Meltdown and Spectre

Meltdown and Spectre are the names of fundamental underlying vulnerability of all the computer chip manufactured in the last 20 years. These vulnerabilities were discovered in late 2017 and were publicized in early 2018. There are three variants of this vulnerability. Each of them has its own CVE (Common Vulnerabilities and Exposures) number. two of these variant are known as Spectre and the third one is known as Meltdown.

How it works?

Our devices has two types of memory: the main system memory which is RAM and the cache memory of the processor. The CPU read and write data from the memory. Everytime the processor needs something from the memory, it copies and stores it in the cache and reads it from there.

Our OS stores sensitive information in the main memory eg. WiFi password. It stores this data in the protected memory and CPU make sure no one has its access except the OS itself. But this rule does not work when they are speculating! And this leaves the door for exploits. If some website want to steal the WIFI password first it fills the cache memory with random data and also loads and image from the internet. Now the website tries to read the first letter of the WiFi password from the protected memory with code that might look like this:

if ( readMemory (172458 ) == "A" ) {

readPixel ( 1 )

}

If the password starts with the letter 'A' the site reads the first pixel of the image into memory. We know the OS does not allow the website to read the protected memory. But as the CPU speculates it might have been executed the code in the background and did not notify the user at all! When the CPU reads this pixel from the maim memory it puts a copy of it in its cache. And now the website just has to run a a second program that times how long it take to read the pixel. If this happens fast the attacker knows that the pixel was in the CPU's cache and this could only happen when the CPU was speculating and the password starts with the letter 'A'. If it is not fast then the data comes from the main memory and the attacker knows that the password does not start with the letter 'A'.

This technique can be extended to retrieve the password from the protected memory! Meltdown can read sensitive data at speeds of up to 503KB/s. Almost all the Intel and a handful ARM processors are vulnerable to this bug. But AMD chips are not vulnerable to this bug because they do not speculate when protected memory is being accessed.

Spectre is very similar to Meltdown but it affects all modern CPU's not just from Intel of ARM! Spectre allows malicious programs to read the memory from any other program running on the system. An example would be the attacker could use Spectre to read the content of a browser tab - where the user might be logged into his bank account.

How to prevent?

1. Updgrade Windows 7/8 to Windows 10. Windows 10 has better security all along than its predecessors!
2. Update hardware. Modern CPU's eg. 2016-era Skylake, Kabylake or newer CPU performs better than older CPU's.
3. Have OS security updates installed.