IdleLeak: Exploiting Idle State Side Effects for Information Leakage

Fabian Rauscher, Andreas Kogler, Jonas Juffinger, and Daniel Gruss

27.02.2024

Where can we find security issues?


INTEL MANUAL

CET: Control-flow Enforcement Technology	Tiger Lake, Sapphire Rapids, Sierra Forest, Grand Ridge
AVX512_VP2INTERSECT	Tiger Lake (not currently supported in any other processors)
Enqueue Stores: ENQCMD and ENQCMDS	Sapphire Rapids, Sierra Forest, Grand Ridge
CLDEMOTE	Tremont, Sapphire Rapids
PTWRITE	Goldmont Plus, Alder Lake, Sapphire Rapids
User Wait: TPAUSE, UMONITOR, UMWAIT	Tremont, Alder Lake, Sapphire Rapids
Architectural LBRs	Alder Lake, Sapphire Rapids, Sierra Forest, Grand Ridge
HLAT	Alder Lake, Sapphire Rapids, Sierra Forest, Grand Ridge
SERIALIZE	Alder Lake, Sapphire Rapids, Sierra Forest, Grand Ridge
Intel® TSX Suspend Load Address Tracking (TSXLDTRK)	Sapphire Rapids

CET: Control-flow Enforcement Technology	Tiger Lake, Sapphire Rapids, Sierra Forest, Grand Ridge
AVX512_VP2INTERSECT	Tiger Lake (not currently supported in any other processors)
Enqueue Stores: ENQCMD and ENQCMDS	Sapphire Rapids, Sierra Forest, Grand Ridge
CLDEMOTE	Tremont, Sapphire Rapids
PTWRITE	Goldmont Plus, Alder Lake, Sapphire Rapids
User Wait: TPAUSE, UMONITOR, UMWAIT	Tremont, Alder Lake, Sapphire Rapids
Architectural LBRs	Alder Lake, Sapphire Rapids, Sierra Forest, Grand Ridge
HLAT	Alder Lake, Sapphire Rapids, Sierra Forest, Grand Ridge
SERIALIZE	Alder Lake, Sapphire Rapids, Sierra Forest, Grand Ridge
Intel® TSX Suspend Load Address Tracking (TSXLDTRK)	Sapphire Rapids

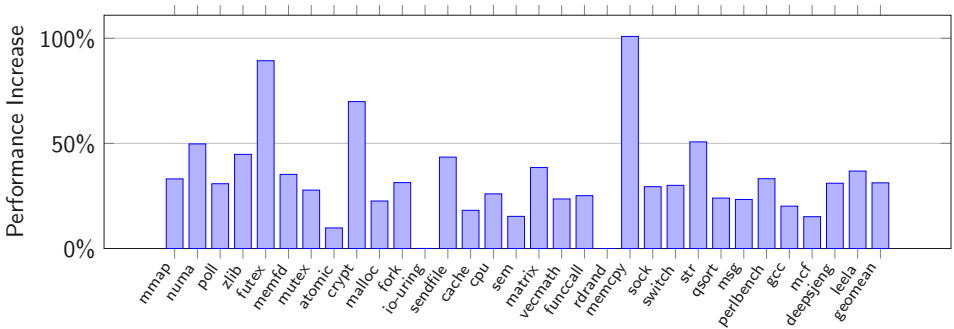
Description

TPAUSE instructs the processor to enter an implementation-dependent optimized state. There are two such optimized states to choose from: light-weight power/performance optimized state, and improved power/performance optimized state. The selection between the two is governed by the explicit input register bit[0] source operand.

