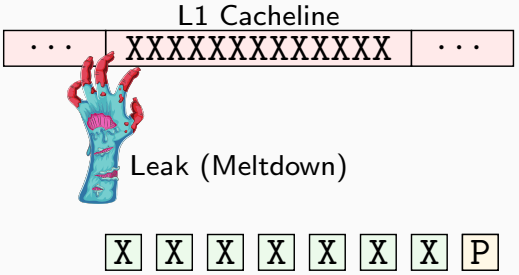
Meltdown Experiment



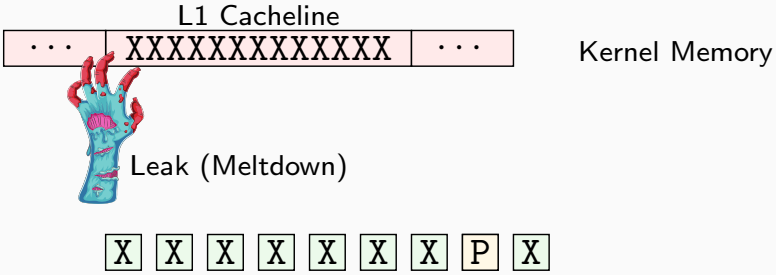
Meltdown Experiment



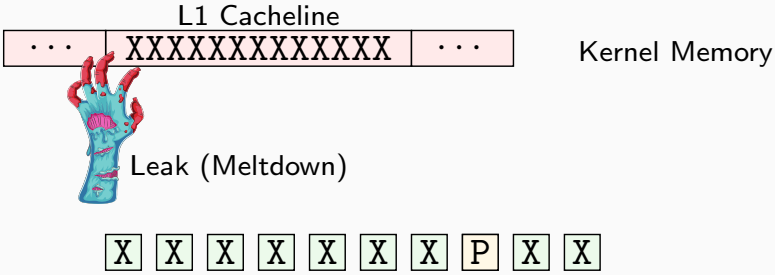
Meltdown Experiment



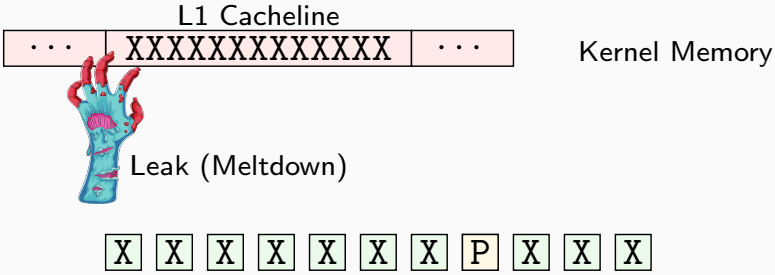
Meltdown Experiment



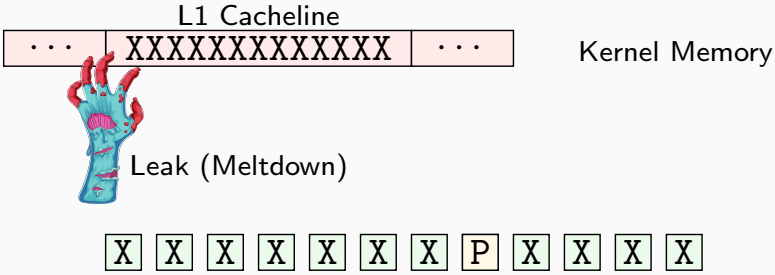
Meltdown Experiment



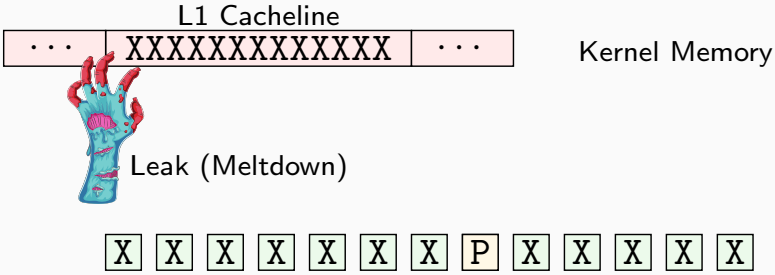
Meltdown Experiment



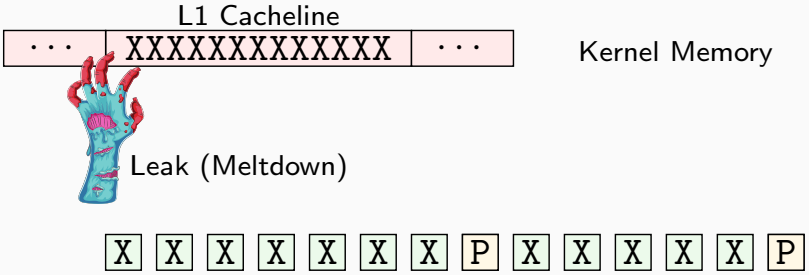
Meltdown Experiment



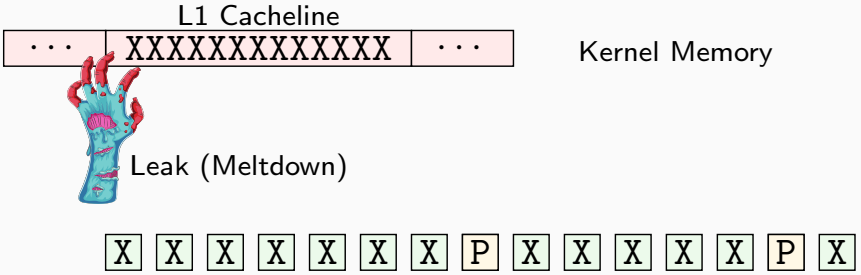
