Week 6 task 1

TPM means a Trusted Platform Module, and it is mainly used to improve the security of computers. TPM is used to create cryptographic keys, which are long and random string of characters that is combined with the data that needs to be encrypted. So TPM uses cryptography to store the critical data in pcs and through that enables secure platform authentication. TPM is either located in a separate chip in your pc or in some processors it is integrated into them. TPM is capable of storing and protecting critical information like credentials, passwords etc

Even though TPM is very widely used it still has incapabilities. For example encryption of specific apps cannot be performed by TPM, it can only provide the cryptographic key and the specific app has to perform the encryption itself. TPM also needs an operating system to work, It cannot work on its own. A service needs to be using TPM in order to work like windows or bitlocker drive encryption.

Virtualization is a technology in cloud computing that enables creation of virtual representations of servers, storage, networks, and other physical machines. With virtualization it is possible to interact with hardware with greater flexibility, meaning that virtualization removes the limitations that physical hardware would bring and allows users to interact with the hardware infrastructure like an application on the web.

Virtualization also has many incapabilities. For example virtualization might have latency and bad performance compared to physical servers. Also virtual TPMS might not provide as good of a security as a physical TPM. Virtualization can also enable new attacks so it can be a security risk. Common security threats and challenges of hardware virtualization include hypervisor attacks, inter-VM attacks, and VM lifecycle attacks.

sources: https://www.intel.com/content/www/us/en/business/enterprise-computers/resources/trusted-platform-module.html, https://aws.amazon.com/what-is/virtualization/, https://www.linkedin.com/advice/0/what-limitations-hardware-virtualization-cloud-computing-tcsmf