



## MELTDOWN

Meltdown exploits two properties of modern CPUs

- ▶ *Out of order execution* of OPs and  $\mu$ OPs
- ▶ Timing side channels for the cache

This allows an attacker to

- ▶ Read all memory mapped<sup>1</sup> in a process
- ▶ This often includes all other processes memory
- ▶ This does NOT allow reading “outside of a VM<sup>2</sup>”

<sup>1</sup> [Virtual vs. physical memory](#) is a subject for another time   <sup>2</sup> For fully virtualised VMs



SPECULATIVE  
EXECUTION

---

**SPECTRE**