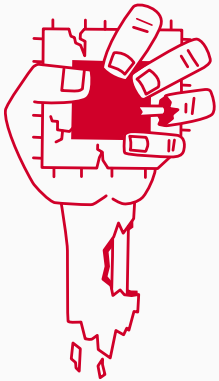
ZombieLoad

Cross-Privilege-Boundary Data Sampling

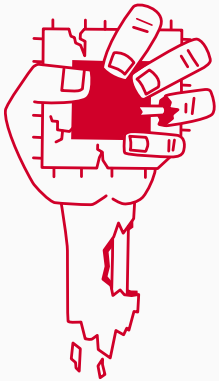
Michael Schwarz[1], **Moritz Lipp**[1], **Daniel Moghimi**[2], **Jo Van Bulck**[3], **Julian Stecklina**[4], **Thomas Prescher**[4], **Daniel Gruss**[1]

November 11, 2019

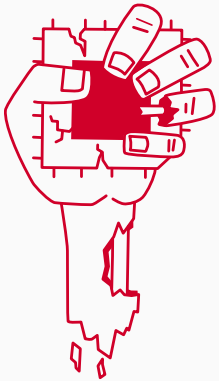
[1] Graz University of Technology, [2] Worcester Polytechnic Institute, [3] imec-DistriNet, KU Leuven, [4] Cyberus Technology



- A new Meltdown-type transient-execution attack



- A new Meltdown-type transient-execution attack
- Leaks data on Intel CPUs



- A new Meltdown-type transient-execution attack
- Leaks data on Intel CPUs
- Really new? Published in May 2019...

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

ZombieLoad

- CVE-2018-12130
- CVE-2019-11091

ZombieLoad

- CVE-2018-12130
- CVE-2019-11091

RIDL

- CVE-2018-12127
- CVE-2018-12130
- CVE-2019-11091

ZombieLoad

- CVE-2018-12130
- CVE-2019-11091

RIDL

- CVE-2018-12127
- CVE-2018-12130
- CVE-2019-11091

Fallout

- CVE-2018-12126

ZombieLoad

- CVE-2018-12130
- CVE-2019-11091
- CVE-2019-11135

RIDL

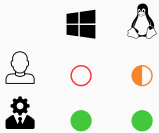
- CVE-2018-12127
- CVE-2018-12130
- CVE-2019-11091

Fallout

- CVE-2018-12126

Variant 1

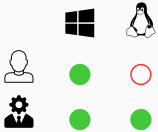
Kernel Mapping



Variant 3

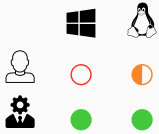
Microcode-Assisted

Page-Table Walk



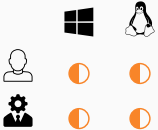
Variant 1

Kernel Mapping



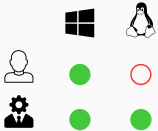
Variant 2

Transactional Asynchronous Abort



Variant 3

Microcode-Assisted Page-Table Walk



Embargo

- Variant 2 embargoed until November 12, 2019

Embargo

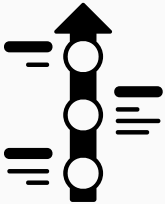
- Variant 2 embargoed until November 12, 2019
- Only variant without hardware mitigations

Embargo

- Variant 2 embargoed until November 12, 2019
- Only variant without hardware mitigations

→ Works on MDS-resistant Cascade Lake CPUs

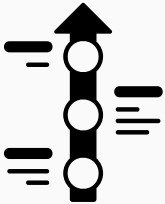
March 28, 2018 We report Meltdown on fill buffer (CVE-2019-11091)

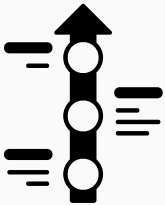


Timeline

March 28, 2018 We report Meltdown on fill buffer (CVE-2019-11091)

September 12, 2018 VUSec reports fill-buffer leakage (RIDL)



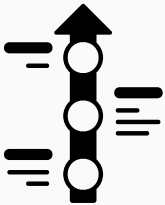


March 28, 2018 We report Meltdown on fill buffer (CVE-2019-11091)

September 12, 2018 VUSec reports fill-buffer leakage (RIDL)

April 12, 2019 We report ZombieLoad Variant 1 (CVE-2018-12130)

Timeline



March 28, 2018 We report Meltdown on fill buffer (CVE-2019-11091)

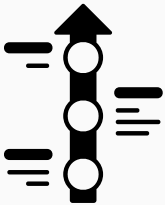
September 12, 2018 VUSec reports fill-buffer leakage (RIDL)

April 12, 2019 We report ZombieLoad Variant 1 (CVE-2018-12130)

→ All embargoed until May 14, 2019 (MDS)

April 24, 2019 We report ZombieLoad Variant 2 (CVE-2019-11135)

Timeline



March 28, 2018 We report Meltdown on fill buffer (CVE-2019-11091)

September 12, 2018 VUSec reports fill-buffer leakage (RIDL)

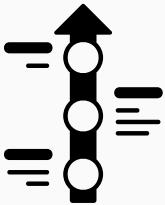
April 12, 2019 We report ZombieLoad Variant 1 (CVE-2018-12130)

→ All embargoed until May 14, 2019 (MDS)

April 24, 2019 We report ZombieLoad Variant 2 (CVE-2019-11135)

May 10, 2019 We report Variant 2 on Cascade Lake

Timeline



March 28, 2018 We report Meltdown on fill buffer (CVE-2019-11091)

September 12, 2018 VUSec reports fill-buffer leakage (RIDL)

April 12, 2019 We report ZombieLoad Variant 1 (CVE-2018-12130)

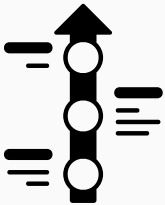
→ All embargoed until May 14, 2019 (MDS)

April 24, 2019 We report ZombieLoad Variant 2 (CVE-2019-11135)

May 10, 2019 We report Variant 2 on Cascade Lake

May 11, 2019 Call with Intel

Timeline



March 28, 2018 We report Meltdown on fill buffer (CVE-2019-11091)

