Sansar Choinyambuu

Graduate Candidate	Sansar Choinyambuu
Examiner	Prof. Dr. Andreas Steffen
Co-Examiner	Andreas Steffen
Master Research Unit	Software and Systems

A Posture Broker Protocol Compatible with Trusted Network Connect

Implementation as a strongSwan Plugin

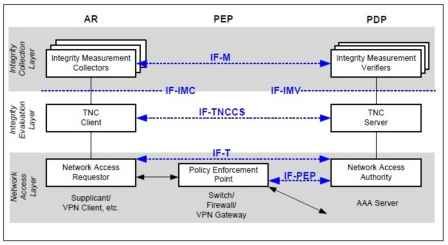

Figure 1: TNC Architecture by Trusted Computing Group

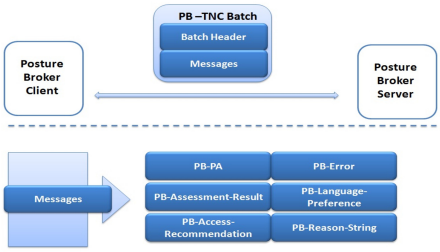

Figure 2: Batch Exchange between PB Server and PB Client

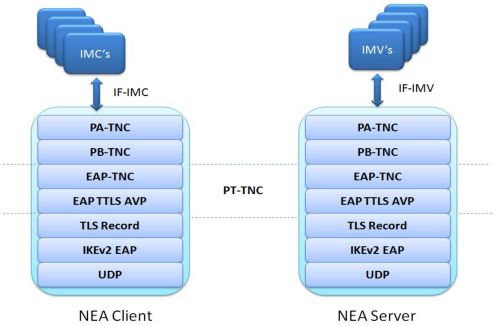

Figure 3: NEA Protocol Stack within strongSwan software

Introduction: The importance of the network security in today's interconnected world is becoming incredibly significant. The network endpoint security has to be maintained by the users whose technical knowledge base and experience may vary broadly. Therefore it would be very favorable if the assignment of securing the network node is simplified and automated through the software solutions. Network Endpoint Assessment (NEA) technologies offer the possibility to enforce necessary security requirements on the devices that are attempting to access the network. Depending on the corporate security policy, the endpoint can be checked against security requirements and is only admitted network access if it qualifies the tests. Contrarily, it can be denied access or get isolated and instructed on means to become admissible in case it didn't pass the test.The standardization effort for the NEA technologies are first made by Trusted Computing Group under the term «Trusted Network Connect». IETF's NEA Working Group has been organized to agree on and publish series of critical standards for NEA. Trusted Computing Group has submitted its Trusted Network Connect (TNC) specifications as proposals for NEA standards. Consequently, a series of RFC's are released by NEA working group which are compatible with TNC standards, including RFC 5793 for PB-TNC (Posture Broker) protocol.

Objective: The goal of the present project is to implement the PB-TNC (RFC 5793) protocol as a plugin for the strongSwan software in order the endpoints which installed and appropriately configured the strongSwan be able to take roles of either Access Requestor or Policy Enforcement Point or Policy Decision Point and carry out the Network Endpoint Assessment.

Solution: The strongSwan software is modular and offers dozens of plugins which enhance the functionality. The implementation of PB-TNC protocol is a strongSwan plugin called tnccs-20 which is the part of the Charon daemon that implements IKEv2.With the implementation of PB-TNC protocol RFC 5793, the strongSwan has become the first Open Source VPN software that is capable of carrying out Network Endpoint Assessment. From the strongSwan developers release version 4.5.1.dr2 on, the tnccs-20 plugin codes are integrated to the git master branch of strongSwan, thus could be downloaded and tested.