Late in 2017 researchers in academia and Google independently confirmed critical vulnerabilities in the design of computer chips that could expose protected data. These vulnerabilities not only impact personal computers but mobile devices, cloud servers, and even IoT (Internet of Things) devices.

There are two distinct type of flaws, named Spectre and Meltdown. There are two variations of Spectre and one of Meltdown and though they take different approaches to accessing protected data they both exploit the same design issues of central processing units (CPUs) have features that optimizes their performance and makes their response time faster.

The CPU, also known simply as the processor, is the heart and brains of a computer. It receives data, executes instructions and processes information. To perform these tasks the processor needs access to memory. When the computer opens an application, information about that application is stored in what is called random access memory (RAM). Accessing this memory, in computer terms, is relatively slow and if the CPU relied only on RAM for running a program computers would seem sluggish and at times unresponsive.

To address this issue, processors are designed with their own memory. A small set of data holding areas on the CPU, known as registers, store special operating instructions. A separate area of the CPU, cache memory, is used to store instructions and data that are used repeatedly in the operation of a computer program. It is cached memory, in combination with a technique chip designers developed called speculative execution that present the opportunity for protected data to be accessed.

Speculative execution is a way for the CPU to access data before it actually knows it will need that data. For example, if a computer program has the following code - if A is true, run function X or if A is false, run function Y, the CPU would start executing both functions before it knows the value of A. As information from both functions is collected it is stored in cache memory. Once it knows if A is true or false it has already started on the proper function giving the process a speed boost.

The security flaw comes into play when cache memory and speculative execution start working with protected memory. In order to access data on a computer, a process needs to have permission. This is an essential of computer security, it prevents the operating system from exposing data in one program to another or preventing users from accessing data not intended for them. In order to determine if the data can be accessed the CPU runs what is called a privilege check. But a privilege check can take a long time to run, and so, using speculative execution, the CPU begins to work with the data before permission to do so has been granted. The protected data is now stored in cache memory.

By exploiting these processes both Spectre and Meltdown can gain access to protected data but they do so from different approaches. Meltdown uses a program hosted on a machine to retrieve data from all over that machine. Think of a cloud server that hosts data from multiple

corporations. By being able to bypass the security processes for protected data, the information from any or all of them could be accessed. Spectre works differently in that it could be used to make a program expose data that should not be exposed, like usernames and passwords. Spectre does not access data from other programs.

We live in an increasingly connected world that is placing a higher demand on computing speed than ever before. The lesson learned from these security flaws is that, given our knowledge of current technology, you cannot have both, speed and security. One has to be sacrificed for the other. The hardware manufacturers and cloud service providers have released patches to address both Spectre and Meltdown by altering or disabling the speculative execution and caching capabilities of their CPUs. But since those features were designed to improve computing performance, inevitably, a reduction in speed will occur.