September 12, 2018 VUSec reports fill-buffer leakage (RIDL)

April 12, 2019 We report ZombieLoad Variant 1 (CVE-2018-12130)

→ All embargoed until May 14, 2019 (MDS)

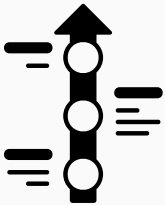
April 24, 2019 We report ZombieLoad Variant 2 (CVE-2019-11135)

May 10, 2019 We report Variant 2 on Cascade Lake

May 11, 2019 Call with Intel

May 12, 2019 Not allowed to publish Variant 2

Timeline



March 28, 2018 We report Meltdown on fill buffer (CVE-2019-11091)

September 12, 2018 VUSec reports fill-buffer leakage (RIDL)

April 12, 2019 We report ZombieLoad Variant 1 (CVE-2018-12130)

→ All embargoed until May 14, 2019 (MDS)

April 24, 2019 We report ZombieLoad Variant 2 (CVE-2019-11135)

May 10, 2019 We report Variant 2 on Cascade Lake

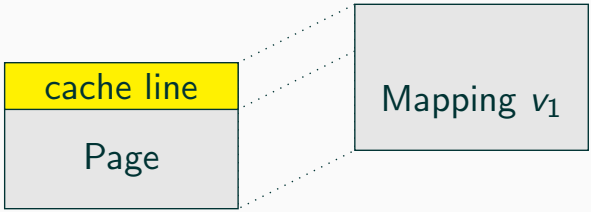
May 11, 2019 Call with Intel

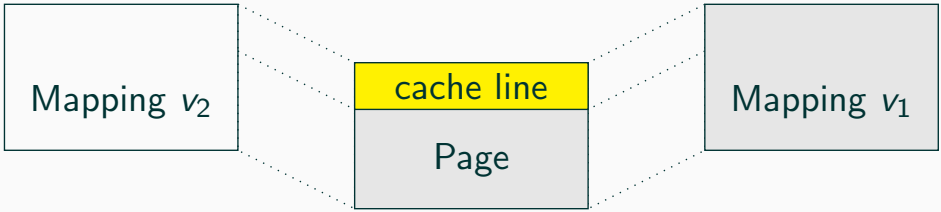
May 12, 2019 Not allowed to publish Variant 2

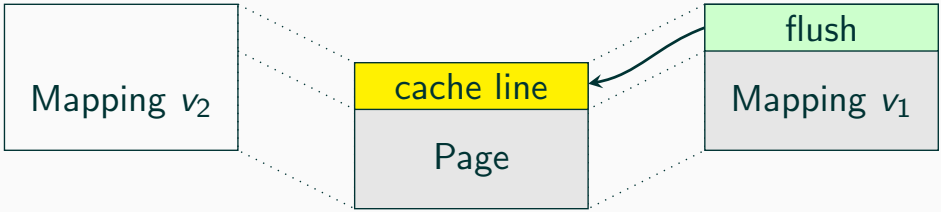
→ Additional embargo until November 12, 2019 (TAA)

	Fill Buffer, Load Ports, ?	Fill Buffer, Load Ports	Store Buffer
	All loads & stores	Uncached loads & stores	Stores
	✓	✗	✗
	✓	✗ (before Cascade Lake)	✗ (before Cascade Lake)

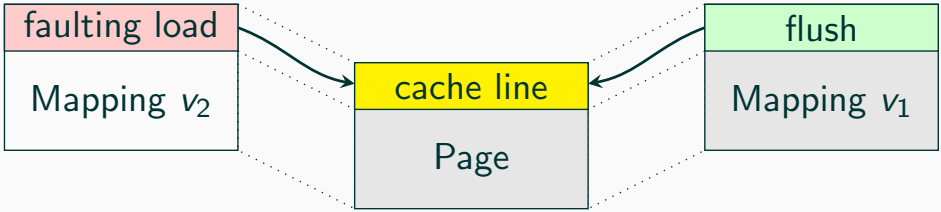
ZombieLoad works **despite** software **mitigations** and even on **MDS-resistant** CPUs (e.g., Cascade Lake)


