Week 5 task 2

- one side channel attack that is similar to spectre and meltdown is ZombieLoad. It is categorized as a Microarchitectural Data Sampling (MDS) attack. This attack works only on intel cpus and for example AMD chips are immune to them. The attack targets a specific component in intel chips. the attack works so that it when the processor loads data, it sends multiple load requests even though it only would need to send one. Intel chips try to predict which operation and data is needed next and that's why it send multiple requests.
  These additional requests then cause the data leakage. So for example attackers can steal user-level data, like content of visited websites password etc. Mitigation methods for ZombieLoad are for example security updates for windows, that Microsoft has released, Intels security updates and usage of the right protection softwares. One mitigation is of course to switch to AMD processors :D.

- The fallout attack is an attack that can leak data from store buffers, which are used by the processor's pipeline to hold or store a data. The malicious acter can after pick which data to leak from the buffers. the fallout is also an MDS attack. The attack affects also Intel processors and every generation of them. The mitigations for this attack are almost the same as in the ZombieLoad vulnerability. Using necessary firmwear, Microsoft security patches, switching cpu etc.

- Intel CSME Bug is a vulnerability that affects all Intel processors that could allow attackers to bypass every hardware-enabled security technology. The vulnerability can be exploited by malicious actors to bypass hardware-enabled security technology. The attacker could exploit this vulnerability that allowed to read the chipset key of the processor, which is a key that can grant access to for example a feature in a device. Intel mitigated this vulnerability by updating fixes to the systems hardwares. Also intel made CSME firmware updates to those systems where the hardware couldn't be fixed.