Anti-Eavesdropping Data Safety Framework for Highly Secured Enterprise Networks

A.A. Imran[1], A.R.F. Shafana (shafana.cst@gmail.com)[2]
[1] School of Computing, ESOFT Metro Campus, Bambalapitiya, Sri Lanka.
[2] Department of Information and Communication Technology, South Eastern University of Sri Lanka, Oluvil, Sri Lanka.

Abstract

The rapid advancement in Internet has paved way for several malicious intrusions which allow information to be accessed without proper authorization and privileges. Thus, the integrity, privacy and confidentiality of data and information are readily lost. One such malicious intrusion is the eavesdropping, man-in-the-middle attack. They often utilize the backdoor of the encryption that jeopardize the security of billions of devices and their communication.

Hardware Security Module (HSM) has been the topper as an anti-eavesdropping device since the time of its introduction, as they were specifically built to create a tamper-resistant environment to perform cryptographic processes. Thus, HSMs are widely used in Military and Security Forces to obtain heightened security and to preserve the privacy of critical data processing. However, high cost, availability of HSM vendors in minor scale and the practical difficulties in its operation and maintenance have made it less prevalent in enterprise networks.

Therefore, there is an immense need for the development of a mechanism that is equally competent to the functionality of HSM to withstand pernicious attacks and unauthorized surveillance on communication, but at a low cost. Since, HSM has proven track record of its performance and tamper-resistant feature, this paper aims to make use of the virtualization process of functionality of the expensive HSM.

The development of the anti-eavesdropping Data Safety Framework can be described, as follows. Through a thorough review of literature, the key features of HSM have been studied and thus, it is proposed to be implemented as a software that comprises its entire functionalities using VMware as the virtualization platform. To the HSM that has been virtually developed, Pretty Good Privacy (PGP), a low-cost privacy ensuring program will be used for encryption processes. A Virtual Private Network (VPN) has to be created by next, as the environment where the particular simulated software will function. The built private network created thus is the test enterprise network in this case. The HSM authorized network system will be managed by an Observer Management Server in order to provide additional benefits such as temporary decryption keys.

Upon building the intended simulated software as HSM and its functioning environment VPN as Enterprise Network, ethical hacking tools will be used to evaluate the robustness and performance of the built simulated software. The simulated software thus implemented and tested will be then tested for interoperability on an Enterprise Network.

Several security policies and security tools exist today. However, security breaches are happening prevalently bypassing the underlying security mechanisms. This particular study has proposed the implementation of a virtual hardware based on HSM, which has proven track record of its robust security feature, as an anti-eavesdropping data safety framework. The simulated software can support enterprise networks to preserve the privacy, confidentiality and security of the data communication.

Keywords: *Hardware Security Module, Anti-eavesdropping, Simulated Software*