Name : Zubaer Ahmed Sakib  
ID : 15-29581-2

**MELTDOWN and SPECTRE**

1. What are Meltdown and Spectre ?

Ans : During late 2017, Security Researchers found out dangerous vulnerabilities in the fundamental code in the kernel of almost every computer chipset manufactured within the last 2 decades. Then in 2018 their research was published and the world came to know about these vulnerabilities having 3 variations. The researchers primarily categorized the vulnerabilities into 2 main parts :

1. Spectre (consists of 2 variants)
2. Meltdown (consists of 1 variant)

In short, all of these 3 variants can be defined as :   
When a malicious application/program gains access to and uses the data which it was not authorized to access. Meaning, if a rogue process tries to or gains access to any data that it does not have the permission to see, it can be called “Spectre” or “Meltdown”, based on which variant of vulnerability was exploited by the rogue process of that malicious program.

1. Which platforms are being affected due to Spectre and Meltdown ?

Ans : The two techniques, “Speculative Execution” and “CPU Caching” are exploited by the malicious program to find a way through the hardware-based security layer of the chipset. Currently, almost all of the Intel x86 based microprocessors, IBM POWER processors and some of the ARM-based microprocessors are being affected by both Meltdown and Spectre.

1. How does Spectre and Meltdown affect a system ?

Ans : To understand how Spectre and Meltdown affects a system, we need to understand 3 basic concepts :

1. Speculative Execution
2. CPU Caching
3. Protected Memory

“Speculative Execution” is a technique where a chipset predicts a user’s next move by keeping track of frequently used processes and starts executing those processes even before receiving instruction from the user. It runs multiple processes parallelly and stores the resultant data in the CPU’s memory called “Cache memory”. It takes much more time for the CPU to fetch data from the main memory. So “CPU Caching”, a small but very effective memory system was introduced to enable the CPU to keep very frequently used data in a small chunk of memory called “Cache”. In this way, all the necessary processes are executed much faster than usual.  
Now, another memory called “Protected memory” is also used by a chipset to keep a program from accessing data of another program. But if a program need protected data of other programs to function, it may gain access to Protected memory but with a Privilege Check. This check is responsible for giving permissions or restricting a process to access the Protected memory. Since, the privilege check is a relatively slower process than accessing the “Cache memory”, where resultant data from the “Speculative Execution” phase is stored, a malicious program or a rogue process can easily fetch data of other programs which it has no permission to see.   
This data theft is done even before the Privilege check ends, because as soon as the check ends, the program will be denied access to the protected memory. But the time that is taken by the Privilege Check is the real vulnerability in this case. Within this short period of time, the data remains vulnerable and can be stolen by a program unauthorized see that data.

1. What can be done to resolve these vulnerabilities ?

Ans : Operating Systems like Linux, macOS, iOS and Windows are being affected by these vulnerabilities. But Security patches have been introduced to resolve this huge problem. On one hand the patches prevent malicious programs from exploiting the 2 techniques mentioned above used by chipsets to optimize computing time, on the other hand those patches reduced system performance due to lack of the optimization that was done by using “Speculative Execution” and “Caching”. Because the parallel process execution that was previously performed were restricted to some extent thus affecting the overall execution time of processes which finally affect overall system performance.

But whatever patches are introduced at the software level the main problem remains, because the hardware level problems can never be patched. But still patches are being introduced and welcomed by most cloud vendors which strengthens the security. Even if we do get affected by Spectre or Meltdown, those patches can significantly reduce the level of damage. In this way this problem is being handled with software patches for the moment.