http://dx.doi.org/10.14400/JDC.2014.12.8.243

Issues and Security on IPSec: Survey

Sunghyuck Hong

Baekseok University, Division of Information and Communication

IPSec 보안 이슈와 대응 방안

홍성혁

백석대학교, 정보통신학부

Abstract IPSec provides two services that are authentication header and Encapsulating Security Payload(ESP). In this research work, security issues on the Internet and the basic concept of IPSec are described. Security issues on the Internet are presented and proposed a possible solution for DDoS attack using IPSec. Therefore, this research will be able to contribute for building secure communication against DDoS attack.

Key Words : Cryptography Protocol, Cryptography communication, VPN(Virtual Private Network), Encapsulating Security Payload (ESP), IP Security

요 약 IPSec은 네트워크상에서 안전한 통신환경을 제공하기 위해 사용하는 보안 프로토콜로, 헤더 인증(Authentication Header)과 데이터와 송신자를 인증하는 Encapsulating Security Payload (ESP) 서비스를 제공하며, 이에 대한 기본적인 개념과, IPSec의 종류를 알아보고 활용되는 방법에 대해서 조사하였다. IPSec 프로토콜이 악용되었을 때의 문제점과 그에 대한 대응책을 알아보고 IPSec을 통한 DDoS 공격에 대한 해결방법을 제시하여 IPSec 프로토콜 사용을 통한 안전한 통신환경을 구축하고자 한다.

주제어 : 통신 프로토콜, 암호화 통신, VPN, ESP, IP Security

1. Introduction

Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPsec includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session. IPsec can be used in protecting data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host)[1].

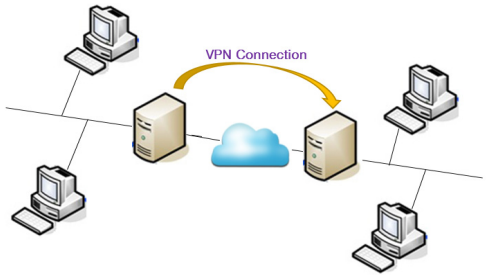
Internet Protocol security (IPsec) uses cryptographic security services to protect communications over Internet Protocol (IP) networks. IPsec supports network-level peer authentication, data origin authentication, data integrity, data confidentiality

* This research is supported by 2014 Baekseok University research fund.
Received 11 June 2014, Revised 25 July 2014
Accepted 20 August 2014
Corresponding Author: Sunghyuck Hong(Baekseok University, Division of Information and Communication)
Email: shong@bu.ac.kr

ISSN: 1738-1916

(encryption), and replay protection.

Further, it is not only the provision of the basic elements of secure communication, and means of protection against IP Spoofing attacks. Connection of network layer logic through the Hand Shaking process for communication: Establish a (SA Security Associaton), by using a SA that is created, you can share key, the encryption algorithm, and help for mutual authentication.



[Fig. 1] IPSec Overview

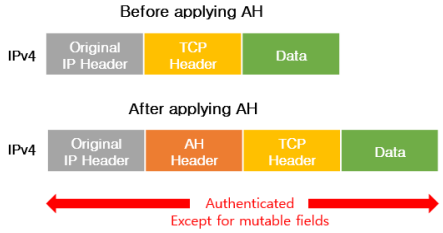
2. IPSec protocol

IPSec consists of Authentication Header (AH) provides a user who is a authorized person, ESP(Encapulating Security Pay-load), and IKE (Internet Key Exchange) protocols. AH also provides data authentication and data encryption for protecting from unauthorized users[2]. IPSec is being developed on an ongoing basis for processing security of network communication and network communication[12]. The proposed IPSec implementation attempts to ensure data communication security. Sending and receiving data packets with IPSec needs more time as compared to sending data packets without IPSec. Between AH implemented and ESP implemented data packets, ESP implemented data packets consume more time due to handling encryption. The simulation result of this research also shows the similar result that the research expects theoretically. If an application needs only authentication, then this research proposes to use only AH-implemented data packets with minimum time overhead. The research encourages implementing IPSec with ESP for all security services with moderate time overhead[11].

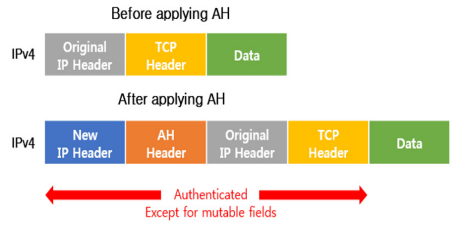
2.1 Authentication Header protocol

AH will provides us with the security services of the sender authentication of the data against intruders. Further, it is possible according to the selection of the recipient. However, it also provides protection against replay attack from attackers. The AH can provide authentication of the IP header of a number as possible, it is also provided when they are in sealing the outside of the IP header AH.

