TU Graz

SCIENCE
PASSION
TECHNOLOGY

A Systematic Evaluation of Novel and Existing Cache Side Channels

Fabian Rauscher, Carina Fiedler, Andreas Kogler, Daniel Gruss

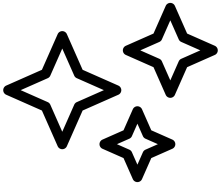
NDSS 2025

Intel Introduced a New Instruction!

New Instruction

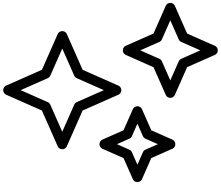
Fabian Rauscher @v4m1n www.responsible.fyi

New Instruction



Fabian Rauscher @v4m1n www.responsible.fyi

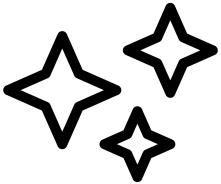
New Instruction



`cldemote:`

Fabian Rauscher @v4m1n www.responsible.fyi

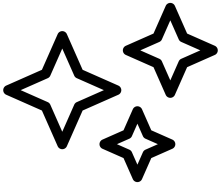
New Instruction



`cldemote`:

- available with recent Xeon CPUs (Sapphire Rapids)

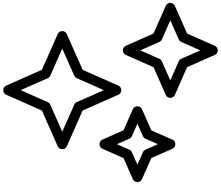
New Instruction



`cldemote`:

- available with recent Xeon CPUs (Sapphire Rapids)
- moves cache lines from higher (L1, L2) to lower cache levels (L3)

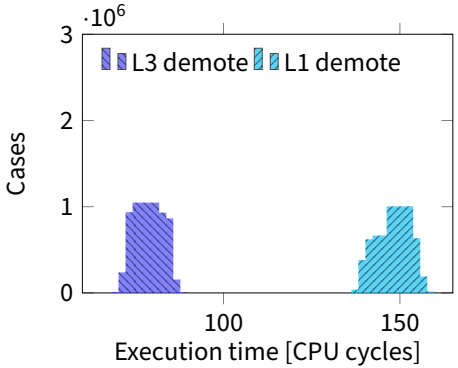
New Instruction



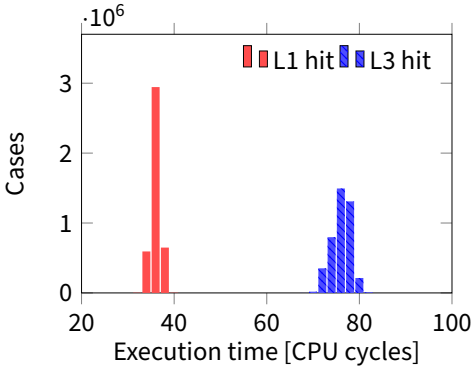
`cldemote`:

- available with recent Xeon CPUs (Sapphire Rapids)
- moves cache lines from higher (L1, L2) to lower cache levels (L3)
- cache line has to be accessible