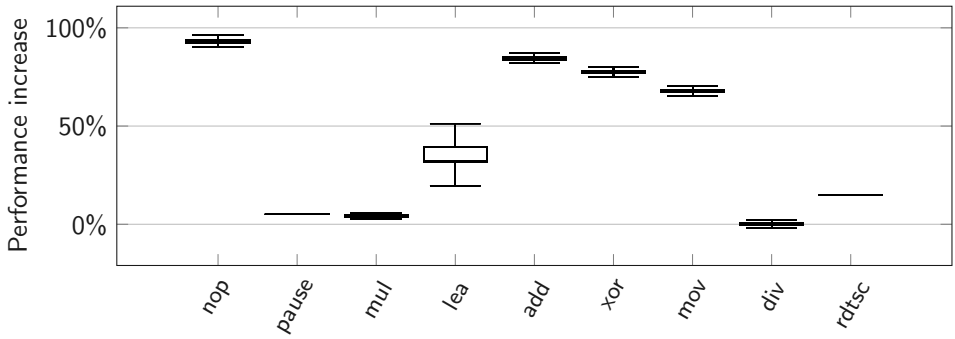
New Sleep States

State Name	Wakeup Time	Power Savings	Other Benefits
C0.2	Slower	Larger	Improves performance of the other SMT thread(s) on the same core.
C0.1	Faster	Smaller	N/A
N/A	N/A	N/A	Reserved

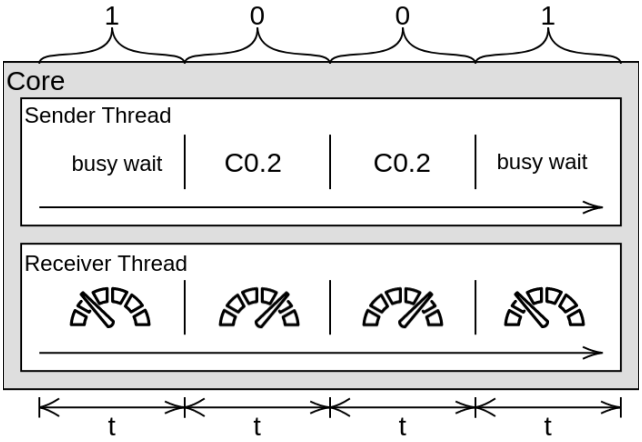
C0.2 Speedup



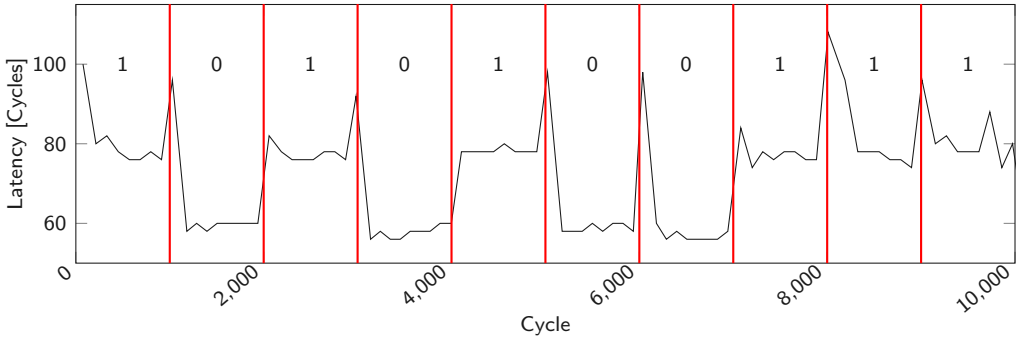
Performance increase in the Phoronix Test Suite and SPEC CPU 2017 on a logical core while the sibling logical core is in the C0.2 idle state.



Performance increase of a set of x86 instructions on an Intel i7-1260P, when the sibling logical core is in idle state C0.2 compared to a busy wait.

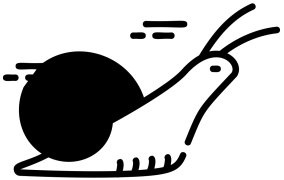

1
0
0
1
Core
Sender Thread
busy wait
C0.2
C0.2
busy wait
Receiver Thread
t
t
t
t

Covert Channel Transmission

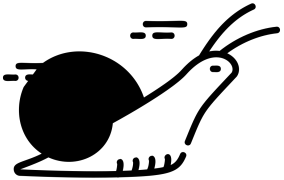


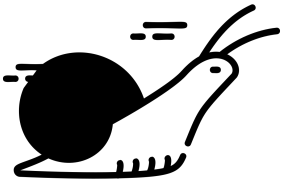
Covert Channel Speed

Covert Channel Speed



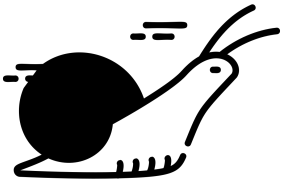
Covert Channel Speed





- Native: 7.1 Mbit/s ($\sigma_{\bar{x}} = 0.004$ Mbit/s, $n = 512$)

