Spectre and Meltdown attacks

Meltdown and Spectre are two exploits of computer systems, that are both relatively recent in their discovery, and similar in their potential to cause damage and concern. These exploits make use of vulnerabilities found in modern processors and allow malicious programs to harvest data while it is being processed by the machine; data that the program in question should otherwise be unable to access. The nature of this vulnerability means that any data that gets processed by an effected processor can be maliciously accessed: including passwords, documents, bank details; any data that is being processed can be stolen.  
Meltdown and Spectre were both first reported January 2018 by three teams (Google Project Zero, Cyberus Technology and Graz University of Technology) (Anon. , 2020). Since their discovery, the extent and scope of the vulnerabilities has been shown to cover a vast portion of most modern processors.

“Spectre and Meltdown individually represent classes of hardware vulnerabilities, each with a number of variants dependent on specific silicon-level functionality.” (Fruhlinger 2018) Whilst full of jargon, the meaning of this sentence is simple. Both Spectre and Meltdown are two techniques that can be used to exploit vulnerabilities in the most basic systems in a computer. They do however, work differently.   
Meltdown is the simplest to understand, and perhaps counterintuitively, arguably harder to implement. In short, Meltdown is a vulnerability that allows a process to read the entire memory of a given system (Fruhlinger 2018). The way in which it does this takes advantage of an otherwise beneficial aspect of modern processor architecture; speculative execution. In essence, the CPU executes code in parallel, even including code that might never be used (Anon. 2020).

References

ANON., 2020. *Meltdown and Spectre* [viewed 7 May 2020]. Available from: <https://meltdownattack.com/>

FRUHLINGER, J., 2018. *Spectre and Meltdown explained: What they are, how they work, what’s at risk* [viewed 8 May 2020]. Available from: <https://www.csoonline.com/article/3247868/spectre-and-meltdown-explained-what-they-are-how-they-work-whats-at-risk.html>

ANON., 2020. *How Meltdown Works* [viewed 8 May 2020]. Available from: <https://www.i-programmer.info/news/149-security/11437-how-meltdown-works.html>