Timings

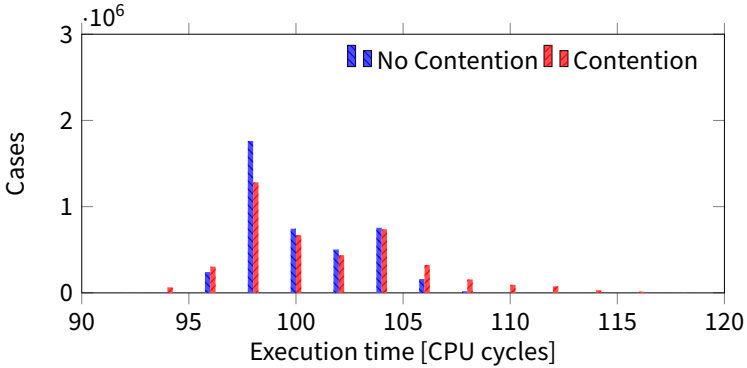


(a) `cldemote` Timings



(b) Memory Access Timings

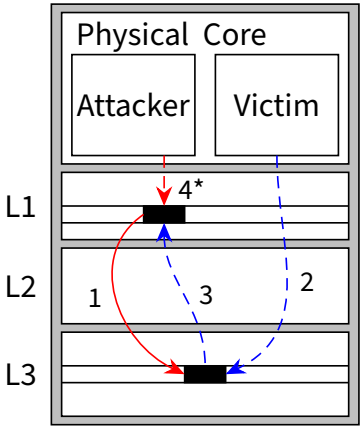
Hit-miss Margins



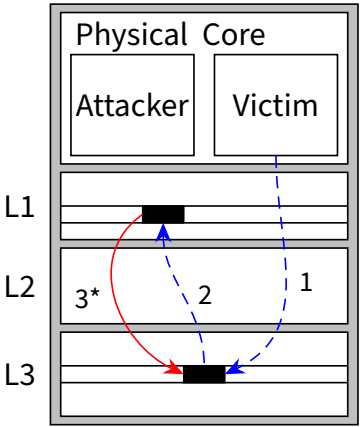
L3 contention

New Attacks

Demote+Reload & Demote+Demote

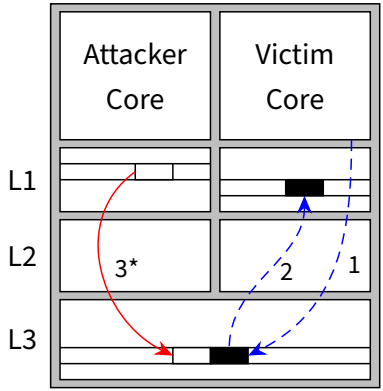


Demote+Reload



Demote+Demote

DemoteContention



DemoteContention

Systematic Analysis

Systematic Analysis

Systematic Analysis

Systematic Analysis

7 Cache Attacks:

7 Cache Attacks:
- Existing:

Systematic Analysis

7 Cache Attacks:

- Existing:
  - Flush+Reload (SMT & cross-core)

7 Cache Attacks:

- Existing:
  - Flush+Reload (SMT & cross-core)
  - Flush+Flush (SMT & cross-core)

7 Cache Attacks:

- Existing:
  - Flush+Reload (SMT & cross-core)
  - Flush+Flush (SMT & cross-core)
  - Prime+Probe (L1)

Systematic Analysis

7 Cache Attacks:

- Existing:
  - Flush+Reload (SMT & cross-core)
  - Flush+Flush (SMT & cross-core)
  - Prime+Probe (L1)
  - Evict+Reload (L1)

Systematic Analysis

7 Cache Attacks:

- Existing:
  - Flush+Reload (SMT & cross-core)
  - Flush+Flush (SMT & cross-core)
  - Prime+Probe (L1)
  - Evict+Reload (L1)
- Novel:

Systematic Analysis

7 Cache Attacks:

- Existing:
  - Flush+Reload (SMT & cross-core)
  - Flush+Flush (SMT & cross-core)
  - Prime+Probe (L1)
  - Evict+Reload (L1)
- Novel:
  - Demote+Reload

Systematic Analysis

7 Cache Attacks:

- Existing:
  - Flush+Reload (SMT & cross-core)
  - Flush+Flush (SMT & cross-core)
  - Prime+Probe (L1)
  - Evict+Reload (L1)
- Novel:
  - Demote+Reload
  - Demote+Demote

Systematic Analysis

7 Cache Attacks:

- Existing:
  - Flush+Reload (SMT & cross-core)
  - Flush+Flush (SMT & cross-core)
  - Prime+Probe (L1)
  - Evict+Reload (L1)
- Novel:
  - Demote+Reload
  - Demote+Demote
  - DemoteContention

Systematic Analysis

7 Cache Attacks:

- Existing:
  - Flush+Reload (SMT & cross-core)
  - Flush+Flush (SMT & cross-core)
  - Prime+Probe (L1)
  - Evict+Reload (L1)
- Novel:
  - Demote+Reload
  - Demote+Demote
  - DemoteContention

Tested on two Microarchitectures:

Systematic Analysis

7 Cache Attacks:

- Existing:
  - Flush+Reload (SMT & cross-core)
  - Flush+Flush (SMT & cross-core)
  - Prime+Probe (L1)
  - Evict+Reload (L1)
- Novel:
  - Demote+Reload
  - Demote+Demote
  - DemoteContention

Tested on two Microarchitectures:

- Sapphire Rapids (Xeon Silver 4410T)

Systematic Analysis

7 Cache Attacks:

- Existing:
  - Flush+Reload (SMT & cross-core)
  - Flush+Flush (SMT & cross-core)
  - Prime+Probe (L1)
  - Evict+Reload (L1)
- Novel:
  - Demote+Reload
  - Demote+Demote
  - DemoteContention

Tested on two Microarchitectures:

- Sapphire Rapids (Xeon Silver 4410T)
- Emerald Rapids (Xeon Silver 4514Y)

Systematic Analysis

Systematic Analysis

Systematic Analysis

9 Metrics:

Systematic Analysis

9 Metrics:

- Hit-miss margin

Systematic Analysis

9 Metrics:

- Hit-miss margin
- Temporal Precision

Systematic Analysis

9 Metrics:

- Hit-miss margin
- Temporal Precision
- Spatial Precision

Systematic Analysis

9 Metrics:

- Hit-miss margin
- Temporal Precision
- Spatial Precision
- Topological Scope

Systematic Analysis

9 Metrics:

- Hit-miss margin
- Temporal Precision
- Spatial Precision
- Topological Scope
- Attack Time

Systematic Analysis

9 Metrics:

- Hit-miss margin
- Temporal Precision
- Spatial Precision
- Topological Scope
- Attack Time
- Blind Spot Size

Systematic Analysis

9 Metrics:

- Hit-miss margin
- Temporal Precision
- Spatial Precision
- Topological Scope
- Attack Time
- Blind Spot Size
- Channel Capacity

Systematic Analysis

9 Metrics:

- Hit-miss margin
- Temporal Precision
- Spatial Precision
- Topological Scope
- Attack Time
- Blind Spot Size
- Channel Capacity
- Noise Resilience

Systematic Analysis

9 Metrics:

- Hit-miss margin
- Temporal Precision
- Spatial Precision
- Topological Scope
- Attack Time
- Blind Spot Size
- Channel Capacity
- Noise Resilience
- Detectability

