Name: Rahman, Tauhidur

ID: 14-27132-2

Meltdown and Spectre allow attackers to get access to data previously considered completely protected. Meltdown exploits caching and speculative execution to allow programs to read information that should only be accessible to the operating system. Spectre allows programs to read data from each other’s memory when both programs are running on a single processor. This is a problem for systems with multiple users on one machine but can also be an issue for single user systems.

Meltdown works by running an attack program that reads privileged data from kernel address space – the data that should only be accessible to the operating system.

Spectre works by tricking a victim program into reading data it wouldn’t normally access and leaking data to a second attack program running on the same machine.

Meltdown is simpler to implement but can be prevented by the KAISER patch. Spectre is CPU specific, much harder to implement, but currently has no patch. The attacks are not easy to implement, but they are also hard to protect against and leave no trace. Both vulnerabilities are hardware level vulnerabilities that exist because of a flaw in CPU architecture. They are very serious vulnerabilities because they are operating system and software independent. The long-term fix for both issues will require that CPU makers change the way their chips work, which means redesigning and releasing new chips.