## Name:bhuiya,md ullash id:16-31109-1

## What is Meltdown and Spectre:

## Spectre is a vulnerability that attacks microprocessors. It attacks all modern microprocessors. Meltdown is a hardware vulnerability affect intel x86 microprocessors, IBM power processors, some arm base processors. Those allows to access memory in the state of unauthorized to access. Meltdown only allows to read the protected memory, Spectre allows malicious program to read data from other program.

## How they work:

## Meltdown and Spectre attack memory and read personal information. Flaws in processors help to read data from the memory. Flaws caused by speculative execution. Two main memory are cache and ram. Sensitive information holds in ram and cache. Only operating System can read the sensitive information. But when there is meltdown and spectre attack, the sensitive data can be accessed through unauthorized things. Meltdown can read data upto 503 kb/s speed.

## Which platform they attack:

## Meltdown and Spectre can attack computer, mobile device, cloud storage.

## Way of protection:

## We can fix these with the update of operating system and software. We can’t replace the processors to solve this problem. Patches are created to protect the affected system. But these solutions can slow down your computer or any device.

## Speculative execution:

## Speculative execution is the way of identifying which tasks are needed and which task are not needed. Tasks are thrown away which has no need.