ShowTime

CPU Timing Attacks with the Human Eye

Antoon Purnal **Marton Bognar**

Frank Piessens Ingrid Verbauwhede

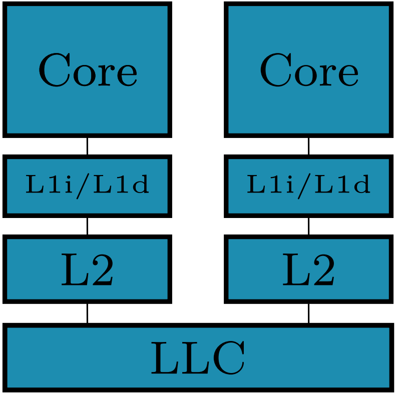
KU LEUVEN

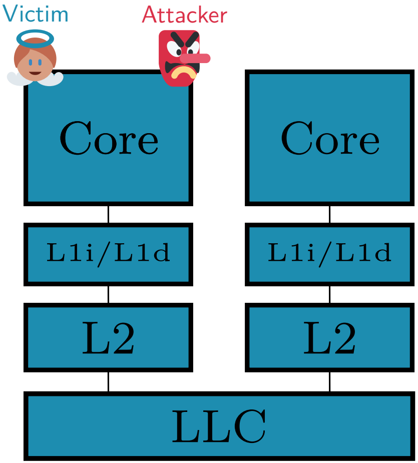
fwo

erc

Time to Start

1687330800


Core
Core
L1i/L1d
L1i/L1d
L2
L2
LLC



Victim

Attacker

Core

Core

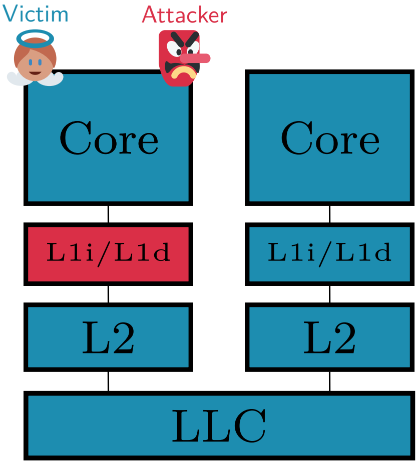
L1i/L1d

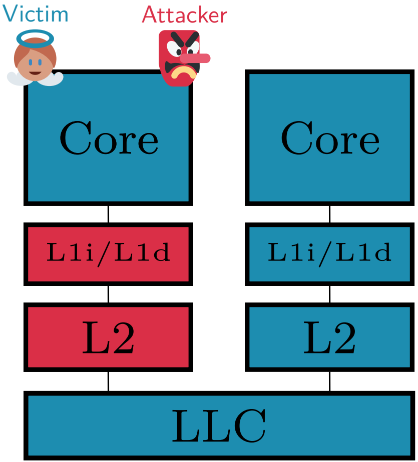
L1i/L1d

L2

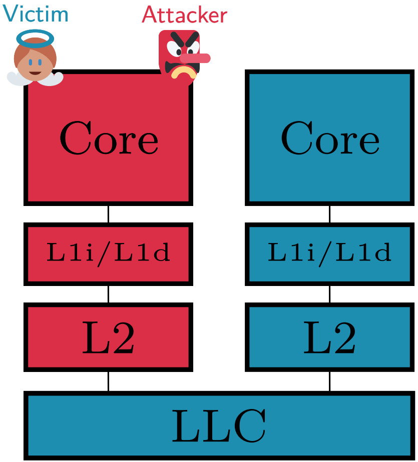
L2

LLC

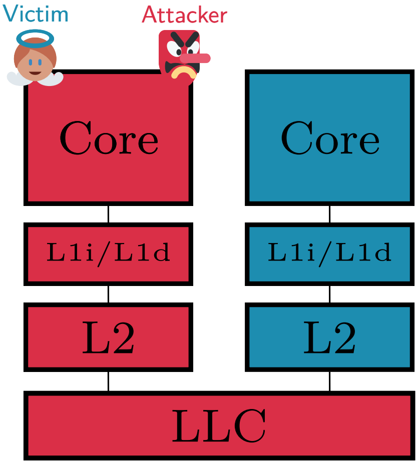

Victim
Attacker
Core
Core
L1i/L1d
L1i/L1d
L2
L2
LLC

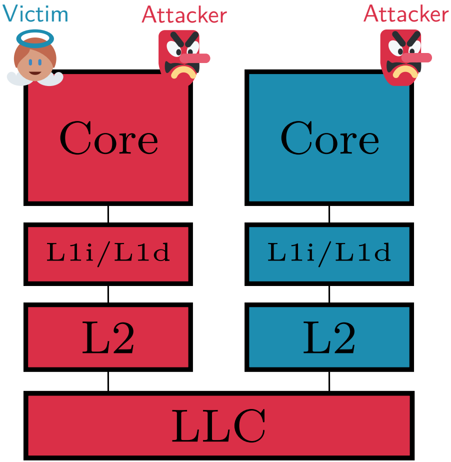

Victim
Attacker
Core
Core
L1i/L1d
L1i/L1d
L2
L2
LLC

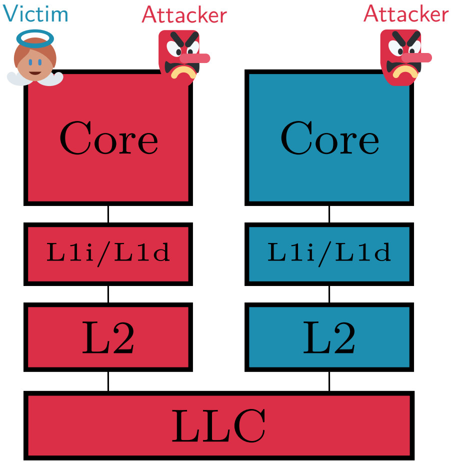
Execution Ports
Variable-Latency ops
μop cache
Scheduler Queue



