

ShowTime

CPU Timing Attacks
with the Human Eye

Antoon Purnal

Marton Bogнар

Frank Piessens

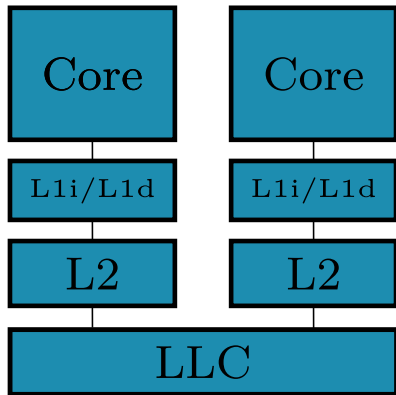
Ingrid Verbauwhede



Time to Start

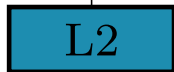
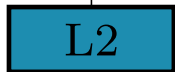
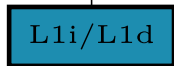
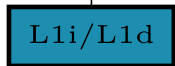
1683796500





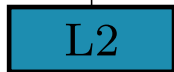
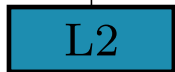
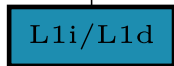
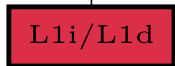
Victim

Attacker



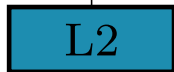
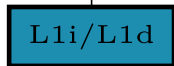
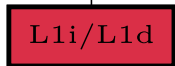
Victim

Attacker



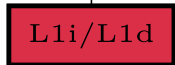
Victim

Attacker

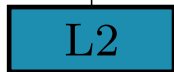
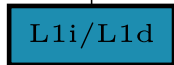


Execution Ports
Variable-Latency ops
 μ op cache
Scheduler Queue

Victim

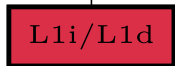


Attacker

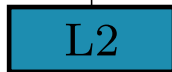
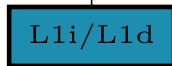


