Meltdown and Spectre

Began Bajrami, Rahmi El Mechri

June 25, 2022

Abstract

1 Introdutcion

2 Introduction

3 Out of Order Execution

Out of order is a technique used by many CPUs nowadays the main reason being the improvements on perfomance that it brings, allowing CPU to decide what to execute first and what after. To make it possible, different techniques where developed.

3.1 Reservation Station

> In 1967, Tomasulo [33] developed an algorithm [33] that enabled dynamic scheduling of instructions to al- low out-of-order execution.

Tomasulo developed a way to allow instructions that operate on the same physical registers to rename registers and use the last logical one to solve read-after-write (True data dependeny, or RAW), write-after-read (Antidependency, or WAR) and write-after-write (WAW) hazards: the Reservation Station. In other words, this lets the CPU use data values as soon as they are computed instead of reading value from a register, writing the result on the register and then again reading it. The Reservation unit connects all execution units via a common data bus (CDB), where operands of instructions are passed so.

4 Meltdown

5 Spectre

6 Exploits

7 Impact

8 Mitigations

9 Conclusion