**Rafian , Jaber Al**

**14-25564-1**

**Sec -A**

**Meltdown and Spectre**

**What are these ?**

Computers will always have some security issues. In the beginning og this year all the mainstream medias were flooded with news about security issues called Meltdown and Spectre that allow cyber criminals to steal sensitive information from almost any computer, mobile device, or even from the cloud.

**How & when they were discovered ?**

On the first of June, 2017 researcher working for Google’s Project Zero found two major security flaws in modern processors. These flaws allow any program to read sensitive information from memory. Google decided to keep it a secret until vendors had come up with workarounds that would protect us.

**How they work?**

Back in the 1960s, ‘speculative execution’ was invented . Meaning - the processor will guess what the outcome of an instruction will be and execute all the subsequent steps in the background. Whenever computers perform calculations that aren't actually needed, the results are thrown away. This data ends up in an unsecured part of the computer's cache memory, where unauthorized users can access it through a side channel.

**What to do ?**

Patching processors isn’t possible because we can’t change hardware that has already been installed. Instead we have to mitigate it with software updates. There are already patches available for Windows, MacOS and Linux. Updates for iOS are already available and also Google has patches available for Android. Browser’s like Firefox and Chrome are also offering patches to mitigate the risk of websites stealing sensitive information. But these fixes might slow down computer performance.