Execution Ports
Variable-Latency ops
µop cache
Scheduler Queue

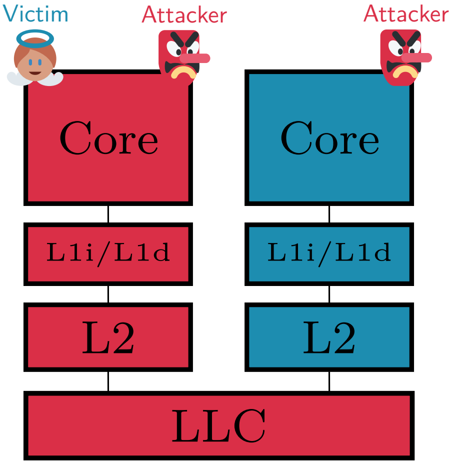



Victim
Attacker
Attacker
Core
Core
L1i/L1d
L1i/L1d
L2
L2
LLC



Side-channel attacks exploit
minuscule timing differences

1-100 ns



Victim

Attacker

Attacker

Core

Core

L1i/L1d

L1i/L1d

L2

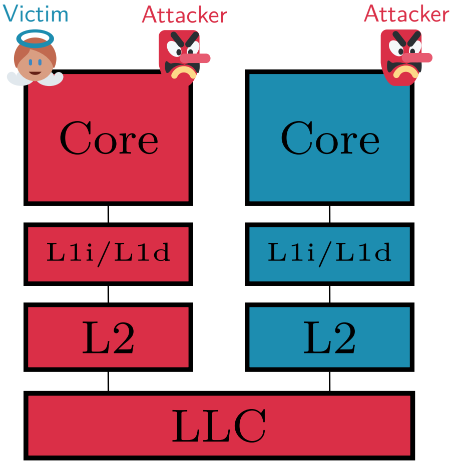
L2

LLC

Side-channel attacks exploit
minuscule timing differences

1-100 ns

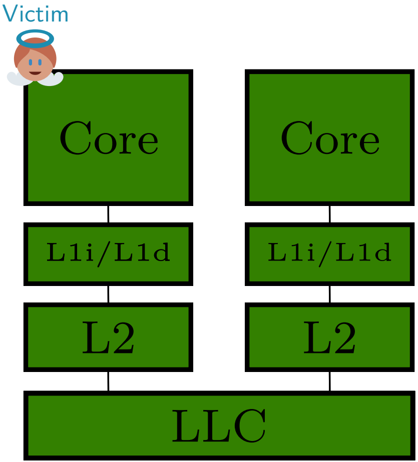
>100 µs



Side-channel attacks exploit minuscule timing differences

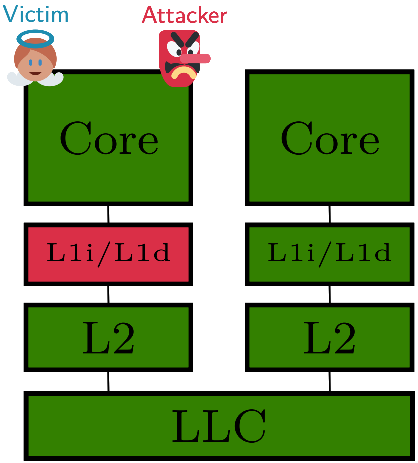
1-100 ns

>100 µs



1-100 ns

>100 µs



Victim

Attacker

Core

Core

L1i/L1d

L1i/L1d

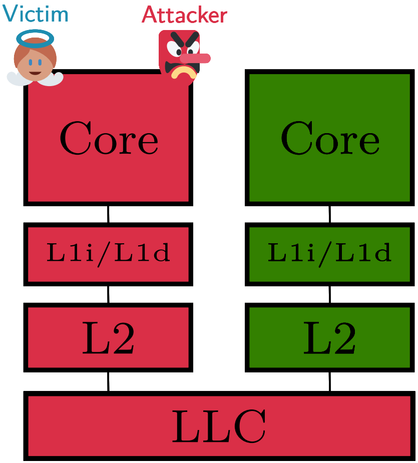
L2

L2

LLC

1-100 ns

>100 µs



Victim

Attacker

Core

Core

L1i/L1d

L1i/L1d

L2

L2

LLC

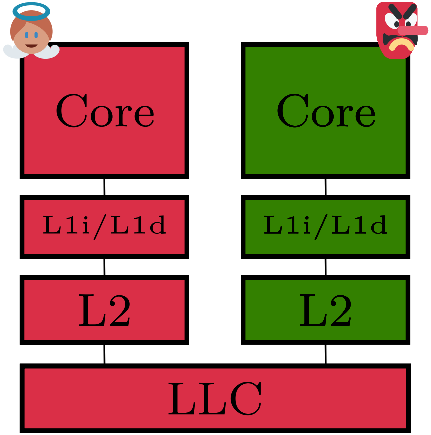
ShowTime

1-100 ns

>100 µs

Victim

Attacker



Core

Core

L1i/L1d

L1i/L1d

L2

L2

LLC

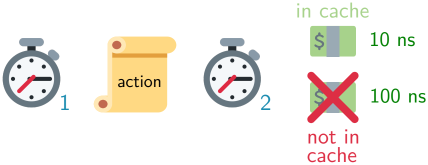
ShowTime

1-100 ns

>100 µs

action

1
action
2



1

action

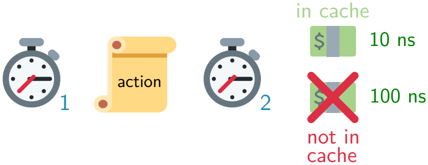
2

in cache

10 ns

100 ns

not in cache



1 action 2

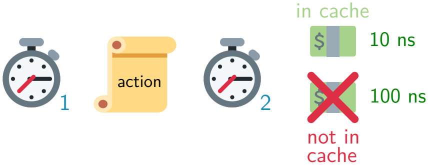
in cache

10 ns

100 ns

not in cache

1 action 2



1

action

