LVI: Hijacking Transient Execution through Microarchitectural Load Value Injection

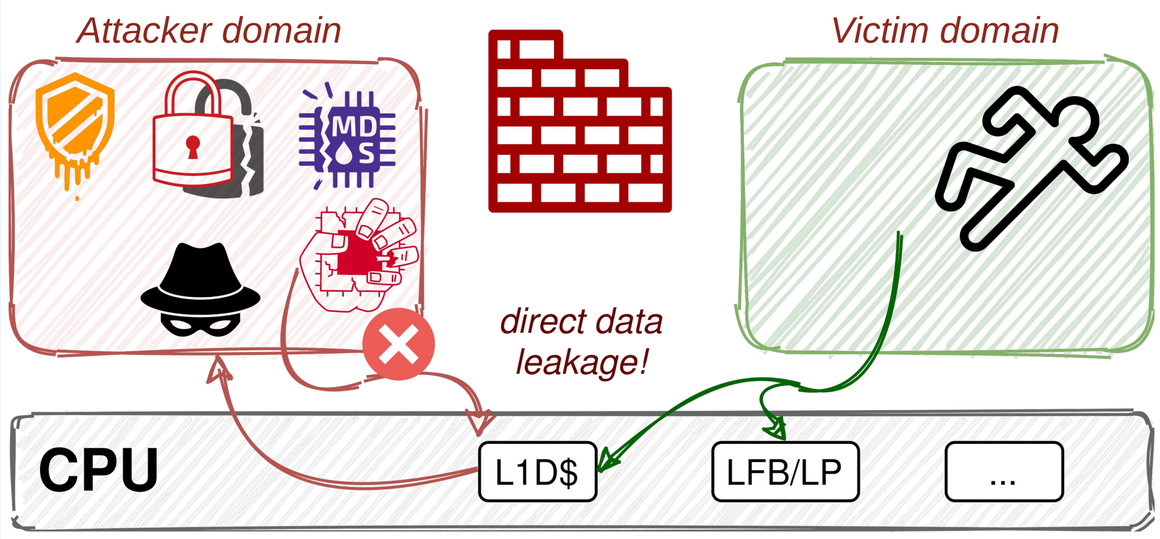
Jo Van Bulck[1], Daniel Moghimi[2], Michael Schwarz[3], Moritz Lipp[3], Marina Minkin[4], Daniel Genkin[4], Yuval Yarom[5], Berk Sunar[2], Daniel Gruss[3], and Frank Piessens[1]
[1] imec-DistriNet, KU Leuven, [2] Worcester Polytechnic Institute, [3] Graz University of Technology, [4] University of Michigan, [5] University of Adelaide and Data61

https://lviattack.eu/ https://github.com/jovanbulck/sgx-step https://youtu.be/baKHSXeIIaI

SCAN ME

Teaser

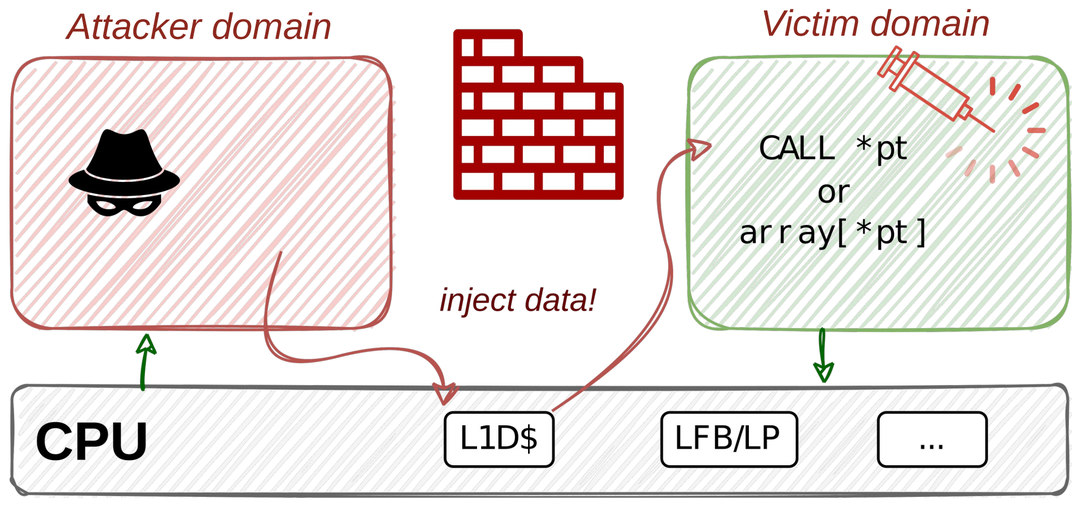
From microarchitectural data leakage...



