**Spectre and Meltdown:**

Spectre and Meltdown are the names given to a trio of variations on a vulnerability that affects nearly every computer chip manufactured in the last 20 years. The flaws are so fundamental and widespread that security researchers are calling them catastrophic.

**Working Method:**

**Meltdown:**

Meltdown breaks the most fundamental isolation between user applications and the operating system. This attack allows a program to access the memory, and thus also the secrets, of other programs and the operating system.

**Spectre:**

Spectre breaks the isolation between different applications. It allows an attacker to trick error-free programs, which follow best practices, into leaking their secrets. In fact, the safety checks of said best practices increase the attack surface and may make applications more susceptible to Spectre.

**Affects:**

The Meltdown vulnerability primarily affects Intel microprocessors, but some ARM microprocessors are also affected.The vulnerability does not affect AMD microprocessors. Intel has countered that the flaws affect all processors,but AMD has denied this, saying "we believe AMD processors are not susceptible due to our use of privilege level protections within paging architecture"

Researchers have indicated that the Meltdown vulnerability is exclusive to Intel processors, while the Spectre vulnerability can possibly affect some Intel, AMD, and ARM processors. However, ARM announced that some of their processors were vulnerable to Meltdown. Google has reported that any Intel processor since 1995 with out-of-order execution is potentially vulnerable to the Meltdown vulnerability (this excludes Itanium and pre-2013 Intel Atom CPUs). Intel introduced speculative execution to their processors with Intel's P6 family microarchitecture with the Pentium Pro IA-32 microprocessor in 1995.