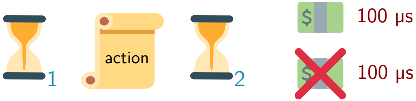
2

in cache

10 ns

100 ns

not in cache



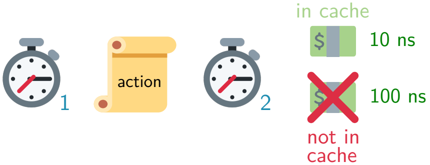
1

action

2

100 µs

100 µs



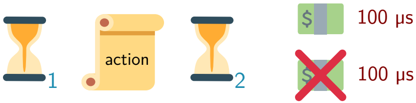
1 action 2

in cache

10 ns

100 ns

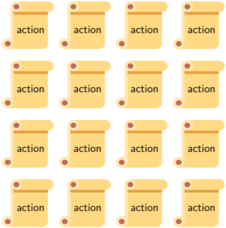
not in cache



1 action 2

100 μs

100 μs



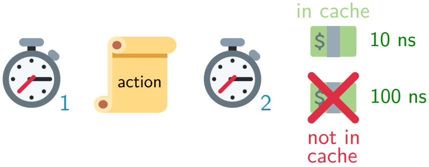
action action action action

action action action action

action action action action

action action action action

multi-shot amplifier



1

action

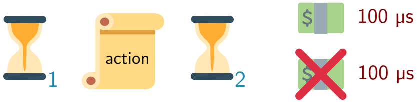
2

in cache

10 ns

100 ns

not in cache



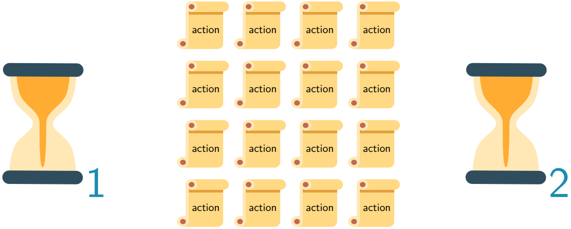
1

action

2

100 µs

100 µs



1

action action action action

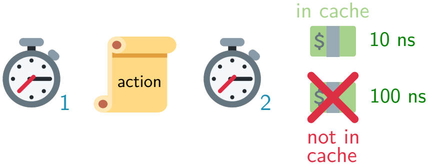
action action action action

action action action action

action action action action

2

multi-shot amplifier

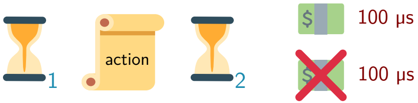


in cache

10 ns

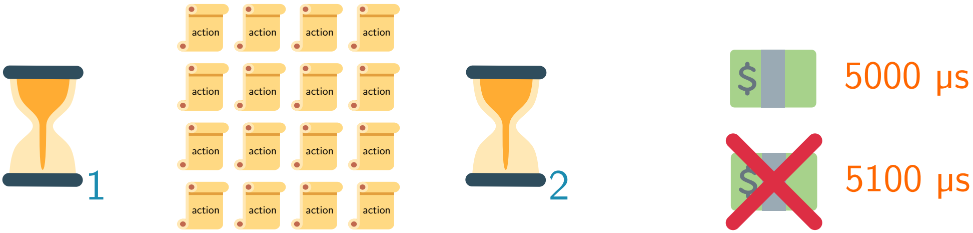
100 ns

not in cache



100 µs

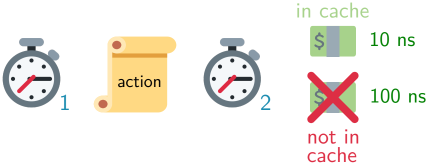
100 µs



5000 µs

5100 µs

multi-shot amplifier



1

action

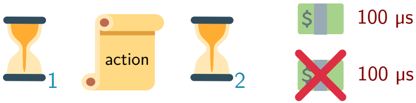
2

in cache

10 ns

100 ns

not in cache



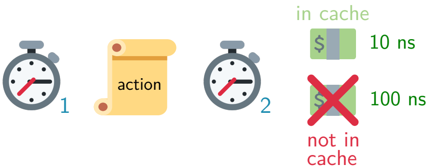
1

action

2

100 μs

100 μs



