Performance Analysis of Internet Key Exchange Algorithms on IPSec Security Association Initiation

Supriyanto Praptodiyono*[1], *Moh.* Furqon[1], *Alief* Maulana[1], *Iznan* H. Hasbullah[2], *Shafiq* Ul Rehman[3]

[1]Universitas Sultan Ageng Tirtayasa, Indonesia
[2]Universiti Sains Malaysia, Malaysia
[3]Singapore University of Technology and Design, Singapore

Abstract. Naturally, the Internet as an open network allows millions of users to interact each other. Furthermore, the giant network vulnerable to various malicious activities that potentially causes many (losses) for both resources and humanity. In order to reduce the potential attacking activities, Internet Engineering Task Force has standardized a network level security so-called IP Security. The key process behind the IP Security is a Security Association that is identified by Security Parameter Index. The initiation of Security Association performance depends on the encryption algorithm used. Hence, the performance of the algorithm candidate is an important consideration. This paper aims to evaluate some encryption algorithm to be used in IPv6 network. Results of the experiments shows that ECP 384 based on the elliptic curve algorithms outperforms than the traditional algorithm such as MODP 1024 and MODP 3072.

1 Introduction

Nowadays, the Internet as the giant computer network has connected millions of people around the world. The network is able to share information to all users every time and everywhere. The emerging of the Internet gives the human many benefits and advantages such as ease of accessing information, remote communication, entertainment and so forth. However, but this technology also opened many vulnerabilities and risks that can make losses for both resources and humanity. Security holes on the Internet network include data theft, identity fraud, privacy theft and denials of service [1]. Since the Internet network includes a variety of sensitive data that is very important, both for individuals and organizations, it needs a high security system. Even though, it is almost impossible to get very high security without any vulnerabilities [2], the security system used is at least able to handle one of the security threats that exist in the Internet. Hence, the users can use the security system based on the vulnerability.

[1] Corresponding author: supriyanto@untirta.ac.id

There are three aspects on the network security including confidentiality, data integrity and availability. Currently there are several methods in network security to serve the three aspects. The method is usually developed based on the security hole that will be faced. One of the methods used in network security is the IP-Based security system [3]. This protocol can co-exist with IP datagrams to support secure data transmission over unprotected public networks. IPSec is a set of protocols that provide security for Internet communication on the network layer [4]. The most common use of IPSec is to provide a virtual network or VPN (Virtual Private Network) that is used between gateway-to-gateway, host-to-host, or end-to-end [5]. IPSec consists of several subprotocols, they are Authentication Header (AH), Encapsulating Security Payload (ESP), and Internet Key exchange (IKE). AH and ESP aims to provide cryptographic services, while IKE handles the Security Association parameter management.

One of the considerations on the implementation of IPSec with IKEv2 is the selection of key exchange cryptography algorithms. This is very important because the key exchange is the process of connecting two or more hosts that want to connect in a secret communications network but through the public network without having to enter into an agreement between the parties involved. In addition, choosing the right key exchange algorithm will affect the performance of the exchange speed, the performance of the encryption strength and the performance of the network itself. This research will evaluate some candidates to obtain the best cryptographic algorithm to be implemented on IPSec and IKEv2.

2 Overview of IPSec

IPSec is a security standard for the use of Internet-based communication protocols by encryption or authentication of all passing IP packets [6]. IPSec is designed as a cryptographic protocol that works for data security and key exchange. The IPSec protocol is implemented into the network layer. IPSec has two modes in operation, which are the transport method and tunnel method. Transport Mode is commonly used for end-to-end communication. Transport Mode provides data security or is called IP Payload which consists of TCP/UDP headers and data, via AH or ESP protocol. This payload is encapsulated by headers and trailers from IPSec. IP Header originated intact, the IP protocol field changed to ESP or AH and the contents of the original protocol will be stored in the IPSec trailer and will be returned when the packet is decrypted.