Meltdown Experiment



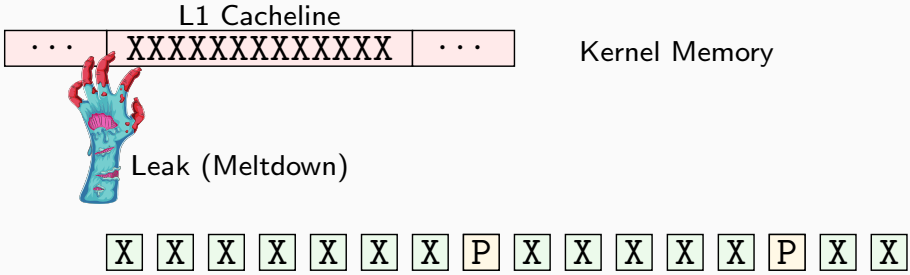
Meltdown Experiment



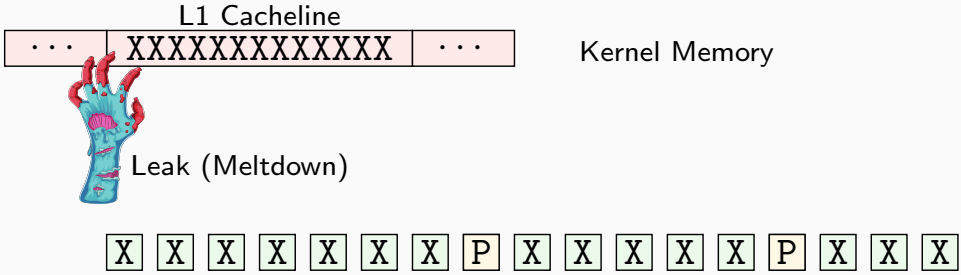
Meltdown Experiment



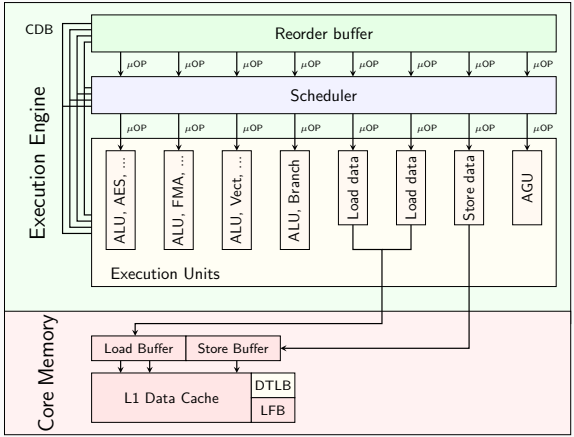
Meltdown Experiment



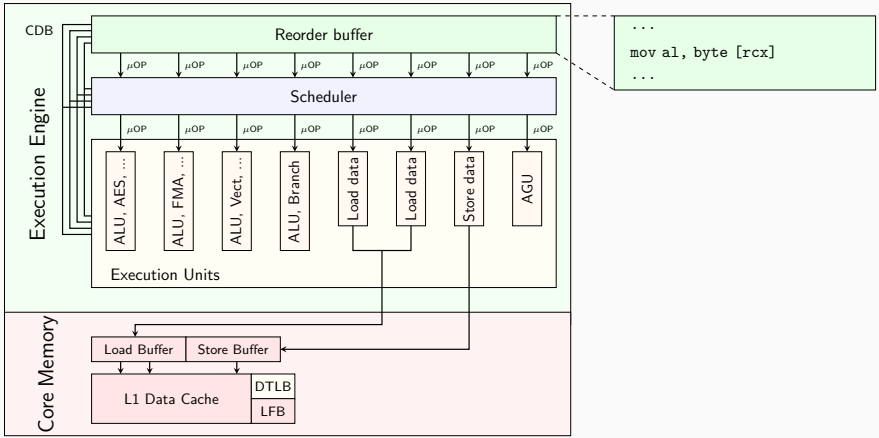
Meltdown Experiment



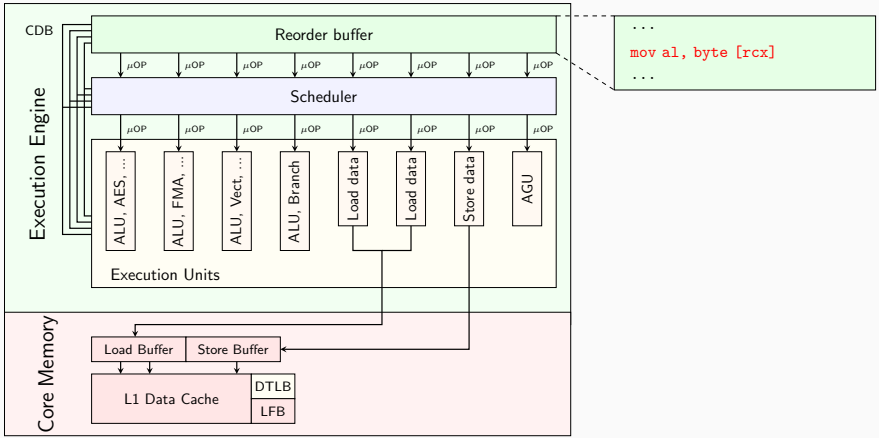
Complex Load Situations



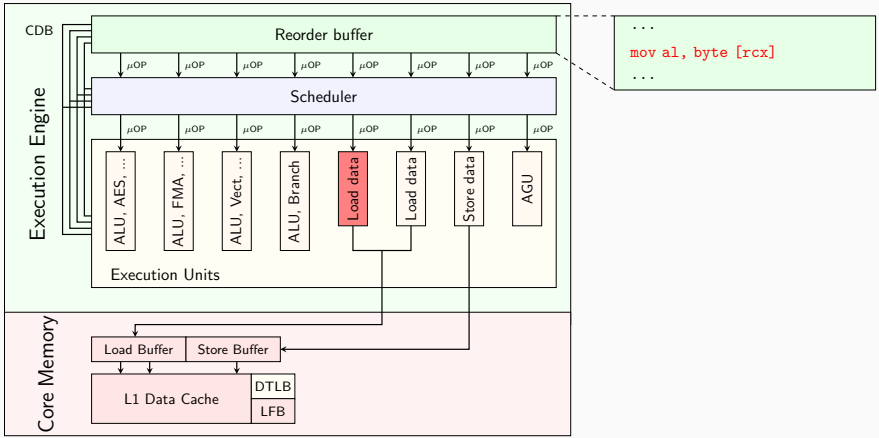
Complex Load Situations



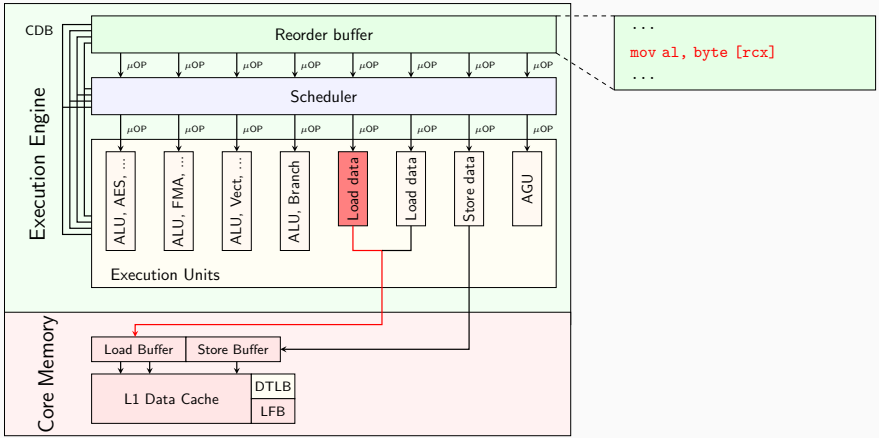