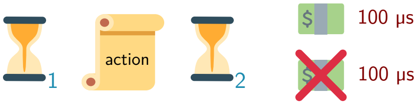
1 action 2

in cache

10 ns

100 ns

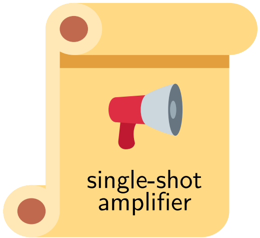
not in cache



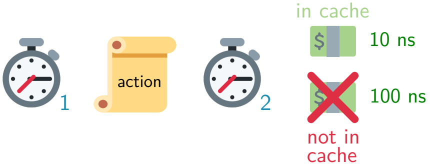
1 action 2

100 µs

100 µs



single-shot amplifier



1

action

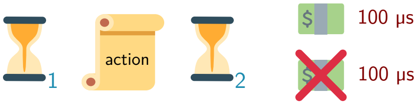
2

in cache

10 ns

100 ns

not in cache



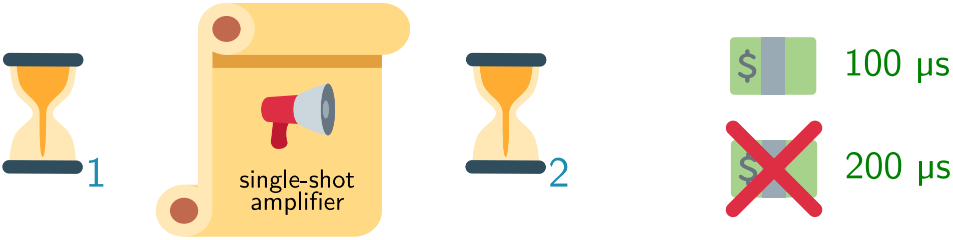
1

action

2

100 μs

100 μs



1

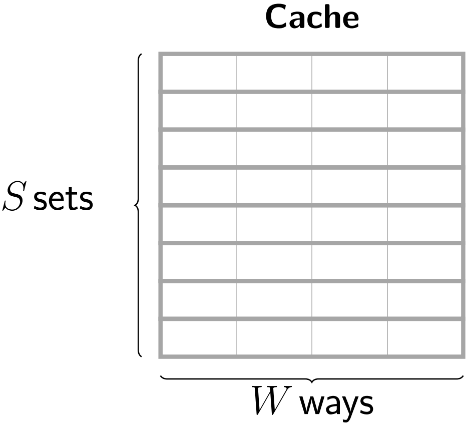
single-shot amplifier

2

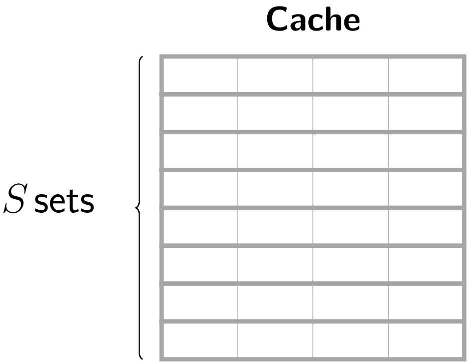
100 μs

200 μs

Sets and Eviction



Sets and Eviction

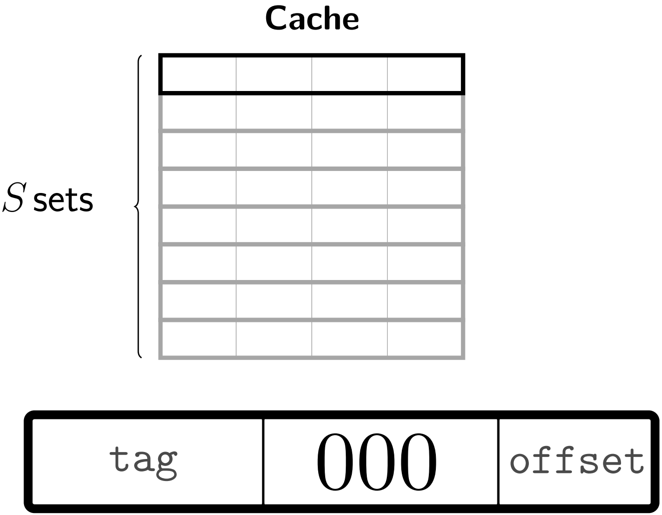


Cache

S sets

`tag`	`index`	`offset`

Sets and Eviction



Cache

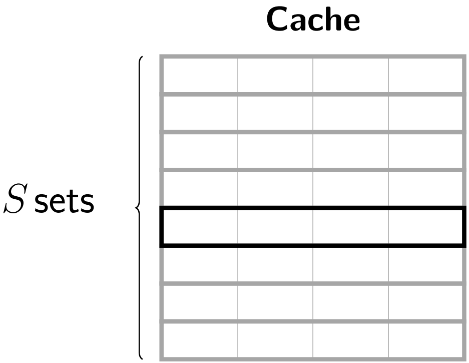
S sets

tag

000

offset

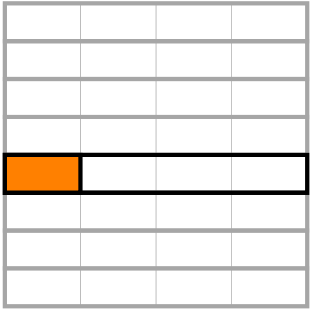
Sets and Eviction



tag	101	offset

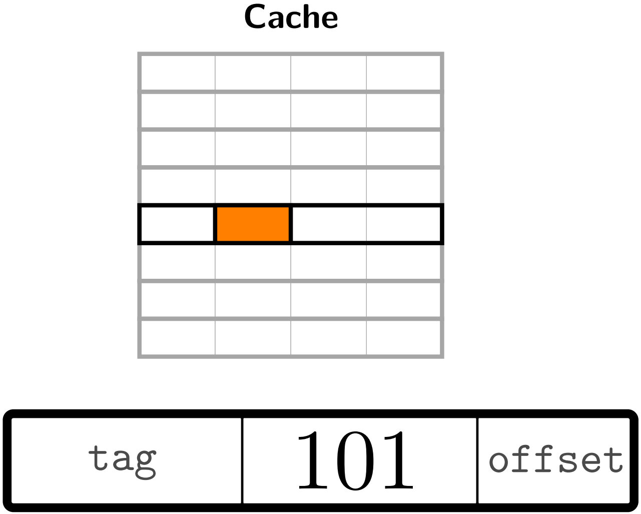
Sets and Eviction

Cache



tag	101	offset

Sets and Eviction

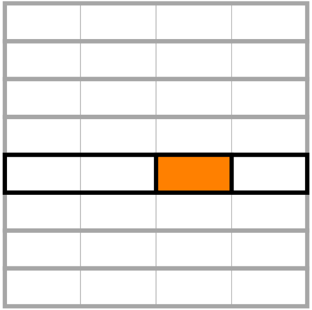


Cache

tag | 101 | offset

Sets and Eviction

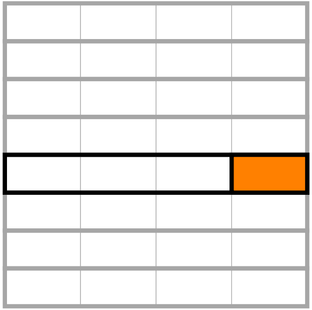
Cache



tag	101	offset

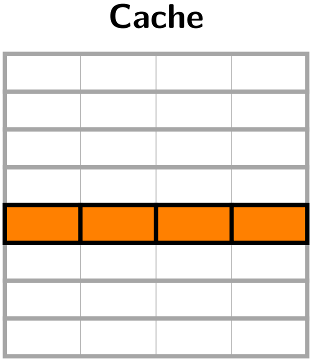
Sets and Eviction

Cache



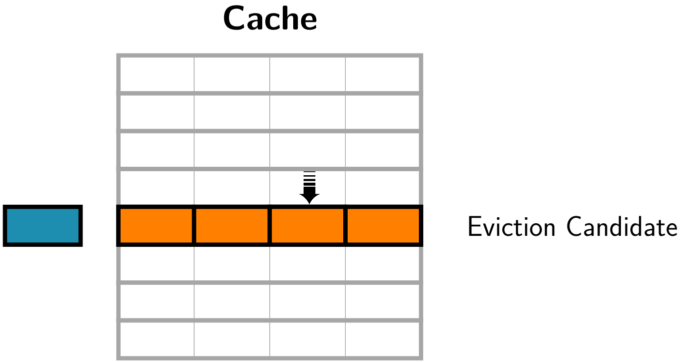
tag	101	offset

Sets and Eviction



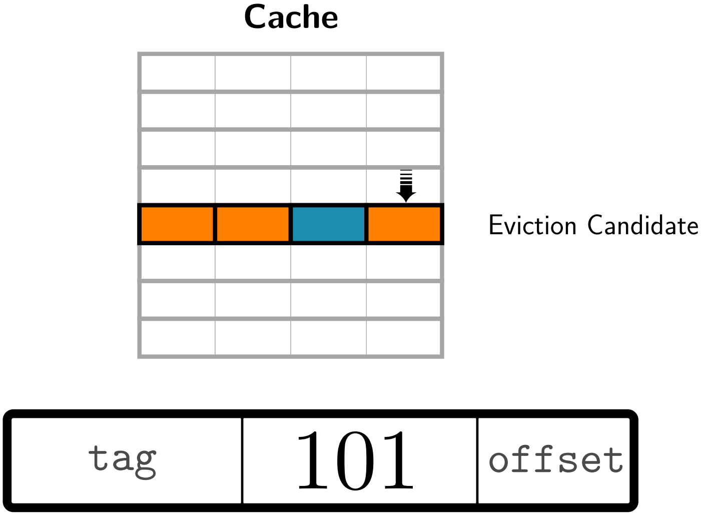
