S-wane Model Designed to Improve Security Association Negotiation Process in IPv6

Mme Khadidiatou Wane Keïta
Mr Alex Corenthin
Laboratoire Traitement Information(LTI)/ESP/UCAD
Dakar, Sénégal
e-mail:wane.keita@esp.sn ;alex.corenthin@gmail.com

Mr Claude Lishou, Mr Sidi Mouhamed Farssi
Laboratoire Traitement Information(LTI)/ESP/UCAD
LIMBI/ESP/UCAD
Dakar, Sénégal
e-mail: claudelishou@yahoo.fr; farsism@yahoo.com

***Abstract*— Network security is a major concern as well as a very active research field today. Internet Protocol version 6 has been developed as a result. For a matter of fact, this new IP protocol is based on a number of mechanisms designed to handle specific security services. The main security services supported are authentication, confidentiality and access control. Hence, IPv6 defines several layers of which the main one is the Security Association negotiation, which is based on the Diffie-Hellman Key Exchange. This layer has loopholes which can cause security defects, as technology advances. In this research paper, we propose a negotiation model of Security Associations, integrating s-wane model to enhance the existing security mechanism. Results obtained show the impossibility of intercepting data transmitted with a relatively less complex algorithm compared to conventional methods such as STS, HMQV and New-two-Pass.**

Keywords-security, IPv6, Diffie-hellmann, Security Association (SA)

I. INTRODUCTION

Security issue is a major concern today. Thus, the new version of Internet Protocol (IPv6) [1] sounds like an answer after numerous attempts to secure IPv4 [1]. In fact, IPv6 addresses the following issues: addressing, routing, IP mobility, autoconfiguration, the quality of services and safety [1] [2]. This security, explicitly supported by IPSec mechanisms, is based on Security Association negotiation (SA: Security Association). This is necessary to establish security parameters as well as algorithms to secure communication. It uses specific mechanisms at certain layers of the negotiation. In this research work, our goal is to show the level of reliability of existing mechanisms in implementing this negotiation. Thus, we will review important layers of the Security Association negotiation to detect major limitations of existing mechanisms and make possible corrections to flaws observed.

To do this, we will, first of all, talk about Security Association and the negotiation of this Security Association used in IPv6 security mechanisms. The second part will propose an optimization of security mechanisms described above to address detected problems. The third part will focus on the literature review of existing mechanisms and compare them to the performance of our proposal.

II. THE NATIVE SECURITY OF IPV6

IPSec is an integral part of the security model of IPv6 [3] [4]. These IPsec security mechanisms are therefore made up of protocols, databases and require a security association to connect them.

A. IPSec protocol suite

Two types of protocols are used by IPsec to manage the security of IPv6 datagrams:

- Security protocols
- Key Exchange Protocol

Security protocols used are AH protocols (Authentication Header) [5] and ESP (Encapsulating Security Payload) [6]. Extension fields exist in IPv6 packet header to explicitly reflect, all of the mechanisms proposed by IPsec. However, the operation of IPsec requires a set of keys to be exchanged between users. The use of a key exchange protocol is therefore necessary. With IPsec, the key exchange protocol used is IKE (Internet Key Exchange) [15]. This key exchange protocol provides the following functions:

- authentication and protection of the users identities
- negotiation of a security policy among peers to ensure the protection of the Exchange
- authenticated Exchange based on Diffie-Hellman Key [7] in order to have shared secret keys
- implementation of a tunnel to negotiate phase 2 parameters of IKE.

IKE provides these two production modes: Main Mode and Aggressive Mode. The Main Mode is available in three exchanges in both directions between the initiator and receiver:

-First Exchange: relates to the negotiation of algorithms and hash functions;

-Second Exchange: here, a Diffie-Hellman Exchange Key is used to set the shared secret: to produce shared secret keys, pass announcements (random numbers sent to the other party and then signed and returned to prove their identity);

-Third Exchange: the identity of two-thirds users is checked.

