ENHANCING THE IKE PRESHARED KEY AUTHENTICATION METHOD

Raed Bani-Hani

Dr. Gordon Springer, Dissertation Supervisor

ABSTRACT

Internet Key Exchange (IKE) protocol is part of the IP Security (IPsec) protocol suite. It is responsible for generating and maintaining Security Associates and for establishing session keys between two entities before applying any security services. In addition, it authenticates parties involved in the IKE exchange. In this dissertation, we explain the preshared key authentication method, show how the keys negotiated in this method can be compromised, and propose an improvement to make the method more secure.

A programming module is built in this dissertation to show the viability of the proposed improvement. C programming language is used, and running results are showed.