Covert Channel Speed



- Native: 7.1 Mbit/s ($\sigma_{\bar{x}} = 0.004$ Mbit/s, $n = 512$)
- Cross-VM: 46.3 kbit/s ($\sigma_{\bar{x}} = 0.15$ kbit/s, $n = 370$)

Wake-Up Reasons

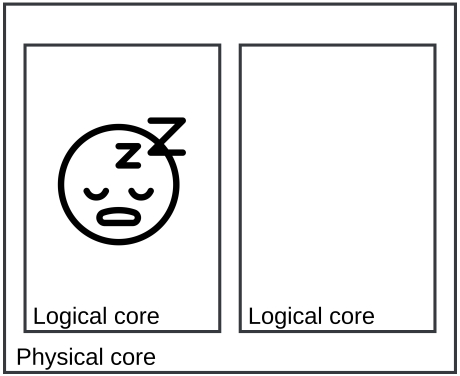
The instruction execution wakes up when the time-stamp counter reaches or exceeds the implicit EDX:EAX 64-bit input value.

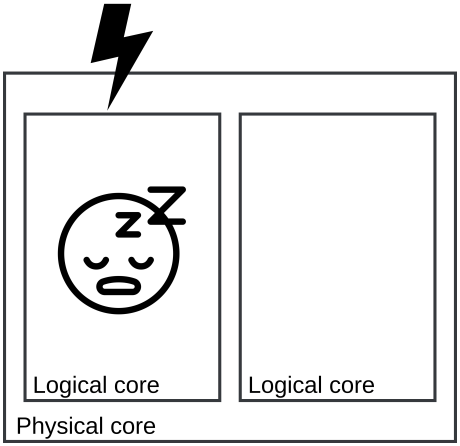
Wake-Up Reasons

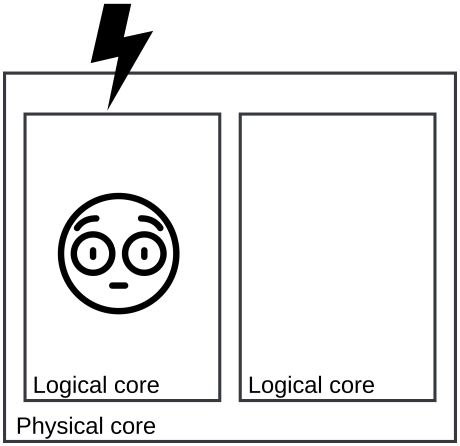
Other implementation-dependent events may cause the processor to exit the implementation-dependent optimized state proceeding to the instruction following TPAUSE. In addition, an external interrupt causes the processor to exit the implementation-dependent optimized state regardless of whether maskable-interrupts are inhibited (EFLAGS.IF =0). It should be noted that if maskable-interrupts are inhibited execution will proceed to the instruction following TPAUSE.

