Task 1: Secure Running Environment

TPM (Trusted Platform Module):

TPM is a hardware security feature that helps to protect important data like encryption keys. It checks the computer during startup to make sure nothing has been changed without permission. TPM keeps things like passwords and keys safe from hackers. However, it has some limits. Since it is hardware-based, if the hardware is hacked or TPM isn't set up correctly, it can be bypassed. Also, TPM mainly works to protect the system when it starts up but doesn't protect applications or data while they are running.

Containers:

Containers are a method to run applications in small, separate environments with everything they need to work. This makes sure the application can run the same way on different systems. Containers provide some security by keeping applications separate, reducing the risk of attacks. However, they still depend on the main operating system, so if the OS is hacked, the containers are at risk too. Also, if containers are not set up properly, like if they are given too many permissions, they can be exploited. Containers are less secure than virtual machines because they don't have as much isolation from the system.

So, the TPM gives good security for the startup process and important data but doesn't help once the system is running. Containers keep applications separate but can be vulnerable if the operating system or setup is weak.

Sources

Engineering security lectures

IOP Science, https://iopscience.iop.org/article/10.1088/1757-899X/376/1/012117