The major results of this Main Mode enable the definition of a tunnel between users.

As for the Aggressive Mode, few exchanges are carried out and, with a minimum of packages. Almost everything is focused on the Diffie-Hellman public key. The receiver returns all that is necessary to carry out the Exchange and

confirmation of the Exchange back to the transmitter. The relative weakness of this mode is that the two communicating parties exchange information prior to a blocked channel. Therefore, it is possible to "sniff" medium and discover the initiator of the new SA. However, it is faster than the Main Mode.

B. Security Association

Before secure communication can be established, it is necessary that the parties negotiate the terms that will be defined in a security association (SA). A SA therefore defines the transformations to be applied to datagrams and their deployment. It indicates:

- if it is a AH or ESP protection,
- the authentication algorithm for AH and ESP,
- the cryptographic algorithm for ESP,
- authentication and encryption keys,
- the SA lifetime,
- the mode of the Protocol, namely tunnel, transport or wildcard. The wildcard mode means that the choice of the protection mode is determined by the application and is usable only from a workstation.

During an SA negotiation, a 32-bit number called SPI (Security Parameters Index) is assigned. An SA is unidirectional causing the use of two SA for two-way communication between two stations (one for datagrams in one direction and one in the other direction).

C. IPSec databases

The databases internal to IPSec are Security Policy Database (SPD) and Security Association Database (SAD). Depending on the chosen selector, the SPD specifies actions to perform on a package. Three actions are possible:

- either the package is not allowed to be processed by a station, to pass through a security gateway or to be received by an application: it is therefore deleted;
- traffic is allowed but requires no security services: it is then ignored.
- either traffic requires IPSec protection in which case the SPD specifies for each packet the association or security associations to apply. This (or these) association (s) is (are) defined in the SAD database.

SAD contains the whole active security associations. This database specifies for each security associations, services and security mechanisms to be applied. Thus, security associations to apply can be found easily through the index of security settings, the recipient address and the Security Protocol (AH or ESP) selected.

D. Operation

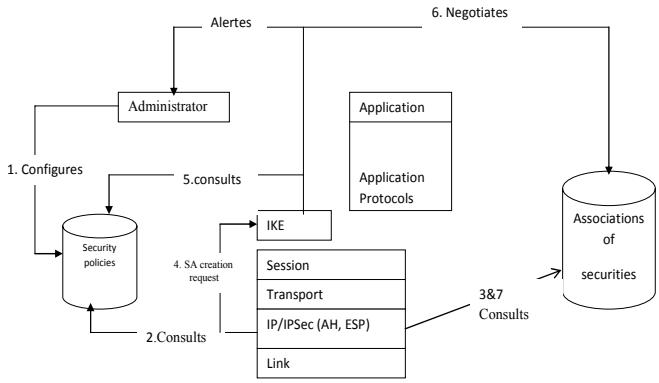

Figure 1: IPv6 security mechnism

This diagram defines the deployment of IPSec-based security in IPv6. In order to secure communications between two entities of the network, the network administrator configures the security policy database (step 1), the SPD. This database will facilitate the decision on the type of security services to provide for each packet resulting from the communication with the other entity. The second database, (SAD: Security Association Database) containing the parameters for active security associations, exists. Thus, when data is transmitted, these two databases are consulted (layers 2 and 3) to find out how to process the data with an active security association. In the absence of SA, the creation of an SA is required for IKE (layer 4). Internet Key Exchange (IKE) consults with the SPD, negotiates a new SA taking into account specific characteristics (it is at this stage that Diffie-Hellman is involved) and sends alerts to the administrator (layers 5 and 6).

Upon receipt of a package, extensions are examined in order to determine whether the packet is protected. If so, the SAD is accessed for verification and/or decryption (layer 7) settings.

