TPM2

TPM2 (Trusted Platform Module 2) est un module de sécurité matériel conçu pour améliorer la sécurité des systèmes informatiques. Il est conçu pour stocker des clés de cryptage, des signatures numériques et d'autres informations de sécurité de manière sécurisée.

Le TPM2 est intégré dans la carte mère d'un ordinateur et fonctionne comme un coprocesseur de sécurité indépendant du processeur principal. Il peut être utilisé pour protéger le démarrage du système, pour chiffrer des données sensibles, pour authentifier des utilisateurs et pour garantir l'intégrité du système.

Le TPM2 est devenu une norme de l'industrie et est largement utilisé dans les ordinateurs professionnels et les serveurs. Il est également de plus en plus utilisé dans les appareils mobiles et les systèmes embarqués. Le TPM2 est souvent utilisé en conjonction avec d'autres technologies de sécurité telles que Secure Boot, BitLocker et Windows Hello.

Voir :

- https://fedoramagazine.org/automatically-decrypt-your-disk-using-tpm2/