week 5 (task 2)

Spectre and meltdown are two original side channel attacks discovered in 2017 that target cpu. I will focus three other attacks what have founded. And how they are used. I will focus Foreshadow, MMIO and Microarchitectural.

Foreshadow is known as L1 Terminal fault by Intel. Is very intresting because it was vulnerability what affects modern microprocessors. It was founded by two independent team january 2018 and it was disclosed in august 2018. According to wikipedia it is a speculative execution attack on Intel processors that may result in the disclosure of sensitive information stored in personal computers and third-party clouds. Foreshadow is many similarities with Spectre security vulnerabilities discovered earlier to affect Intel and AMD chips. Foreshadow may be very difficult to exploit. Companies performing cloud computing may see a significant decrease in their overall computing power; people should not likely see any performance impact, according to researchers

https://en.wikipedia.org/wiki/Foreshadow

MMIO as Memory-mapped I/O and port-mapped I/O are two complementary methods of performing input/ output between the central processing unit (CPU). Peripheral devices in computer. An alternative approach is using dedicated I/O processors. Commonly known as channels on mainframe computers. It was found in 2022. I/O operations can slow memory access if the address and data buses are shared. Memory-Mapped I/O (MMIO) allows the CPU to communicate with peripheral devices through regular memory addresses, simplifying hardware design. However, in the MMIO Stale Data vulnerability, this mechanism becomes exploitable when internal CPU buffers are not properly cleared.

https://en.wikipedia.org/wiki/Memory-mapped_I/O_and_port-mapped_I/O

Microarchitectural data sampling vulnerabilities are a set of weakness in Intel 86x microprocessor that use hyper-threanding. Leak data across protection boundaries that are architectually supposed to be secure. According to magazine wired it was found 2018. Intel reaserchers discovered the vulnerabilities in 2018. Intel processors dating back to 2011 or 2008 are affected. Fixes may be associated with performance drop. Intel reported that processors manufactured in the month before the disclosure have mitigations against the attacks. It was vulnerability low-medium.

https://en.wikipedia.org/wiki/Microarchitectural_Data_Sampling