The CYBER GURU

Vong Sopha
Cybersecurity
Analyst

By now, you've probably heard about the latest vulnerabilities that impact modern processors. Meltdown and Spectre are the names given to these vulnerabilities, which affect nearly all computer processors manufactured roughly in the last 20 years. The flaw comes from a feature that is built into the processor chip itself that, if exploited, would allow the hacker to read data from protected areas in the memory such as passwords and encryption keys. For this article, I will give an overview of the Spectre vulnerability and a brief explanation on how attackers can retrieve sensitive data from protected memory.

To understand how data is retrieved from protected memory, we will need to know how modern processors use two techniques to speed up the time it takes data to travel back and forth, from the memory to the processor. These important techniques used to speed up your computer chip are called *speculative execution* and *caching*.

Central processing unit (CPU) caching is a technique used to speed up the time it would take for your processor to access memory. Since it takes a long time for the processor to retrieve data from random-access memory (RAM), there is a feature where a very small amount of space on the processor can store data that it will need soon or often. And since this small space lives on the processor chip itself, the data is retrievable much faster.

Speculative execution in essence implicates a processor chip attempting to guess or predict an outcome in order to work faster. If the chip knows that a certain program is associated with a logical branch, it will start working out the formula prior to getting all information from memory. For example, if B is true, then compute function X; if B is false, then compute function Y. The chip can start computing both functions X and Y before it even knows if B is true or false. The reason behind this is, since it already has both formulas on hand, the chip already has a head start and speeds up the overall processing time.

The issue at hand is when the CPU is required to retrieve data from protected memory (passwords, encryption key) into the CPU cache. The attacker can potentially compute if the protected memory data is stored in RAM or CPU cache by viewing the response time it takes to retrieve the data. If certain data is retrieved more quickly that the rest, that means the data is stored on the CPU cache. Just knowing where data is stored within the processor can allow an attacker to view the content of the data, including passwords. This is known as a *side-channel attack*.

Since the fundamental vulnerability exists in the hardware, which runs beneath the software we use every day, it cannot be patched. However, vendors are releasing software patches that work around this issue at the operating-system level.