cache line
Page
Mapping v_1


Mapping v_2
cache line
Page
Mapping v_1


Mapping v_2
cache line
Page
flush
Mapping v_1

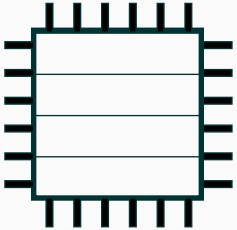
ZombieLoad Cache-line Conflicts



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

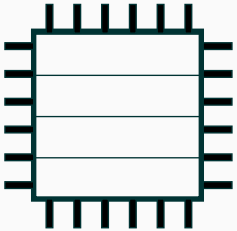
```
char value = faulting[0]
```

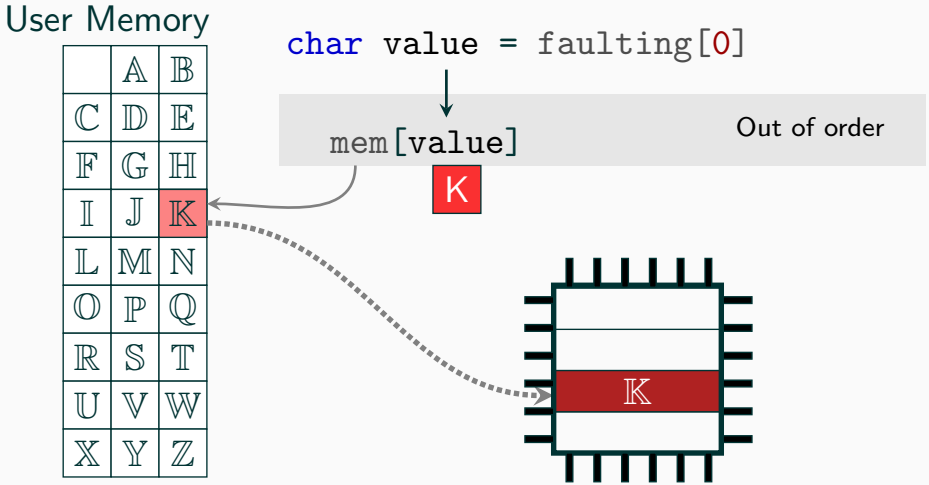
↓

```
mem[value]
```

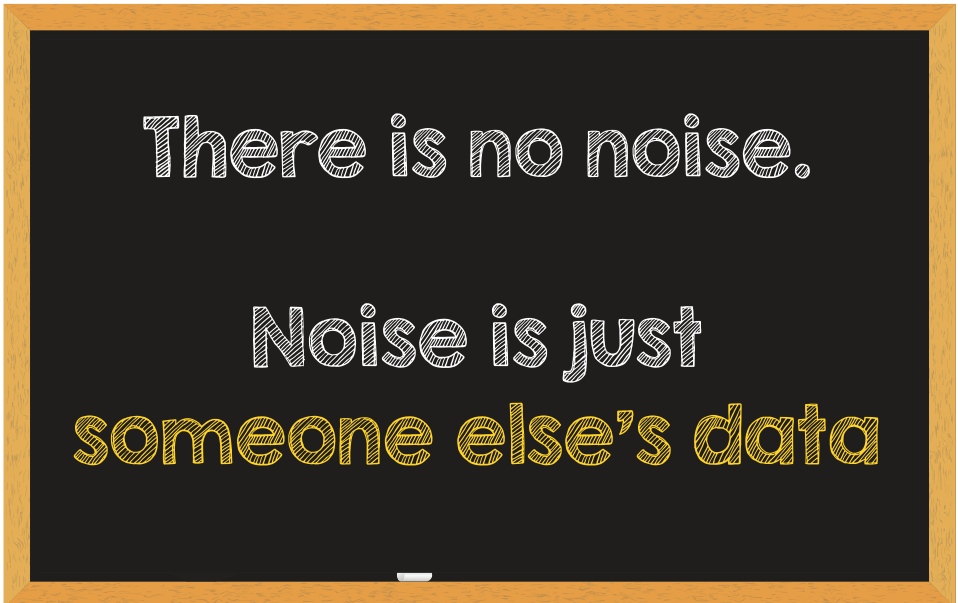
Out of order

K

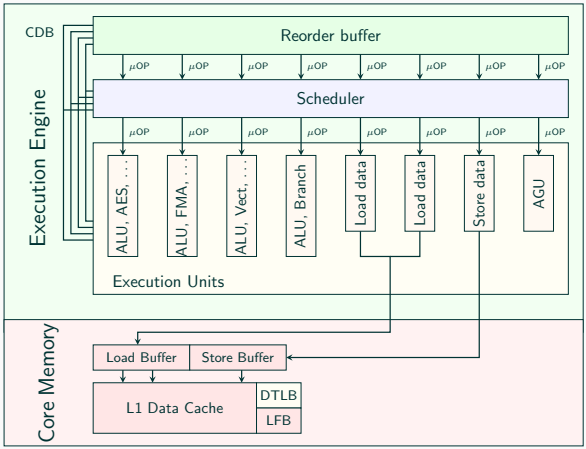



User Memory
A B
C D E
F G H
I J K
L M N
O P Q
R S T
U V W
X Y Z
char value = faulting[0]
mem[value]
Out of order
K
K

