République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Ecole supérieure d'informatique

Mémoire de fin d'études

Pour l'obtention du diplôme d'Ingénieur d'État en Informatique

Option : ingénierie des systèmes informatiques

Secure Key Exchange Against Man-in-the-Middle Attack: Modified Diffie-Hellman Protocol

Réalisé par

M. Mansour Aboubaker

Encadré par: Dr. Amina Souyah (ESI-SBA)

Date de soumission: / /2023

Thanks

In the first place,

we would like to thank ALLAH, the Almighty and the Most Merciful for giving us faith, strength and courage.

We want to express, through these few lines of thanks, our gratitude to all those in whom, through their presence, their support, their availability and their advice, we have found the ardor to accomplish this project.

We would also like to express our deep gratitude and our sincere thanks to Dr. Amina Souyah who did us the honor of directing this work. Her invaluable advice was of considerable help to us.

Finally, we cannot complete this project without expressing our gratitude to all the teachers in the Higher School of Computer Science ESI-SBA for their dedication and assistance throughout our studies.

Abstract

One of the most famous key exchange protocols is Diffie-Hellman Protocol (DHP) which is a widely used technique on which key exchange systems around the world depend. This protocol is simple and uncomplicated, and its robustness is based on the Discrete Logarithm Problem (DLP). Despite this, the protocol is vulnerable to the Man-in-the-Middle (MitM) attack. The scope of this thesis is to provide a relevant review on secure key exchange mechanisms that are employed in practice to deal with the issue of sharing securely the secret key between the authorized partied in symmetric cryptosystems.

On the other hand, the practical aspect of this thesis is concerned by the redesign and realization of a modified version of the DHP protocol. The proposal is based on two verification stages to withstand the issue of Man-in-the-Middle (MITM) attack. In the first stage, the pseudo-random value α that one of the communicating parties (sender) sends to the other legitimate party (the receiver) will be verified weither there exists any malicious manipulation on it. In the second stage, the random value β that the receiver sends to the sender will be also verified weither there exists any malicious manipulation on it.

Mathematical proofs have been carried out to demonstrate the effectiveness of our contribution and its robustness against Man-in-the-Middle (MitM) attack.

Keywords: Cryptography, Secret key exchange, Diffie-Hellman Protocol (DHP), Man-in-the-Middle (MitM) attack.