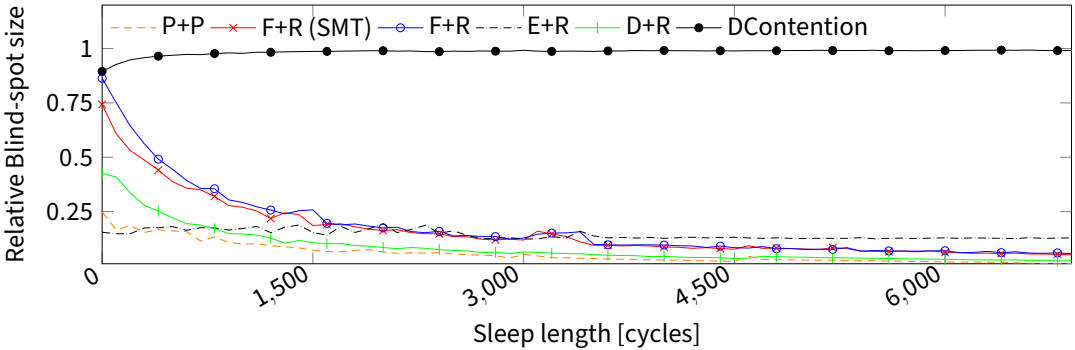
Systematic Analysis

9 Metrics:

- Hit-miss margin
- Temporal Precision
- Spatial Precision
- Topological Scope
- Attack Time
- Blind Spot Size
- Channel Capacity
- Noise Resilience
- Detectability

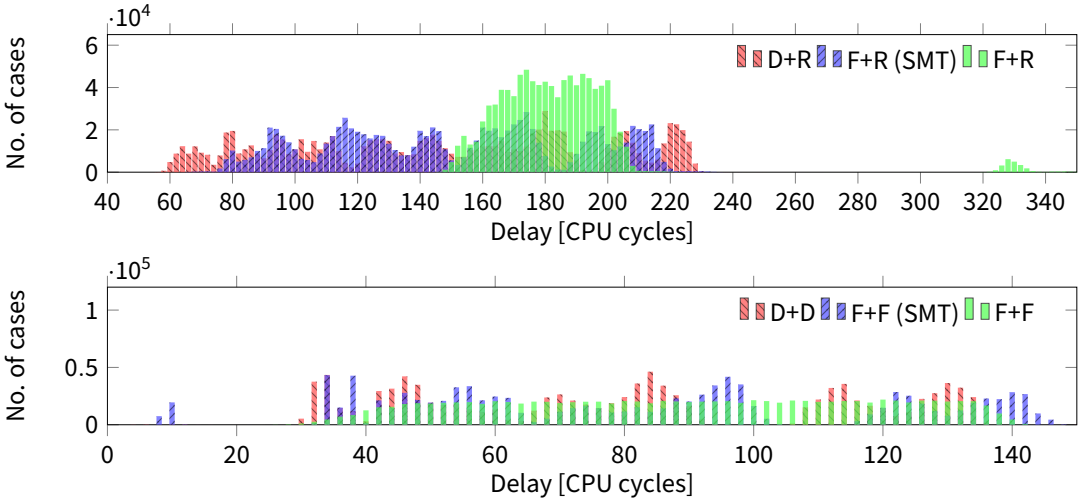
Blind Spot

Blind Spot

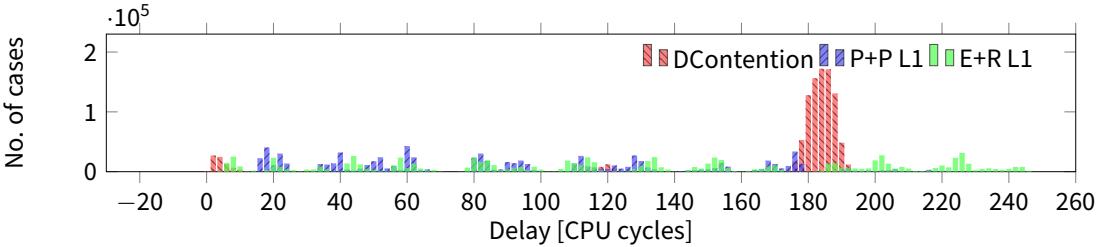

P+P
F+R (SMT)
F+R
E+R
D+R
DContention
Relative Blind-spot size
1
0.75
0.5
0.25
0
1,500
3,000
4,500
6,000
Sleep length [cycles]

