LVI

Hijacking Transient Execution through Microarchitectural Load Value Injection

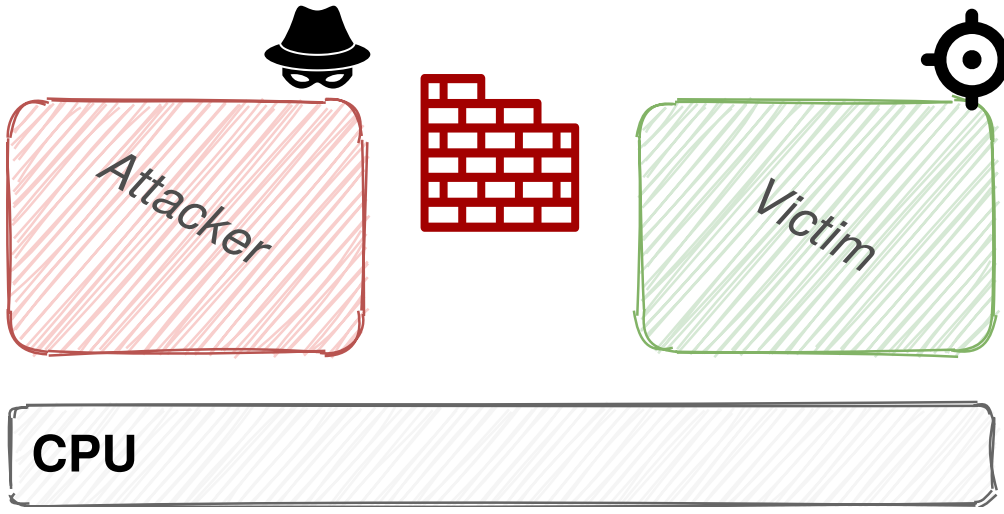
Jo Van Bulck [1] **Daniel Moghimi** [2] **Michael Schwarz** [3] **Moritz Lipp** [3] **Marina Minkin** [4]
Daniel Genkin [4] **Yuval Yarom** [5] **Berk Sunar** [2] **Daniel Gruss** [3] **Frank Piessens** [1]

CSAW'20 Applied Research Competition – November 6, 2020

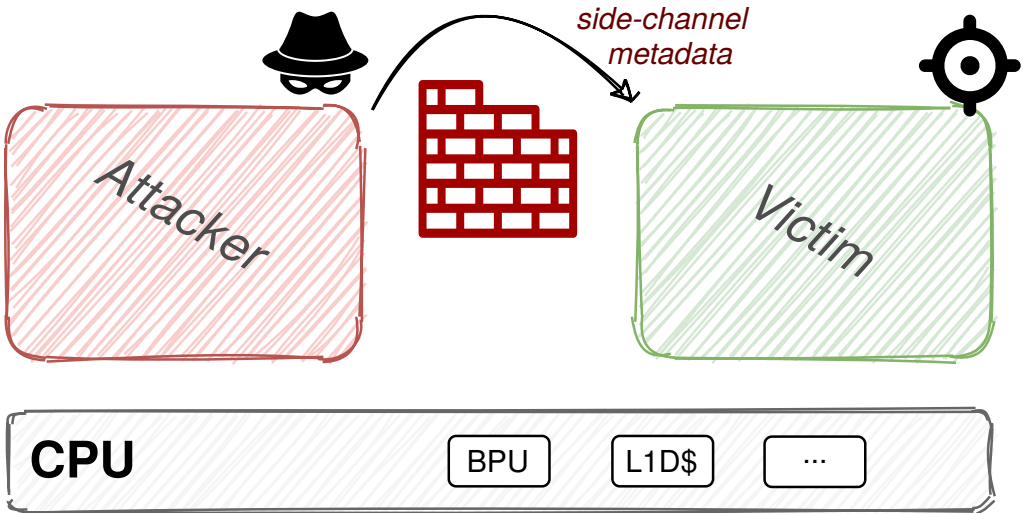
[1]imec-DistriNet, KU Leuven [2]Worcester Polytechnic Institute [3]Graz University of Technology
[4]University of Michigan [5]University of Adelaide and Data61

A very specific type of security...