Status of integrity protection can be known by using the Hash value generated by the (MAC) algorithm Message Authentication Code fixed. The Hash algorithm general, while generating a Hash value at a base of only Message, MAC algorithm will generate a Hash value is placed on the basis of the private key Message.



[Fig. 2] AH Protocol Tunnel mode



[Fig. 3] AH Protocol Transport mode

Hash values generated in this way is added to the packet, it transmits to others packets, so that with a password of public and regenerate the Hash value of the packet to the other party. It is possible to verify

that to compare the Hash value own a Hash value then stored in the packet is created, the value you get the same, the contents of the transfer processing of the packet has not changed it means that the integrity of the protection value (integrity protection) is come out are those had not been, it makes them discard the packet in question. In order to solve these problems, several values that are changed on a regular basis as described above, except when generating the Hash value in the MAC algorithm. For this reason, is not compatible with the NAT AH protocol. Because, IP address is because is changed by NAT. The NAT (Netwotk Address Translator), a feature that by using the address allocation mechanism, us to convert the IP address of the global network, the IP address of the private network, the saving of IP addresses such as routers and firewalls, are built is used for the purpose[3].

2.2 Capsule Security Payload protocol (ESP: Encapsulating Security Pay – laod)

AH provides integrity and authentication of IP but, ESP to provide data encryption and integrity check in addition to authentication of data. Encryption of this data provides data confidentiality. All features of AH is included ESP, which is encrypted, it is to prevent attacks on the data that has not been authenticated[7]. ESP is using (null) encryption null. The null encryption though similar to AH except the authentication of the IP header, the NAT permit transfer possible address of the IP header is so varied.

First, IPSec has provided a packet encryption, but from the second version, I was not only provides encryption, also protection of integrity with authentication. However, the authentication of these, the outermost of the IP header was not previously the protection of integrity overall.

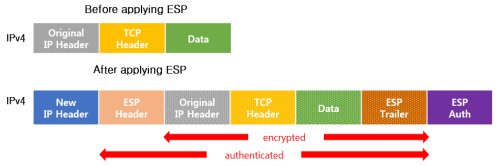
Encryption, so you can be disabled using the null ESP encryption algorithm, if it represents specifically in the IPSec ESP version of the initial in most cases[8].

IP payload is encrypted for check consistency soon as it receives a packet that, after completing the integrity verification process soon as it receives a packet, encryption of the data payload of the packet is released.

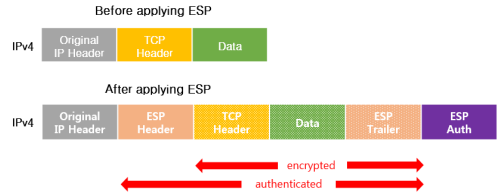
2.3 IKE protocol

IKE is a protocol for creating a security-related settings and manage to negotiate. Is called (Security Association) SA security settings applied to IPSec connections, to generate the SA, IKE is implemented through the following elements.

- Main Mode: six messages exchange
- Aggressive Mode: three messages exchange
- Quick Mode: generating SA instead of the IKE protocol
- Informal
- Group



[Fig. 4] ESP Protocol Tunnel mode



[Fig. 5] ESP Protocol Transport mode

Quick Mode (Quick mode) is protected message exchange is encrypted by the IKE SA, but to create an IPSec SA in Quick mode for that, through a message exchange of aggressive mode or main mode, IKE SA has previously must be set. IKE is a synthetic protocol that works with ISAKMP to obtain the keying material that is authenticated for use with ISAKMP SA and used in IPSec, using some SKEME of (Security Key Exchange Mechanism) and part of Oakley is. As a step for the key exchange and authentication, ISAKMP is

provide us with steps 1 and 2.

Oakley refers to the key exchange mode is a free-form that allows each object to advance the state of the protocol to match the pace of their own.

IKE to generate the SA over the two stages.

- IKE Phase 1 (IKE SA): key exchange to generate the SA
- IKE Phase 2 (IPSec SA): key exchange that defines the use of SA is IPSec protocol Ring[3].

It is required in addition to the elements provide basic communication security, IPSec, it will be a defense against IP spoofing (IP Spoofing) attacks. Using a VPN ((Virtual Private Network), IPSec is an efficient access can be for the user.

3.1 VPN (Virtual Private Network) remote access

The Internet is a network that can be shared by everyone. Further, VPN is a technology that is able to help to be able to use the private network as a (Private Network) to the user the public network.

The network boundary point, IPSec VPN system, it is possible to configure a virtual private network between the IPSec VPN gateway and IPSec VPN system of Gateway to Gateway types that make up a virtual private network with IPSec VPN between gateways that are connected to the router there is a system of IPSec VPN Client to Gateway types can. Electrons, have the advantage of not requiring any work or change the installation of additional programs as required by the configuration of IPSec VPN on the user side. It has the advantage of being able to provide a service to connect to the corporate network outside the road which can provide security services practical, user or telecommunication, IPSec VPN Later systems[4].