Temporal Precision

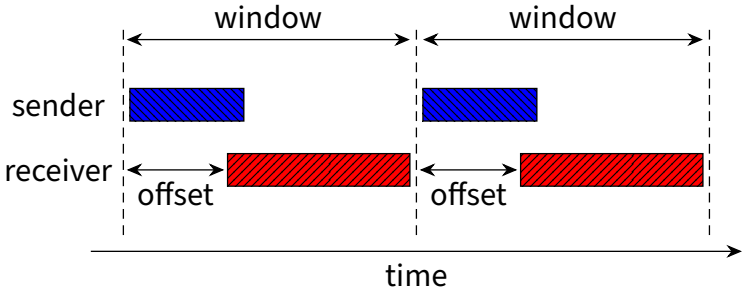
Temporal Precision



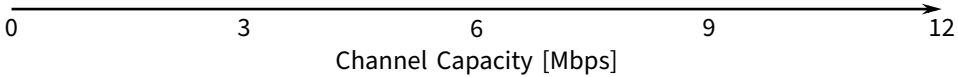
Temporal Precision



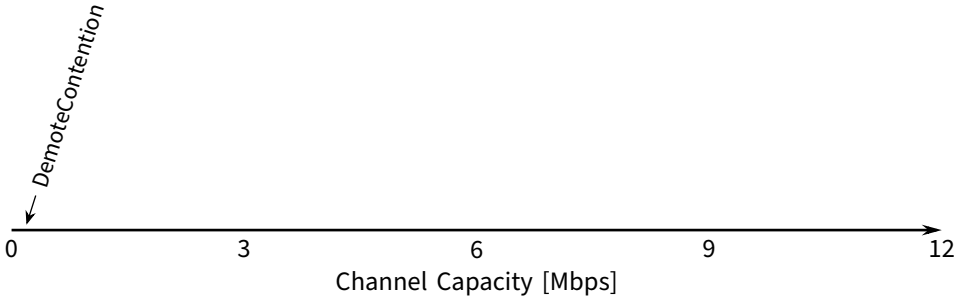
Covert Channel


window
window
sender
receiver
offset
offset
time

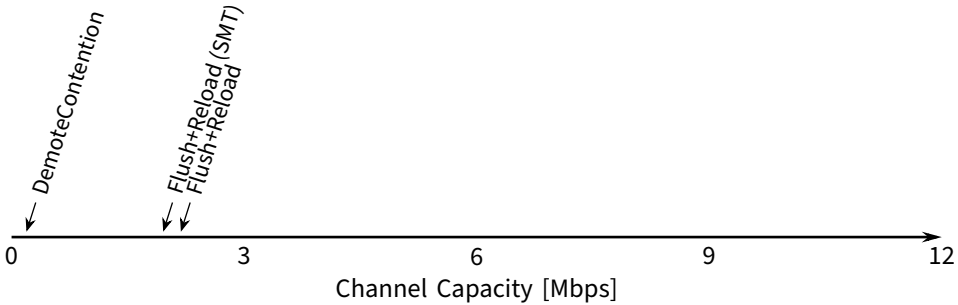
Covert Channel Speed



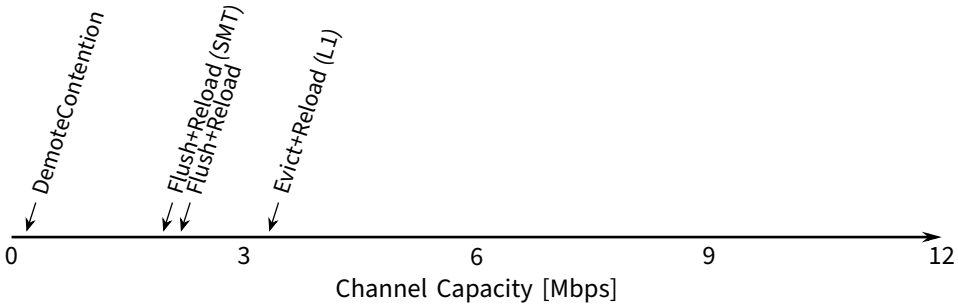
Covert Channel Speed



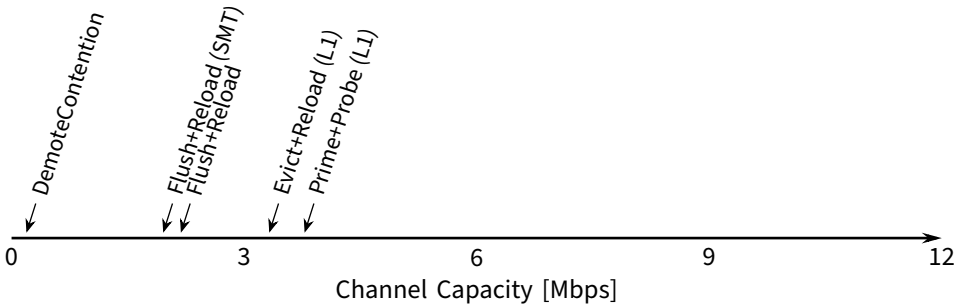
Covert Channel Speed



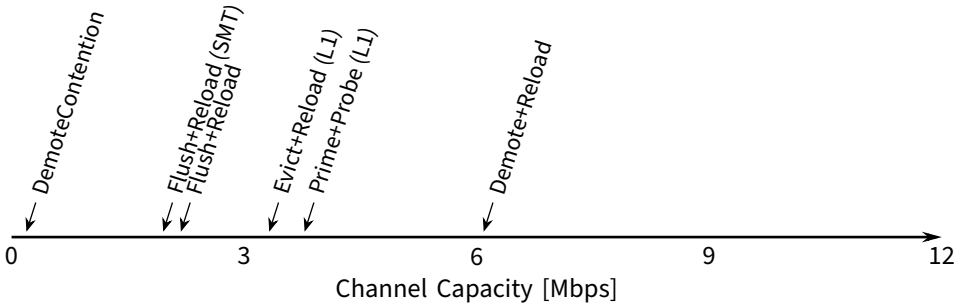
Covert Channel Speed



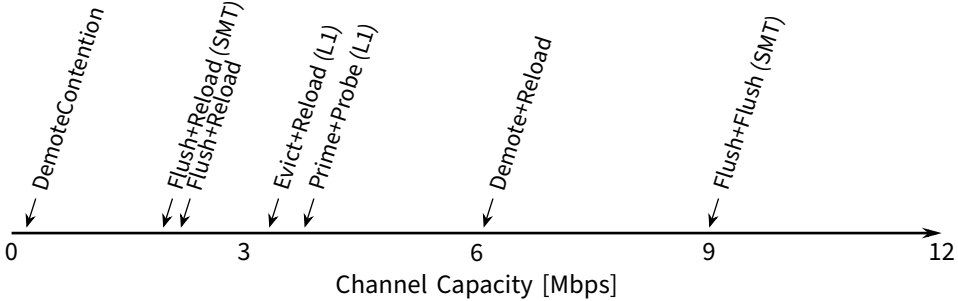
Covert Channel Speed



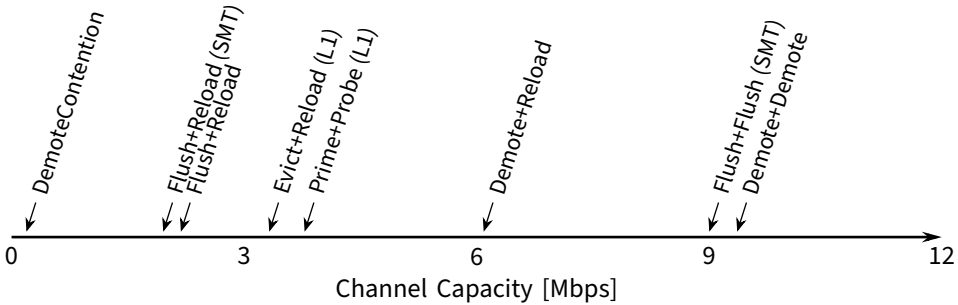
Covert Channel Speed



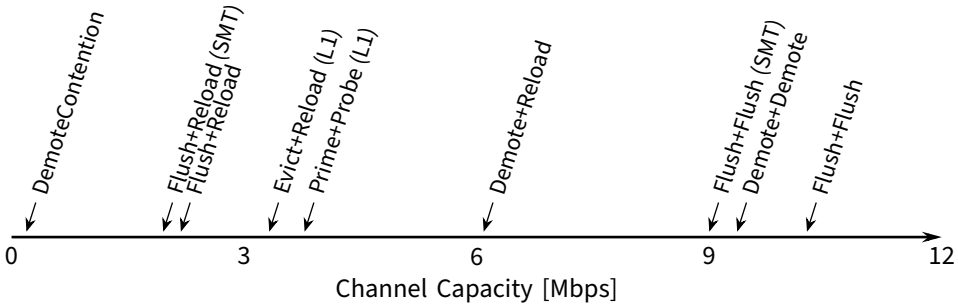
Covert Channel Speed



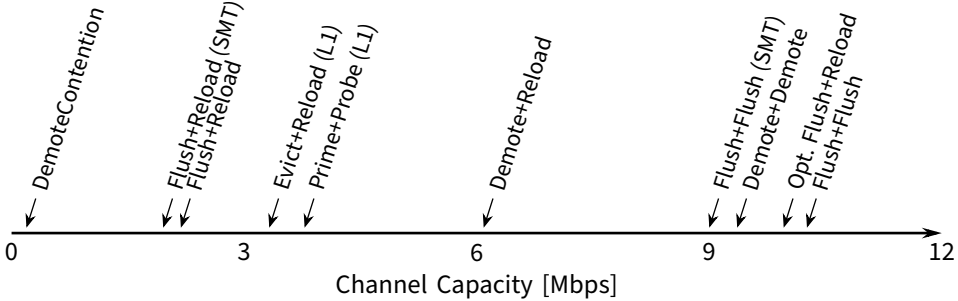
Covert Channel Speed



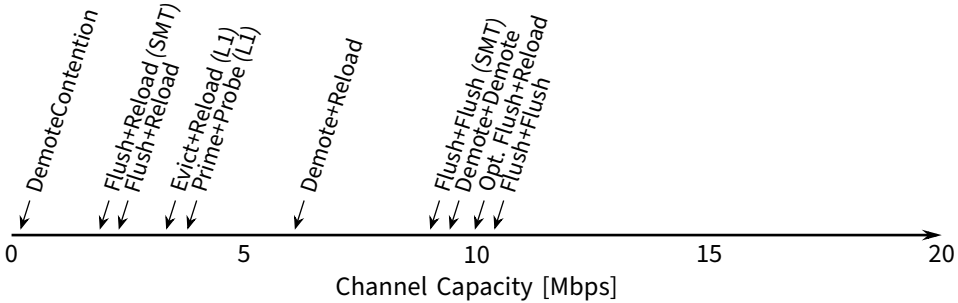
Covert Channel Speed



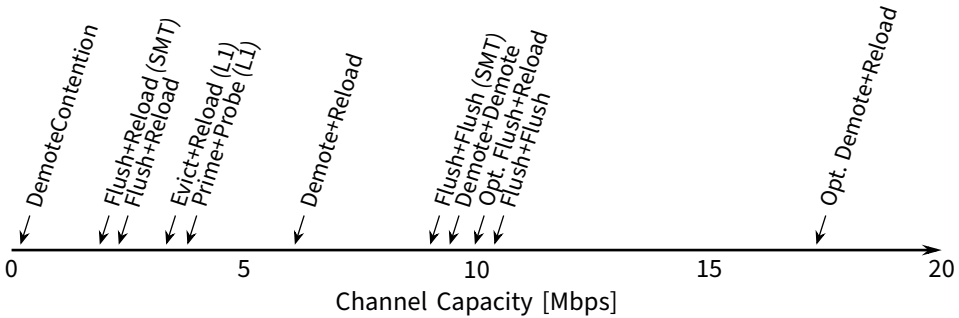
Covert Channel Speed



Covert Channel Speed



