Internet Protocol Protection

Hasan Mohamed AL Gghammoudy [1] , Salma Ali Attayeb[2]

1Ministry of education, Ajdabyah, Libya, Email: hqadrbwh@ gmail.com
2 Polytecnic, Ajdabyah, Libya, Email: asma.alfergani@uob.edu.ly

Abstract

The main purpose of this paper is to study the security of the Internet Protocol and the method of exchanging keys, extract weaknesses in them, and provide appropriate solutions. The second goal is to find another more reliable way to share the Diffie-Hellmankey.The search takes the following steps; Background study of Internet Protocol security(IPSec), Study the key exchange protocol (IKE), Discuss the application of the algorithm Diffie-Hellman. Through these steps we reached; Identify weaknesses and problems related to those methods, Optimal methods for distribution of public keys, Provide another, more reliable way to share the Diffie-Hellman key, Improved Harn's and phan protocols for Diffie-Hellman interchange protocols that are integrated into the digital signature algorithm, The authentication is provided before the public keys, and then developed our idea of optimizing the integrated Diffie-Hellman-DSAkey exchange protocol. use internal encryption keys to increase confidentiality.

Keywords: Internet Protocol Protection, Diffie-Hellman-DSAkey, key exchange protocol (IKE), Internet Protocol security(IPSec)

1. Introductio

For considerable period of time, many applications have been based on the internet and the computer networks such as the financial transactions and e-commerce. On the other hand, many hacking techniques have been developed in order to attack the systems to get valuable information in illegal way. These techniques include the Man-in-the-middle, sniffing and others. These attacks and their consequences have motivated researchers to develop defense techniques and security systems that can be used against the hackers attack to protect the transmission processes and their information. Secure Socket Layer (SSL) is one of these techniques. SSL is used to protect the communication channels [1].

HTTP over SSL is used in the commercial sites and e-mail. Secure hyper text transfer (https), port 443, are used instead of http port 80 in these applications. Transport Layer security (TLS) and Server Message Block (SMB) is another technique where it is used for the same applications [1].

All these techniques or methods work at the application layer and their functions are limited and suitable just for their applications. In this paper, a new technique of IP security is created, where it works at the network layer instead of the application layer.

Network layer is very important for network administrators for put protection policies. At this layer the packets are transmitted across the networks. All connections can be secured. Because of all the packets are encrypted before they are transmitted from network to network. Also the net work layer get the information from the transport layer and encapsulate it.it protect the data inside the packets [2].

Internet Protocol Security is a protocol that is used to protect the communication and achieve all the goals of protection. The confidentiality is achieved based on the encryption. The data integrity and the authentication, in addition to non repudiation are achieved based on the digital signature.

This paper seeks to help organizations to reduce the seriousness transfer of important information on the networks are not protected. Based on Internet Protocol Security (IPsec). In addition to, it explains the weakness in keys exchange protocols that are depended on Diffie-Hellman algorithm, and provide solutions for all the weaknesses in those the protocols. We offer a new protocol provides solutions for the problems and the weaknesses of previous protocols. In addition to that our protocol gives new ideas to support the protection of sensitive information and increase the authentication and integrity and confidentiality for both the keys and information.

2. Analysis of Internet Key Exchange

IPSec uses the Diffie-Hellman algorithm to offer security for encryption keys.

The Diffie-Hellman Algorithm

To explain the steps for Diffie-Hellman key exchange protocol, assume that, Fatma and Mohammed exchange the public keys on untrusted network such as the internet. The result of this exchange, Fatma and Mohammed generate the same key. This key is used for encrypt and decrypt message [3][4].

In the first step, agreement between Fatma and Mohamed on prime p and integer g modulo p. Then, both Fatma and Mohamed choose random integer values those is secret. Only they know those the secret numbers [3] [4].

Assume, the random integer value for Fatma is a, the random integer value for Mohamed is b.