Complex Load Situations



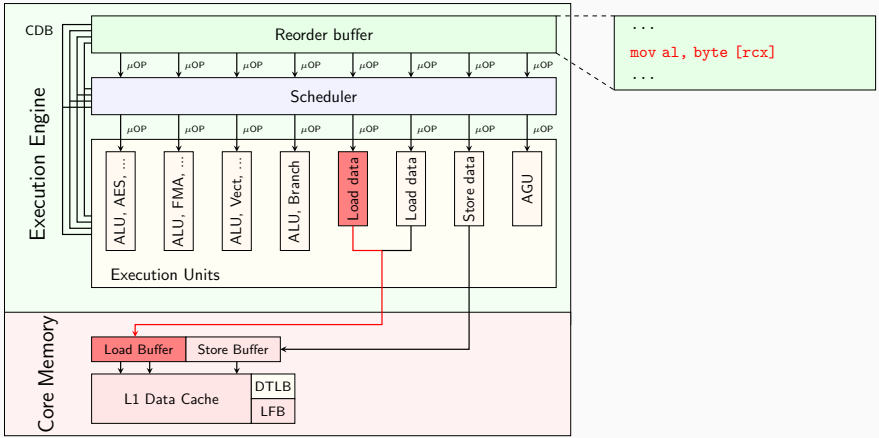
Complex Load Situations



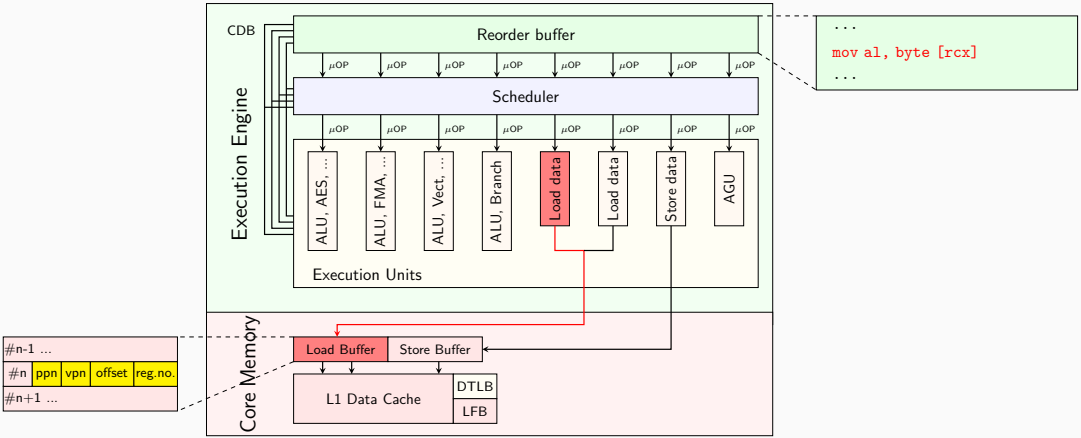
Complex Load Situations



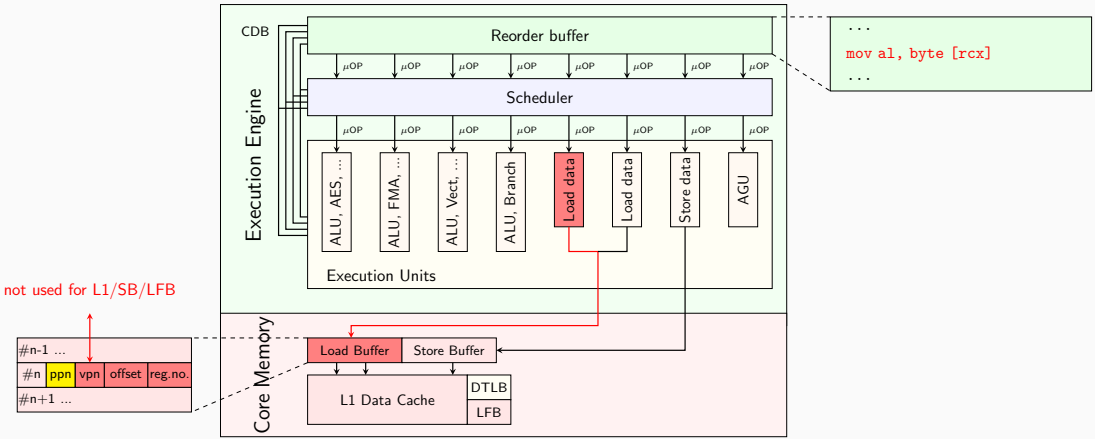
Complex Load Situations



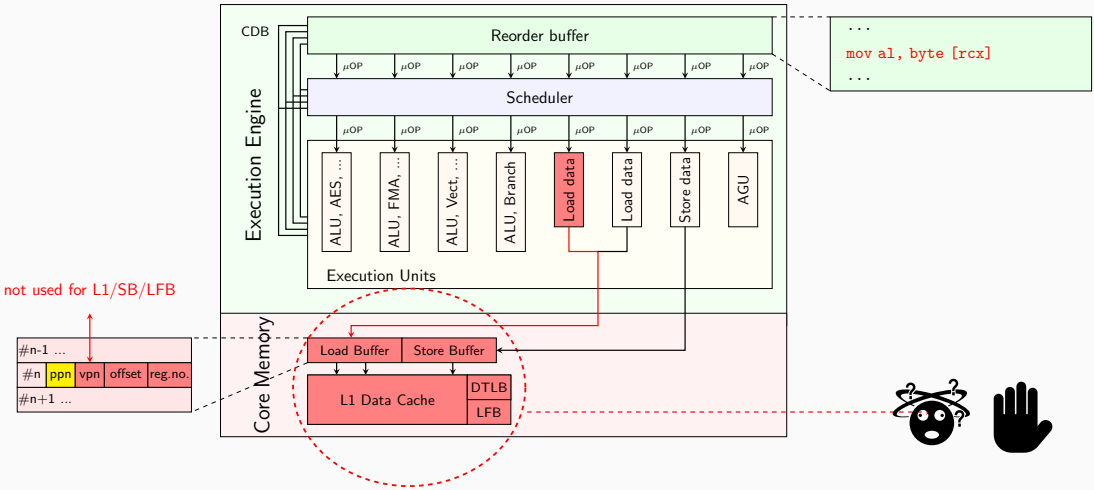
Complex Load Situations



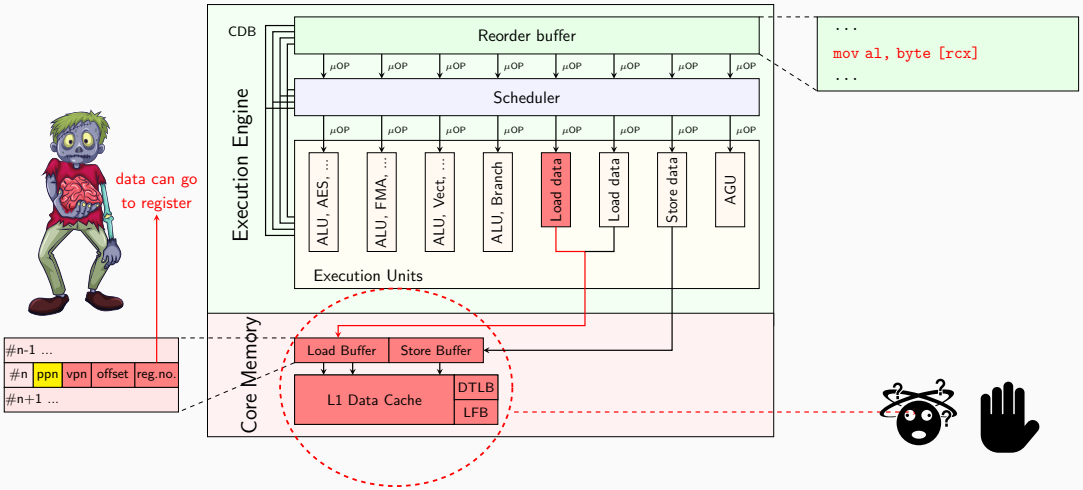
Complex Load Situations

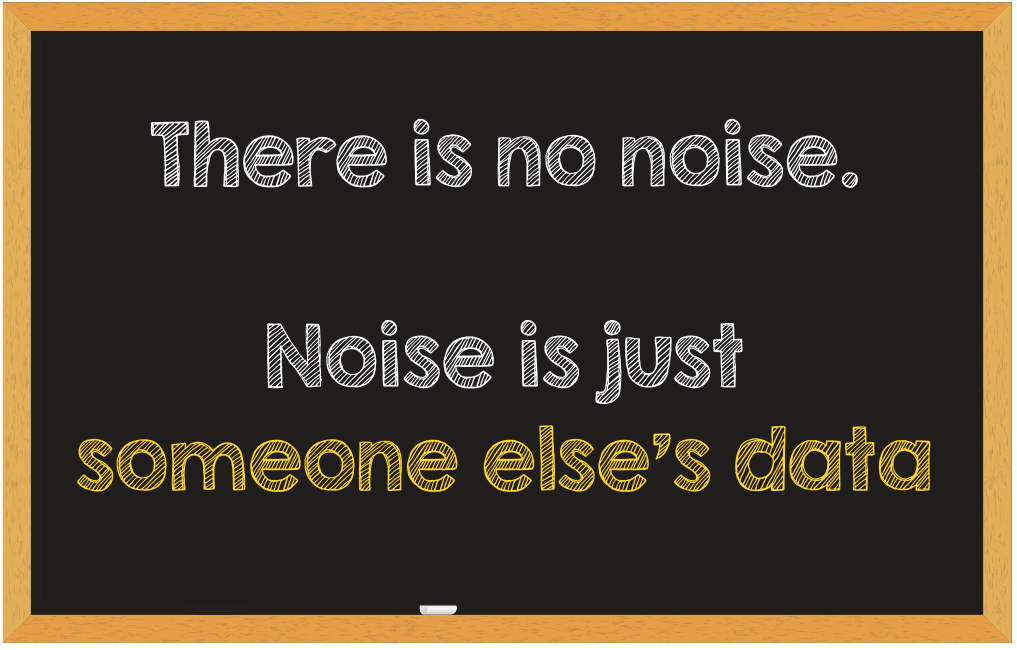


Complex Load Situations

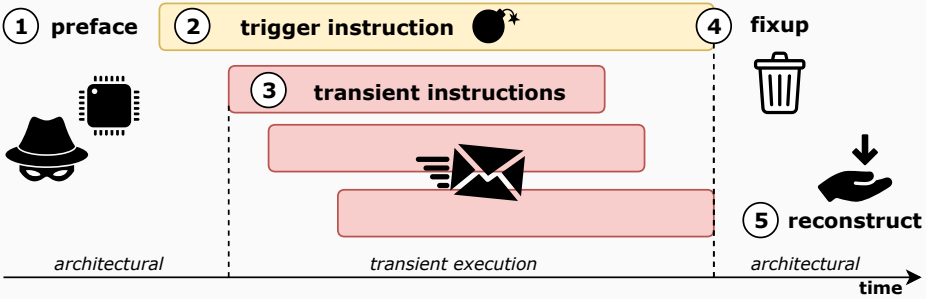


