Sansar Choinyambuu

Graduate Candidate	Sansar Choinyambuu
Examiner	Prof. Dr. Andreas Steffen
Co-Examiner	Dr. Carolin Latze, Swisscom Innovations, Bern, BE
Master Research Unit	Software and Systems

Platform Trust Service Protocol

PTS binding to TNC IF-M

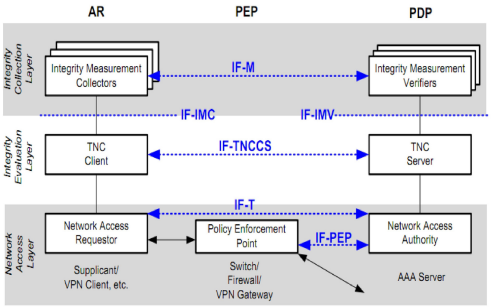

Figure 1: TNC Architecture

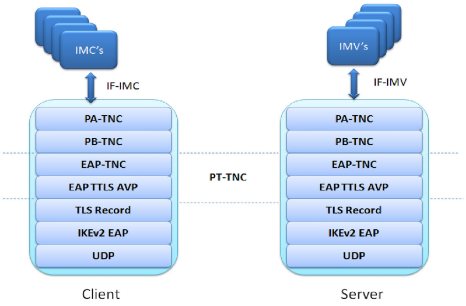

Figure 2: TNC protocol stack within strongSwan

Introduction: Trusted Computing Group (TCG) designed the Trusted Network Connect (TNC) architecture, which standardizes the way to realize a remote assessment on network nodes by auditing the configurations and health state of endpoints and enforcing the corporate security policy before network connectivity is established. The policy can cover the endpoint security requirements ranging from a desired operating system to a certain patch version of the anti- virus software installed. Endpoints should be trusted to report their health state accurately and correctly to the challenger, otherwise the TNC architecture design is confronted by the "lying endpoint problem". Unfortunately, the TNC architecture does not explicitly specify how to detect or prevent the lying endpoint.

Approach/ Technologies: The usage of the TCG- defined Trusted Platform Module (TPM) increases the trust in an endpoint substantially. The TPM serves as a hardware-based root of trust for the integrity measurements and integrity reports describing the health state of the platform, thus this integrity information can be doubtlessly factored into network access control decisions made by the challenger. The binding of TPM usage in TNC architecture is realized with the "TCG Attestation PTS Protocol: Binding to TNC IF-M Version 1.0" specification.

Result: The goal of the present thesis is to implement this PTS protocol as dynamically loadable Attestation Integrity Measurement Collector and Integrity Measurement Verifier within strongSwan: the open source IPSec-based VPN solution. The implementation builds upon existing TNC capabilities of strongSwan. The final deliveries of the thesis are to facilitate remote attestation on the endpoints where the client platform optionally possesses a TPM and where the strongSwan is installed and configured correctly.

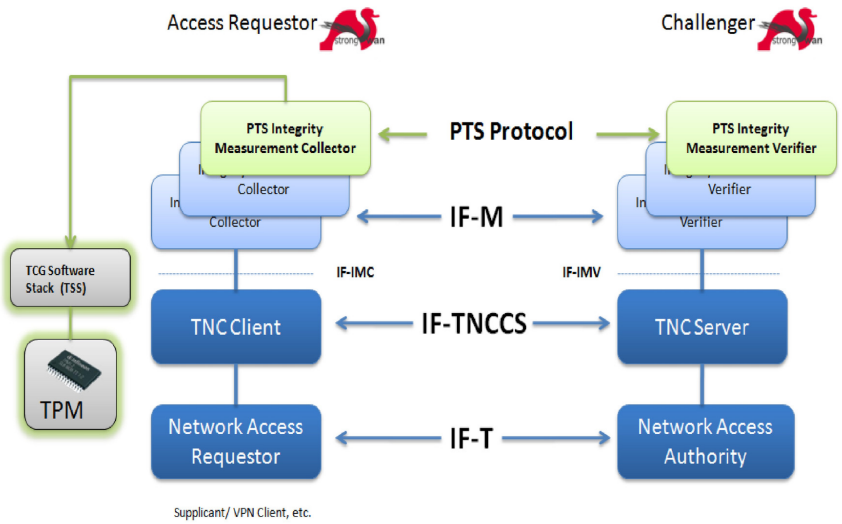

Figure 3: PTS Protocol integration with TNC Architecture in strongSwan