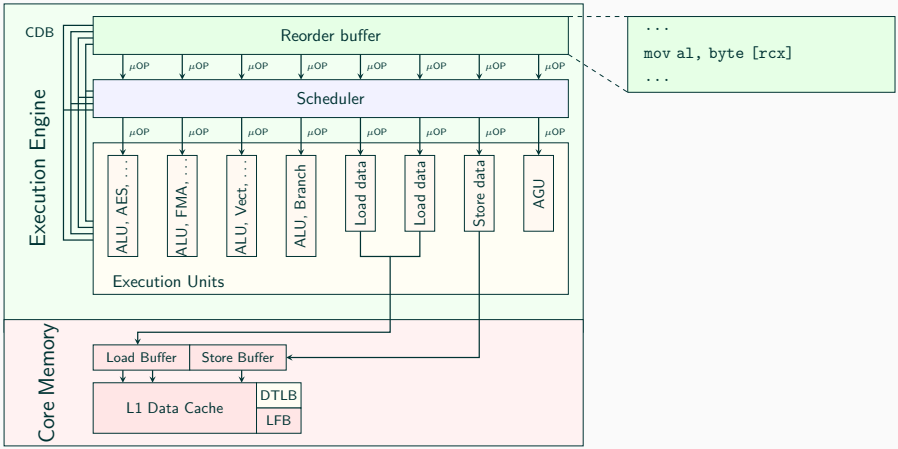

NOISE


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

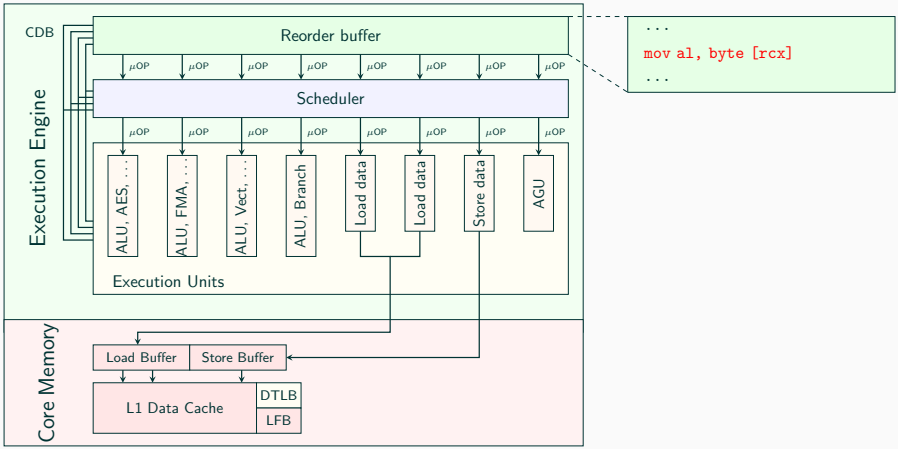
Complex Load Situations



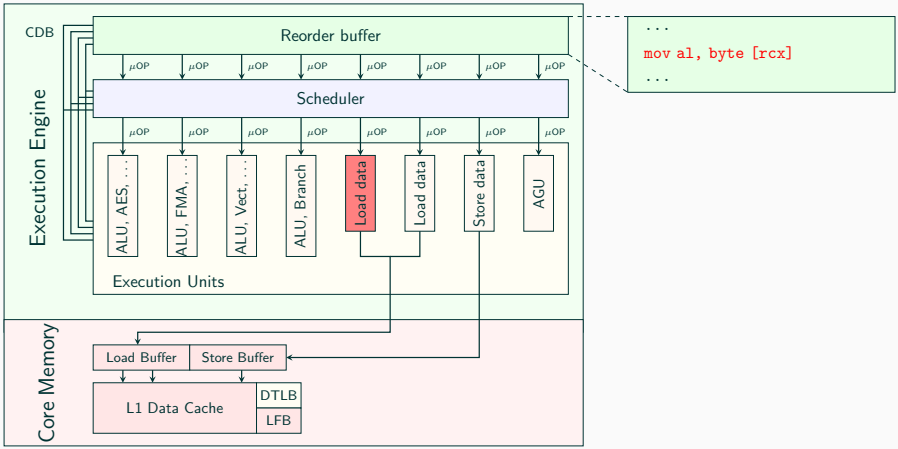
Complex Load Situations



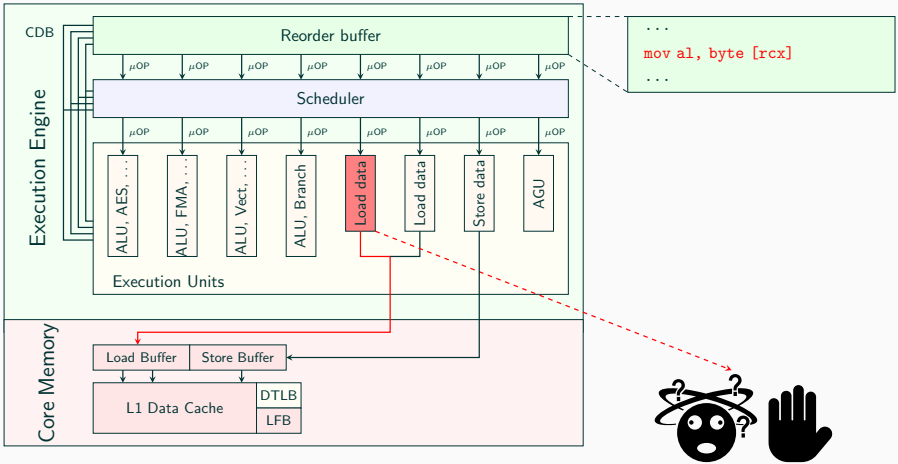
Complex Load Situations



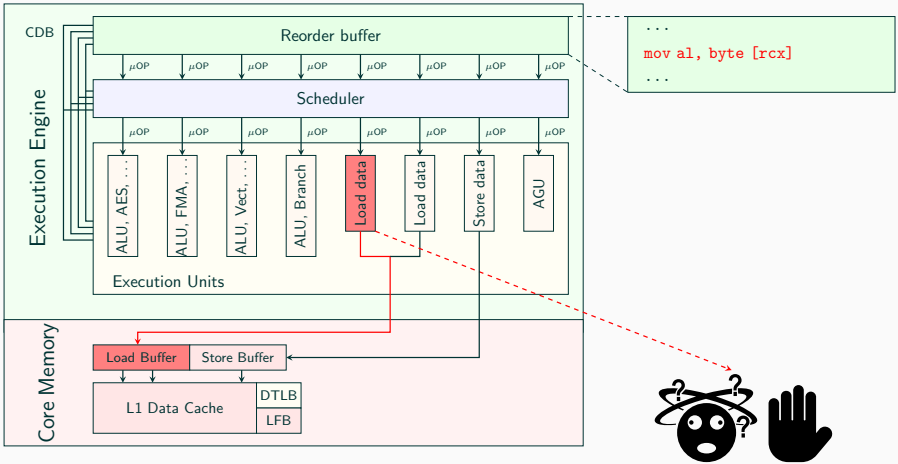
Complex Load Situations



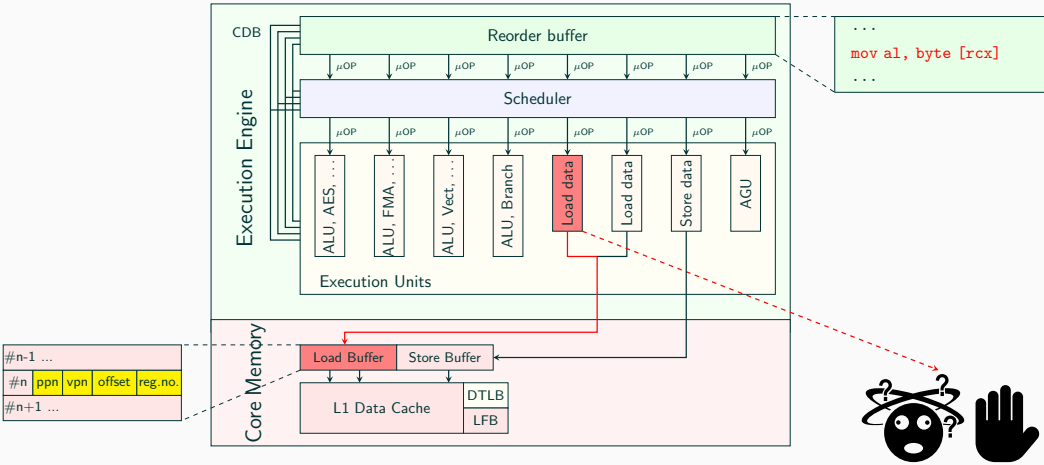
Complex Load Situations



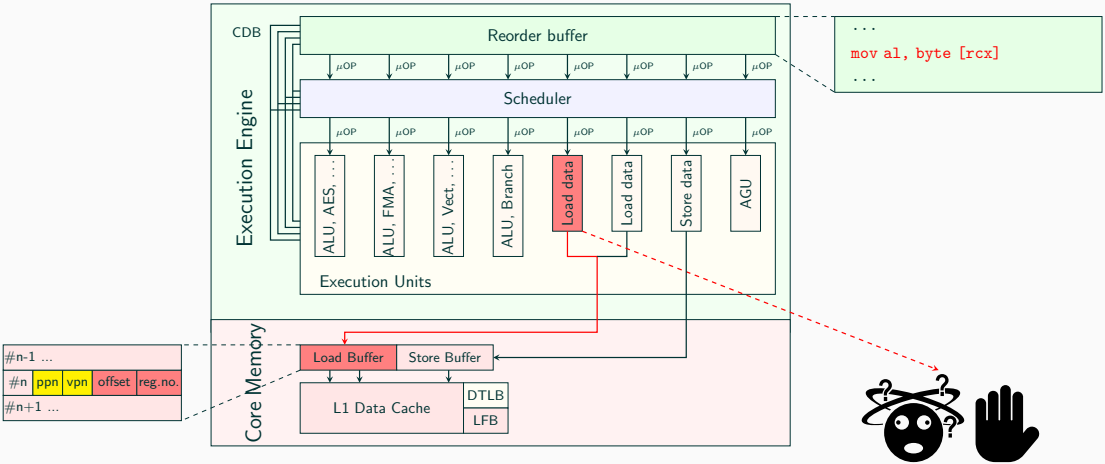
Complex Load Situations