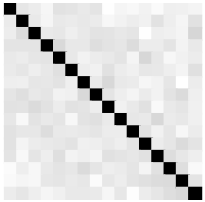
Covert Channel Speed



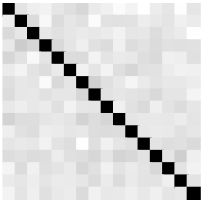
Check out the Paper for the other Metrics!

Attacks

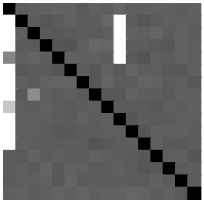
AES T-Table Attack



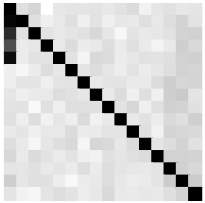
(a) Demote+Reload



(b) Flush+Reload

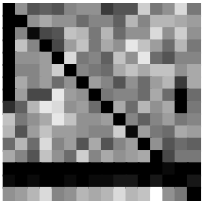


(c) Evict+Reload



(d) Demote+Demote

(e) Flush+Flush



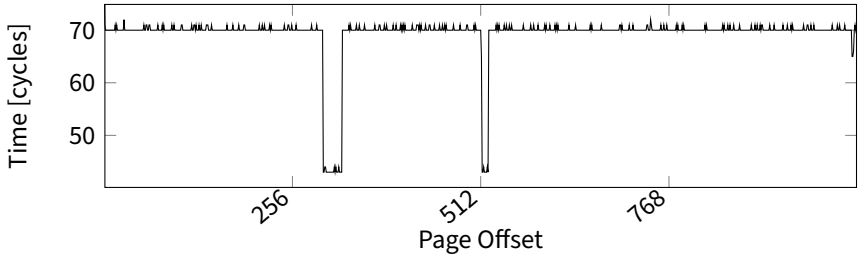
(f) Prime+Probe

What else?

64-Bit Mode Exceptions

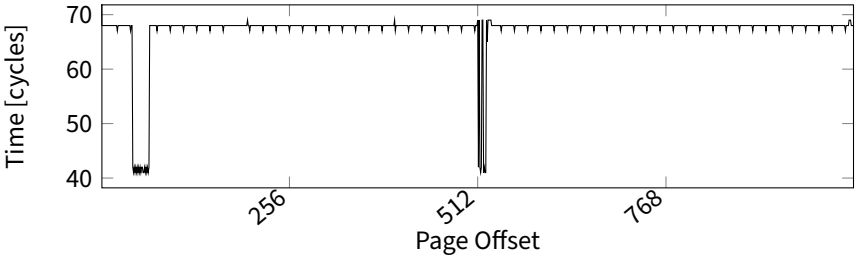
#UD	If the LOCK prefix is used.

KASLR Break (Emerald Rapids)



Xeon Silver 4514Y

KASLR Break (Alder Lake)



Core i7 1260P

Demote Support

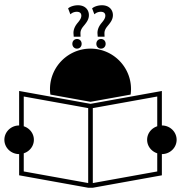
```
frauscher@ipn044 ~ cpuid | grep demote
      CLDEMOTE supports cache line demote      = false
      CLDEMOTE supports cache line demote      = false
      CLDEMOTE supports cache line demote      = false
      CLDEMOTE supports cache line demote      = false
      CLDEMOTE supports cache line demote      = false
      CLDEMOTE supports cache line demote      = false
      CLDEMOTE supports cache line demote      = false
      CLDEMOTE supports cache line demote      = false
      CLDEMOTE supports cache line demote      = false
      CLDEMOTE supports cache line demote      = false
      CLDEMOTE supports cache line demote      = false
      CLDEMOTE supports cache line demote      = false
      CLDEMOTE supports cache line demote      = false
      CLDEMOTE supports cache line demote      = false
      CLDEMOTE supports cache line demote      = false
      CLDEMOTE supports cache line demote      = false
```

Demote Support

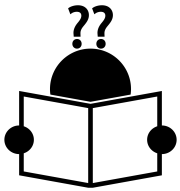
"On processors which do not support the CLDEMOTE instruction (including legacy hardware) the instruction will be treated as a NOP."
- Intel SDM

What Happened?