Complex Load Situations




There is no noise.
Noise is just
someone else's data

Systematic Analysis



BBC

Intel Zombieload bug fix to slow data centre computers

THE VERGE

ZombieLoad attack lets hackers steal data from Intel chips

FORTUNE

'Zombieload' Flaw Lets Hackers Crack Almost Every Intel Chip Back to 2011. Why's It Being Downplayed?

How-To Geek

Only New CPUs Can Truly Fix ZombieLoad and Spectre

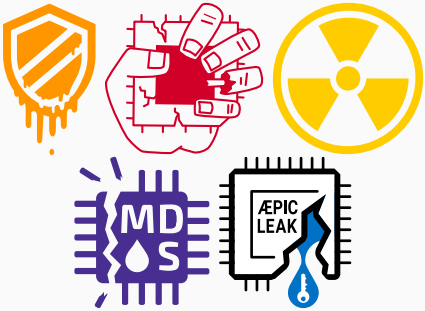
That Escalated Quickly

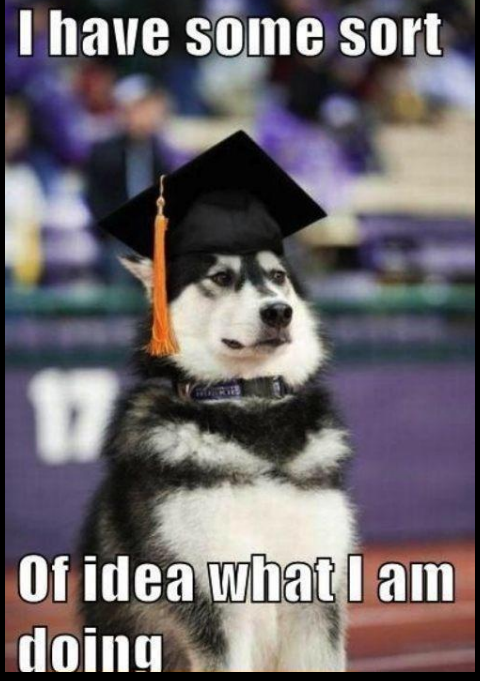
How it started

That Escalated Quickly

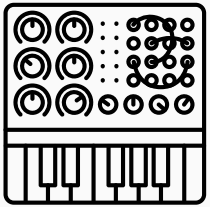
How it started

How it's going




I have some sort
Of idea what I am doing

MDS Analysis

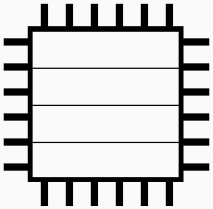


- Many Microarchitectural Data Sampling (MDS) attacks
  → ZombieLoad, RIDL, Fallout, Meltdown-UC
- Different variants and leakage targets
- Complex to reproduce and test all variations
- Common: require a fault or microcode assist