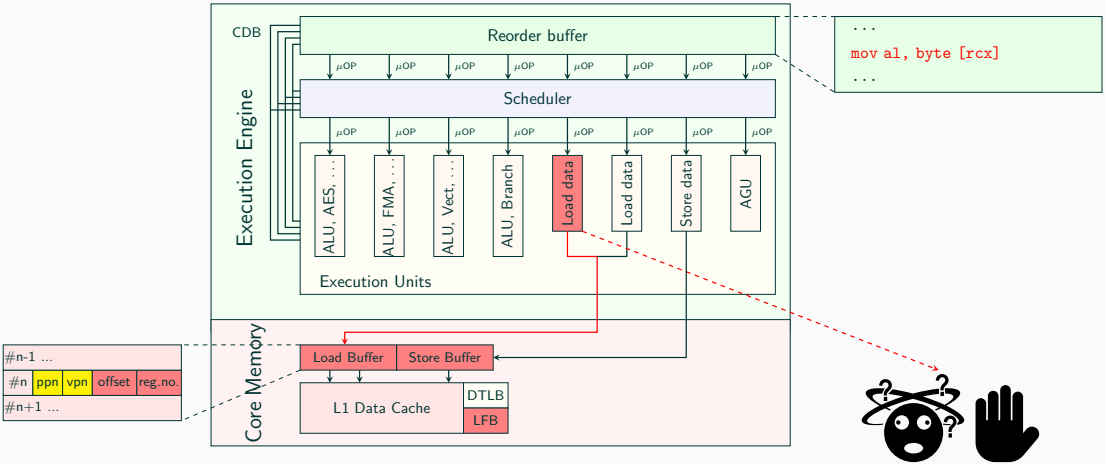
Complex Load Situations



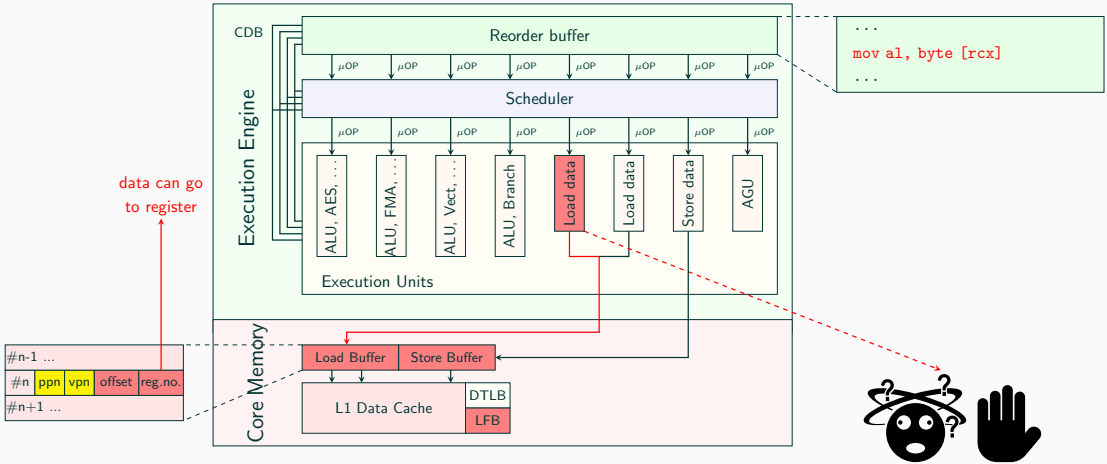
Complex Load Situations



Complex Load Situations



Complex Load Situations



- Complex situations handled in microcode

- Complex situations handled in microcode
  - Setting accessed/dirty bit

- Complex situations handled in microcode
  - Setting accessed/dirty bit
  - TSX abort + rollback

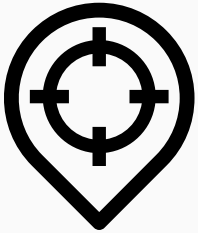
- Complex situations handled in microcode
  - Setting accessed/dirty bit
  - TSX abort + rollback
  - ...