Execution Ports
Variable-Latency ops
 μ op cache
Scheduler Queue

Victim



Attacker



Victim



Attacker



Attacker



Core

Core

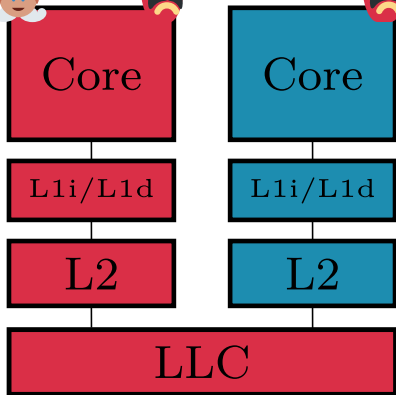
L1i/L1d

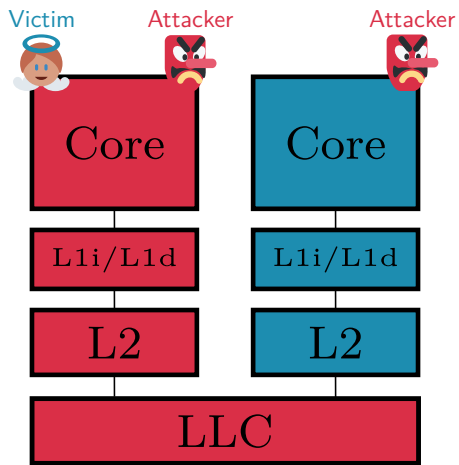
L1i/L1d

L2

L2

LLC

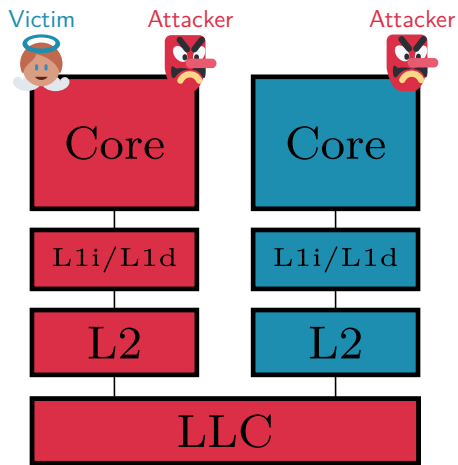




Side-channel attacks exploit
minuscule timing differences



1-100 ns



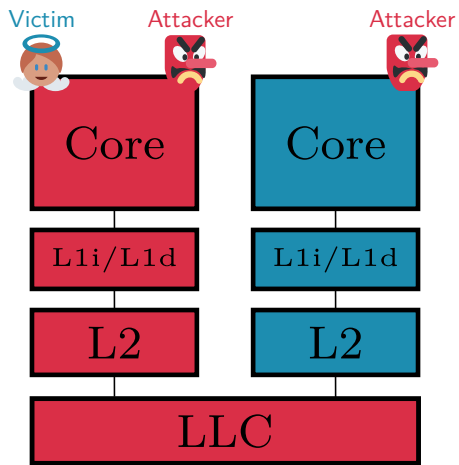
Side-channel attacks exploit
minuscule timing differences



1-100 ns



>100 μ s



Side-channel attacks exploit
minuscule timing differences



