MELTDOWN

Meltdown exploits two properties of modern CPUs

▸ *Out of order execution* of OPs and µOPs

▸ Timing side channels for the cache

This allows an attacker to

▸ Read all memory mapped[1] in a process

▸ This often includes all other processes memory

▸ This does NOT allow reading "outside of a VM[2]"

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

SPECULATIVE
EXECUTION

SPECTRE