- Complex situations handled in microcode
  - Setting accessed/dirty bit
  - TSX abort + rollback
  - ...
- Load needs to be re-issued

- Complex situations handled in microcode
  - Setting accessed/dirty bit
  - TSX abort + rollback
  - ...
- Load needs to be re-issued
- Meltdown effects due to "microarchitectural fault"

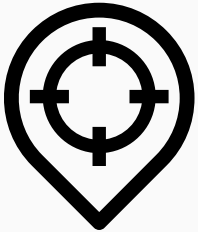
- Complex situations handled in microcode
  - Setting accessed/dirty bit
  - TSX abort + rollback
  - ...
- Load needs to be re-issued
- Meltdown effects due to "microarchitectural fault"
- No architectural fault handling required

Attack Targets



- Leak data on same and sibling hyperthread

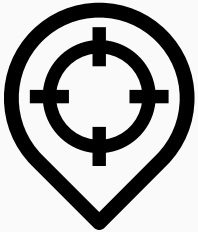
Attack Targets



- Leak data on same and sibling hyperthread

Applications

Attack Targets

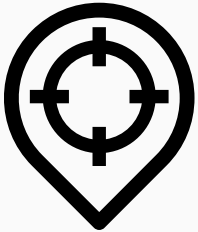


- Leak data on same and sibling hyperthread

Applications

Operating System

Attack Targets



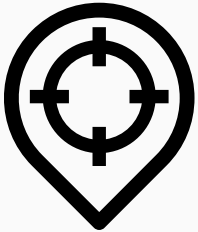
- Leak data on same and sibling hyperthread

Applications

Operating System

SGX Enclave

Attack Targets



- Leak data on same and sibling hyperthread

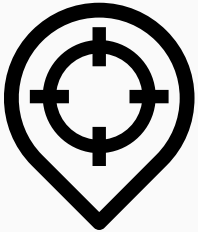
Applications

Operating System

SGX Enclave

Virtual Machine

Attack Targets



- Leak data on same and sibling hyperthread

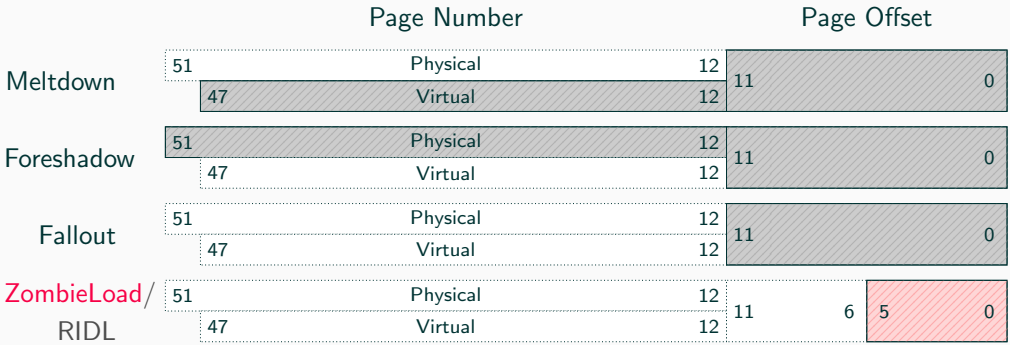
Applications

Operating System

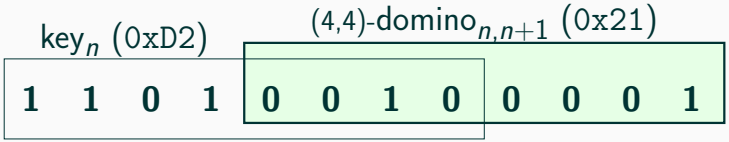
SGX Enclave

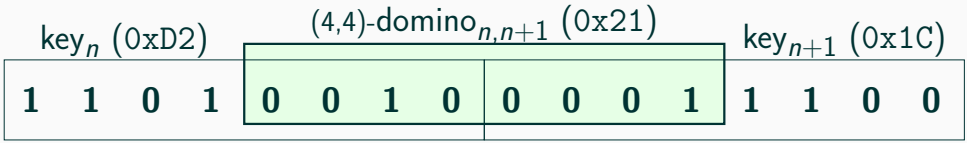
Virtual Machine

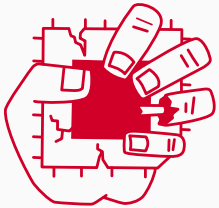
Hypervisor


Page Number
Page Offset
Meltdown
51
Physical
12
11
0
47
Virtual
12
Foreshadow
51
Physical
12
11
0
47
Virtual
12
Fallout
51
Physical
12
11
0
47
Virtual
12
ZombieLoad / RIDL
51
Physical
12
11
6
5
0
47
Virtual
12


key$_n$ (0xD2)
1 1 0 1 0 0 1 0

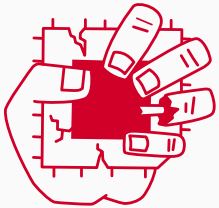

key$_n$ (0xD2)
(4,4)-domino$_{n,n+1}$ (0x21)
1 1 0 1 0 0 1 0 0 0 0 1


key$_n$ (0xD2)
(4,4)-domino$_{n,n+1}$ (0x21)
key$_{n+1}$ (0x1C)
1 1 0 1 0 0 1 0 0 0 0 1 1 1 0 0