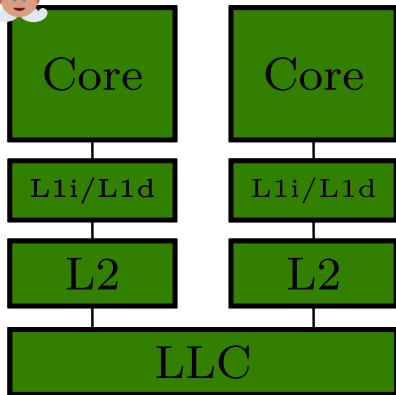
1-100 ns



>100 μ s



Victim



1-100 ns

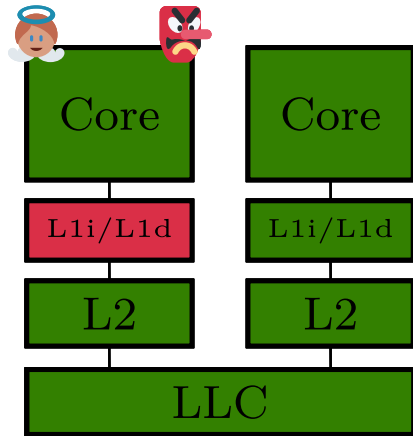


>100 μ s



Victim

Attacker



1-100 ns

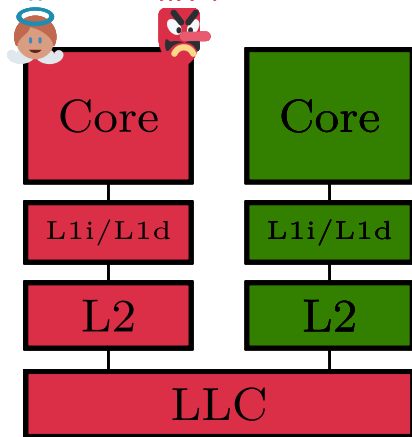


>100 μ s



Victim

Attacker



1-100 ns



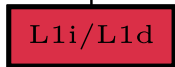
ShowTime



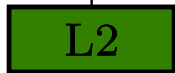
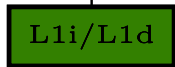
>100 μ s



Victim



Attacker



ShowTime



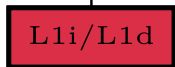
1-100 ns



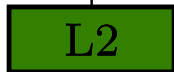
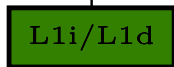
>100 μ s