Tunnel mode is the default mode used in IPSec that is used to secure all IP packets, the packet is encapsulated and encrypted and then added a new IP header and sends it to the other side of the VPN tunnel. The tunnel mode is commonly used between the gateway or on the end-station to the gateway, this gateway will serve as the proxy of the host using this mode. In tunnel mode an IPSec Header (AH or ESP Header) is inserted between IP headers and the upper layer protocols.

2.1 Security Association

IPsec requires some values on some of its security parameters in order to operate properly. Hosts that communicate within a virtual network will share the same situation and parameters previously negotiated before building a virtual network session. The creation of security parameters in IPsec is done through a mechanism called security association (SA) [7]. SA controls the data traffic of security protocols in one direction. As an illustration, one SA can control the ESP protocol data traffic from host A to host B, but it takes another SA to control traffic from the opposite direction. Hence, a SA pair is required for each protocol used, one for input and one for output. If a VPN session uses the ESP protocol, then each

endpoint will use two SAs. After the negotiation, then SA will be applied to the protocol concerned. IPsec stores SA data in a database called SAD (Security Association Database).

2.2 Internet Key Exchange Version 2 (IKEv2)

IKEv2 (Internet Key exchange version 2) is an updated of the old IKE protocol and a standard defined in RFC 7296. IKEv2 is a protocol used to perform SA management tasks such as creation, renewal, and deletion [4]. IKEv2 uses the Diffie-Hellman exchange technique to create a shared secret, which will be used to generate derived cryptographic keys. The IKEv2 header format is shown in Figure1. In addition, IKEv2 is responsible for performing authentication functions on each party that communicates. IKE messages on IKEv2 protocol implementation using UDP port 500 and port 4500. Each UDP packet contains one IKE message. If the message is sent using the UDP port 500, then the IKE message is exactly after the UDP header. Whereas if sent with UDP port 4500, then IKE message preceded by four octets (32 bits) of zero. These four octets of zero are not part of the IKE message and are not included in the length field or checksum. Each IKE message starts with an IKE header followed by IKE payload in accordance with the identification of the Next Payload field in the IKE header or the previous payload.

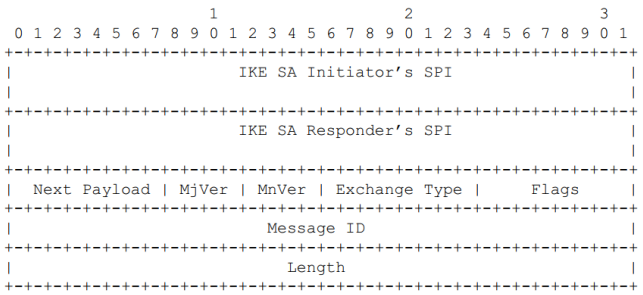

Fig 1. IKEv2 Header Format

The key exchange algorithm used for internet key exchange applications (IKEv1) originally used a collection of Diffie-Hellman algorithms called the Oakley Group [8]. There are 4 main groups used, two of which are MODP group and the other are ECN group. This key group is estimated to have the power equivalent of a symmetry key algorithm with 70-80 bits, while for the Internet Key Exchange Version 2 (IKEv2) application, based on the RFC7296 standard document defines two Diffie-Hellman groups, 768-bit MODP Group and 1024-bit MODP Group.