III. SECURITY ASSOCIATION NEGOTIATION

The negotiation of the security association is an essential layer in the dynamic management of the security of IPsec settings. This negotiation is done in four phases which are: the negotiation of parameters (layer 1), the generation of Diffie-Hellman and parameters of hazards (layer 2), mutual authentication (layer 3), the definition of both SA (layer 4). Most of these negotiation layers use Diffie-Hellman. As a result, the exchange done through Diffie-Hellman is a very important phase : secret of Diffie-Hellman and risk-sharing

The principle of Diffie-Hellman consists of these layers:

1. Two users share two non-secret parameters: a prime number p and an integer g with $g < p$;
2. These users will then choose a random private value (a and b);
3. They each compute a public value. The one with secret a computes and the other user computes
4. These public values computed are then exchanged

5. Finally the one that sent X_a calculates $K_1 = (X_b)^a$ and the other $K_2 = (X_a)^b$. Thus, we have $K_1 = (X_b)^a = (g^b)^a \bmod p = g^{ba} \bmod p = (g^a)^b \bmod p = (X_a)^b = K_2$. Thus, there is effective sharing of the secret $K_s = K_1 = K_2$.

This Exchange based on Diffie-Hellman could be represented by figure 2:

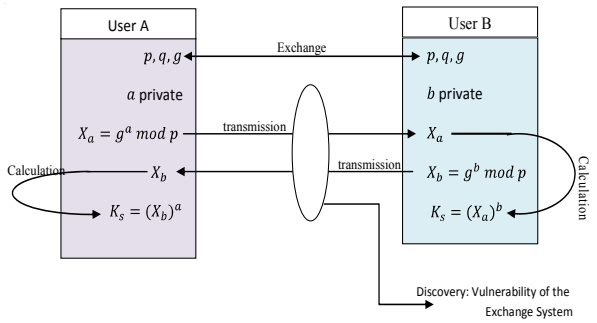

Figure 2 : Diffie-Hellmann Exchange

As noted in the diagram of figure 2, the Diffie-Hellman exchange system is vulnerable. For a matter of fact, the vulnerability is related to the exchange of secret information through a network not necessarily secure. This vulnerability could be represented by figure 3.

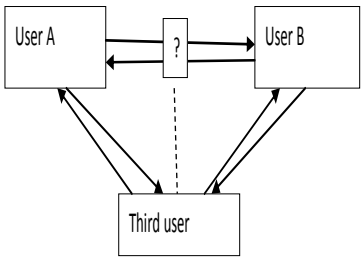

Figure 3: Vulnerability of the Exchange System

This vulnerability could be observed from two angles:

- Interpretation of data exchanged

Information exchanged could be intercepted and analyzed to reconstruct the secret. Indeed, Xa and Xb data can be analyzed and enable, thanks to p and q values, the discovery of non-shared values a and b through a logarithmic calculation. This discovery of a and b will facilitate the calculation of KS which is the shared secret between the two communicating users. Though proven robust considering the current characteristics of computers, Diffie-Hellman must deal with quantum computers.

- "Man-in-the-middle" attack

This system must therefore face certain attacks such as "a man-in-the-middle" attack. A third person could stand between the two communicating users during the Exchange and pass it off as one of them in the exchange of data by modifying a portion or all of the received messages. This will enable the attacker to masquerade as one of the communicating entities and therefore violate the confidentiality associated with the secret and in consequence, IPV6 can no longer ensure the integrity, which it should.

Solutions have been proposed. But most of them are interested only in a specific type of attack which is: "man-in-the-middle. So they focused on the authentication of the communicating users. Although these solutions reduce the vulnerability of Diffie-Hellmann key exchange, the interception of information has not been tackled.

The s-wane model we offer in the suite is designed to address these two problems. This will further reduce vulnerability.

