Lecture 1: Meltdown/Spectre and Intro

Tuesday, January 2, 2018 3:55 PM

ECS 154B

Outline

- Introduce myself
- Meltdown/Spectre and computer architecture
- Syllabus, etc.

Introduction

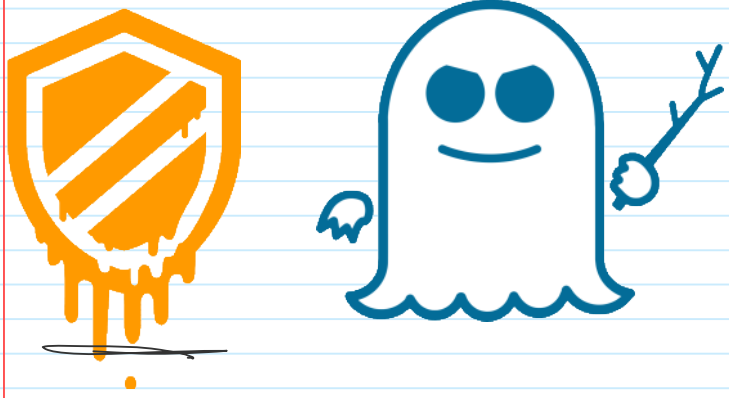
Jason Lowe-Power

Meltdown and Spectre

Many more details: https://meltdownattack.com/

Researchers Discover Two Major Flaws in the World's Computers

By CADE METZ and NICOLE PERLROTH JAN. 3, 2018



Speculative execution.
1st => predict what might be needed to execute
2nd => execute

Architectural state vs microarch. state

Architectural state vs microarch. state

Virtual memory

each process thinks it can access all physical memory

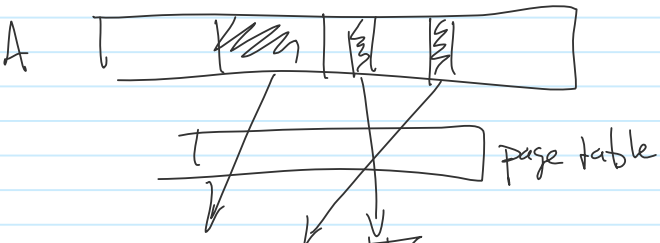
indirection

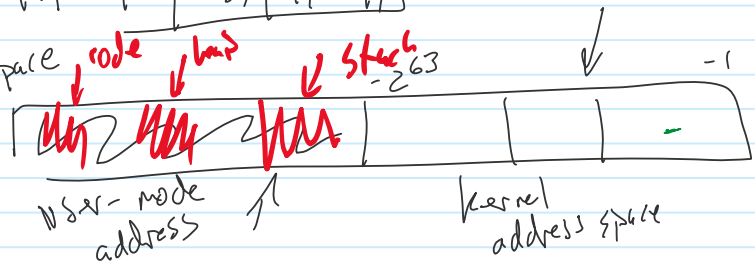
Proc 0 VA → PA

0x1000 → 0x3af000

Proc 1 VA

0x1000 → 0x3bf000 PA





user mode or kernel mode

ring 3 ring 0

limited access

Code

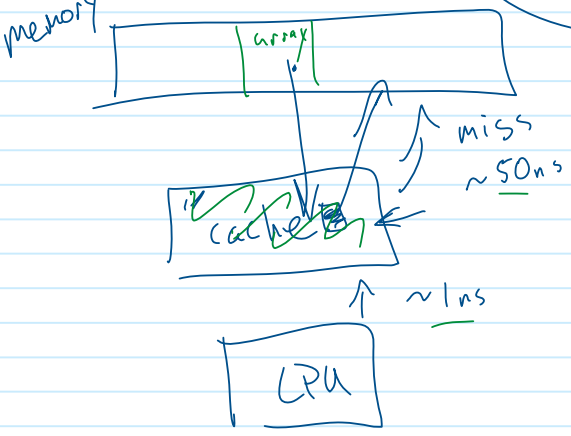
mov %rcx, -0x10000 — Put -10000 into rcx

→ mov %rax (%rcx) — move data in kernel address 0x10000 into register

only 1 byte — mov %rbx, (%rbx + %rax)

cache miss branch ↑ undo

%rbx



Solution

separate user addresses from kernel KPTI
kernel page table Isolation

↳ hurts perf ~ up to 30%

Spectre

Server program