- **2018 -** Meltdown, Foreshadow
- **2019 -** RIDL, Fallout, ZombieLoad, MDS

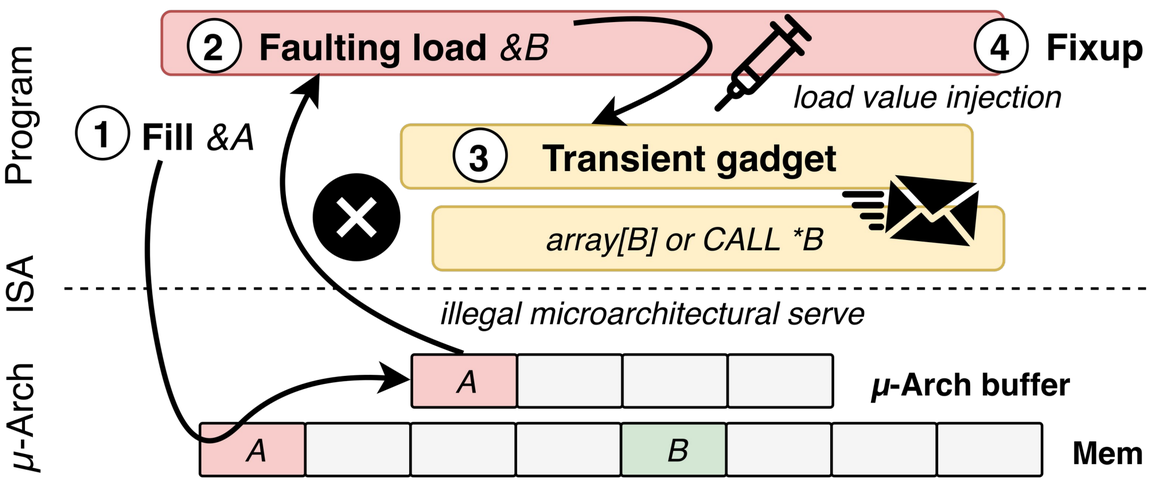
➔ **Flush leaky buffers** on context switch

...To microarchitectural data injection!



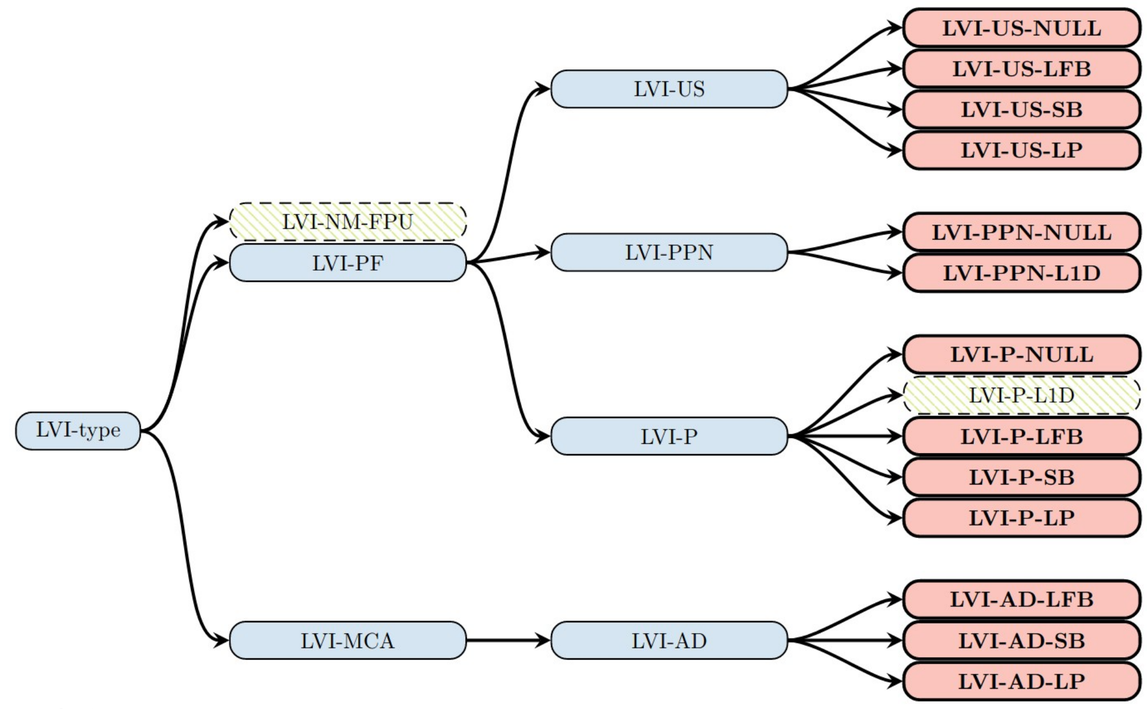
- **Gadget-driven** exploitation of faulting loads
- ≠ Spectre: Hijack *any* load with *unrelated* data

LVI in 4 simple steps



- Induce **page fault** or **μ-code assist** in victim
- Vulnerable platforms: **Intel SGX**

LVI taxonomy: Many buffers, many faults...



LVI-NULL even on Meltdown-resistant CPUs!

Compiler `lfence` mitigations

`-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

Visual C++

`-Qspectre-load`

More Spectre Mitigations in MSVC

March 13th, 2020

Instruction	Possible emulation	Clobber-free
`ret`	`pop %reg; lfence; jmp *%reg`	✗
`ret`	`not (%rsp); not (%rsp); lfence; ret`	✓
`jmp (mem)`	`mov (mem),%reg; lfence; jmp *%reg`	✗
`call (mem)`	`mov (mem),%reg; lfence; call *%reg`	✗

Mitigation impact: March of the `lfences`

23 fences

October 2019—"surgical precision"

49,315 fences

March 2020—"big hammer"

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

- **Slowdown** (application-specific) with **factor 2-19**
- Until **silicon patches** in newer CPUs

Published in 41st IEEE Symposium on Security and Privacy (S&P), 2020.