week 4 task 1

Electromagnetic side-channel attack is an attack where unintented electromagnetic emanations from an electronic device are being exploited to gain information. This means that the attacker does not need physical access to the target device. The Electromagnetic side-channel attack works so that it physically measures the EM radiation from an electronic device and uses various models and techniques to steal information from the data.

The attack affects systems that produce EM radiation like computers, smartphones, smart cards etc.

with this attack information of the target machine like what cryptographic algorithm is being used, what software program is running in the target device and what version of firmware the device is hosting.

One documented case is using electromagnetic side channel attack on Apple CoreCrypto. The study in which the attack is done, over half of a gigabyte of data was acquired in under 2 seconds from Iphone 7.

The attacks demonstrated was a study and it wasn't performed by an attacker. But the attack highlights that there is always a need for side channel defenses for real devices and production, industry-standard encryption software.

sources: https://eprint.iacr.org/2022/230, https://www.allaboutcircuits.com/technical-articles/em-side-channel-attacks-on-cryptography/