TPM Vulnerabilities

Trusted Platform Module (TPM) is an international standard made by the Trusted Computing Group (TCG) for attain high levels of security in computer. The use of Trusted Platforms is a significant move towards improving confidence in doing online business and broadening the scope of e-services.

Trusted Platform Module (TPM) and its Vulnerabilities

Overview of Trusted Platform Module (TPM)

Trusted Platform Module (TPM) is a small chip which can be integrated into a PC, laptop or any computing device to cater with a safe storage of sensitive data and key generation for remote attestation. The recent laptops today contain millions of small chips having the TPM deployed in them serving as a cheap root of trust upon which the operating system and the application could rely for establishing remote trust. It protects the platform against theft and misuse of the secrets held at the platform.

Most of the TPM reside on the Low Pin Count Bus so that it can easily measure BIOS without accessing the CPU. The TPM is given a pair of RSA keys which are called endorsement keys and is unique for each TPM. It is a public-private key pair playing a pivotal role in remote attestation. It is the core requirement of the Endorsement Key that it is protected and not exposed to any external party. TPM is called trusted due its tamper evident nature (Kallath, 2005). Another important component of the TPM is the Platform Configurations Register. Integrity metrics are measured and authenticated, and then its hash is stored in shielded locations called Platform Configurations Registers (PCR's). Integrity measurement involves finding out the factors affecting the trustworthiness of the platform like software and hardware configurations. Remote attestation and access to sensitive data are allowed upon the matching of current integrity metrics with the values stored in PCRs. TPM provides a protected storage for storing cryptographic keys, certificates and passwords which are only accessible by the TPM. TPM provides high level privacy in a sense that if any sensitive data is successfully accessed by a