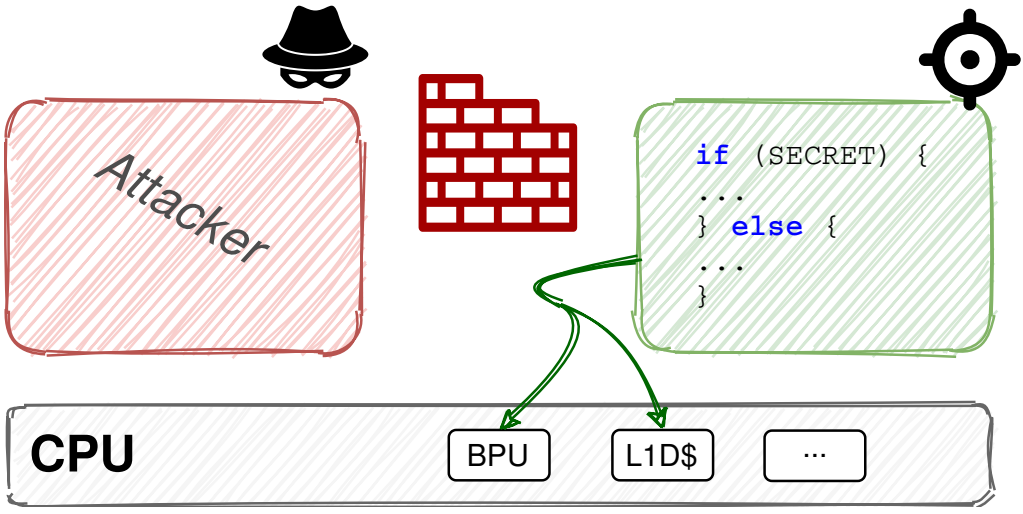
Microarchitectural side-channel attacks 101



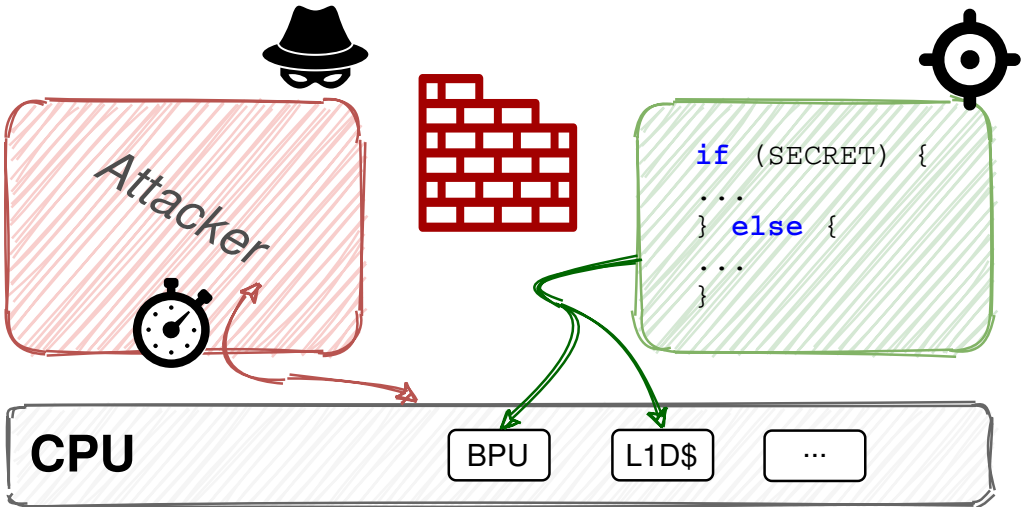
Microarchitectural side-channel attacks 101