Victim



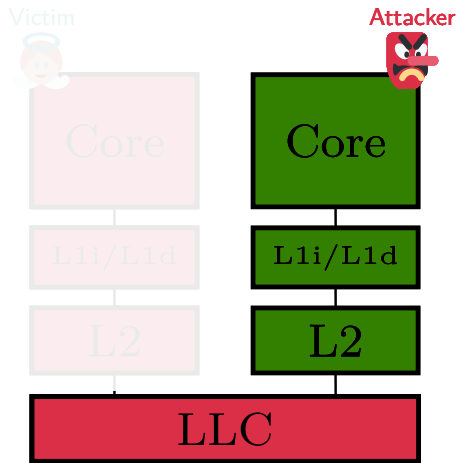
Attacker



ShowTime

Goal: expose secret leakage *anywhere* in the CPU

Visible



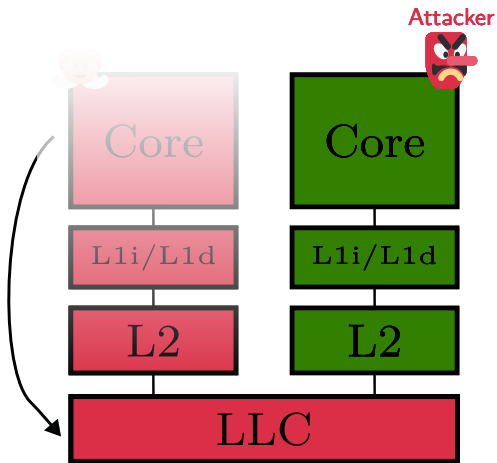
ShowTime

Goal: expose secret leakage *anywhere* in the CPU

Visible



Convert



Goal: expose secret leakage *anywhere* in the CPU

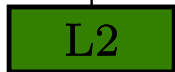
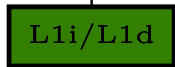
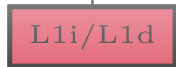
Attacker



Visible
Measurable



Convert



<<



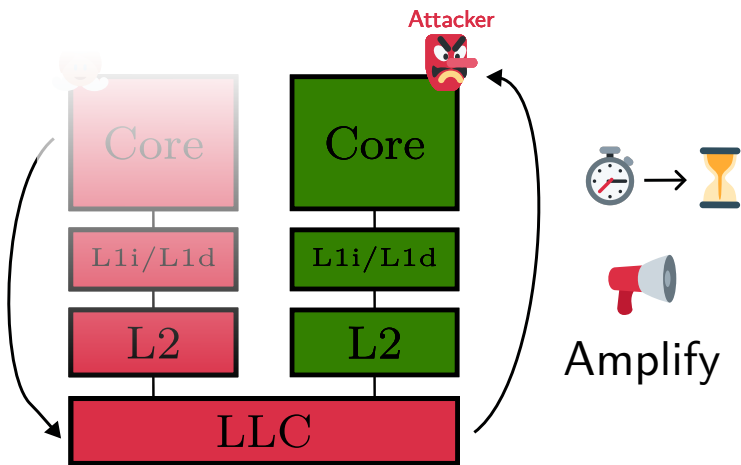
?

Goal: expose secret leakage *anywhere* in the CPU

Visible
Measurable



Convert



Goal: expose secret leakage *anywhere* in the CPU

Attacker Model

Basic capabilities

Cross-core

No hugepages

No fixed CPU frequency









in cache

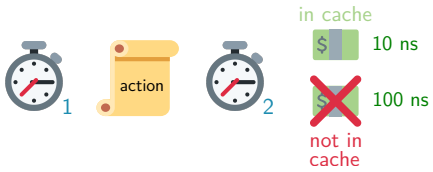


10 ns

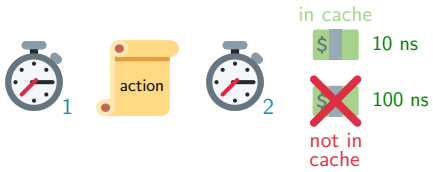


100 ns

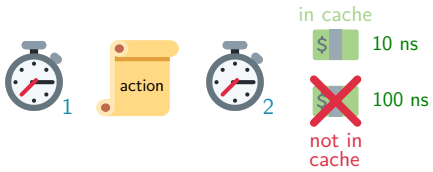
not in
cache



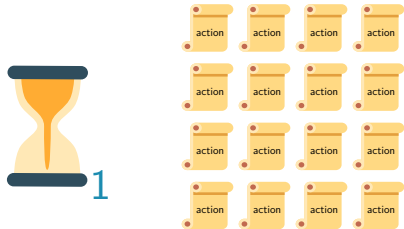
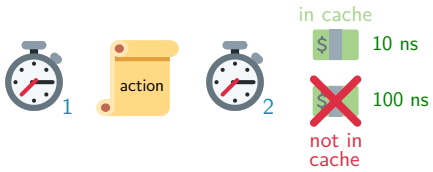