The public key for Fatma is computed by the following equation:

$X = g^a \bmod p$ ……(1)

On the other hand, The public key for Mohamed is computed by the following equation:

$Y = g^b \bmod p$ ……..…(2)

Fatma sends her public key to Mohamed, Mohamed computes the shared secret key by the following method:

$K_b = X^b \bmod p$ …..……...(3)

By the same method, Mohamed sends his public key to Fatma , Fatma computes the shared secret key by the same method.

$K_a = y^a \bmod p$ ……..(4)

The key K_a is equal to the key K_b [3[4].

$K_a = g^{ab} \text{mode } p = K_b = \left(g^b\right)^a \text{mode } p$.....(5)

How Can Man-in-The-Middle Attack Get The Public Key?

Diffie-Hellman protocol does not give any authentication before the exchanging of the public keys.

Suppose user A sends his public key to user B. Man in the middle attack takes the key that is sent by user A and creates other public key and sends it to user B. In the same method, Man in the middle attack takes the key that user B is sent to user A and creates other public key and sends it to user A.

User A will think that the key from user B, and user B will think that the key from user A. Both user A and user B calculate the shared key. In the same time Man in the middle attack combines his private key that will be shared with user A and the private key which will be shared with user B [6].

User A encrypts the important information by using his secret key and sends it to user B. Man in the middle attack gets this the massage, modifies it, and encrypts it for the second time. Then sends it to user B. On the other hand, user

B encrypts the important information by using his secret key and sends it to user A. Man in the middle attack gets this the massage, modifies it, and encrypts it for the second time. Then sends it to user A. Therefore, Man in the middle attack would know all the confidential information that is sent from the first user to the second user and vice versa [6].

3. The Weakness of Diffie–Hellman Protocol

No authentication is offered by Diffie- Hellman algorithm before the exchanging of the secret information[5][3].
The Diffie- Hellman protocol does not use the digital signature through the exchange of the public keys.
Diffie- Hellman protocol uses the same secret shared key to transfer and receive the information[5].
The big weakness in Diffie- Hellman protocol is the key life time.

4. Harn's Three-Round Key Exchange Protocol

Because of no authentication or digital signature is offered by Diffie-Hellman key exchange protocol, and because of Diffie-Hellman key exchange protocol does not use the digital signature to achieve the authentication. Harn et al. combined the digital signature and Diffie-Hellman key exchange, in order to avoid the previous problems [7].
Harn's key exchange protocol does not provide forward security or key freshness [7].
in Harn et al's key exchange protocol, if the attack could get the random integer value (x_b) that the user B uses to calculate the key for direction from A to B, that is explained by the following equation [7]:
$K_{AB=}(M_a)^{x_b} \text{mod} p$ ……(6)
It can compute the key that the user A is used easily.
$K_{AB} = Y_b{}^{v} \text{mod} p\ g^{v\,x_b} \text{mod}\ p$.....(7)

Phan's Fixing

Phan could solve some the problems of Harn et al's key exchange protocol.
Forward security and key freshness is offered by Phan's protocol. Those are not found in Harn et al's key exchange protocol. On the other hand, there are some problems and weakness in Phan's protocol.
For example, the equation :
$k_{AB} = g^{x_b wv} \text{mod}\ p$……(8)

This equation contains random integer values $x_{b,}w, v$. Those the random integer values are similar to the random integer values $x_{a,}v, w$ those the following equation is contented:

$k_{BA} = g^{x_a vw} \bmod p$…… (9)

This makes the two keys k_{BA}, k_{AB} are similar, and this similarity will give the attack opportunity to break the algorithm [7].

On the other hand, Phan's protocol has dangerous weakness, the keys those are sent by user A to be vulnerable to eavesdropper. Because no authentication occurs before keys are exchanged. They were sent without digital signature.

