**NAME: RAHMAN ASHIQUR**

**ID:15-30021-2**

**Meltdown and Spectre**

Meltdown and spectre is a hardware vulnerability affecting Intel microprocessors, IBM power processors, and some ARM-based microprocessors. Meltdown and Spectre, that are found in almost all CPUs used in modern devices. Mobile phones, laptops, desktop computers, cloud services. These hardware vulnerabilities allow programs to steal data which is currently processed on the computer.

**How do they work**

Meltdown and spectre  exploit a bug in a behavior known as speculative execution. Speculative execution is when the CPU guesses what code path will execute before knowing what the correct code to executes. Meltdown can be partially patched by providing full kernel isolation. Most OSes map themselves into the application’s address space for speed. Meltdown can be used as part of Spectre and not all attacks are against the kernel.  As a result patches for various types of Meltdown and Spectre attacks may appear over a long period of time. Arguably, both exploit fundamental attributes of the computer architecture and cannot be fully patched.

**How to protect it**

* Have to update operating system
* Check for firmware updates
* Have to update browser
* Update other software
* Keep antivirus active