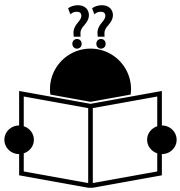
What Happened?



What Happened?

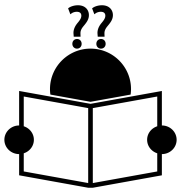


What Happened?



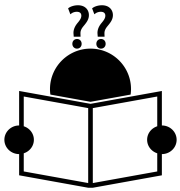
- `cldemote` is treated as a `nop`

What Happened?



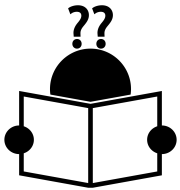
- `cldemote` is treated as a `nop`
  - ... on Intel CPUs pre 12th Gen

What Happened?



- `cldemote` is treated as a `nop`
  - ... on Intel CPUs pre 12th Gen
- on 12th Gen and newer it does check the page tables

What Happened?



- `cldemote` is treated as a `nop`
  - ... on Intel CPUs pre 12th Gen
- on 12th Gen and newer it does check the page tables
  - ... but nothing else(?)

Summary

Summary

Summary

We

Summary

We

... introduce 3 new attack primitives

Summary

We

- ... introduce 3 new attack primitives
- ... perform a systematic analysis of 7 attack primitives using 9 metrics

Summary

We

- ... introduce 3 new attack primitives
- ... perform a systematic analysis of 7 attack primitives using 9 metrics
- ... compare the primitives by attacking AES T-Tables (first- and last-round)

Summary

We

- ... introduce 3 new attack primitives
- ... perform a systematic analysis of 7 attack primitives using 9 metrics
- ... compare the primitives by attacking AES T-Tables (first- and last-round)
- ... compare the primitives by detecting inter-keystroke timings

Summary

We

- ... introduce 3 new attack primitives
- ... perform a systematic analysis of 7 attack primitives using 9 metrics
- ... compare the primitives by attacking AES T-Tables (first- and last-round)
- ... compare the primitives by detecting inter-keystroke timings
- ... preform 2 attacks, KASLR break and Collide+Power, only possible with `cldemote`

Acknowledgments

This research was made possible by generous funding from:

Supported in part by the European Research Council (ERC project FSSec 101076409) and the Austrian Science Fund (FWF) [10.55776/I6054]. Additional funding was provided by generous gifts from Red Hat, and Intel. Any opinions, findings, and conclusions or recommendations expressed in this paper are those of the authors and do not necessarily reflect the views of the funding parties.

TU Graz

SCIENCE
PASSION
TECHNOLOGY

A Systematic Evaluation of Novel and Existing Cache Side Channels

Fabian Rauscher, Carina Fiedler, Andreas Kogler, Daniel Gruss

NDSS 2025

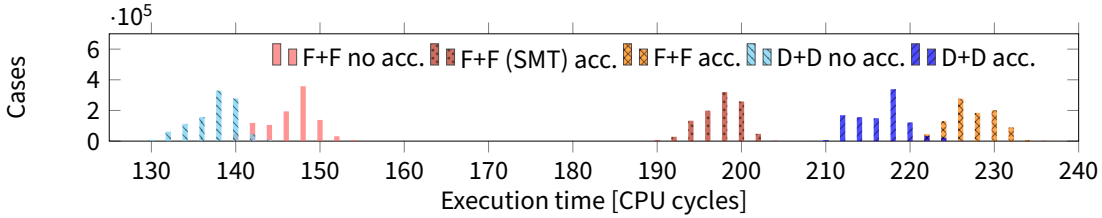
Covert Channel

Single-bit (1-bit) and multi-bit (n-bit) covert-channel true capacity in **Mbit/s** and error ratio of all tested attacks on an Intel Xeon Silver 4514Y.

Attack	Cap. (1-bit)	BER (1-bit)	Cap. (n-bit)	BER (n-bit)
Opt. Demote+Reload	11.10	0.6 %	17.03	1.4 %
Opt. Flush+Reload	6.51	2.2 %	10.01	1.2 %
Opt. Flush+Reload (SMT)	5.31	1.7 %	9.24	1.0 %
Demote+Reload	6.09	0.7 %	6.09	0.7 %
Demote+Demote	8.17	1.7 %	9.36	2.3 %
DemoteContention	0.19	1.9 %	0.19	1.9 %
Flush+Reload	2.15	3.6 %	2.15	3.6 %
Flush+Reload (SMT)	2.01	3.2 %	2.01	3.2 %
Flush+Flush	5.74	2.0 %	10.26	1.9 %
Flush+Flush (SMT)	5.03	2.1 %	9.03	2.6 %
Prime+Probe (L1)	3.78	2.0 %	3.78	2.0 %
Evict+Reload (L1)	3.32	1.4 %	3.32	1.4 %