User Memory

	A	B
C	D	E
F	G	H
I	J	K
L	M	N
O	P	Q
R	S	T
U	V	W
X	Y	Z

```
char value = faulting[0]
```

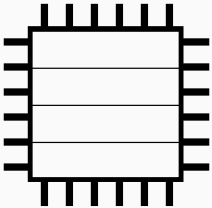


User Memory

	𝔸	𝔹
ℂ	𝔻	𝔼
𝔽	𝔾	ℍ
𝕀	𝕁	𝕂
𝕃	𝕄	ℕ
𝕆	ℙ	ℚ
ℝ	𝕊	𝕋
𝕌	𝕍	𝕎
𝕏	𝕐	ℤ

```
char value = faulting[0]
```

Fault



User Memory

	A	B
C	D	E
F	G	H
I	J	K
L	M	N
O	P	Q
R	S	T
U	V	W
X	Y	Z

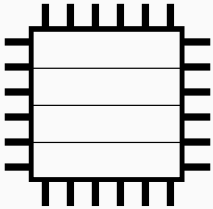
```
char value = faulting[0]
```

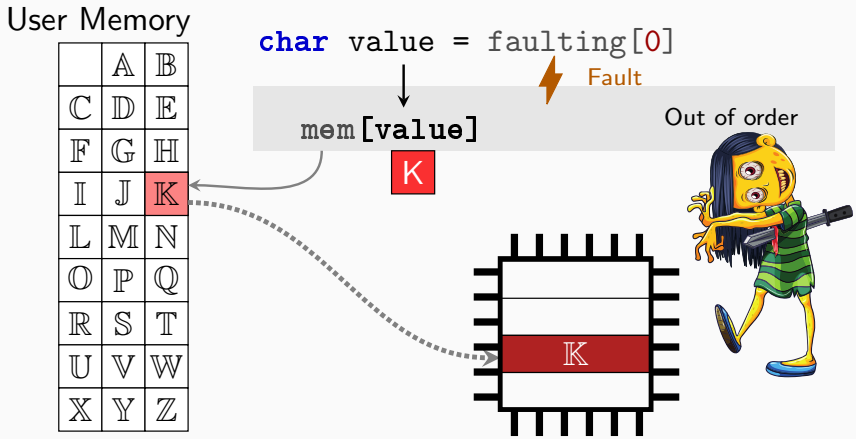
Fault

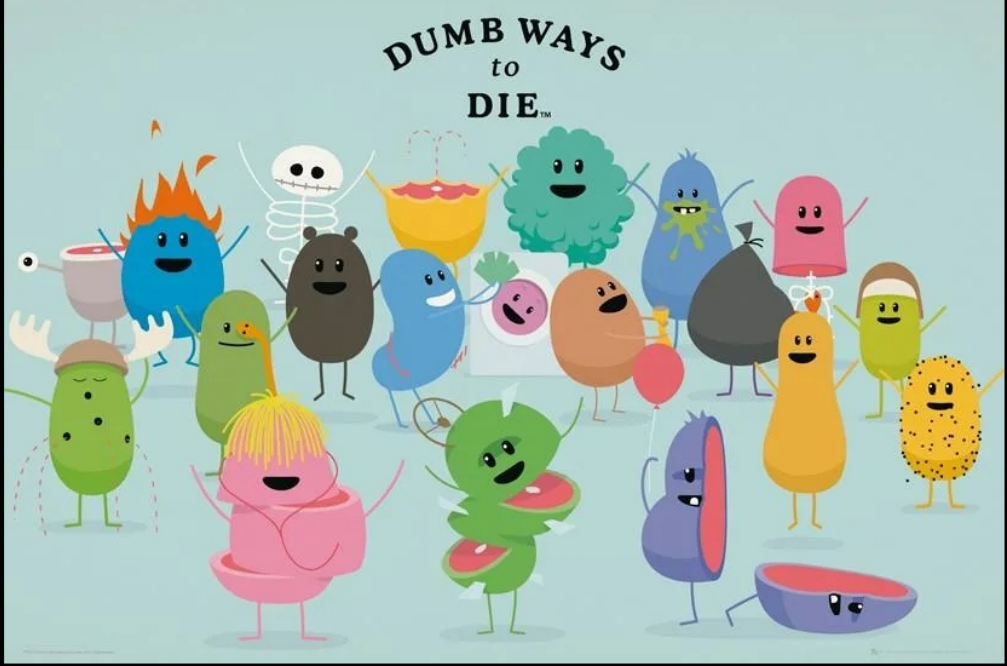
Out of order

```
mem[value]
```

K




User Memory
A B
C D E
F G H
I J K
L M N
O P Q
R S T
U V W
X Y Z
char value = faulting[0]
Fault
mem[value]
K
Out of order
K

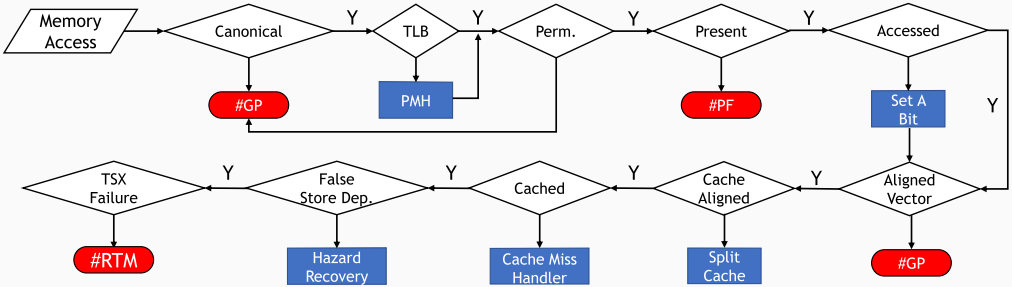

DUMB WAYS
to
DIE™

Memory Access Checks (simplified)