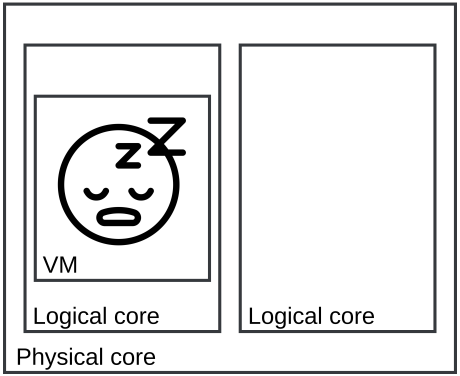
Wake-Up Reasons

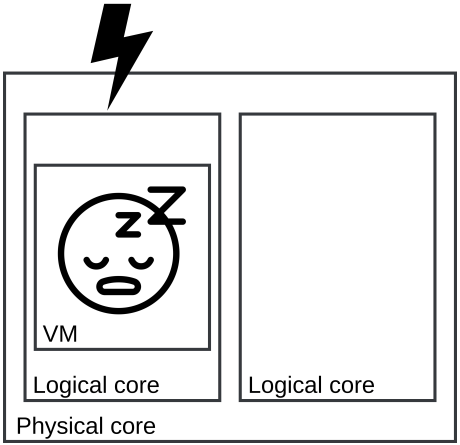
Other implementation-dependent events may cause the processor to exit the implementation-dependent optimized state proceeding to the instruction following TPAUSE. In addition, an external interrupt causes the processor to exit the implementation-dependent optimized state regardless of whether maskable-interrupts are inhibited (EFLAGS.IF =0). It should be noted that if maskable-interrupts are inhibited execution will proceed to the instruction following TPAUSE.

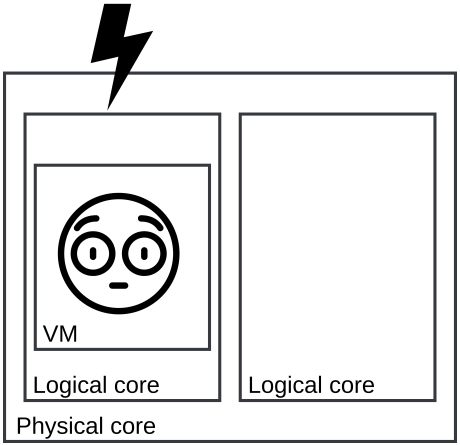

Logical core
Logical core
Physical core


Logical core
Logical core
Physical core

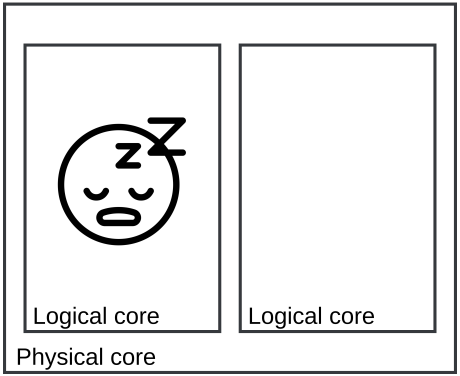

Logical core
Logical core
Physical core

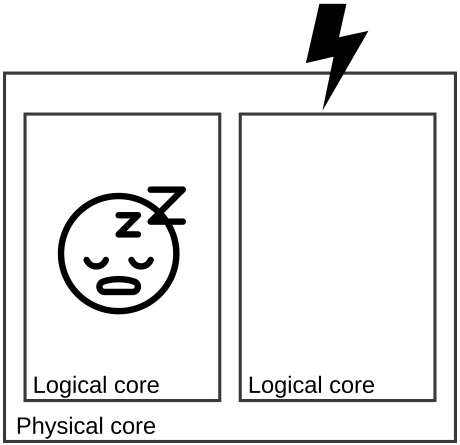

VM
Logical core
Logical core
Physical core

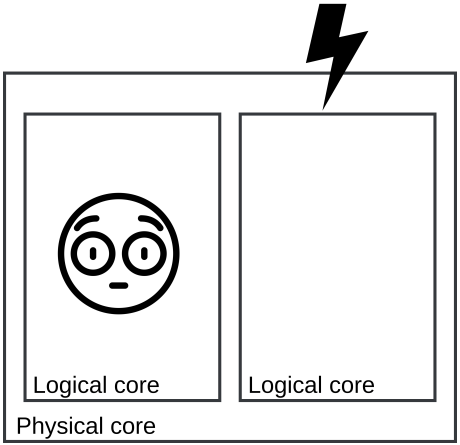

VM
Logical core
Logical core
Physical core


VM
Logical core
Logical core
Physical core

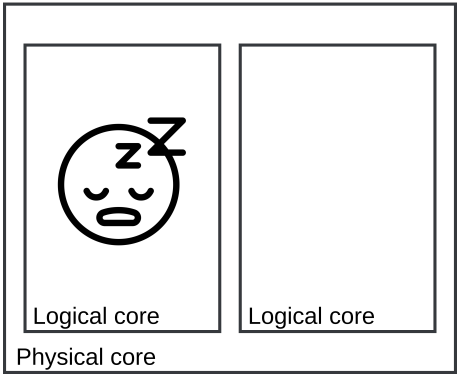
Undocumented Behaviour 2 (C0.1)