IV. S-WANE MODEL

After researching on the negotiation of Security Associations, it is clear that most of IPsec vulnerability is based on Diffie-Hellmann Key Exchange. This section will help mitigate this vulnerability by encrypting Diffie-Hellmann exchanges. The proposed s-wane model uses in addition RSA (Rivest Shamir and Ademann) [8] and consists of the following layers:

1. Two users (A and B) share two non-secrets parameters: p, a prime and g an integer with g < p;
2. These users will then choose each, a private random value (a and b)
3. They will exchange their public keys (RSApu (A), RSApu (B)) based on RSA principle while each keep secret their private keys;
4. They respectively calculate Xa and Xb. User A must encrypt Xa with the public key RSApu (B) of user B. Xb will be encrypted by user B with public key RSApu (A) of user A. The two users will need to exchange these figures.
5. Each user decrypts the received message in layer 4 by using each their private key
6. Finally, the shared secret k can be calculated.

S-wane model could be represented by the following diagram:

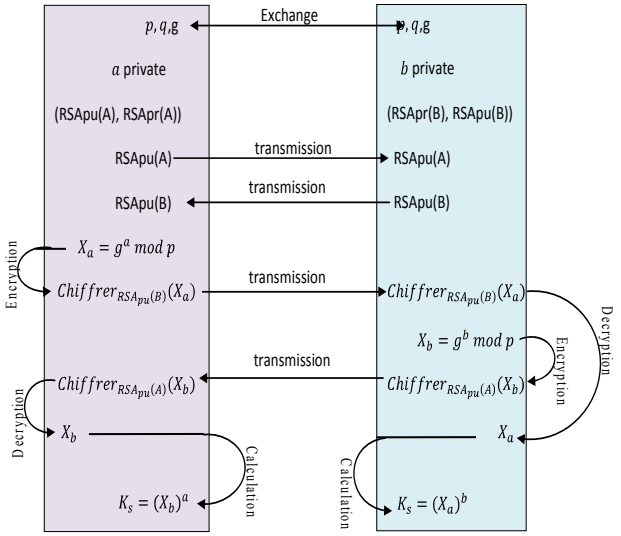

Figure 4 : proposed model

This model proposes a reduction of the negotiation vulnerability of Security Association using RSA. In this model, Xa and Xb are transmitted confidentially. Thereby enhancing the confidentiality of the secret.

The negotiation period of AS has increased significantly. In fact, RSA deployment should be added to the usual negotiation period.

V. COMPARISON OF S-WANE MODEL WITH EXISTING SOLUTIONS

The model is relevant in the sense that it adds value to existing solutions. That is why we chose to compare it with Station - To - Station Protocol (STS) [9], New two-Pass Key Agreement [10] and HMGV(Hashed Menezes-Qu-Vanstone) [11]. The Protocol choice is motivated by shared concerns. In addition, this Protocol is considered more appropriate.

A. Existing solutions

A.1. STS Protocol

STS Protocol combines DH algorithm with digital signature. This combination facilitates mutual authentication of two communicating users.

Users A and B have a pseudo-random generator, an encryption system whose encryption function is Є and decryption D, function s signature and checker V. One user sends the encrypted session key and signs; the other receives this information, decrypts and verifies the signature; if the test is conclusive he performs the same operations in turn.

STS provides a digital signature for mutual authentication of users before accepting the session key which prevents "a man-in-the-middle" type attack.

However STS is seriously vulnerable to some attacks [12] and some of its limits are:

- High-delay due to the time-lag between operations
- Complexity of the mechanism;
- No encryption key.

A.2. A new-two-pass Key agreement Protocol

This Protocol defines a session key that is a combination of A and B keys.

The two entities separately generate secret information and a key agreement is produced. The key agreement is tested and if the result is zero then there is failure. In that case, the secret produced will constitute the session key.

Limits

- complex;
- High-delay due to the time-lag between operations
- does not encrypt the session key.

A.3. HMQV

HMQV protocol (Hashed MVQ) is a chopped MQV variant which is a variant of DH. And the hash is done with different lengths.

This Protocol can use certificates.

B. Comparison of lookup attempts and s-wane model

All strategies are designed to overcome "a man-in-the-middle" attack. On the other hand, the proposed s-wane model encrypts Xa and Xb before transferring. Making it stand out from others.

