# Spectre Attack

Side Channel Used: Spectre use , in modern CPUs, the timing difference during speculative execution. It utilizes a dependent cache timing side channel based on the fact that during speculative execution , different data is kept in the CPU cache.

Systems Affected:Systems running on modern processors from Intel, AMD, and ARM will be affected by Spectre , putting every PC, server, smartphone, and all cloud infrastructure at risk.

Leaked Information: The side channel reveal sensitive information about passwords, encryption keys, and other private information handled by the CPU, which should otherwise remain inaccessible.

Documented Real-Life Use: Although Spectre has been widely demonstrated in security labs, no large-scale real-life attacks have been definitively linked to Spectre. Its presence has raised concern because it could be exploited.

The mitigations involve software patches for limiting speculative execution and hardware updates for better isolation between processes. Patches have been released by Intel and AMD, as well as OS vendors like Microsoft, Linux, etc. Fixing Spectre without degradation in performance is perfect.

Sources:

Lipp, Moritz, et al. "Meltdown: Reading Kernel Memory from User Space." USENIX Security Symposium, 2018.
https://meltdownattack.com/meltdown.pdf

Kocher, Paul, et al. "Spectre Attacks: Exploiting Speculative Execution." arXiv preprint arXiv:1801.01203 (2018).
https://arxiv.org/abs/1801.01203

Intel, "Intel Analysis of Speculative Execution Side Channels."
https://www.intel.com/content/www/us/en/architecture-and-technology/facts-about-side-channel-analysis-and-intel-products.html