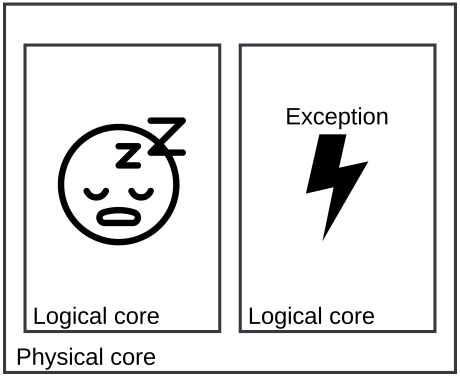

Logical core
Logical core
Physical core


Logical core
Logical core
Physical core

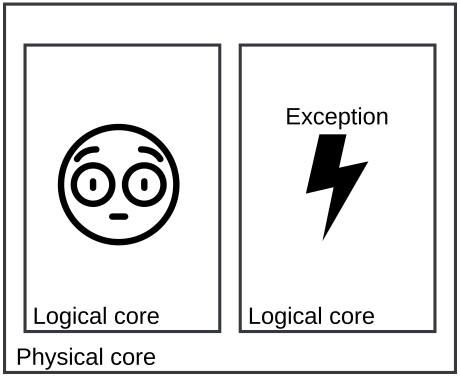
Undocumented Behaviour 3 (C0.1)

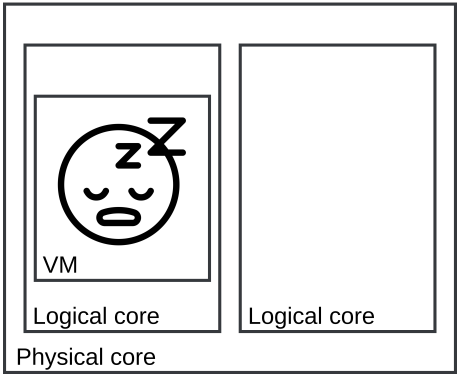


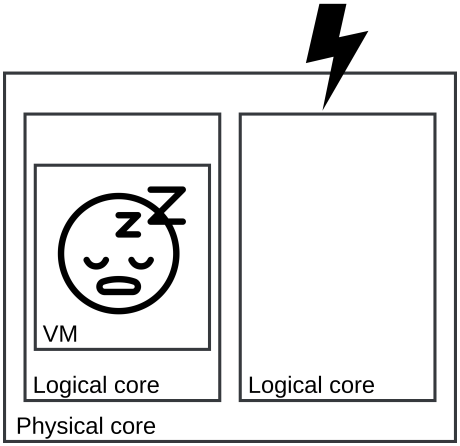
Undocumented Behaviour 3 (C0.1)

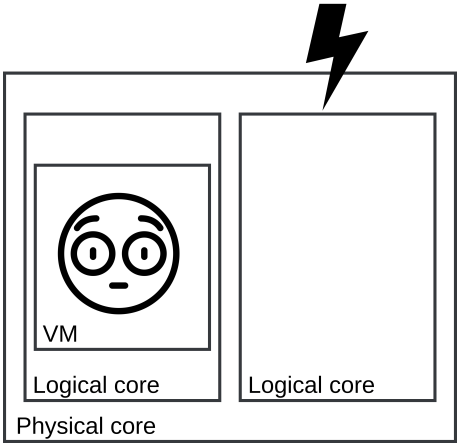


Undocumented Behaviour 3 (C0.1)




