INFORMATICS INSTITUTE OF TECHNOLOGY

In collaboration with

UNIVERSITY OF WESTMINSTER

Prevent Man-in-the-Middle Attack in Diffie Hellman Key Exchange

A dissertation by

M.A.D.U.Manathunga

Supervised by

Mr. Geethapriya Liyanage

Submitted in partial fulfilment of the requirements for the MSc in Cyber Security and degree at the University of Westminster.

Abstract

When communication starts over the network, there are two parties involve. In order to start communication they need to have a secure communication. In order to establish a communication people use Diffie Hellman key change protocol. When using this protocol the both parties will come up with a common secret key. But this key only know those two parties. By using this security key they can encrypt their messages and continue the communication. The real world problem is, this mechanism has a vulnerability to man in the middle attack. This paper is conducting to prevent this vulnerability.

As explain in previous paragraph, there is a vulnerability in Diffie Hellman key exchange to the man in the middle attack. After conducting literature review and get the deep understanding author has discovered lack of authentication caused this vulnerability. Based on this conclusion author has suggested the conceptual framework which has an authentication functionality in the key exchange level. As a solution, in the initial handshake first person creates hash code based on the information on first handshake. Then second person will store this hash table and continues. Once first person gets the packet, he will check the new hash and his initially stored hash value. If it is same, then communication conclude as secure. If not it is possible that there is a man in the middle.

This conceptual framework shred with selected evaluators in order to evaluate the conceptual framework. The agreed on this solution with good approach and also there are some improvements need to be done. Those improvements and answers will discuss in detail evaluation chapter.

Keywords: Diffie Hellman, Cryptography, RSA encryption, AES algorithm

Subject Descriptors: Diffie-Hellman Key Exchange, Man-in-the-Middle Attacks, Cryptographic Protocols, Network Security