Neer,Muktasid Islam

14-26746-2

Meltdown and Spectre are two security issues that allows cyber criminals to steal sensitive information from almost any computer, mobile device or even from the cloud. A process called speculative execution lets devices do some work ahead of time to speed up routine tasks. Researcher working for Google’s project zero found those two major security flaws in modern processors. Almost all intel processors and some ARM processors are susceptible to Meltdown bug. Spectre is more dangerous than Meltdown. While Meltdown only allows program to read protected memory, Spectre allows malicious programs to read the memory from any other program running on a system. Such as, a website could use Spectre to read the contents of another browser tab – one where a person might be logged into his bank account. Spectre is more difficult to patch compared to Meltdown and that’s also why they named it Spectre. A ghost that will haunt us for some time.