Microarchitectural side-channel attacks 101

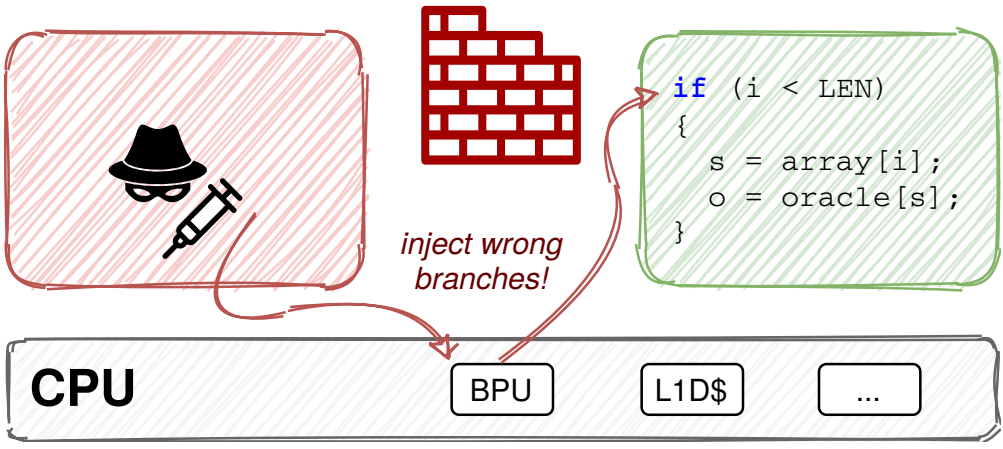


Microarchitectural side-channel attacks 101

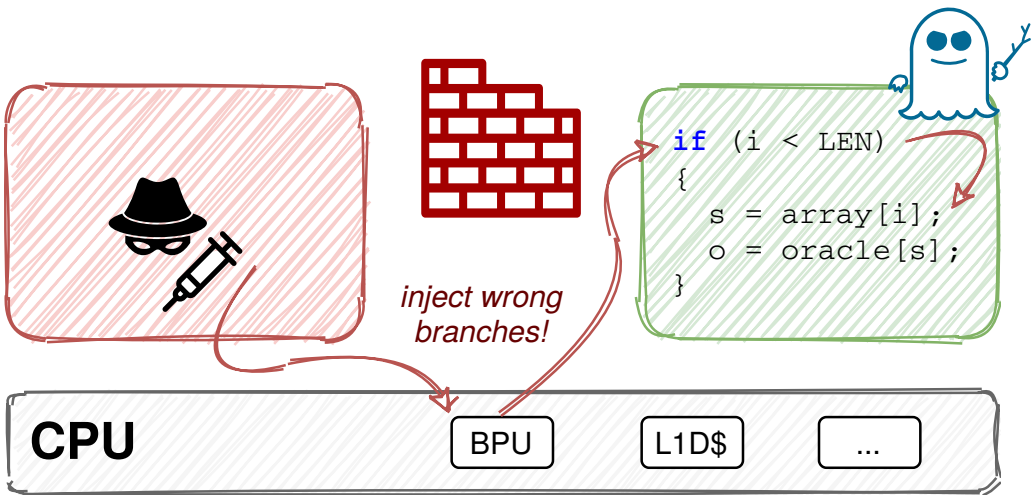



BUT EVERYTHING CHANGED...
...WHEN THE FIRE NATION
ATTACKED

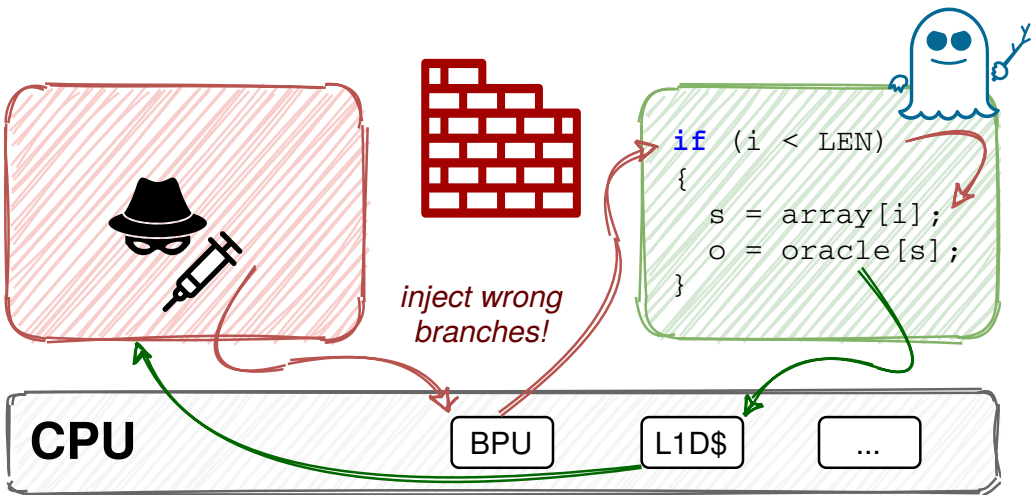
2018: The discovery of transient-execution attacks (Spectre)



