



MELTDOWN

Meltdown exploits two properties of modern CPUs

- ▶ *Out of order execution* of OPs and μ OPs
- ▶ Timing side channels for the cache

This allows an attacker to

- ▶ Read all memory mapped¹ in a process
- ▶ This often includes all other processes memory
- ▶ This does NOT allow reading “outside of a VM²”

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



SPECULATIVE
EXECUTION

SPECTRE