AES-NI key

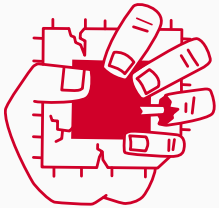
Results



AES-NI key

SGX sealing key

Results

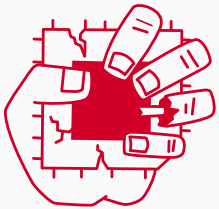


AES-NI key

SGX sealing key

Cross-VM covert channel

Results



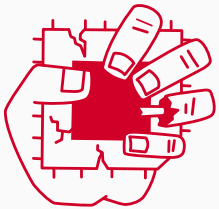
AES-NI key

SGX sealing key

Cross-VM covert channel

Keyword matching

Results



AES-NI key

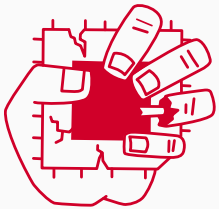
SGX sealing key

Cross-VM covert channel

Keyword matching

URL recovery

Results



AES-NI key

SGX sealing key

Cross-VM covert channel

Keyword matching

URL recovery

Targeted leakage

Variant 1

Kernel Mapping

5.30 kB/s

Variant 1

Kernel Mapping

5.30 kB/s

Variant 2

Transactional
Asynchronous Abort

39.66 kB/s

Performance

Variant 1

Kernel Mapping

5.30 kB/s

Variant 2

Transactional Asynchronous Abort

39.66 kB/s

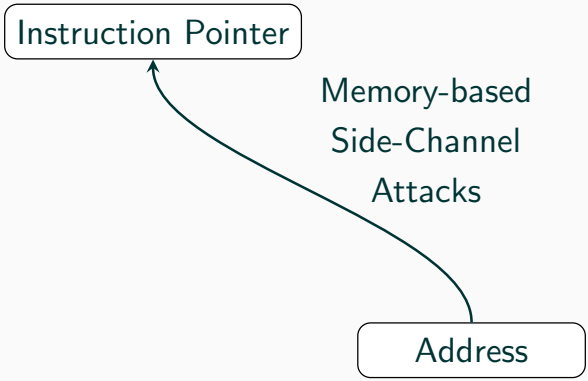
Variant 3

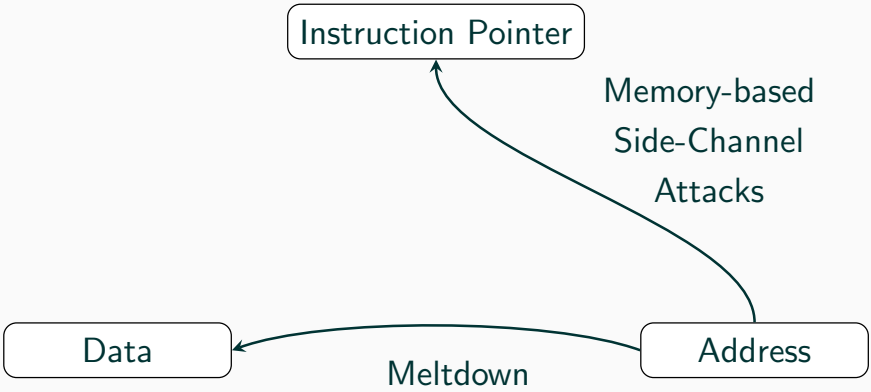
Microcode-Assisted Page-Table Walk

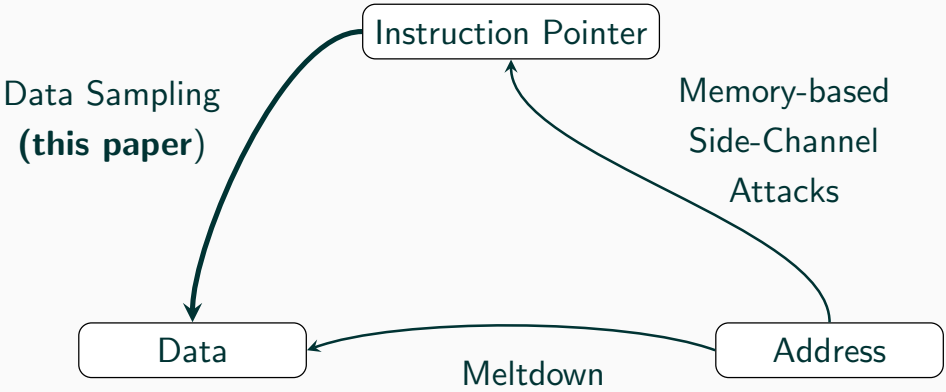
7.73 kB/s


zombieload : zsh — Konsole <2>
File Edit View Bookmarks Settings Help
michael@hp /tmp/zombieload %
zombieload : zsh

Address


Instruction Pointer
Memory-based
Side-Channel
Attacks
Address


Instruction Pointer
Memory-based
Side-Channel
Attacks
Data
Address
Meltdown


Instruction Pointer
Data Sampling
(this paper)
Memory-based
Side-Channel
Attacks
Data
Address
Meltdown

- Disable hyperthreading or group scheduling

- Disable hyperthreading or group scheduling
- Overwrite microarchitectural buffers

Intel Mitigations

- Disable hyperthreading or group scheduling
- Overwrite microarchitectural buffers
  - `VERW` instruction (microcode update)

Intel Mitigations

- Disable hyperthreading or group scheduling
- Overwrite microarchitectural buffers
  - `VERW` instruction (microcode update)
  - Software sequences

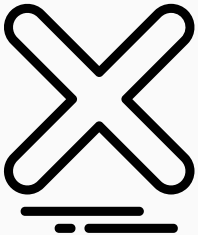
Intel Mitigations

- Disable hyperthreading or group scheduling
- Overwrite microarchitectural buffers
  - `VERW` instruction (microcode update)
  - Software sequences
- New CPUs which are not affected

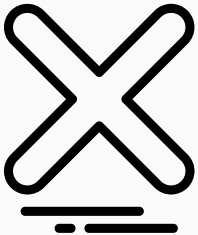
CPU	Meltdown	Foreshadow	RIDL	Fallout	MLPDS	MDSUM
8th/9th gen. Intel Core Coffee Lake	✗	✗	✗	✗	✗	✗
Intel Xeon Cascade Lake	✗	✗	✗	✗	✗	✗

- Disable hyperthreading or group scheduling
- Overwrite microarchitectural buffers
  - `VERW` instruction (microcode update)
  - Software sequences
- New CPUs which are not affected

CPU	Meltdown	Foreshadow	RIDL	Fallout	MLPDS	MDSUM	ZombieLoad
8th/9th gen. Intel Core Coffee Lake	✗	✗	✗	✗	✗	✗	???
Intel Xeon Cascade Lake	✗	✗	✗	✗	✗	✗	???