VM
Logical core
Logical core
Physical core


VM
Logical core
Logical core
Physical core


VM
Logical core
Logical core
Physical core

Covert Channel Speed


7


7

- Sender and Receiver each on a logical core

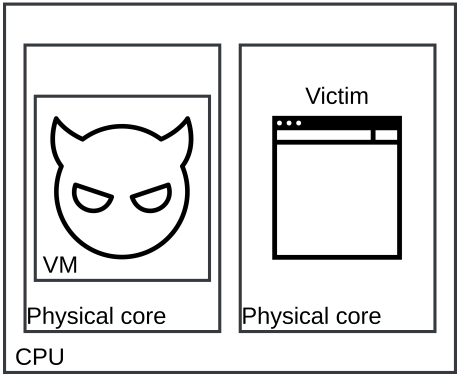
Covert Channel Speed

- Sender and Receiver each on a logical core
- Sender triggers exceptions or busy waits

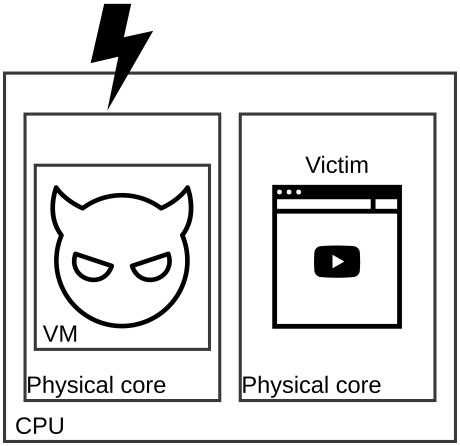
- Sender and Receiver each on a logical core
- Sender triggers exceptions or busy waits
- Receiver measures interrupt frequency with C0.1

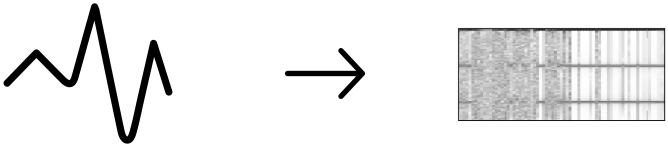
- Sender and Receiver each on a logical core
- Sender triggers exceptions or busy waits
- Receiver measures interrupt frequency with C0.1

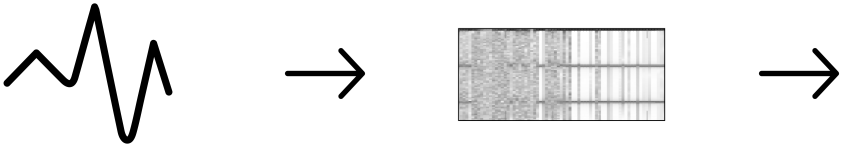
$\rightarrow$ 656.37 kbit/s ($\sigma_{\bar{x}} = 0.63$ kbit/s, $n = 1\,024$)

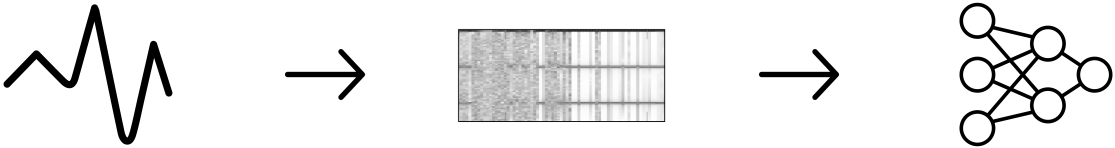

Victim
VM
Physical core
Physical core
CPU

Fingerprinting Setup









- Top 100 Websites

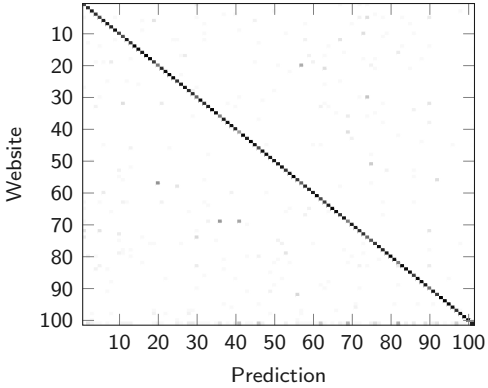
- Top 100 Websites
- Closed World:

