Task 1: Side-channels

Task 1:

CPU attacks such as Metdown or Spectre, choose an example of a side-channel attack and explain the following information about.

I will answer these five questions:

Brief explanation of what side-channel the attack uses and how? What systems does it affect? What information is leaked via the side channel? Is there a documented case of it being used ina real life attack? Has it been fixed? If yes, how it was fixed?

Brief explanation of what side-channel the attack uses and how? Side-channel the attack uses information leaks accidentally via some medium. Side-channel attacks are everywhere. They are very vulnerability and cost are usually a lot. According to Ross Anderson they are important things to understand. Usually they are very bad because side-channel attacks are difficult to notice.

What systems does it affect? They are usually in the hardwire systems like economics of electromagnetism, timing attack and power consumption and acoustic emissions. Like access to sensitive information. (wikipedia)

What information is leaked via the side channel? According to wikipedia there are many things that side channel could leaked many things. In all cases could leaked informations are things like a extra information about secrets in the systems and cryptocgraphic key and partial plaintext.

Is there a documented case of it being used in a real life attack? Yes there are a many cases. Famous are metdown and spectre what happened in 2018. They are famous ones. Both of them used CPU and memory reads. Meltdown creates a race condition between memory access and privilege checking. Spectre could the target process into revealing.

According to Ross Anderson these cases are famous ones. They have fixed. Meltdown and spectre have made more updated. They are both fixed better way. But according to Ross Anderson he said that it is difficult to fixing everything. It takes time. Structure of architecture is so complex nowadays that there is always backdoor.

Notes:

Anderson Ross: Cybersecure engineering (3th edtion 2020)

https://en.wikipedia.org/wiki/Side-channel_attack (read 1.10.2025)