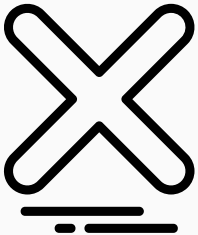


- Variant 2 works on all CPUs



- Variant 2 works on all CPUs

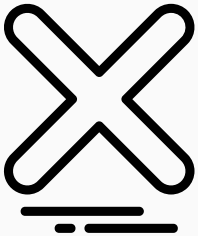
→ Embargoed until November 12, 2019



- Variant 2 works on all CPUs

→ Embargoed until November 12, 2019

- Microcode and software sequences do not prevent ZombieLoad

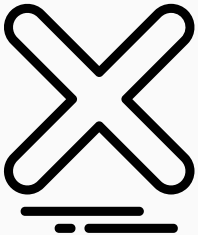


- Variant 2 works on all CPUs

→ Embargoed until November 12, 2019

- Microcode and software sequences do not prevent ZombieLoad

→ Reported on May 16, 2019



- Variant 2 works on all CPUs

→ Embargoed until November 12, 2019

- Microcode and software sequences do not prevent ZombieLoad

→ Reported on May 16, 2019

- ZombieLoad might not only leak from fill buffer

- Disable hyperthreading

ZombieLoad Mitigations

- Disable hyperthreading
- Flush all buffers on privilege-level change

ZombieLoad Mitigations

- Disable hyperthreading
- Flush all buffers on privilege-level change
  - Fill buffer, store buffer, load ports → `VERW`

ZombieLoad Mitigations

- Disable hyperthreading
- Flush all buffers on privilege-level change
  - Fill buffer, store buffer, load ports → `VERW`
  - Flush L1 cache → `MSR_IA32_FLUSH_CMD`

ZombieLoad Mitigations

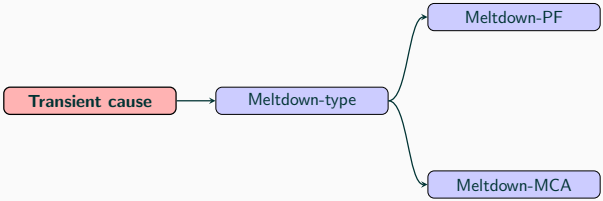
- Disable hyperthreading
- Flush all buffers on privilege-level change
  - Fill buffer, store buffer, load ports → `VERW`
  - Flush L1 cache → `MSR_IA32_FLUSH_CMD`
- Disable Intel TSX (`MSR_TSX_FORCE_ABORT`)

Transient Execution Attack Tree

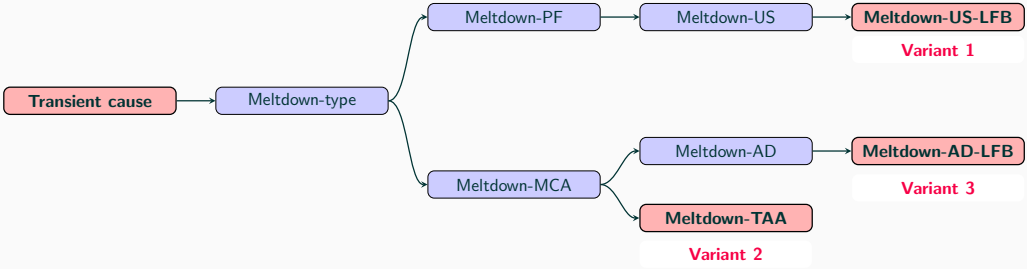
Transient cause

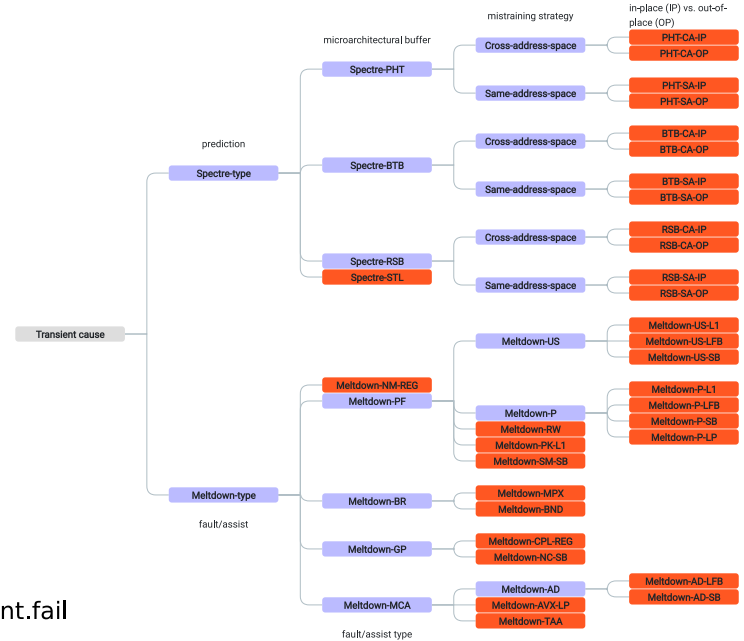
Transient Execution Attack Tree

Transient Execution Attack Tree



Transient Execution Attack Tree





https://transient.fail

You can find our proof-of-concept implementation on:

- `https://github.com/IAIK/ZombieLoad`

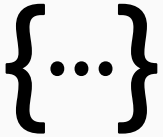
{...}

- Transient-execution attacks: the gift that keeps on giving

{...}

- Transient-execution attacks: the gift that keeps on giving
- Class of Meltdown attacks is larger than expected

Conclusion



- Transient-execution attacks: the gift that keeps on giving
- Class of Meltdown attacks is larger than expected
- CPUs are deterministic - there is no noise


MORITZ LIPP
MICHAEL SCHWARZ
DANIEL MOGHIMI
JO VAN BULCK
ZOMBIELOAD
GRAZ UNIVERSITY OF TECHNOLOGY PRESENTS IN COLLABORATION WITH
WORCESTER POLYTECHNIC INSTITUTE, KU LEUVEN, AND CYBERUS TECHNOLOGY
AN ACM CCS 2019 PAPER "ZOMBIELOAD: CROSS-PRIVILEGE-BOUNDARY DATA SAMPLING"
WRITTEN BY MICHAEL SCHWARZ, MORITZ LIPP, DANIEL MOGHIMI, JO VAN BULCK, JULIAN STECKLINA, THOMAS PRESCHER, DANIEL GRUSS

ZombieLoad

Cross-Privilege-Boundary Data Sampling

Michael Schwarz, Moritz Lipp, Daniel Moghimi, Jo Van Bulck, Julian Stecklina, Thomas Prescher, Daniel Gruss

November 11, 2019

Graz University of Technology