Name: **Faisal Ahamed**

Id: **15-30352-2**

**Meltdown and Spectre vulnerability**

Google’s Project Zero found two major security flaws in modern processors. The flaws allows any program to read sensitive information from memory.

This bugs are called Meltdown and Spectre.

A processor is responsible for executing all the instructions that our operating system and our programs give it. How fast a processor is, depends on its clock speed. The higher this is, the more work your processor can do per second. So for a while, chip makers were in a fight to keep increasing the clock speed. They however reached a ceiling when they hit the 3-4GHz range. Increasing it further was impossible, so instead chipmakers had to get creative and they came up something called “speculative” execution.

Basically it means that the processor will guess what the outcome of an instruction will be and execute all the subsequent steps in the background.

The last thing we need to understand is memory.

Our devices have two types of memory: the main system memory, also called RAM and the cache memory in the processor.

The CPU needs to constantly read and write data from the main memory. However the main memory is way slower then the CPU.

So chipmakers added a small cache on the processor itself to store the data that it’s working with.

Every time the processor needs something from the main memory, it copies it, stores it in its cache and reads it from there.

**Meltdown**

Our operating systems stores sensitive information in the main memory of our devices.

Think about our Wi-Fi key for instance.

They store this data in protected memory and CPU’s make sure that no one has access to this part of the memory, except the operating system itself. Except that they don’t enforce this rule when they are speculating!

And that leaves the door open for exploits!

Let’s assume that you visit a website that wants to steal your WiFi password, which for now is safely stored in protected memory.

First the attacking website has to make sure that your CPU’s cache doesn’t contain your actually WiFi password. To do that it reads and writes some random data to the main memory. Remember: when you access the main memory, the processor keeps a copy of the data in it’s own cache for faster retrieval.It also loads an image from the internet that will be used later on. Now that your CPU’s cache is filled with random data, the website tries to read the first letter of your Wi-Fi password from the protected memory with code that might look like this. If your password starts with the letter S,the site reads the first pixel of the image into memory.

But the CPU will prevent the website from accessing the protected memory!

But because the CPU speculates, it might have executed this code in the background and didn’t tell us about it.

If your Wi-Fi password indeed starts with the letter S, the CPU will execute our “readPixel” command while it’s speculating. And when the CPU reads this pixel from the main memory, it puts a copy of it in its cache.

All the website has to do now is run a second program that times how long it takes to read hat pixel.

If it happens super fast we know that the pixel was in the CPU’s cache and this could

have only happened when the CPU was speculating and only if our password starts with the letter S. If it’s not so fast, the data comes from the main memory and then we know the password doesn’t start with an S. It’s clear how this technique can be extended to not only read the first character, but to read your full password from protected memory.

In fact, with Meltdown it’s possible to read sensitive data at speeds of up to half a megabyte per second! (503 KB/s).

Almost all Intel processors and a handful of ARM processors are susceptible to this bug. Only AMD chips are resilient because they don’t speculate when protected memory is being accessed.

**Spectre**

Let’s move on to Spectre, a weakness that is very similar to Meltdown but affects all modern CPU’s, not just the ones from Intel! While Meltdown only allows programs to read protected memory, Spectre allows malicious programs to read the memory from any other program running on your system!

To give a concrete example: a website could use Spectre to read the contents of another browser tab - one where you might be logged in to your bank account. This becomes an even bigger problem in professional situations.

Public clouds like AWS, Google Cloud and Microsoft Azure are rushing to implement safeguards against Spectre and Meltdown.

If left unpatched it would allow one customer’s virtual machine to steal data from another customers VM.

Spectre is more difficult to patch compared to Meltdown and that’s also why they named it “Spectre”.

Now that we know how the exploits work, what can we do about them?

Patching processors isn’t possible because we can’t change hardware that has already shipped. Instead we have to mitigate it with software updates. There are already patches available for Windows, MacOS and Linux, so make sure that you have the latest versions installed. Mobile devices also need to be patched. Updates for iOS are already available and also Google has patches available for Android,

However they depend on the manufactures to make the updates available to users.

And finally: we need to make sure that the rest of your software is up-to-date as well.

Browser’s like Firefox and Chrome are also offering patches to mitigate the risk of websites stealing sensitive information.