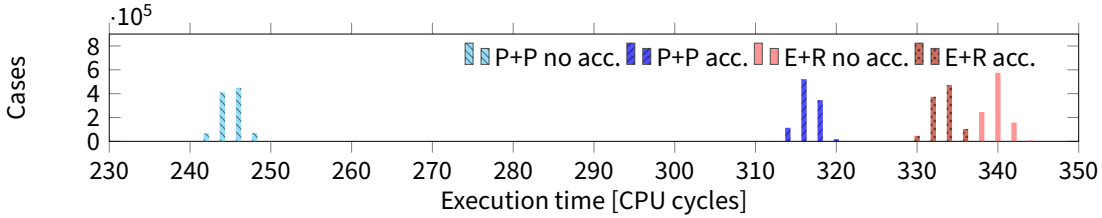
Execution Time

Flush+Reload & Demote+Reload



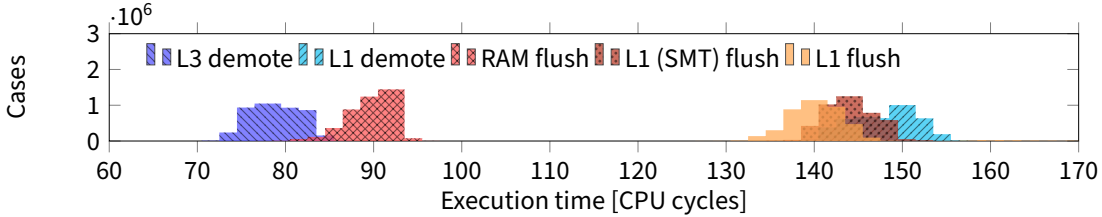
Flush+Flush & Demote+Demote

Execution Time

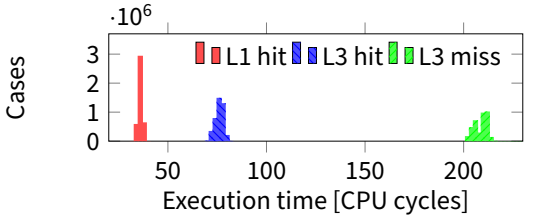


Prime+Probe & Evict+Reload

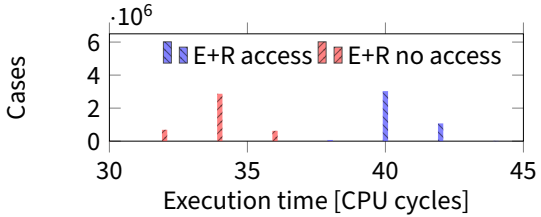
Hit-miss Margins



(a) `cldemote` & `clflush` Timings

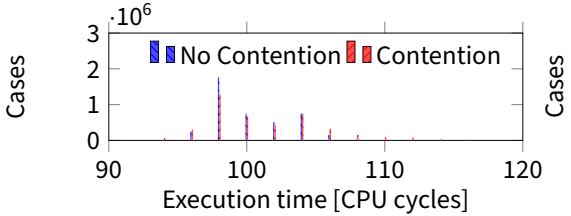


(b) Memory Access Timings

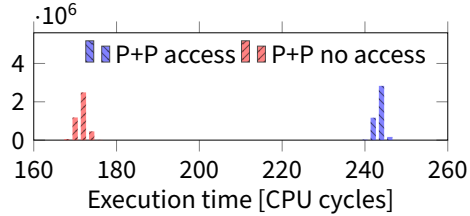


(c) Evict+Reload

Hit-miss Margins



(a) Cross-core DemoteContention



(b) Prime+Probe

Performance counter values for 10^6 runs of each tested attack without a victim access on our Xeon Silver 4514Y.

Attack	L1 misses	L2 misses	L3 misses	Retired Branches
Base (SMT)	47 121	11 299	1496	10 630 295
cc Base	2 895 991	2 886 008	1412	11 744 772
Demote+Demote	44 239	9136	1367	10 886 159
DemoteContention	2 988 775	2 975 436	1338	11 781 288
Demote+Reload	1 052 979	1 011 615	1337	10 884 189
Flush+Flush (SMT)	40 709	9722	1446	10 884 115
Flush+Flush	2 795 098	2 784 195	1781	11 714 560
Flush+Reload (SMT)	1 075 286	1 016 118	1 001 531	10 882 563
Flush+Reload	4 042 492	4 026 895	1 001 513	11 713 327
Evict+Reload	13 023 103	10 946	1468	10 881 358
Prime+Probe	41 488	9483	1753	10 874 922

Detectability

Performance counter values for 10^6 runs of each tested attack with a victim access on our Xeon Silver 4514Y.

Attack	L1 misses	L2 misses	L3 misses	Retired Branches
Base (SMT)	55 672	13 004	1582	10 629 320
Base	2 933 579	2 922 245	1452	11 682 440
Demote+Demote	1 045 714	1 011 050	1525	10 882 479
DemoteContention	2 979 165	2 964 159	1468	11 745 555
Demote+Reload	1 053 159	1 011 066	1409	10 885 386
Flush+Flush (SMT)	1 051 465	1 011 173	1 001 311	10 887 482
Flush+Flush	4 291 916	4 280 915	1 001 030	11 742 261
Flush+Reload (SMT)	1 068 255	1 012 946	1 001 391	10 885 194
Flush+Reload	5 444 751	5 429 372	1 001 418	11 748 249
Evict+Reload	13 021 365	11 188	1569	10 885 999
Prime+Probe	13 020 591	12 295	1470	10 881 335