- Many possibilities for faults

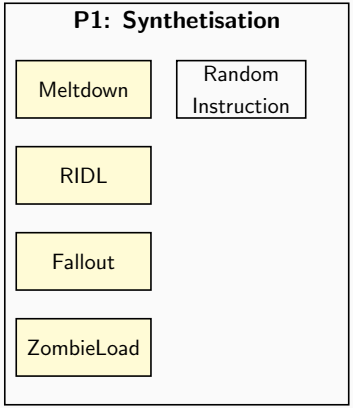
Memory Access Checks (simplified)

- Many possibilities for faults

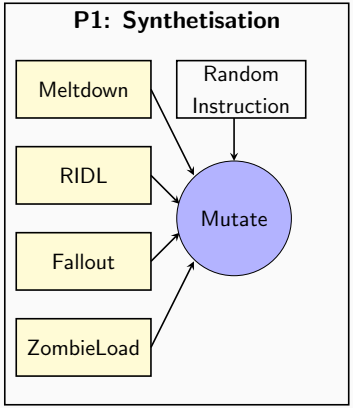


- Idea: mutation fuzzing for new variants

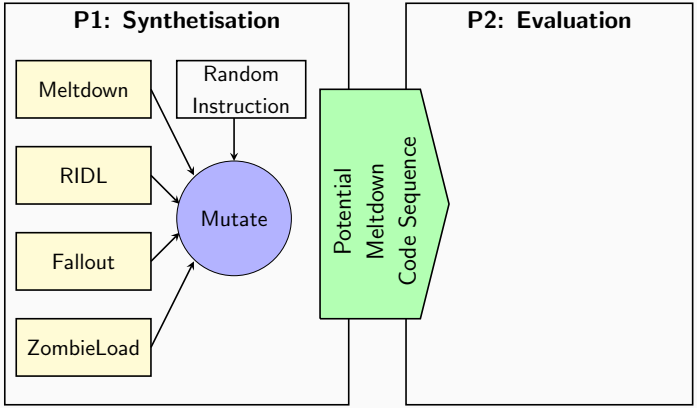
Transynther



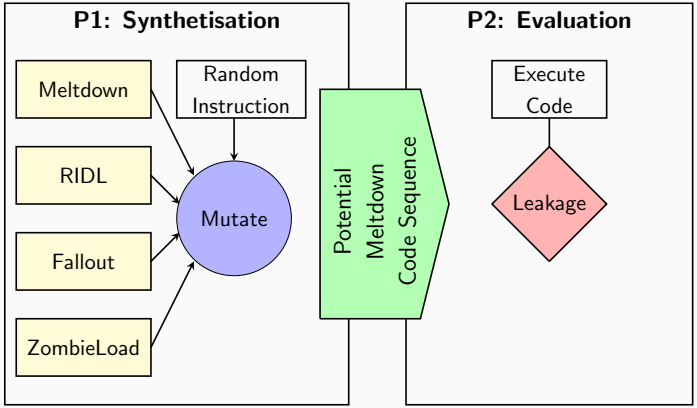
Transynther



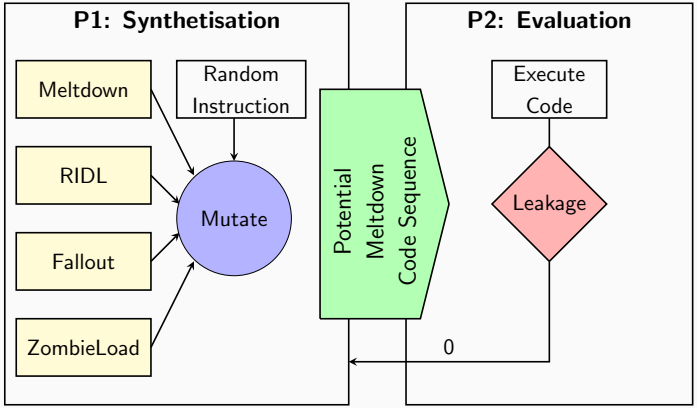
Transynther



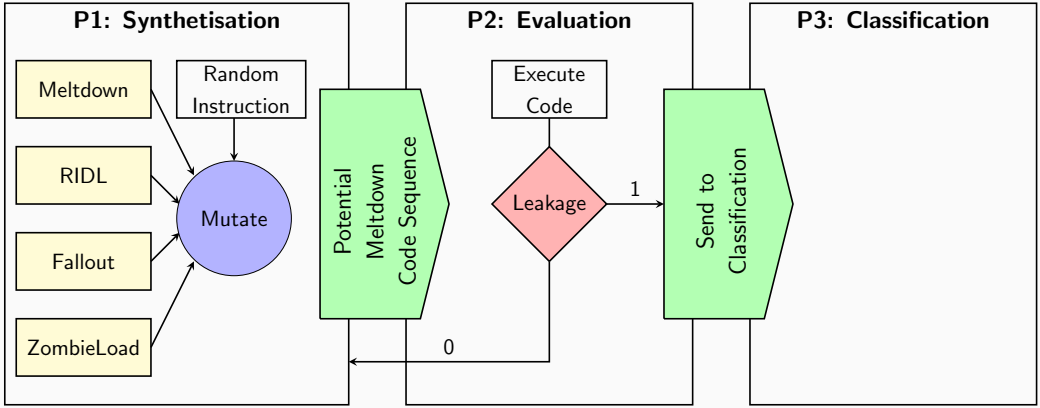
Transynther



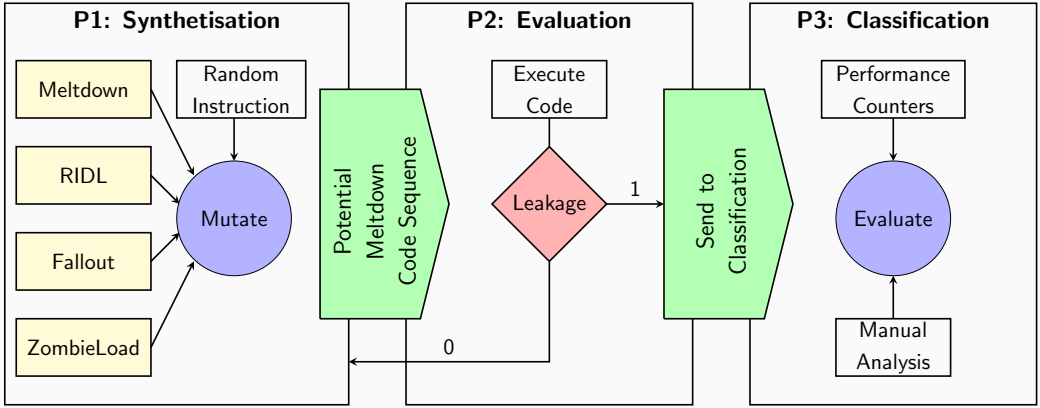
Transynther



Transynther

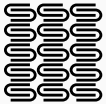


Transynther



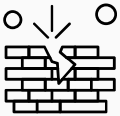
Transynther Results

26 hours runtime



100 unique leakage patterns

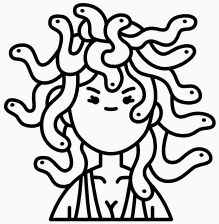
7 attacks reproduced



1 new vulnerability

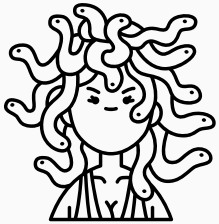
1 regression

Medusa



- Medusa: new variant of ZombieLoad

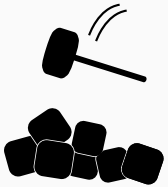
Medusa



- Medusa: new variant of ZombieLoad
- Leaks from write-combining buffer, i.e., `REP MOV`
- Used for fast memory copy, e.g., in OpenSSL or kernel

$\rightarrow$ Leaked RSA key while decoding in OpenSSL

Ice Lake Regression



- Ice Lake microarchitecture reported no vulnerabilities
- Transynther found a regression via a small mutation

→ Re-enabled a “mitigated” variant

- Fixed via microcode update

Software vs. Hardware Fuzzing

- All low-hanging fruit
- Approximately as sophisticated as software fuzzing in 1990
- Majority of fuzzers does not use any guidance
- More research on feedback necessary

