Meltdown and Specter

**What is it?**

Specter and Meltdown are security bugs that take advantage of a hardware vulnerability that has been recently discovered in all major CPU architectures. The fact that it is a hardware level vulnerability makes this extremely dangerous irrespective of which operating system the system is running. These vulnerabilities have been found in the processors of PCs, laptops, mobile phones and even cloud based systems. This security issue allows hackers to steal sensitive information from the cache memory of a CPU by running malicious processes inside a system.

**How they work?**

Modern CPUs use speculative execution and caching to make execution much faster. In speculative execution the processor basically tries to predict which type of process will come next and executes it beforehand so that it can give an output faster. If a different process is requested, then the data is dumped into the cache memory of the CPU. To understand this, imagine a customer goes to a grocery store every Friday and orders the same products. The store owner can make a prediction based on this and prepare the products beforehand so that the store owner can instantly serve the customer as soon as he arrives. If the customer decides to one-day order a different set of products, then the store owner dumps the products that was prepared earlier in a store house and prepares the new products.

The CPU acts like our store owner in the example above. The data that the CPU dumps in its cache was previously thought of as secure and unreachable from outside. But now we know that the data inside the CPU cache can be accessed indirectly. The data inside CPU cache is protected data and processes which does not have permission can’t access it. Every time a process tries to access the data, the OS does a privilege check to see if the process has the privileges to access that data. If the data is in the cache, then the request by the process will be rejected faster than if the data is not in the cache. This allows malicious processes to identify the memory addresses of the cached data and use side-channel attacks to deduce what the data is. Specter and meltdown exploits this vulnerability to steal sensitive data from a system.

**Which platforms they can be infect?**

The hardware vulnerability that specter and meltdown exploits is present in almost every CPU manufactured in the last 20 years. The use of speculative execution and caching in built into all modern CPUs to provide faster speeds. Because of this, expert have said that this vulnerability is catastrophic as it allows almost any modern computing device from cloud based systems all way down to our smartphones to become infected. A simple JavaScript run on a web browser can take advantage of this security issue to steal usernames and passwords from a system. Even if applications use good code to build secure applications the fact that this is a hardware level vulnerability specter and meltdown can be used to steal secure applications data as well

**How to prevent infections?**

As the issue lies at the hardware level it can’t be completely fixed using software patches. Still various companies are trying to atleast reduce the risks using software patches. As JavaScript in the web browser pose significant risks, all the web browsers are getting patched to address this issue. Operating systems are also getting patched but there have been reports that these patches are making processors slow down to a certain extent. The only way to comprehensively address this issue is by changing the architecture of the CPUs and all the manufacturers have announced that their future CPUs will address this vulnerability.

For average customers there are certain precautions that they can to reduce the risk of infection. Some of them are listed below.

1. Make sure the devices have the latest OS updates.
2. Make sure all the applications are updated to their latest versions.
3. Make sure anti virus software is upto date.
4. Never click on links that are suspicious.
5. Never open email or visit websites that are not trusted.
6. Store sensitive data in an external hardrive and not the cloud as the cloud systems that use the processors are vulnerable to attack.

Submitted by  
Name-Akibur Rahman Akib  
Id- 15-30437-3