

Design flaws in new computer chips

Design flaws in central processor units (CPUs) could allow hackers to trick apps into revealing sensitive data such as passwords. The CPU “kernel” – the core of the operating system – is leaking memory

1 Speculative execution: Program executes instructions based on assumptions that are considered likely to be true. Program tells CPU to switch to **kernel mode** – technique improves performance

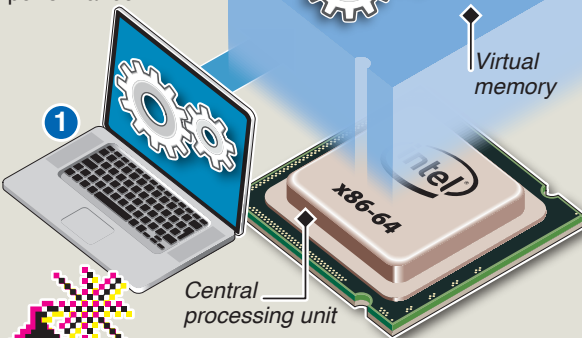
2 Kernel mode: During speculative execution, code and data remains invisible in **virtual memory**

Assumption A

Assumption B

3 Best guess: Kernel predicts code to be run next and executes it. Code is ignored if not needed – CPU switches back to user mode.

Flaws allow kernel access protections to be bypassed



Patches Meltdown: Most dangerous flaw could let hackers steal data such as passwords and login files
Spectre: Flaw affects CPUs in smartphones and tablets. Patches move kernel into separate address space – expected to cause five to 30 percent slow down to processing speed