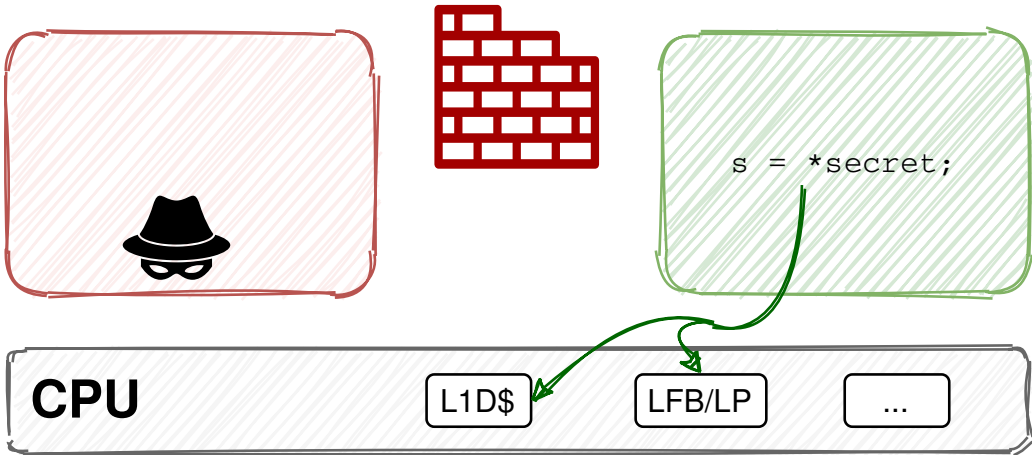
2018: The discovery of transient-execution attacks (Spectre)



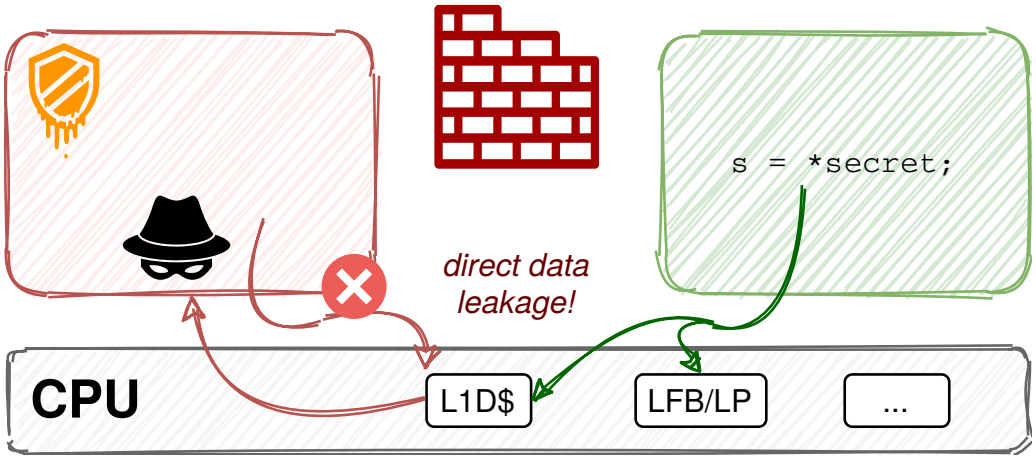
2018: The discovery of transient-execution attacks (Spectre)