multi-shot amplifier



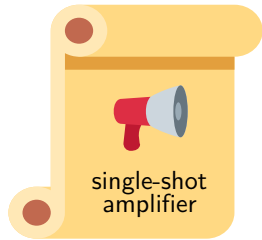
multi-shot amplifier

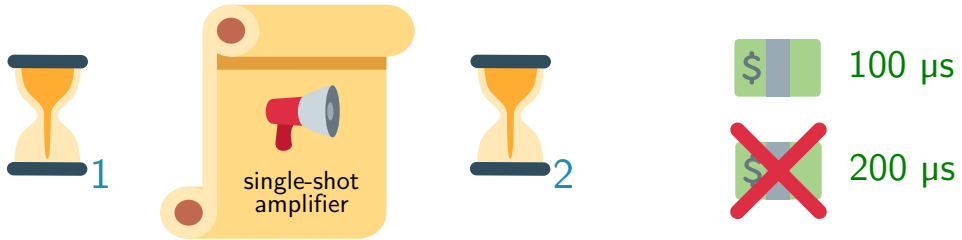


multi-shot amplifier

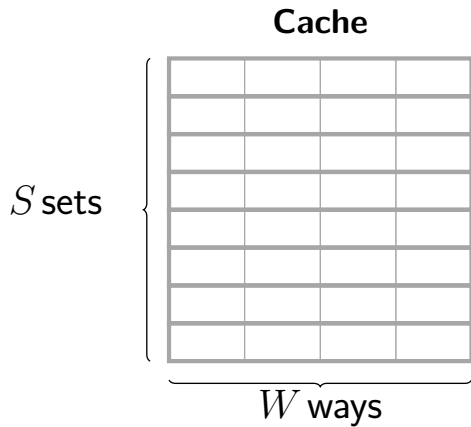




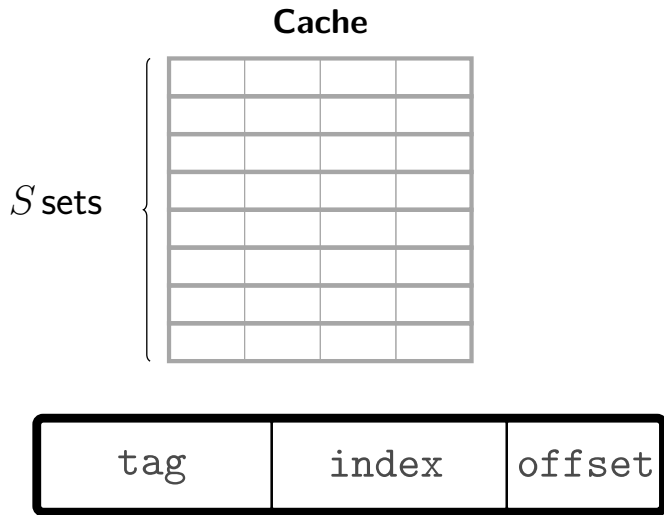




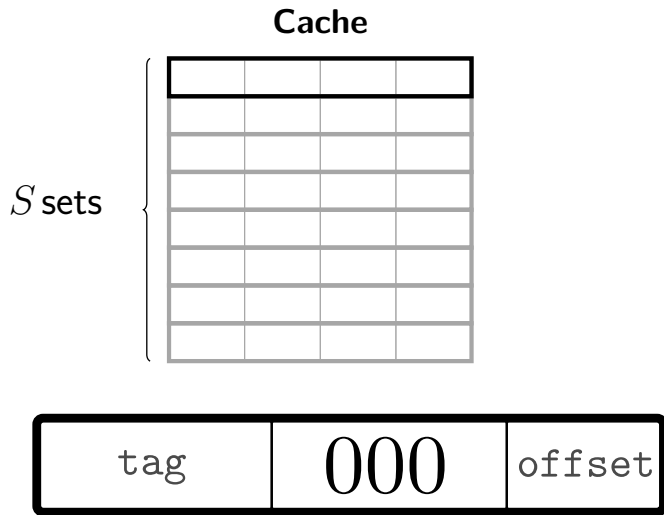
Sets and Eviction



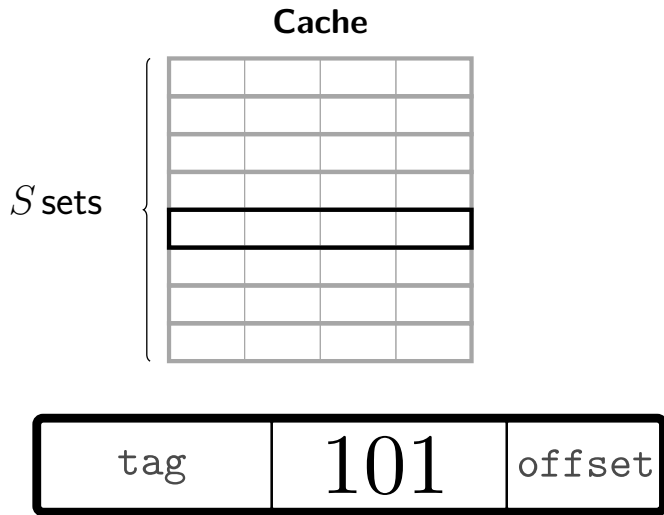
Sets and Eviction



Sets and Eviction



Sets and Eviction



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

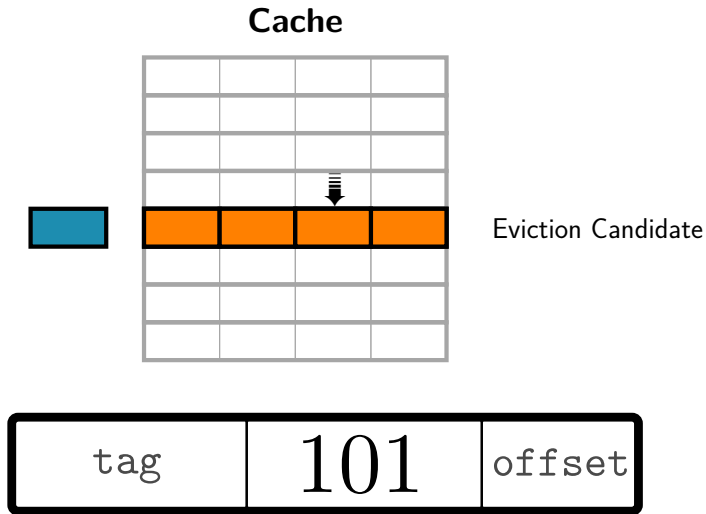
tag	101	offset
-----	-----	--------

Sets and Eviction

Cache

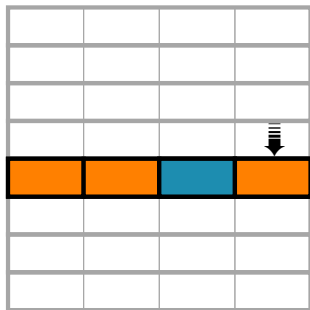
tag	101	offset
-----	-----	--------

Sets and Eviction



Sets and Eviction

Cache



Eviction Candidate





Victim



Attacker



Attacker



Core

Core

L1i/L1d

L1i/L1d

L2

L2

LLC



Victim



Attacker



Attacker



Core

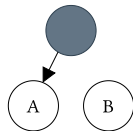
Core

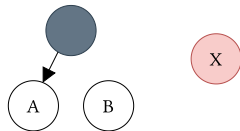


