Mehzabin, Raiya

ID: 15-29498-2

Advanced Operating System

**Assignment**:

Meltdown and Spectre are found in almost all the CPU’s that are used in modern device. This includes Mobile Phones, Laptops, Desktop computers, Cloud Services and IOT devices which are all vulnerable. In the first days of 2018, a published research revealed that in the last 20 years nearly every computer chip that was manufactured contains fundamental security flaws, with specific variations on those flaws dubbed as Spectre and Meltdown.

As for known information that when and where does this occurs, these flaws arise from feature built into chips that help them run faster and during the available software patches. It is suspected that may also have impacts on the system performance.

**Meltdown**:

Central security is needed in today’s operating system and it’s one of the features is Memory Isolation. This memory isolation of operating system ensures that user applications cannot access each other’s memories and prevent user applications from read/write Kernel Memory. In this segment comes the term ‘MELTDOWN’. Meltdown is an attack that clears the path of overcoming memory isolation. It works by providing a simple way for other user’s processor to give access to read the entire Kernel memory of the machine it accessed on. This includes all the physical memory that was mapped in the Kernel region. Though the attack don’t convoy on software’s.

**Spectre**:

Spectre is a security vulnerability. It is a specific bug that is affecting all the excisable chips including in Smartphones, Tablets as well as Computer chips from Intel and AMD. This Spectre allows the hackers an easier way to manipulate apps into leaking sensitive information. Though this bug is expected to be more difficult to patch, it is labeled as less dangerous than Meltdown.