tag	101	offset

Sets and Eviction



tag	101	offset

Sets and Eviction

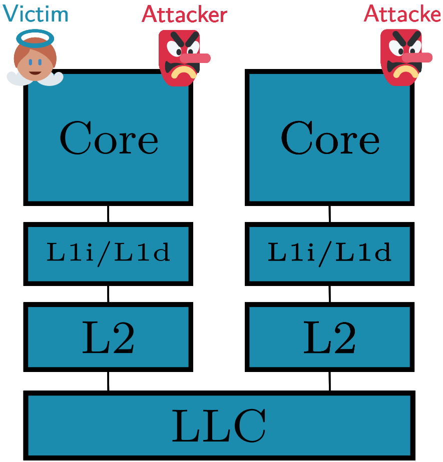


Cache

Eviction Candidate

tag | 101 | offset

🌲 📣



Victim

Attacker

Attacker

Core

Core

L1i/L1d

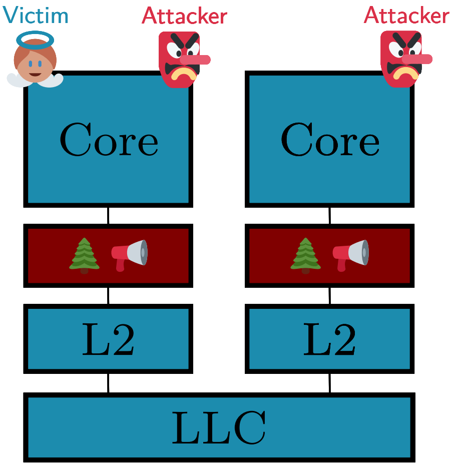
L1i/L1d

L2

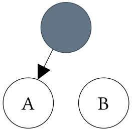
L2

LLC

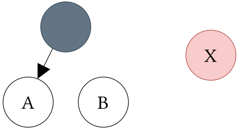
🌲 📣


Victim
Attacker
Attacker
Core
Core
L2
L2
LLC

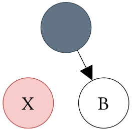
🌲 📣


A
B

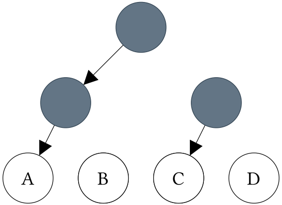
🌲 📣


X
A
B

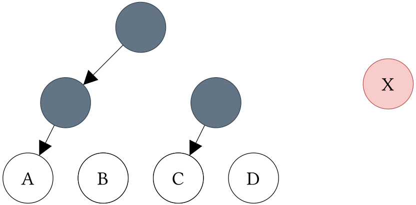
🌲 📣


X
B

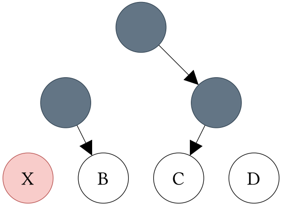
🌲 📢


A
B
C
D

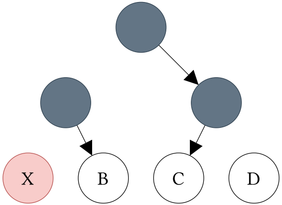
🌲 📣


X
A
B
C
D

🌲 📣

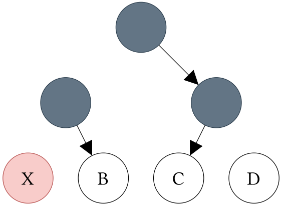

X
B
C
D

🌲 📣



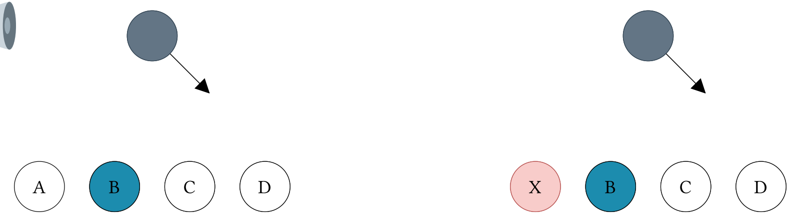
B

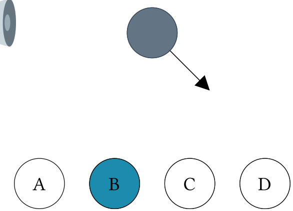
🌲 📣

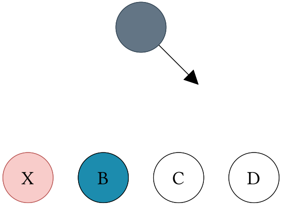


BABCBDBA···

🌲 📣


A
B
C
D
X
B
C
D

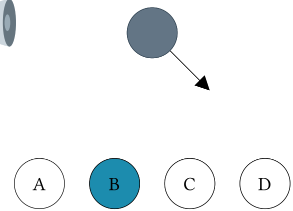


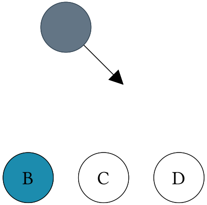


BABCBDBA···

all L1 hits

🌲 📣

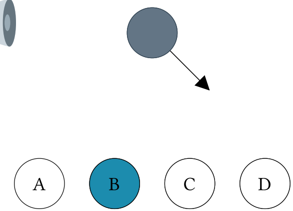




BABCBDBA···

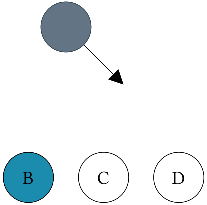
all L1 hits

🌲 📣



BABCBDBA···

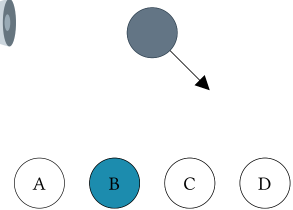
all L1 hits

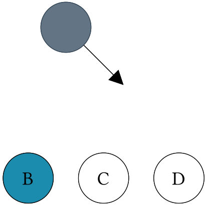