5. Improved Protocol:-

Improved Protocol could solve the problems of previous protocols. It avoids the weaknesses and provides solutions for the problems in them. In improvement protocol, there are three extra temporary random integers and three keys. The first one for direction from A to B (K_{AB}) and the second key for direction from B to A (K_{BA}). Those keys are used as external encryption keys .The third is the secret shared key (K_H), that is used as internal encryption key. In order to increase confidentiality and integrity we use internal encryption key, this means that, even if the eavesdropper could get the external encryption keys, he cannot obtain the information. Forward secrecy and key freshness are provided by this protocol. This makes the eavesdropper instead of having to know one key to decrypt the message. It needs to know two keys for each direction. The internal encryption key and the external encryption key. The keys are completely deferent each other. Moreover, the key K_{AB} in improvement protocol consists of number of the random integer values. Those the random integer values are totally deferent from the random integer values in the key K_{BA} and the random integer values in the key K_H. This makes the keys K_{AB} and K_{BA} and K_H are completely deferent each other.

Meanwhile, in order to increase the authentication, the improved protocol uses certificates for the distribution of public keys

The table of Improvement Protocol

Step	User A	User B
	Select random integer v_1, v_2, v_3 $M_{a=} g^{v_1} mod\ p$ $N_{a=} Y_a{}^{v_2} mod\ p$ $H_{a=g^{v_3} mod\ p}$ *User A send* M_a, N_a, H_a	
2		*Select random integer* w_1, w_2, w_3 *and calculate* $K_{AB} = M_a{}^{x_b w_1} mod\ p = g^{v_1 w_1 x_b} mod\ p$ $K_{BA} = N_a{}^{w_2} mod\ p = g^{x_a v_2 w_2} mod\ p$ $K_H = H_a{}^{w_3} mod\ p = g^{w_3 v_3} mod\ p$ $M_b = Y_b{}^{w_1} mod\ p$ $N_b = g^{w_2} mod\ p$ $H_b = g^{w_3} mod\ p$ $r_b = N_b mod\ q$ $s_b = \left((w)^{-1}\left(H\left(m_b \vert\vert k_{BA} \vert\vert k_{AB} \vert K_H\right) + x_b r_b\right)\right) mod q$ *User B send* M_b, N_b, H_b, s_b *to user A*
3	*User A calculate* $K_{AB} = M_b{}^{v_1} mod\ p = g^{v_1 w_1 x_b} mod\ p$ $K_{BA} = (N_b)^{x_a v_2} mod\ p = g^{x_a v_2 w_2} mod\ p$ $K_H = H_b{}^{v_3} mod\ p = g^{w_3 v_3} mod\ p$ $r_b = N_b mod\ q$ *Verify DSA signature* (r_b, s_b) $r_a = M_a mod q$ $s_a = \left((v)^{-1}\left(H\left(m_a \vert\vert k_{BA} \vert\vert k_{AB} \vert K_H\right) + x_a r_a\right)\right) mod q$	
		$r_{a=M_a mod\ q}$ *Verify DSA signature*(r_a, r_b)

M_a, N_a, H_a.

N_a, N_b are public key

Forward security and key freshness is offered by our protocol. Those are not found in Harn's key exchange protocol.

H_a, H_b are public keys

K_{AB}, K_{BA} are external encryption keys .

K_H is internal encryption key.

The key for the direction from user A to user B (K_{AB}), that is computed by user A is equals with the key for the direction from A to B (K_{AB}), that is computed by user B. Also the key for the direction from user B to user A (K_{BA}), that is computed by user A is equals with the key for the direction from B to A (K_{BA}), that is computed by user B.

Improvement protocol uses the hash and the digital signature to exchange the public keys. The user A hashes the values of the keys and translates them to message digest. Improvement protocol encrypts this value and sends it to user B. User B decrypts the message digest, then computes new message digest of the keys those are sent, after that, user B compares the two message digest. If the two message digest is equally, this means the keys are not fake.

Improvement protocol provides the digital signature. After create the hash of the keys, sign this value using the secret key. The hash and the digital signature ensure the authentication and integrity and the confidentiality for the keys.