Summary

- Simple models are sufficient to find leakage
- Dumb fuzzers find leakage within hours
  - New vulnerability variants
  - New side channels
  - Regression in new CPUs
- Prediction: smarter fuzzers $\rightarrow$ more vulnerabilities

Open Source

https://github.com/CISPA/Osiris

USENIX'21

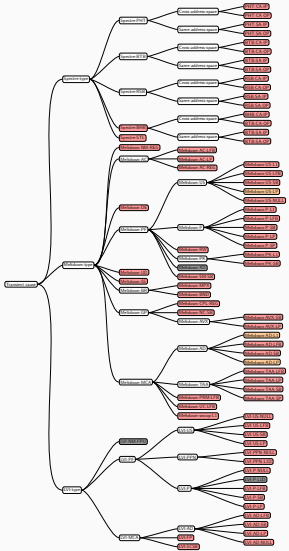
Daniel Weber, Ahmad Ibrahim, Hamed Nemati, Michael Schwarz, Christian Rossow.
Osiris: Automated Discovery of Microarchitectural Side Channels.

https://github.com/vernamlab/Medusa

USENIX'20

Daniel Moghimi, Moritz Lipp, Berk Sunar, Michael Schwarz.
Medusa: Microarchitectural Data Leakage via Automated Attack Synthesis.

Spectre, Meltdown, and LVI Variants



Twittern

Josh Walden @jmw1123 · 19. Nov.

Case of beer on it's way/there later this week thanks Daniel! Thanks again for the partnership!

> **Daniel Gruss** @lavados · 13. Nov.
> Antwort an @Desertrold und @jmw1123
> I'm in favor!

2 5 34

Daniel Gruss
@lavados

Antwort an @jmw1123

Thanks again Josh!

We already received the case a month ago but only found time this weekend to sit together and enjoy some!

We wish you a merry Christmas and look forward to continue working with Intel next year.

cc @cc0x1f @mlqxyz @misc0110 @tugraz_csbme #tugraz

Tweet übersetzen

Du und Claudio Canella

5:45 nachm. · 24. Dez. 2019 · Twitter Web App

23 „Gefällt mir"-Angaben


FUZZ
ALL THE THINGS

From Random Timings to Data Leakage

Michael Schwarz

December 2022

CISPA Helmholtz Center for Information Security