# Meltdown & Spectre

André Sintzoff

10 february 2018

## Meltdown & Spectre

### Introduction

Begin of January 2018, a new family of flaws has been publicly announced.

The main difference between the previous ones is these new vulnerabilities are not due to software flaws but to hardware ones.

### Vocabulary/Context

On a device (like a computer, a smartphone), there are several components. The ones of interest to describe these hardware flaws are:

- processor (performing the operations like arithmetic ones, conditional ones, memory accesses)
- main memory (RAM)
- cache memory

On fast processors, main memory is very slow compared to the processor. Therefore, cache memory is added to speed up accesses.

On such processors, some other specific tricks are used to optimize the performance.

On less powerful processors, each operation is done sequentially meaning that the processor performs one operation at the time. Therefore if an operation takes a long time (for instance to access memory), the processor is idle. This is called **in-order execution**.

To improve the use of the processor, it can also perform next operations before the previous ones are finished. This is possible if these operations are independent. This is called **out-of-order execution**.

Similarly, when the processor has to take a decision, its result can take some time to be obtained due to memory access. In this case, the processor bets

on the next instructions to be executed. Depending on the decision result, the executed instructions are necessary or not.

Unfortunately, it is possible to observe some effects of these instructions. This is called **speculative execution**.

## Meltdown

The Meltdown attack exploits a race condition between the memory access and the permission verification. This can occur due to out-of-order execution. From a user point of view, the memory is not accessed but there is some information remaining in the cache memory. This information is used later on to retrieve the data which should not be accessible to the attacker.

## Spectre

In the Spectre attack, the processor executes in advance code which is unnecessary using speculative execution. From the user point of view, the effect is similar to Meltdown.

## Impacts

The attacks are ways to read unauthorized data. In the coming months, several variants will be likely to appear.

Why are these attacks embarrassing? Because such attacks are due to hardware flaws and because one cannot ask to replace millions of affected processors.

For existing products, one needs to find software mitigations.

For future products, the design of the processors needs to take more into consideration security aspects. Unfortunately, such aspects were not considered as essential for processor developers. Until now, the performance and the power consumption were the two main improvement domains in processor design.

## Mitigations

Regarding Meltdown, there is already a software correction mitigating most of the effect of the attack.

For Spectre, the corrections are for the moment only partial ones.

## Are you affected?

Surely as most processors used in desktops, laptops, and servers are affected. What is the risk? As the attacker needs to run code on the attacked device, an access to this machine is required. This access can be legit or malicious. Nevertheless, you are giving access to your machine when you browse a website with Javascript enabled. This is the reason why web browsers have been updated recently.

## Existing products

Products like smart cards, Raspberry Pi are not affected as all of them are based on what we could called low powerful processors.

Software based products running powerful processors are likely affected but the exploitation depends on the situation.

## Conclusion

This is only the begin of the story as now the spotlights are focused on the vulnerabilities in computer hardware. In future, more vulnerabilities of this type will surface.

Storing and manipulating secrets (keys, sensitive data...) on the same piece of hardware as the one running untrusted software is not a good idea. On your side, as usual, take care of the software having access to your device and always apply security updates.