BABCBDBA···

many L1 misses

🌲 📢





BABCBDBA···

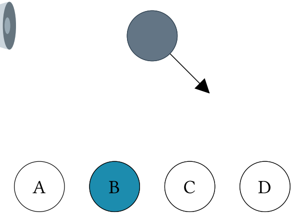
all L1 hits

BABCBDBA···

many L1 misses

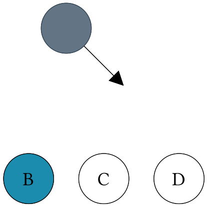
1. 📢 from 1.3x to 2x

🌲 📢



BABCBDBA···

all L1 hits

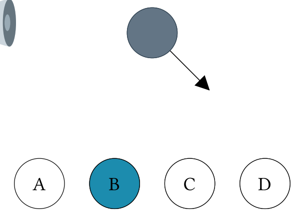


BABCBDBA···

many L1 misses

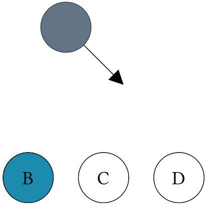
1. 📢 from 1.3x to 2x
2. ⏳ from 500us to 5ms

🌲 📢



BABCBDBA···

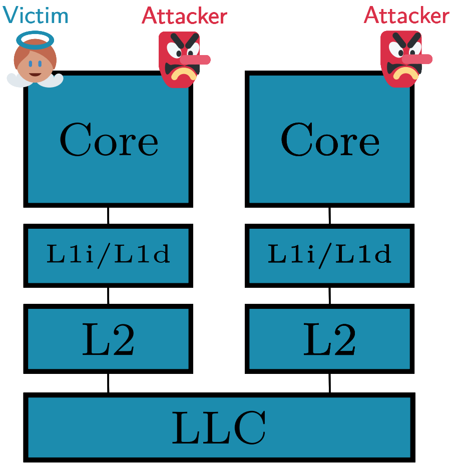
all L1 hits



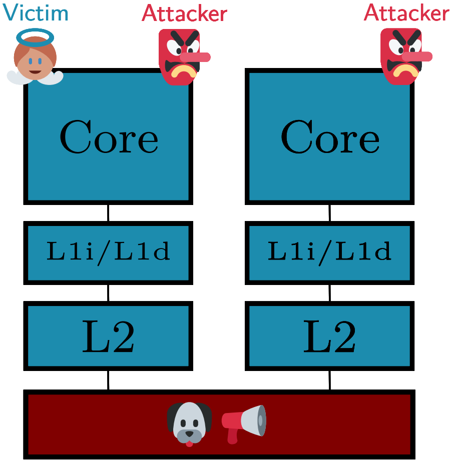
BABCBDBA···

many L1 misses

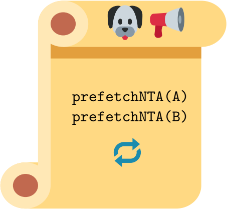
1. 📢 from 1.3x to 2x
2. ⏳ from 500us to 5ms
3. 🎩 amplify more side channels


Victim
Attacker
Attacker
Core
Core
L1i/L1d
L1i/L1d
L2
L2
LLC

🐶 📢


Victim
Attacker
Attacker
Core
Core
L1i/L1d
L1i/L1d
L2
L2
🐶 📢

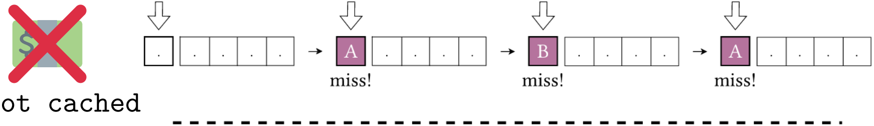
🐶 📢



🐶 📢

```
prefetchNTA(A)
prefetchNTA(B)
```

🔁

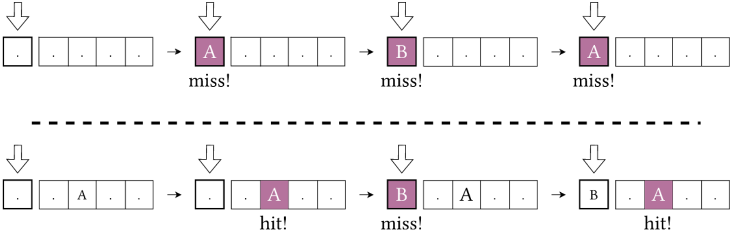


A not cached

```
prefetchNTA(A)
prefetchNTA(B)
```

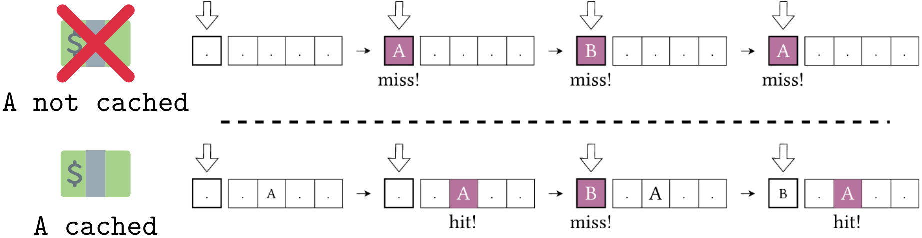
A not cached

A cached



```
prefetchNTA(A)
prefetchNTA(B)
```

🐶 📢



A not cached

A cached

```
prefetchNTA(A)
prefetchNTA(B)
```

1. 📢 10x
2. ⏳ ? ms

Live Demo

Can the audience perform a cache attack with their eyes?