The two secret key for direction from A to B is computed by following equation :

$K_{AB} = {M_b}^{v_1} \bmod p = g^{v_1 w_1 x_b} \bmod p$ (10)

$K_H = g^{w_3 v_3} \bmod p$……..……. (11)

And it is computed for direction from B to A by following equation :

$K_{BA} = {N_a}^{w_2} \bmod p = g^{x_a v_2 w_2} \bmod p$(12)

$K_H = g^{w_3 v_3} \bmod p$…….... (11)

The key for the direction from A to B is completely deferent from the key for direction from B to A. The keys (K_{AB}) , (K_{BA}) have not the same random integer values. The random integer values for the key (K_{AB}) v_1, w_1, x_b, those explained in the equation (10) are totally different from the random integer values for the key (K_{BA}) x_a, v_2, w_3, those explained in the equation (12).

In addition to ,eavesdropper needs to know two keys in each direction instead of one key to be able to decipher the message. This makes information is given more confidentiality and integrity by our improvement.

Meanwhile, if there is any backwardness in the external keys K_{BA}or K_{AB} , it will be there second key K_H. This makes the calculations more difficult and more complexity for a terrorist and more protection for algorithm.

Improvement protocol provides new idea for improvement combination of the digital signature with Diffie Hellman key exchange protocol.

In our improvement, A public keys with specific period of time, instead of key life time.

The specific interval equal to session time divided number phases of public keys.

For example, assume that, the communication session takes 27,000 seconds and it is divided to three parts. Every part uses special public keys. By divide 27,000 seconds (The time of the communication session) on number of the public key phases. We need 9000 seconds to change the first stage keys to the second stage keys which need the same time to change to the third stage keys, to transfer of the information is finished. This means, if the attack could get the first part of the session, it will is very difficult to get the second part or the third part of the session [8][9].

The biggest advantage of this idea, the second stage keys and the third stage keys appear in the certificate only during communication session. Except that the first phase keys only are apparent in the certificate. Therefore, our protocol be more protection and safety. This makes the opportunity for terrorist to get the keys is too weak.

Our development gives not only authentication. But ensures that information is more confidentiality and integrity.

6. Evaluation and Discussion:

In improved protocol, the random integer values those are used to compute the public keys M_a, N_a, H_a are not the same. Therefore, the keys K_{AB}, K_{BA}, K_H are not equal.

In addition to that, our improvement gives authentication , integrity and confidentiality more than other protocols. We will explain that as following:

The keys K_{AB}, K_{BA} are used as external encryption keys. The key (K_H) is used as internal encryption key

The internal encryption key is computed by user A :

$$K_H = {H_b}^{v_3} \bmod p = g^{w_3 v_3} \bmod p \ldots (11)$$

The internal encryption key is computed by user B :

$$K_H = {H_a}^{w_3} \bmod p = g^{w_3 v_3} \bmod p \ldots (11)$$

Confidentiality and integrity is increased by using the internal encryption key. Because even if the eavesdropper could get the external encryption keys, he cannot obtain the information.

We note that, the internal encryption key is not equal external encryption keys. Because our protocol does not use the same random numbers to

calculate internal encryption key and external encryption keys. Therefore, improvement protocol provides security more than other protocols.

Our protocol provides forward security, that is explained in the following steps:

The external encryption key K_{AB} is computed by the following equation:

$$K_{AB} = M_b{}^{v_1} \bmod p = g^{v_1 w_1 x_b} \bmod p \ldots (10)$$

On the other hand, the internal encryption key is computed by the following equation:

$$K_H = H_a{}^{w_3} \bmod p = g^{w_3 v_3} \bmod p \ldots (11)$$

The external encryption key K_{AB} contains three random integer values v_1, w_1, x_b ,

If the attack could get the random integer value X_b, it cannot get the external encryption key or the internal encryption key.

Improvement protocol provides Key freshness. That is explained as following:

The external encryption key K_{AB} is explained by the equation:

$$K_{AB} = M_b{}^{v_1} \bmod p = g^{v_1 w_1 x_b} \bmod p \ldots\ldots\ldots\ldots (10)$$

The internal encryption key:

$$K_H = H_a{}^{w_3} \bmod p = g^{w_3 v_3} \bmod p \ldots \ldots (11)$$

Those keys contain number of the random integer values, they do not depend on one random value, also the random integer values in those the equations are new values for both users.