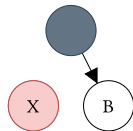
L2

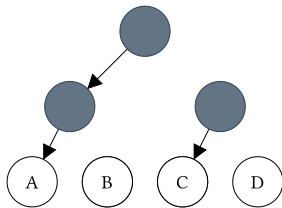
L2

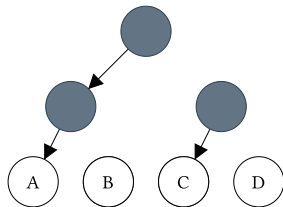
LLC

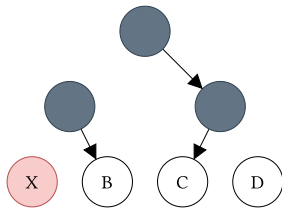


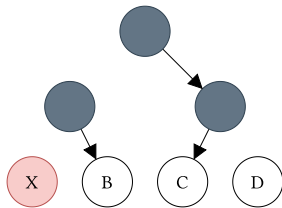




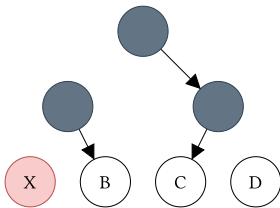








B



BABCBDDBA...



A

B

C

D

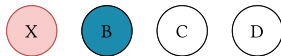
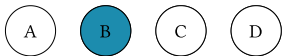


X

B

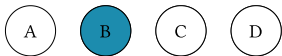
C

D



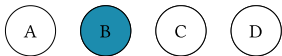
BABCBDDBA...

all L1 hits



BABCBDDBA...

all L1 hits



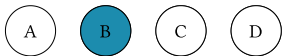
BABCBDDBA...

all L1 hits



BABCBDDBA...

many L1 misses



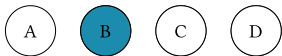
BABCBDDBA...

BABCBDDBA...

all L1 hits

many L1 misses

1.  from 1.3x to 2x





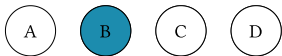
BABCBDDBA...

BABCBDDBA...

all L1 hits

many L1 misses

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



BABCBDDBA...

BABCBDDBA...