- Top 100 Websites
- Closed World:
  - same logical core as interrupts

- Top 100 Websites
- Closed World:
  - same logical core as interrupts
  - sibling logical core of the interrupt core

- Top 100 Websites
- Closed World:
  - same logical core as interrupts
  - sibling logical core of the interrupt core
- Open World:

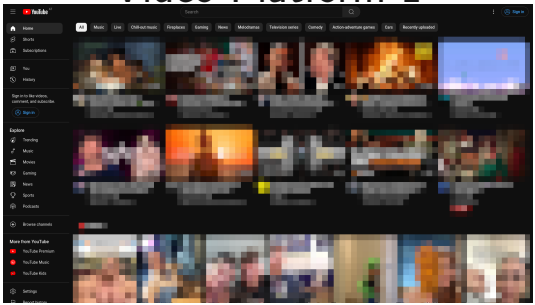
- Top 100 Websites
- Closed World:
  - same logical core as interrupts
  - sibling logical core of the interrupt core
- Open World:
  - additional `other`-class



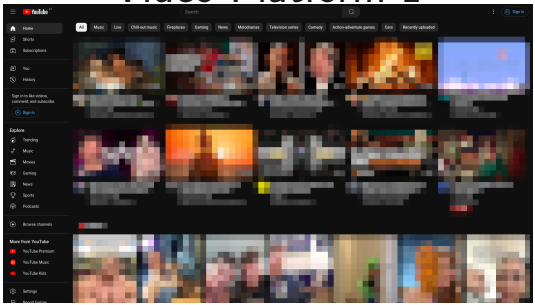
The confusion matrix for our open-world website-fingerprinting attack, with network interrupts arriving on a sibling logical core. F1-score of 85.2 % (87.4 % on other).

What else can we fingerprint?

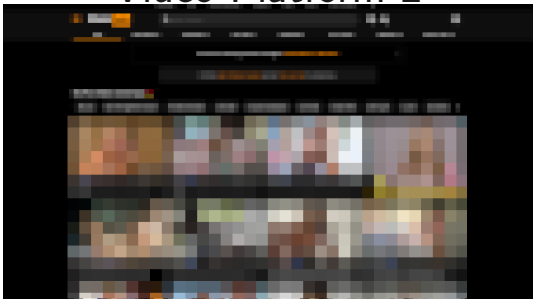
Video Platform 1

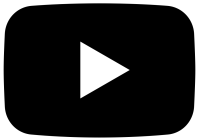


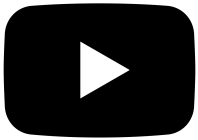
Video Platform 1

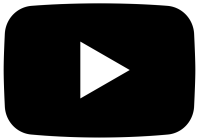


Video Platform 2

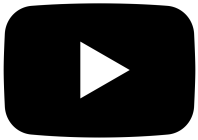




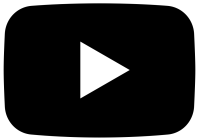




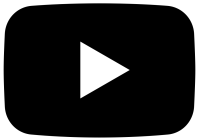
- 20 popular videos on each platform



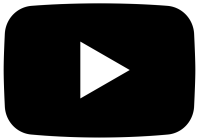
- 20 popular videos on each platform
- Closed World:



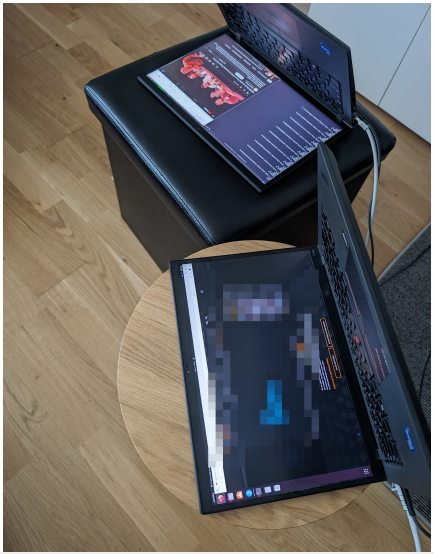
- 20 popular videos on each platform
- Closed World:
  - sibling logical core of the interrupt core