When s-wane model is used, the vulnerability observed in DH is reduced significantly. In fact, even if the risk is low, it further reduces it because in addition to the size of the keys, constituting an obstacle to the correct interpretation of the intercepted information, knowledge of the recipient's private key is necessary.

Moreover, when user A encrypts Xa by using user B's public key, only this user (B) can decrypt using its private key and therefore when a third party intercepts it, because of being unable to decipher the information received, will have difficulties to alter or replace it. So the third party will not be able to pass off as one or the other.

The new s-wane proposal can be compared to the three lookup attempts for DH vulnerability based on these criteria:

- "the-man-in-the-middle" attack: this problem is addressed in the same way by the four solutions;
- Exchanged secret encryption: s-wane is the only solution to encrypt information exchanged during the transfer;
- Complexity: the new s-wane solution is less complex than other lookup attempts because it combines two very simple mechanisms and some operations can take place concomitantly;
- Lead-time: the lead-time of s-wane is short because upon the exchange of the keys all other operations may take place concomitantly;
- robustness: s-wane addresses two concerns that are “the-man-in-the-middle” attack and data interception during transfer; this justifies the fact that s-wane is more robust than STS, HMQV and New-Two-Pass

Table 1 presents the summary of comparisons between s-wane and other solutions:

.MECHANISMS / CRITERIA	s-wane	STS	HMQV	New-Two-Pass
Man-the-middle	Yes	Yes	Yes	Yes
Encryption of the information exchanged	Yes	No	No	No
Interception of transmitted data	impossible	possible	possible	possible
complexity	Less significant	significant	significant	significant
Lead-time	shorter	high	high	high
robustness	significant	Less significant	less significant	less significant

Table 1: summary comparison of s-wane model and existing solutions

VI. CONCLUSION

This article enabled us to look into negotiation layers in Security Associations and to highlight a certain vulnerability of this AS negotiation system. This flaw is due to the fact that DH is used to exchange secret data on a network which is not necessarily secure. The s-wane (combination of RSA and DH) solution ensures the secure exchange of data.

By encrypting data exchanged through RSA, the vulnerability of the DH system is significantly reduced. As a result, the robustness of SA negotiation mechanism increases.

The comparison of the proposed model with STS, HMQV and New-Two-Pass helped to show the contribution of our work compared to existing solutions especially with regard to the inability to intercept data transmitted with a relatively less complex algorithm.

However, a relative increase in the negotiation period is to be noted. This concern could be addressed in our future work.

BIBLIOGRAPHY

[1] S. Deering Cisco, R. Hinden Nokia, “Rfc 2460 Internet Protocol Version 6 (IPv6) Specification” December 1999

[2] G. Cizault, “IPv6 : théorie et pratique” O’REILLY, 2005 (320p)

[3] S. Kent, K. Seo BBN technologies Security Architecture for the Internet Protocol Rfc 4301 December 2005

[4] N. Doraswamy, D. Harkins, “IPSec”, Campus Press référence 2003 (285p)

[5] S. Kent, R. Atkinson, “Rfc 2402 : IP Authentification Header”, November 1998

[6] S. Kent, R. Atkinson, “Rfc 2406 IP Encapsulating Security”, November 1998

[7] E. Rescorla RTFM Inc., “Rfc 2631 Diffie-Hellmann Key Agreement Method”, June 1999

[8]http://www.bibmath.net/crypto/index.php?action=affficheandquoi=modern e/rsa, last consulted on January 4, 2013

[9]http://en.wikipedia.org/wiki/Station-tStation_protocol, last consulted on January 10, 2013

[10] Khaled Al_Sultan, Magdy Saeb, Medhat Elmessiery, Usama Abd El-Raouf Badawi, “A New two-pass key agreement protocol”, 2005

[11] Hugo Krawczyk HMQV: A High-Performance Secure Diffie-Hellman Protocol, July 2005

[12] Blake-Wilson S., Menezes A. “Unknown Key-Share Attacks on the Station-To-Station (STS) Protocol” 1999