Spectre and Meltdown - CPU Security Flaws

Introduction:

Before we understand what Spectre and Meltdown are, it is important to understand what they negatively affect: computer chips. A ***computer chip*** stores computer memory, performs arithmetic/logical operations, makes decisions and also executes certain instructions based on those decisions. When several of these computer chips are put together, they form the **CPU** (Central Processing Unit) which acts as the **powerhouse of the computer**. So any kind of mishap that happens to the CPU can deteriorate the performance of the computer or affect the computer itself. This brings us back to our initial point of discussion - Spectre and Meltdown.

Spectre and Meltdown are the names of two variations of the same underlying vulnerability, that affects every computer chip made in the last 20 years. They were both publicized by security researchers in 2018. These flaws arose because of certain **side effects** of using some speed boosting features of the chips, which could result in impacting the computer's overall performance. Spectre and Meltdown involve using a **malicious program** that can be used by attackers to access all of the user's private data stored on the computer. Let's talk specifically about each security flaw to understand how they both can uniquely attribute to this vulnerability:

Meltdown:

Meltdown is an attack that generally applies to Intel and Apple processors, and it can **read the entire kernel memory of the machine**. A ***kernel*** is the central part of a computer's operating system, which is responsible for handling the hardware, memory, external peripherals like a mouse or printer and a lot of other important operations. All of these core processes of the operating system, require an amount of memory to work, so the ***kernel memory*** is just that; memory allocated to ensure that these core processes take place whenever your computer boots up. So anyone who exploits Meltdown, can read any concealed information that your computer and its OS kernel is protecting.

Meltdown makes use of an important performance feature of these processors, called ***Out-of-Order execution***. This feature is responsible for accelerating the execution of time-consuming tasks. Instead of stalling the other tasks and waiting for the slow one to finish, processors can run all these tasks out-of-order i.e, they **look ahead** and schedule the idle execution units with some other work, while the busy ones take their time. One way to imagine this is by thinking of a restaurant. Imagine this restaurant is run by a single chef and there is a waiter to wait on the customers. Instead of the waiter waiting for every meal to be made before serving it to each customer, he can wait on the subsequent tables in the time it takes for the chef to prepare a meal for the previous customer. The execution units would work in a similar way. Now a flaw with out-of-order execution is that, sometimes, there can be small time differences between each task execution and this can cause a **leak of information**. Meltdown exploits this flaw to access secret information on the user's computers.

Spectre:

Spectre is an attack that applies to Intel, Apple, ARM and AMD processors. It technically works by **tricking the processors** into executing instructions they should not have been able to execute under normal circumstances. This helps the attacker gain access to the confidential information in the memory of other applications. For example, the **Javascript code** of a website's login page could use a Spectre attack to trick the user's web browser to give up their username and password. This is a reason why it is important to keep your browsers up to date.

Spectre specifically attacks processors that perform branch prediction and ***speculative execution***. If, for instance, an out-of-order execution reaches a ***conditional branch*** (should I perform Instruction A or should I perform Instruction B?), the processor may not know what to do because the instructions that determine which branch to take, haven't been executed yet (because out-of-order executions go ahead of instructions to finish all the tasks sooner). When this happens, the processor can **save its current state, make a prediction and move forward speculatively**. If it turns out to be the right prediction, it will permanently save the state and continue. If not, the processor realizes that it made an incorrect prediction, abandons whatever steps it took so far and will go back to the previously saved state it was before it made any predictions at all. Using this form of execution, the processor is tricked into speculatively executing instructions into the **attacker's channel**.

Actions Taken:

Patches can be used to **protect the computer systems** against the Spectre and Meltdown attacks. A ***patch*** can help make changes to a computer program to fix it or make updates. Patches have been issued to all kinds of devices like servers, desktops, notebooks, iOS and Android devices and also cloud computing services. Installing the latest patches for your system can help ensure a minimal probability of attack. The probability is minimal because new patches are rolled out every now and then to address new variants of the attacks. So it's always **better to keep updating the patches**.