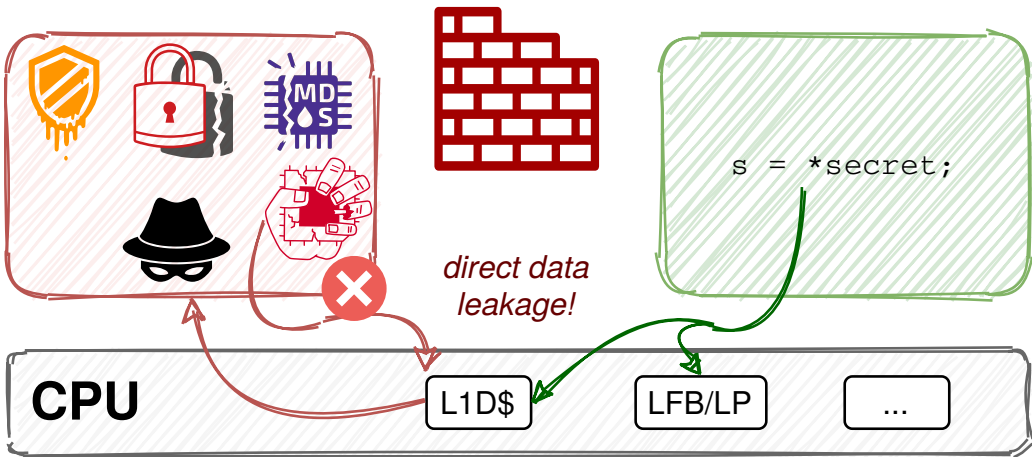
2018-2019: Leaking microarchitectural data buffers (Meltdown & friends)



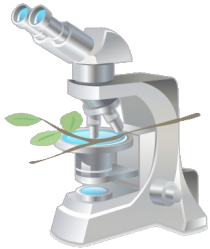
2018-2019: Leaking microarchitectural data buffers (Meltdown & friends)

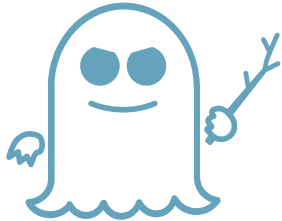


2018-2019: Leaking microarchitectural data buffers (Meltdown & friends)



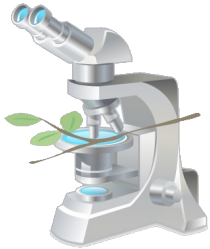
The last square...

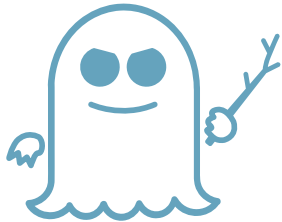




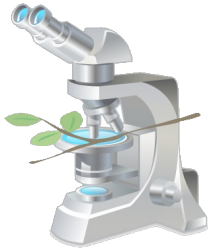

MD
S

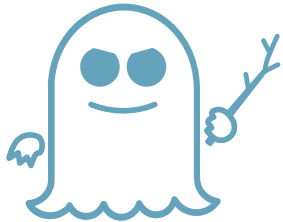
?



