Hardware Vulnerabilities

November 2020

1 Introduction

Hardware vulnerability is a weakness in computer hardware caused due to flaw in procedures, design or implementation. It may lead loss or theft of data stored in hardware. It may lead to wrong execution of process, giving undesired results.

2 Three Hardware Vulnerabilities

2.1 Row Hammer Attack

In dynamic random access memory (DRAM), each bit is stored in the form of charge in memory cell which contains one capacitor and one transistor. These cells are arranged in a matrix and addressed using rows and columns. When computer needs to read a particular cell, whole row containing the cell is copied into the row buffer then the cell is accessed using column address. Then the cells are rewritten into the row[3].

Modern DRAM come with very high cell density and smaller memory cells which store smaller charges. Thus, in the presence of high disturbance the possibility of leakage of charges stored in adjacent cells increases[3].

Row hammer attack exploits this vulnerability to change the content stored in DRAM within refresh interval. It affects mainly DDR3 and DDR4 SDRAM. It does this by repeated, rapid activation of a particular cell which leads to voltage fluctuations in the row selection lines. Thus, leading to disturbance errors in adjacent rows (victim rows)[3].

2.2 Speculative execution vulnerabilities

To increase the speed of execution the processors do a process called speculative execution. It is the process where the chip predicts a set of possible operations that will be performed in the future. It performs those operations and stores it in the cache for very high-speed delivery of information[4].

In the processors made by Intel and ARM prior to 2018 the speculative execution fetches and performs the operations even on private memory without privilege test being completed. The results are store the results in the cache[4].

Spectre is a class of attack where it exploits this fact to gain access to memory of other running programs. Spectre works by directing the speculative execution into wrong path and stealing the data that was accessed by speculative execution and stored in cache[5, 1].

2.3 Reminiscence of memory in RAM

When the RAM is disconnected from the motherboard the memory stored in the RAM may persist for an appreciable amount of time (seconds to minutes). Furthermore, the time for which the memory will remain can be predicted by knowing the DRAM specifications and the physical variables (high density RAM tend to lose data quicker). The researchers mention that at -50 C with air cooling the decay was only 1% in 10min[2].

So, the data in DRAM can be stolen by the attacker if he/she has physical access to the it. The attack methods have mainly three variants viz., First, to reboot the computer and launch a custom kernel with a small memory footprint. Second, Attacker can cut the power off briefly then restore power and boots a custom kernel (this method does not give the OS to scrub memory). Third, Attacker can transplant the DRAM into PC which does not clear the memory on boot[2].

3 Conclusion

We observe that the vulnerability can be caused by various reasons like implementation, physics involved in the working of the hardware etc. Some vulnerabilities are due to optimisation over size and speed. They provide an opportunity of study and urges to redefine and understand the concepts in depth.

References

[1] intel newsroom. Understanding spectre and meltdown.

[2] Princeton University. Lest we remember: Cold boot attacks on encryption keys.

[3] Wikipedia. Row hammer.

[4] Wikipedia. Speculative execution.

[5] Google Project Zero. Spectre attacks: Exploiting speculative execution.