Kabir, Latif

15-30031-2

**Meltdown & Spectre Vulnerabilities**

In June, 2017 researcher working for Googles project zero found 2 major security flaws in modern processor. This flaw allows any program to read sensitive data from memory. This bug is called meltdown and spectre.

Before explaining Meltdown & Spectre we need to clear two things.

1. Speculative execution.
2. How Cache in processor and Main Memory (RAM) works.

**Speculative execution**

Speculative execution is a technique CPU designer use to improve CPU performance. In Speculative execution the processor guess what is the outcome of the next instruction and compute all the outcome for all branches. It can be simplified like if X is true then compute function func1 and if X is false then compute func2. The processor will calculate both function parallel with getting the true/false result. Then after getting true/false result if won’t calculate again and use the result to continue further. The modern computer uses this technique to calculate faster.

**How Cache in processor and Main Memory (RAM) works**

Processor always have to read and write data from main memory. The Main memory is very slower than cache memory. So, there are some cache memory set in CPU by the manufacturer. When CPU need some data from main memory it copies from main memory and store in cache to calculate faster from there.

**Meltdown**

Our sensitive information is stored in Protected memory where CPU make sure that no one can access that data without Operating system itself. But the problem is this rule wasn’t applied when CPU is speculating. When attacker want to steal data from protected memory the CPU will block the process but as CPU is speculating it already executed next step and stored that data into CPU cache and from there attacker can read that data and steal sensitive information.

# Spectre

Spectre is more harmful than meltdown. Meltdown only allow to read data from protected memory but spectre allow attacker to read data from all other running application on the system.

**Which platform is vulnerable to Meltdown and spectrum**

Meltdown mostly affects Intel processors. AMD and ARM appear largely immune to Meltdown, though ARM’s upcoming Cortex-A75 is apparently impacted. There are differences between how Intel, AMD, and ARM implement speculative execution, and those differences are part of why Intel is exposed on Meltdown in ways that the other vendors aren’t.

Spectre is much more widespread, however. Almost every system is affected by Spectre, including desktops, laptops, cloud servers, and even smartphones.

**Solution for this Problem**

Windows, macOS, and Linux all provide patches through software update. Though the problem cannot be completely fixed by software update. The main problem is that this Speculative execution gives processor huge faster computation so manufacturer can not stop using this technique.