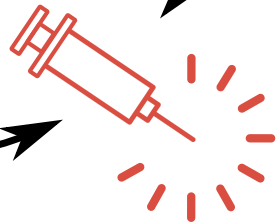



MD
S

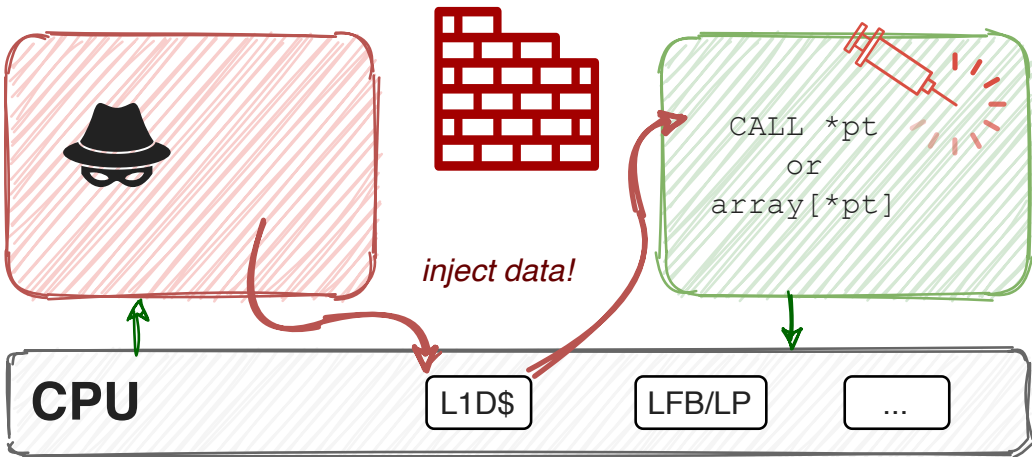





MD
S



Load Value Injection (LVI): The basic idea

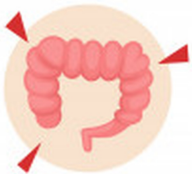


FOOD POISONING

Overdue products

Medicine

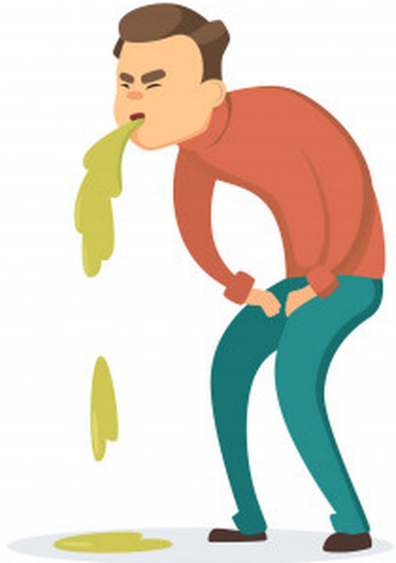
Dizziness



Intestinal colic

Diarrhea

Headache



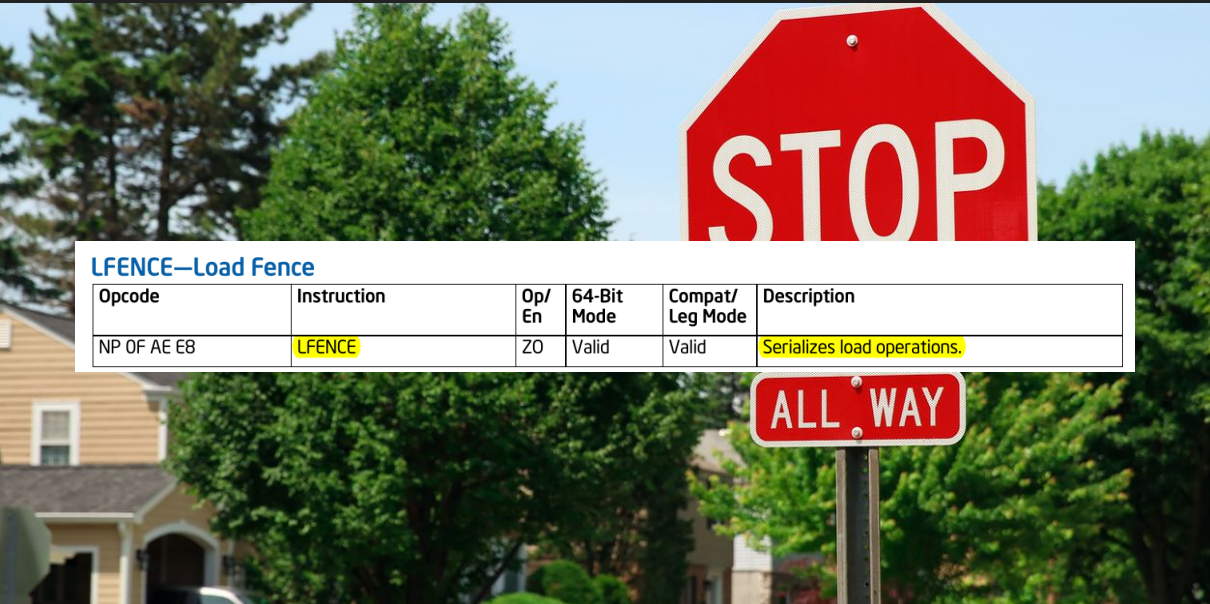
Vulnerable platforms: Intel Software Guard Extensions (SGX)