However, based on the update contained in RFC 8268 documents [9] the United States Information Assurance Directorate (IAD) at the National Security Agency (NSA) dealing with National Security Systems (NSS) published "Commercial National Security Algorithm Suite and Quantum Computing Frequently Asked Questions ". The document states that based on the security interests of using MODP Group of less than 2048-bit size is no longer recommended. In the document also, the user must select the DH group that has been formed strongly and has met the minimum needs and have been validated. The suggested DH Group examples are:

- Elliptic Curve with P-384 group size
- RSA modulo with minimum size of 3072 bits
- MODP Group with a size of at least 3072 bits

3 Network Topology

In order to evaluate the cryptography algorithm on IPSec with IKEv2, a limited network topology was setup as shown in Figure 2. The network system was built by IPSec writer based on IKEv2 protocol using strongSwan software. After the IPSec system has been established, the next step is to conduct experimental testing, at this stage the test is done by replacing the key exchange cryptography algorithm used in IKEv2, this is done to find the best algorithm in terms of performance and security strength that can be applied to the system. In this experiment will determine the best key exchange algorithm that can be implemented on IPSec by considering the performance of algorithm and network performance.

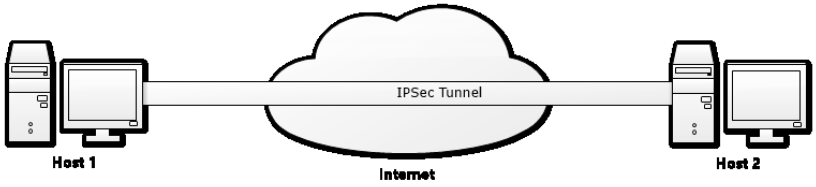

Fig 2. Network Topology

Experiments were conducted to test key exchange cryptographic algorithms running on an IPSec system. There three candidates of algorithms as follows:

1. 1024-bit MODP, an algorithm that has been widely used and no longer recommended
2. 3072-bit MODP, the size increase algorithm from the 1024-bit MODP and it is one of the recommended algorithms
3. ECP 384 bit, a lightweight elliptic curve algorithm and recommended for use as a key exchange algorithm.

4 Result and Discussion

This section provides results of the experiments that was discussed in Section 3. The candidates were implemented at IPSec system to get some parameters such as key exchange speed and network throughput. Experiments have been performed on the network topology for the 1024-bit MODP, 3072-bit MODP and ECP 384-bit respectively.

4.1 Key Exchange Speed

In this first experiment, the test was conducted to do one pair key exchange generation, by measuring the time required to generate the key. This test is purely to measure the performance of the algorithm that has not been implemented into the IPSec system. Table 1 shows the result of key formation experiments on modp1024, modp3072 and ecp384 algorithms for 10 times. In the table, the results with the shortest time, achieved by ecp384 with time less than 0.01 seconds, followed by modp1024 and the last position modp3072.

Table 1. Time Statistics for Key Exchange Generation

Parameter	modp1024	modp3072	ecp384
Mean (s)	0,0172	0,0718	0,007
Min (s)	0,017	0,07	0,007
Max (s)	0,019	0,072	0,007
Standard Deviation	0,001	0,001	0

It can be spoken that the ECP Group algorithm is a relatively more lightweight algorithm compared to the MODP Group. The table also shows that MODP1024 is faster than MODP3072. This because processing of larger bits size requires more time to form a key. It was found that ecp384 had the most superior results compared to other tested algorithms. The ecp384 has the smallest time for the average of key generation time (mean), min key generation as well as max key generation time. The standard deviation of ecp384 shows the value 0 that indicates the data of key generation time for ecp384 has a high stability. Based on this experiment result and analysis on the key generation speed can be concluded that the ecp384 algorithm is the most lightweight from the three candidates.

4.2 Throughput

As discussed in the previous subsection, the key exchange speed is measured to select one of the most lightweight algorithms to be implemented in IPSec. Further, this subsection provides results of IPSec implementation using the three candidates. This is done to know the impact of the key exchange algorithms implementation on the network performance especially on the network throughput. This is to know the actual bandwidth consumed by the network when implementing IPSec using the three key exchange algorithms.

This second experiment includes the plain scenario that means data transmission without IPSec as the reference. This is to know the impact of IPSec implementation using the three candidates on the network throughput. The experimentation results are shown in Table 2. The table consists of four columns: plain, modp1024, modp3072 and ecp384.