all L1 hits

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

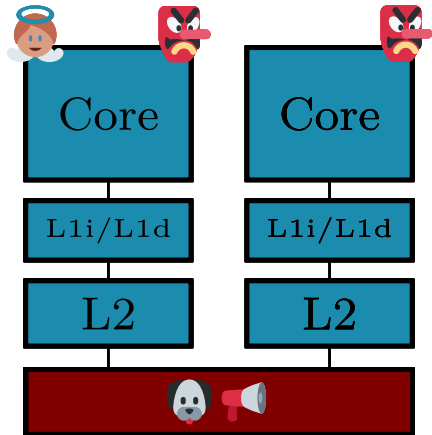
LLC

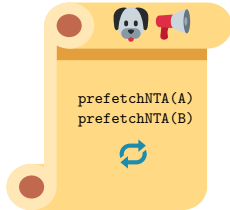


Victim

Attacker

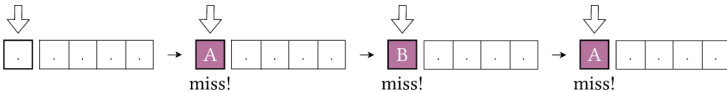
Attacker

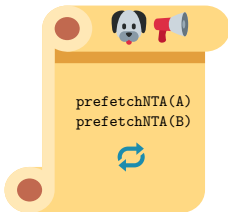






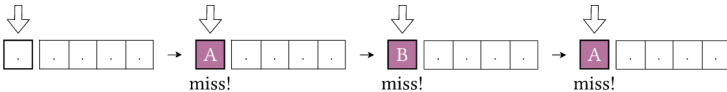
A not cached



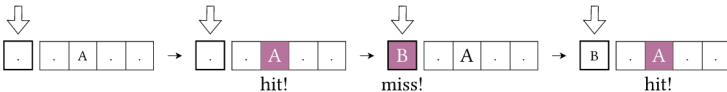




A not cached

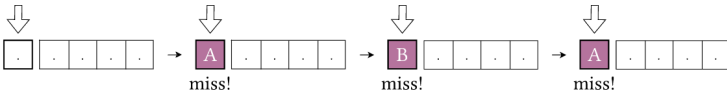


A cached

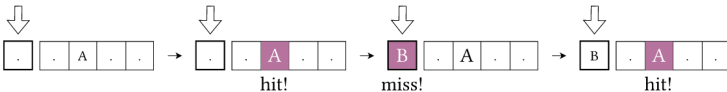




A not cached



A cached



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%

Time to Order



```
res = fn()
```

```
load(res)
```

```
load(x)
```

Time to Order



```
dep = prepare()
```

```
// first leg
```

```
dep1 = secret-delay(dep)  
dep1 = instr-1(dep1)
```

```
// second leg
```

```
dep2 = fixed-delay(dep)  
dep2 = instr-2(dep2)
```

```
race-end(dep1, dep2)
```

Time to Order



```
d = evict(A)
```

```
// first leg
```

```
d1 = secret-delay(d)
```

```
d1 = load(A ^ d1)
```

```
// second leg
```

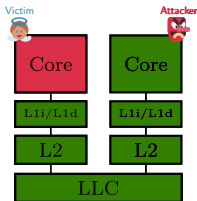
```
d2 = fixed-delay(d)
```

```
d2 = prefetchNTA(A ^ d2)
```

```
load(B ^ d1 ^ d2)
```

Teasers

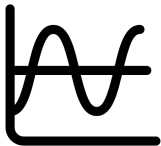
Cross-core port contention



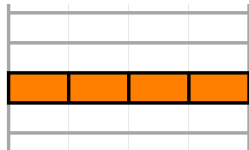
Architectural reordering



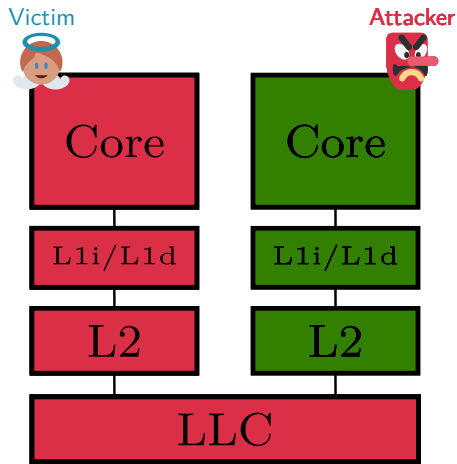
CPU frequency



Eviction set construction



Eviction Set Construction



LLC Eviction Sets



100 μ s



L1 PLRU 



Time To Order

LLC Eviction Sets



100 μ s



L1 PLRU



Time To Order

intel[®]



???



