***Momtaz Begum***

***ID:15-29532-2***

***Advanced Operating System***

***1/ What is meltdown and spectre?***

***Ans:*** Meltdown is one type of hardware vulnerability that allows all memory to be read even if it is unauthorized. Spectre is another type of vulnerability that leaks private data through branch misprediction. These are mainly bugs that exposes information stored deep inside the computer system and exploit critical vulnerabilities in modern processors. Generally meltdown and spectre vulnerabilities are used to steal data which are being processed in the computer. Usually programs are not given permission to read data from others but a malicious program can exploit meltdown and spectre to get access to data stored in the memory of other running programs. This might include passwords stored in a password manager or browser, personal photos, emails, instant messages, encrypted communications and even important business documents.

***2/ How does meltdown and spectre work?***

***Ans***: Meltdown works by destroying the boundary that prevents applications from accessing arbitrary locations in the kernel memory. Memory spaces that are separately protected do not allow applications from accidentally interfering with one another’s data. They also do not allow malicious software from being able to see and modify it at will. Meltdown makes this process completely unreliable. It does not depend on any operating system or other software vulnerability. Meltdown breaks all security assumptions given by address space isolation and reads memory of other processes or virtual machines in the cloud without any permissions affecting millions of pc users. Meltdown works in the following way:

1. The attacker chooses an inaccessible memory and loads it in a register
2. Based on the private content of the register, a cache line is accessed by a transient instruction.
3. Using Flush plus reload the attacker gets access to the private data at the chosen memory location.

In case of spectre, attackers trick users to perform operations that usually do not occur which leads to data being exposed via a side channel to the adversary.

Spectre works in the following way:

1. Spectre shows branch prediction logics based on the internal work of a malicious program.
2. It then shows that the difference between cache hit and misses can be converted into a channel which extracts data from an unrelated process.
3. A Javascript program is shown that reads data from the address space of the browser process running it. The main idea is to look for existing code for places where data is inaccessible.

***3/ On what platforms does meltdown and spectre work?***

***Ans:*** Meltdown usually affects intel processors, android phones, windows pc’s, iphone , macs and so on. Spectre affects pretty much anything with a chip in it like Intel, AMD, and ARM processors. Linux and Microsoft windows are two of the platforms which are seen to be affected by meltdown more often than not. While for spectre the usual platforms are Android, iOS, Macs.

.i**) Linux** :

Meltdown affects multiple version of linux kernel from 2.6.32 to 4.13.0. It bypasses all permission settings and leaks data to attackers. Before kernel 4.12, kernel address space layout randomization (KASLR) was not active by default. But still the kernel can be found out by searching the address space.

**ii) Windows**:

Meltdown affects almost all version of windows including the latest Microsoft windows 10. Meltdown also can leak arbitrary kernel memory on Windows. Unlike Linux, windows does not have identity mapping. Instead a large portion of physical memory is mapped into physical address space. So meltdown reads memory mapped in the kernel address space and leaks data.

Due to meltdown and spectre being architectural level bugs, it doesn’t matter whether a computer or device is running Windows, OS X, Android or something else because all software platforms are equally vulnerable.

***4/ What are the fixes and solution for meltdown and spectre vulnerabilities?***

***Ans:*** To stay safe from meltdown and spectre vulnerabilities it is important to update all system including operating system, CPU firmware and web pronto. It is suggested that the cost of mitigation can reduced by using processors which feature translation lookaside buffer (TLB) flushing. Meltdown can also be fixed by building a stronger wall around the kernel but the kernel will not be able to operate at full capacity. This fix can also reduce the performance of intel chips by 5 to 30 percent. For Android phone, the security update named ‘Mitigation’ should be enabled. For iOS , the software update should be of the latest version to prevent vulnerabilities. In case of windows pc , the windows should be updated and the security update should be of the latest version. For web browsers, the site isolation feature should be used until the mitigation feature is updated to prevent web based attacks. Spectre, on the other hand, is not likely to be fully fixed any time soon. The fact is that the practice that leads to this attack being possible is so hard-wired into processors that the researchers couldn’t find any way to totally avoid it.