Table 2. Network Throughput of IPSec Implementation

Parameter	plain	modp1024	modp3072	ecp384
Mean (Mbit/s)	31,67	19,81	17,3	23,39
Min (Mbit/s)	29	15,6	14,8	19,8
Max (Mbit/s)	37,5	23,5	20,7	27,6
Standard Deviation	2,32	2,52	1,49	2,24

The plain scenario as the reference has the highest throughput because there is no IPSec implementation meaning no overhead on the transmission. Compared to the plain throughput, the nearest value is obtained by the ecp384. The average value of network throughput shown by the ecp384 is 23,39 Mbps or 26% lower than the plain. This is considered as the nearest one compared to the modp1024 that has 37% lower and the modp3072 that has 45% lower. Hence, the ecp384 has the smallest difference compared to the plain scenario. That can be seen on the table the minimum and maximum value of the ecp384 also shows the nearest value to the plain scenario.

From the two experiments, there are found that the ecp384 algorithm is superior to the other candidates. The first experiment shows this algorithm has the smallest generation time that means this is the most lightweight algorithm. The second experiment also shows the

IPSec implementation using ecp384 has the highest network throughput compared to other candidates. At the same time, this algorithm shows the nearest value to the plain scenario. In other word, the IPSec implementation using ecp384 only adds 26% overhead to the plain scenario. This can be concluded that the ecp384 algorithm is the most suitable algorithm to be implemented on IPSec security association. Further, the IPSec implementation using ecp384 can be faster than the current implementation that still using modp1024 algorithm.

5 Conclusion

IPSec is a network layer security protocol that has implemented on the Internet. The protocol consists of some other protocol such as AH, ESP and IKEv2. The implementation of IPSec requires a security association that needs a key exchange. The current IPSec implementation uses modp1024 algorithm on its key exchange. However, the algorithm is considered as heavy if implemented on mobile devices that has limited energy. Furthermore, there is required to find out another algorithm that more lightweight.

The selection of key exchange cryptography algorithm applied to IKEv2 has found that the ecp384 is the most lightweight of the three. The 384-bit cryptography of Elliptic Curve Group Modulo a Prime (ECP) is able to offer the best performance in terms of key generation performance, cryptographic performance applied to IPSec and network performance in general, compared to other cryptographic algorithms. However, there needs to do a next research on the implementation of the selected algorithm on mobile technology.

References

1. A. Marwa, B. Malika, and G. Nacira, “Contribution to enhance IPSec security by a safe and efficient internet key exchange protocol,” 2013 World Congr. Comput. Inf. Technol. WCCIT 2013, pp. 1–5, (2013).
2. P. Lubomski and H. Krawczyk, “Practical Evaluation of Internet Systems’ Security Mechanisms,” IEEE Secur. Priv., vol. 15, no. 1, pp. 32–40, (2017).
3. J. L. Shah and J. Parvez, “Impact of IPSec on Real Time applications in IPv6 and 6to4 Tunneled Migration Network,” ICIIECS 2015 - 2015 IEEE Int. Conf. Innov. Information, Embed. Commun. Syst., pp. 0–5, (2015).
4. C. Kaufman, “Internet Key Exchange Protocol Version 2 (IKEv2),” RFC 7296, pp. 1–142, (2014).
5. S. Frankel, “IP Security (IPSec) and Internet Key Exchange (IKE) Document Roadmap,” RFC 6071, pp. 1–63, (2011).
6. R. S. Pavel, Network Security Advance, vol. 3. Mumbay: University of Mumbay, (2015).
7. B. A. Forouzan, Data Communications and Networking Third Edition. New York: McGraw-Hill, (2003).
8. D. Harkins, “The Internet Key Exchange (IKE),” RFC 2409, (1998).
9. M. Baushke, “More Modular Exponentiation (MODP) Diffie-Hellman (DH) Key Exchange (KEX) Groups for Secure Shell (SSH),” RFC 8268, (2017).