Enarx (Red Hat)

Asylo (Google)

Mitigating LVI: Fencing vulnerable load instructions

Mitigating LVI: Fencing vulnerable load instructions



LFENCE—Load Fence

Opcode	Instruction	Op/ En	64-Bit Mode	Compat/ Leg Mode	Description
NP 0F AE E8	LFENCE	ZO	Valid	Valid	Serializes load operations.

Mitigating LVI: Compiler and assembler support

`-mlfence-after-load`

GNU Assembler Adds New Options For Mitigating Load Value Injection Attack

Written by Michael Larabel in GNU on 11 March 2020 at 02:55 PM EDT. 14 Comments

`-mlvi-hardening`

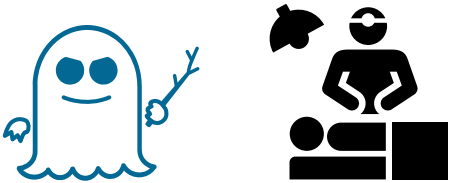
LLVM Lands Performance-Hitting Mitigation For Intel LVI Vulnerability

Written by Michael Larabel in Software on 3 April 2020. **Page 1 of 3**. 20 Comments

`-Qspectre-load`

More Spectre Mitigations in MSVC

March 13th, 2020

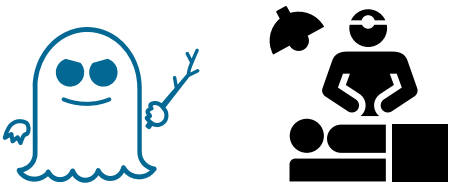


23 fences

October 2019—"surgical precision"

Intel architectural enclaves: `lfence` counts

`libsgx_qe.signed.so`



23 fences

October 2019—"surgical precision"

49,315 fences

March 2020—"big hammer"

GNU Assembler Adds New Options For Mitigating Load Value Injection Attack

Written by Michael Larabel in GNU on 11 March 2020 at 02:55 PM EDT. 14 Comments

The Brutal Performance Impact From Mitigating The LVI Vulnerability

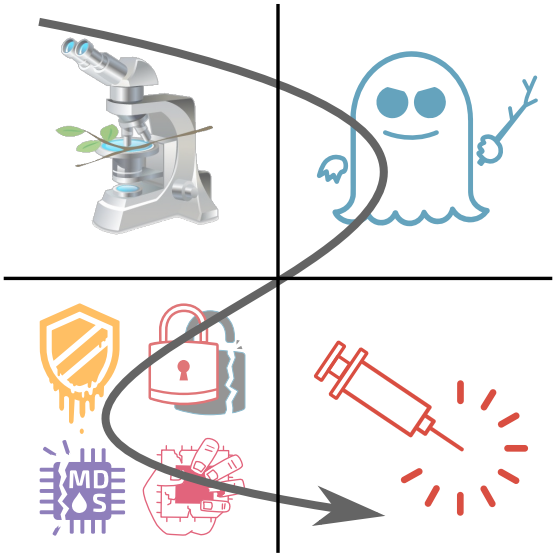
Written by Michael Larabel in Software on 12 March 2020. **Page 1 of 6**. 76 Comments

LLVM Lands Performance-Hitting Mitigation For Intel LVI Vulnerability

Written by Michael Larabel in Software on 3 April 2020. **Page 1 of 3**. 20 Comments

Looking At The LVI Mitigation Impact On Intel Cascade Lake Refresh

Written by Michael Larabel in Software on 5 April 2020. **Page 1 of 5**. 10 Comments


MD
S