Fifteen humans
(100 samples each)

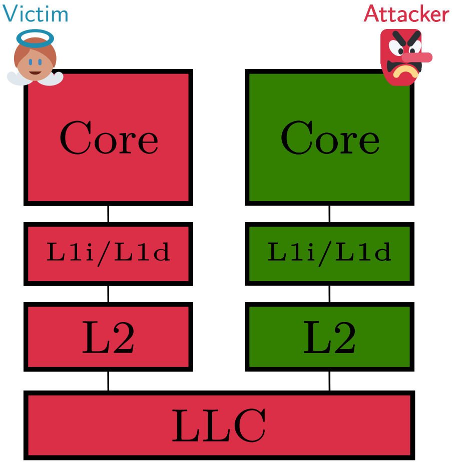
Fifteen humans
(100 samples each)

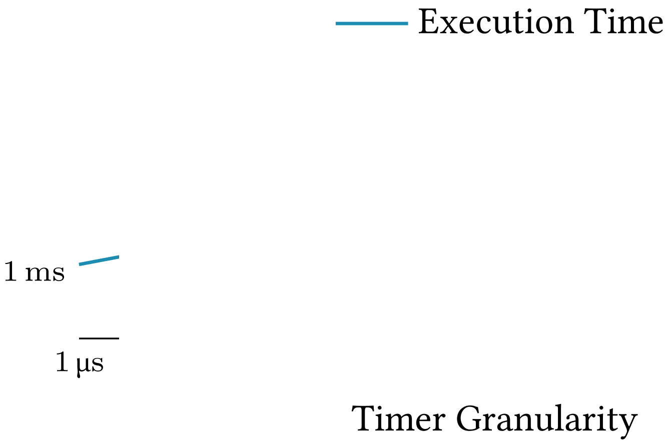
Average 98.4%

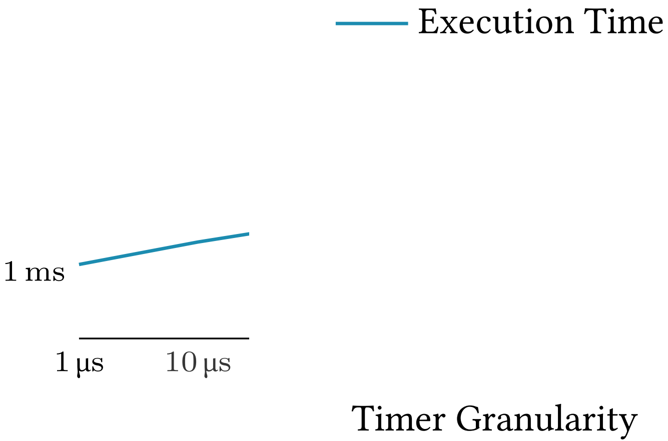
Fifteen humans
(100 samples each)