In previous protocols there is no authentication before the key M_a is exchanged.

Our protocol provides authentication before the keys M_a, N_a, H_a are exchanged. It uses public-key certificates for the distribution of public keys M_a, N_a, H_a.

On the other hand, in order to increase confidentiality and integrity, the internal encryption key is the same for both users. .

In this case, user A will send H_a, to user B.

$$H_a = g^{v_3} \bmod p \ldots \ldots \ldots \ldots (13)$$

User B will compute K_{Ha} ,

$$K_{Ha} = H_a{}^{w_3} \bmod p = g^{w_3 v_3} \bmod p \ldots \ldots \ldots \ldots (14)$$

On the other hand, user B will send H_b, to user A.

$$H_b = g^{w_3} \bmod p \ldots \ldots (15)$$

User A will compute , K_{Hb}

$$K_{Hb} = H_b^{v_3} \bmod p = g^{v_3 w_3} \bmod p \ldots\ldots\ldots (16)$$

(K_{Ha}) for user A equals (K_{Hb}) for user B. Therefore, in this way we set up the second wall in front of the spoiler. The eavesdropper will find great difficultly to get information. This makes information is given more confidentiality and integrity by our improvement. Our protocol solved the problems via division communication session into three phases .

The specific interval has been solved all problems of key life time. Because via this the specific interval there are no a longer key lifetime in order to gives attackers suitable opportunity to break the algorithm. On the other hand a shorter key life time that is reason to a large number of keys generated compared with the time of the communication session. Or the sender continues to send messages and the security association is expired. public keys with specified period of time, instead of key life time, this specific interval is not known to the saboteur. The spoiler cannot guess when will the second stage keys appear. Because the period of communication session is sent with the first part of the massage using the first stage keys. This mean that , even if the eavesdropper could obtain the first part of the information, he cannot get the rest of the information. Because our improvement use three phases of the keys. One phase for each stage of the information that is sent.

7. Conclusion

In this paper, we discussed internet key exchange protocols, and found that internet key exchange protocols does not provide the authentication before the keys are distributed .The digital signature provided two benefits: authentication and data integrity. The hash ensures the data integrity. The better improvement on “the integrated Diffie-Hellman-DSA Key Exchange Protocol” had more secure than other protocols, because the eavesdropper instead of having to know one key to decrypt the message. It needs two keys for each direction. Our protocol provided authentication before the keys M_a, N_a, H_a are exchanged. It used public-key certificates for the distribution of public keys M_a, N_a, H_a,Public keys are provided to Certificate Authority in the form of three stages. Communication session is divided into three phases. Our protocol solved all problems of key life time. public keys with specified period of time, instead of key life time. This specific interval is not known to the saboteur. it gave

not only authentication. But ensures that information is more confidentiality and integrity .

Finally, this thesis accomplished the desired goal, provided anew algorithm be more protective and safer than the original Diffie-Hellman protocol.

8. Reference

[1] Majdi Alshibany“IP Security” Course sheets, higher Institute of industry, Misurata, 2009.

[2] Sheila Frankel . Guide to IPsec VPNs. 2005.

[3]Taha Osman, ’’ Cryptography for Data Security ” Course sheets, School of Computing and Informatics cooperated with Department of Electronic Engineering, Nottingham, 2011

[4] David A. Carts, A Review of the Diffie-Hellman Algorithm and its Use in Secure Internet Protocols, 2001.available at http://www.ietf.org/rfc/rfc2631.txt.

[5] http://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_problem

[6]http://logicalsecurity-ls.blogspot.com/2009/03/diffie-hellman-algorithm.html

[7] Jie Liu and Jianhua Li , A Better Improvement on the Integrated Diffie-Hellman-DSA Key Exchange Protocol, Department of Electronic Engineering, Shanghai Jiao Tong University, 2010. Available at http://ijns.femto.com.tw.