prefetchNTA



-

— Execution Time

1 ms

1 μ s

Timer Granularity

— Execution Time

1 ms

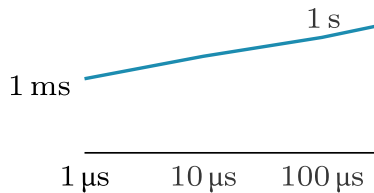
1 μ s

10 μ s

Timer Granularity

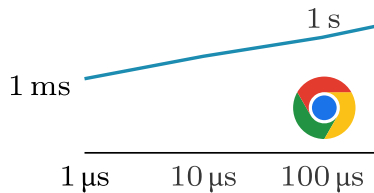


— Execution Time



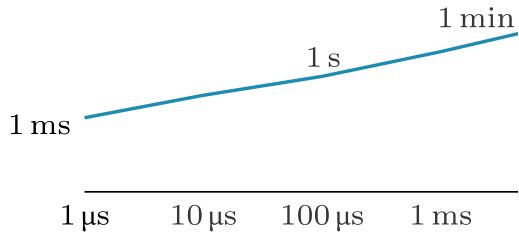
Timer Granularity

— Execution Time



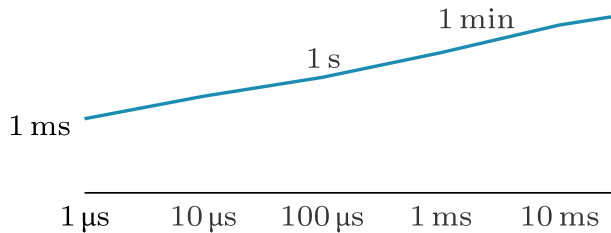
Timer Granularity

— Execution Time

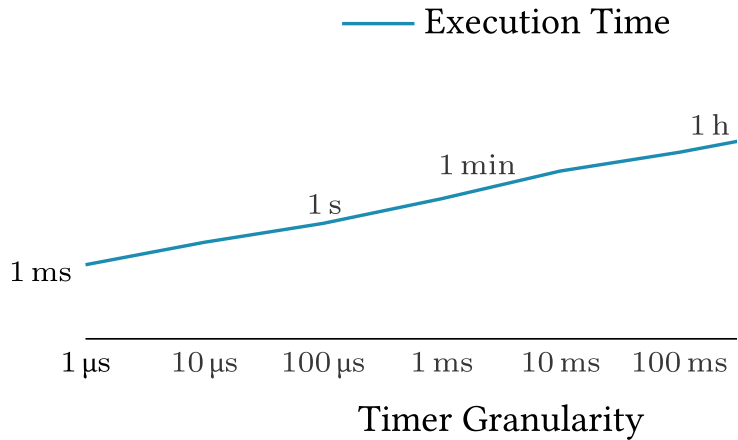


Timer Granularity

— Execution Time



Timer Granularity

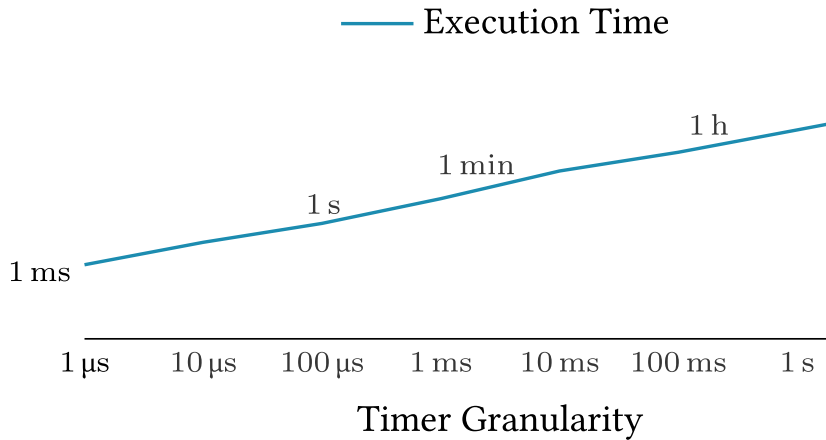


1683796500

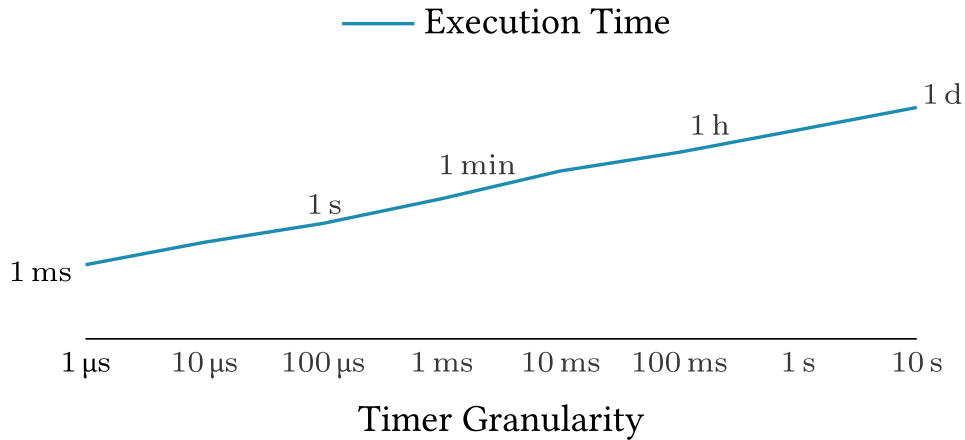
1683796501

1683796502

1683796503



168379650 



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 Bogнар

Frank Piessens

Ingrid Verbauwhede