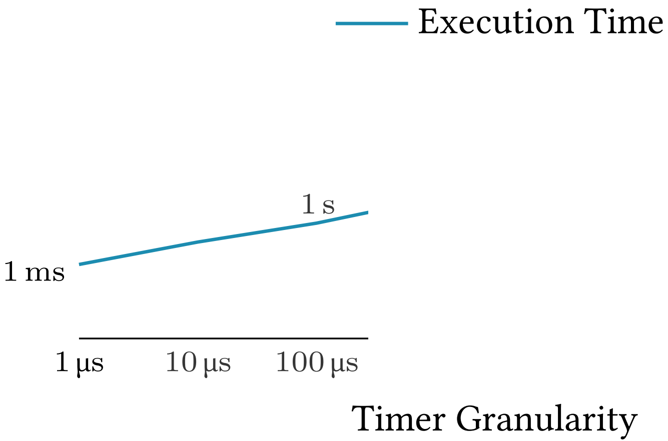
Average	98.4%
Median	99%
Max	100%

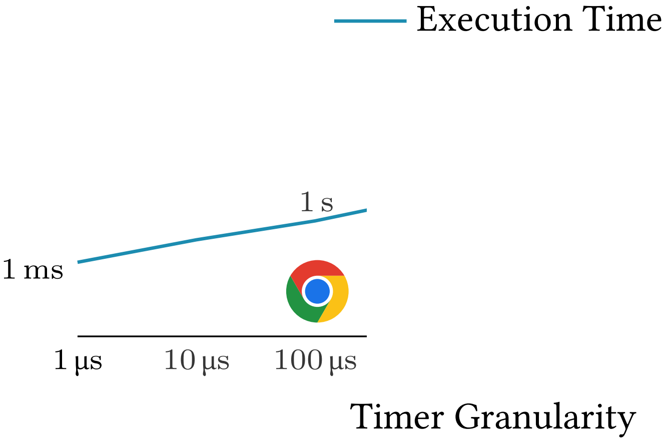
Eviction Set Construction

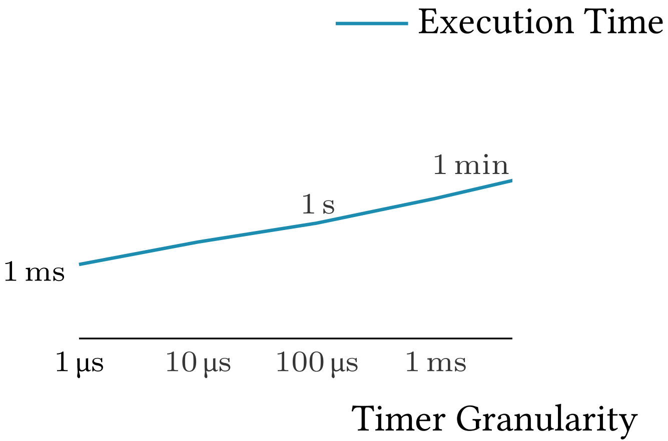


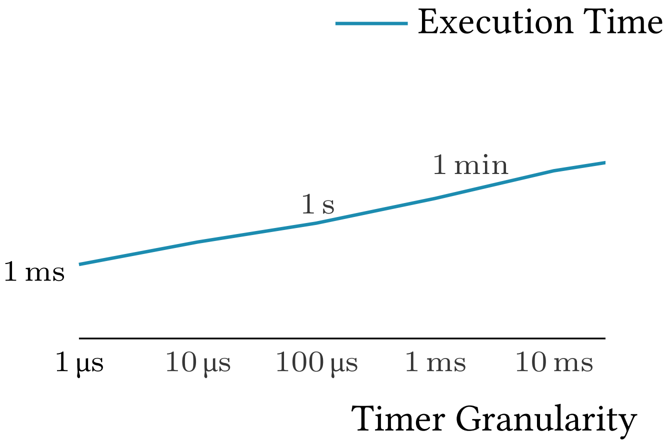

Execution Time
1 ms
1 µs
Timer Granularity

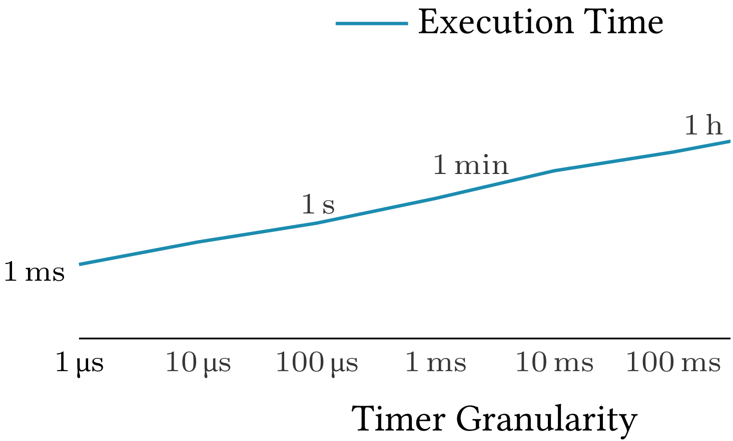

Execution Time
1 ms
1 µs
10 µs
Timer Granularity


Execution Time
1 s
1 ms
1 µs
10 µs
100 µs
Timer Granularity


Execution Time
1 s
1 ms
1 µs
10 µs
100 µs
Timer Granularity


Execution Time
1 min
1 s
1 ms
1 µs
10 µs
100 µs
1 ms
Timer Granularity


Execution Time
1 ms
1 s
1 min
1 µs
10 µs
100 µs
1 ms
10 ms
Timer Granularity

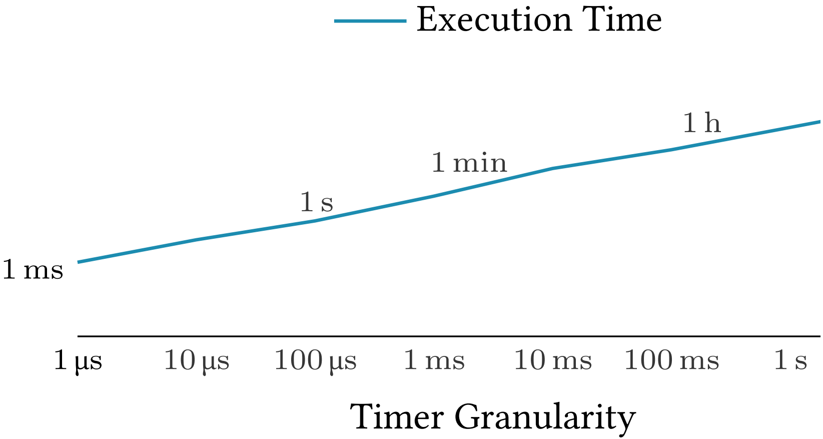

Execution Time
1 h
1 min
1 s
1 ms
1 µs
10 µs
100 µs
1 ms
10 ms
100 ms
Timer Granularity

1687330800

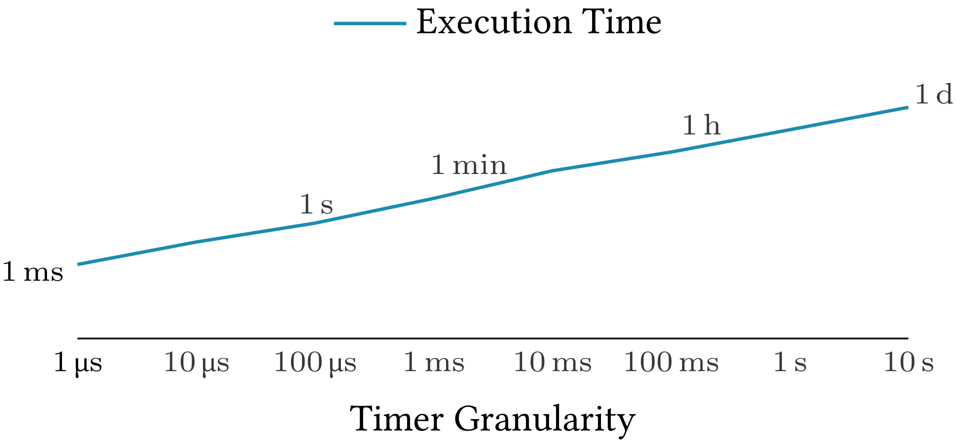
1687330801

1687330802

1687330803


Execution Time
1 ms
1 s
1 min
1 h
1 µs
10 µs
100 µs
1 ms
10 ms
100 ms
1 s
Timer Granularity

168733080


Execution Time
1 ms
1 s
1 min
1 h
1 d
1 µs
10 µs
100 µs
1 ms
10 ms
100 ms
1 s
10 s
Timer Granularity

Takeaways

Restricting timers is not a holistic countermeasure against timing attacks

Takeaways

Restricting timers is not a holistic countermeasure against timing attacks

Side channels can be **amplified** 📢

Takeaways

Restricting timers is not a holistic countermeasure against timing attacks

Side channels can be amplified 📢

Side channels can be converted 🪄

ShowTime

CPU Timing Attacks with the Human Eye

Antoon Purnal **Marton Bognar**

Frank Piessens Ingrid Verbauwhede

Emoji credit: Twitter Open Source (CC-BY)