Mutual remote attestation in IPSec based VPN

ABSTRACT

Secure communication between computer systems is normally established using secure tunnel technologies such as Internet Protocol Security (IPSec). IPSec protocol guarantees authenticity of communication and secure the data at each gateway but it does not provide any assurance on the entity authentication. So, it is important to make sure the trustworthiness of the remote party that already has a faithful system. Trusted Computing Group (TCG) has introduced a platform to solve this issue into the mainstream computer industry through their main approach called Trusted Platform Module (TPM). TPM is a security module which has been designed to store information of system events securely as well as the key component in the attestation realization. Trusted Computing Platform (TCP) provides a mechanism to supports attestation by its Platform Configuration Registers (PCR) which has become the integrity measurement of a platform. Attestation is a mechanism to provide remote assurance of the state of the hardware component running on a computing device. This paper, proposes an extension to the IPSec key exchange protocol by establishing properties-based attestation. An embedded attestation extension is provided in VPN communication such as IPSec protocol by establishing mutual properties based attestation using Internet Security Association and Key Management Protocol (ISAKMP) measurement value as properties that are computed from security policy database (SPD). Hence, the proposed approach will protect both sender's and receiver's platforms integrity at their respective gateways.

Keyword: IPSec protocol; Trusted Computing Group (TCG); Trusted Platform Module (TPM); Trusted Computing Platform (TCP); Platform Configuration Registers (PCR); Security policy database