Omar Salih

As recently discovered, processors created by Intel since 1995 except for Intel Itanium and Intel Atom before 2013, are subject to malware Meltdown and Spectre. This discovery shows how our stringent use of antivirus software, malware scanning, being aware of clicking on suspicious links and practicing extra-carefulness of not creating any communication with sources we are not 100% confident of their identity or intentions, can still be circumvented to access core system trusted files that are traditionally secured from communicating with applications not natively installed. As of currently, only Intel chipsets have been having verified, it is not known if Meltdown will affect an ARM or AMD processors. However, almost every system is affected by Spectre. That includes desktops, laptops, cloud servers and even smartphones. This hardware flaw practically means all computing machines in existence are basically subject to security meltdowns and speculative executions caused by Meltdown and Spectre.

Computer programs are not all made equal, and all don’t deserve the same level of trust, especially the difference between programs that make up the devices operating system and applications that are installed by the system user. Modern hardware, solely trusts and allows, specialized programs that are necessary to keep the device working, to access core system files. When users start installing other applications, those programs are run in isolation, separate from the core system files. This is done by hardware makers, so that non-system applications won’t be able to break one another. Data is shared only through using trusted services and gaining their permissions, which Malware Spectre does.

Intel, which essentially owns the server market, the biggest vulnerability is on cloud service customers like Amazon, Google, and Microsoft. The issue here is that if a joint virtual machine tenant wants to be malicious, theoretically that tenant may invade another peoples space. Defense-wise, this is a problem, because it can be weaponized, leading to security breaches, intellectual property loss, architectural integrity attacks, identity theft, financial theft, as well as leading to an infinite possibility of felonious criminal acts.

**RESOURCES**

Greenberg, Andy (2018, January 07). Triple Meltdown: How so many researchers found a 20-year-old-chip flaw at the same time. https://www.wired.com/story/meltdown-spectre-bug-collision-intel-chip-flaw-discovery/