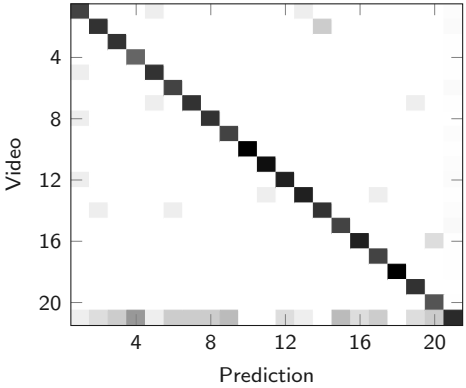


- 20 popular videos on each platform
- Closed World:
  - sibling logical core of the interrupt core
- Open World:

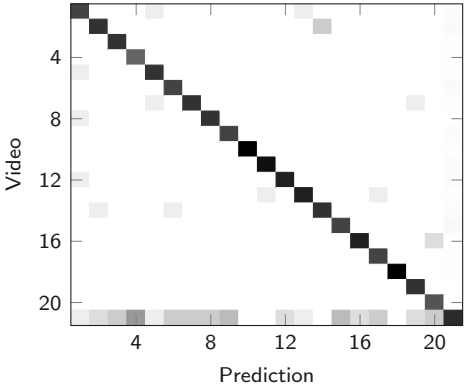


- 20 popular videos on each platform
- Closed World:
  - sibling logical core of the interrupt core
- Open World:
  - additional `other`-class

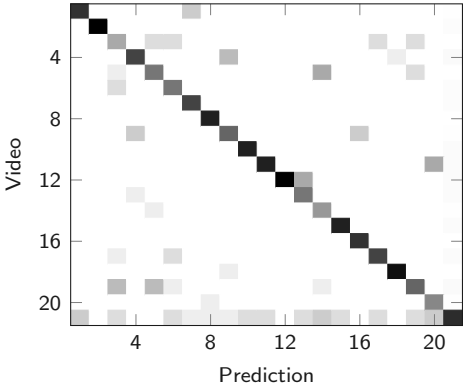




Video platform 1: F1-score of 81.5 %
(83 % on the `other`-class)



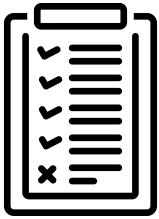
Video platform 1: F1-score of 81.5 %
(83 % on the `other`-class)



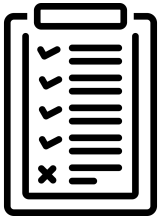
Video platform 2: F1-score of 70.5 %
(82 % on the `other`-class)

Summary

Summary



Summary



We

Summary

We

... analyzed security properties of C0.1 and C0.2

Summary

We

... analyzed security properties of C0.1 and C0.2

... built a high-speed covert channel (7.1 Mbit/s)

Summary

We

- ... analyzed security properties of C0.1 and C0.2
- ... built a high-speed covert channel (7.1 Mbit/s)
- ... performed website fingerprinting (F_1 score of 85.2 %)

Summary

We

- ... analyzed security properties of C0.1 and C0.2
- ... built a high-speed covert channel (7.1 Mbit/s)
- ... performed website fingerprinting (F_1 score of 85.2 %)
- ... performed a video fingerprinting attack

Summary

We

- ... analyzed security properties of C0.1 and C0.2
- ... built a high-speed covert channel (7.1 Mbit/s)
- ... performed website fingerprinting (F_1 score of 85.2 %)
- ... performed a video fingerprinting attack
- ... showed an inter-keystroke timing attack (F_1 score of 90.5 %)

Fabian Rauscher, Andreas Kogler, Jonas Juffinger, and Daniel Gruss. "IdleLeak: Exploiting Idle State Side Effects for Information Leakage". In: NDSS. 2024