Abu Mohd Rifat Tariq

ID:15-29482-1

Meltdown and Spectre takes advantage of critical vulnerabilities in modern processors. These hardware exposures allow programs to steal data which is currently processed on the computer. While programs are typically not permitted to read data from other programs, a malicious program can exploit Meltdown and Spectre to get hold of secrets stored in the memory of other running programs. This might include your passwords stored in a password manager or browser, your personal photos, emails, instant messages and even business-critical documents. Meltdown affects a wide variety of systems, which includes almost all running devices which do not run the latest versions of some Operating Systems.

Spectre and Meltdown exploit the same flaw in the hardware but they use different routes to gather the information. What happens in both cases is that the processor is made to execute instructions it should never execute as part of its speculative execution hardware. Once the processor discovers that it shouldn't have carried out the instructions it removes all trace that the instructions were ever carried out - except of course it forgets to reset the cache back to its original state. It doesn't cache the data that should never have been accessed, but if that data is used to access some other data used as an address then that data is still in the cache. To find the data that is in the cache just needs a comparison of access times to reveal which of a possible set of data has been accessed. Which data have been cached gives you the value of the restricted data that you should never have had access to.