In order to use the public Internet network, VPN was supposed to be operating costs are cheaper than leased lines, and to solve the problem of limited use location.

While it is necessary to increase the line where the private network requiring an external connection, VPN, which then provides the security services and connectivity using tunneling techniques in a public network connected to the conventional[9].

In summary, to maintain security by encrypting the data, VPN, can also additional configuration of a variety of custom services. Access VPN service is well suited for companies that need to be building a network of branch offices and head office and small offices.

3.2 e-commerce (EC: Electronic Commerce)

With the help of the Internet, when commerce between companies, between individuals, e-commerce, can be seen to be an important technology for ensuring the safety of trade and mutual trust between the buyer and seller.

For the development of cyberspace virtual equipped with new technology to the spread of the Internet, e-commerce over the Internet has spread rapidly in recent years.

(Stands for Internet protocol version 4, 4th edition Internet Protocol) IPv4 is a technique by adding an IPSec to and the security environment for the network itself, VPN the aforementioned managing certificates and public keys via a network Public Key Infrastructure PKI for us to is a structure in which the technique is used for the electronic signature, based on the protection of information in order to ensure the integrity of the public key and the confidentiality of the public key encryption algorithm.

The PKI, is used for authentication and secure communication against an unspecified large number if the VPN using IPSec, and is used for communication with the other party already know. In this case, the different populations, in order to use the client and different servers, there is a difficulty in connecting easily. Therefore, a method that may be linked to PKI and IPSec is required.

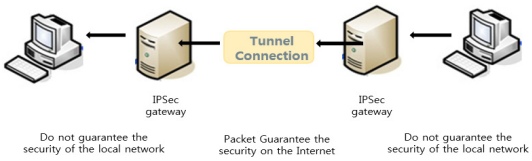
While it is used efficiently, IPSec, has a security issues.

IPv6 that would make me solve the problems of IPv4 is the Internet standard was announced but, IPSec security technology was not considered IPv6 in IPv4 was included. In order to use the tunnel mode is either a mode of IPSec, IPSec gateway is required.

For processing encrypted packets in the tunnel mode of IPSec, if the traffic of the opposite occurs, the IPSec gateway becomes the processing time increases dramatically. This shows the vulnerability to DDoS attacks IPSec gateway. Next, let's examine the problems and solutions of IPSec.

4.1 Security issues for the DDoS attacks

As shown in the figure 6 below, in tunnel mode, place the IPSec gateway, help me to be able to send and receive encrypted packets. At this time, it is protected IP header of the packet is encrypted, the IPSec header newly added, IPSec gateway address is expressed.



[Fig. 6] IPSec gateway

4.2 DDoS attack solution for the problem

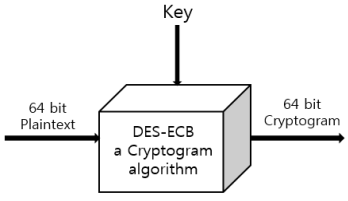
In order to solve this problem, the paper, the reference can not afford IPSec gateway only when the traffic is, assume that traffic was over. Assumed by the above is determined that traffic is generated, the priority-based algorithm is used to randomly discarded IPSec packet is a normal service, so that it can maintain only the traffic inflow. This is followed by a random period of time by using the statistical information of the packet to receive normal service in the white list to create a list of source address and can not afford the traffic packet is not included in the white list, the packet is discarded oriented. The priority value is 1 or more, would target. By using this method than before application After application of the results observed by most attacks was confirmed that the packet is discarded[5].

4.3 ESP protocol

A major role in both IPSec protocol packets in the AH provides authentication and integrity, in addition to the functions provided by ESP encryption is to be added[6,7].

IV (Initialization Vector, the initialization vector) used in the encryption algorithm in the ESP DES-CEC provides encryption of the data in a mode to be used when the initial value.

The first ESP packet is XOR with IV, the encryption is whereabouts, ESP packet to the receiving side, the received packets are then decoded using the IV. ESP IV are included in a payload portion of the packet receiving side is received IV to research in order to decrypt the encrypted data back to the IV value is not encrypted, as it is sent to the publicly exposed. Therefore, a lot of risks, makin transmission even slightly changed, the IV value of the decoding is possible at the receiving side, and in some cases to change the level information of its upper serious problem arises. This problem is to provide data encryption and IPSec security vulnerability in the large. IV In order to overcome the vulnerability to attacks by changing the IV takes place a great deal of research is being conducted[10].



[Fig. 7] DES-ECB The encryption process

4. Conclusion

Authentication is a building block for establishing secure communication because anonymous communications can cause DDoS attacks, and DDoS attacks use a normal request, and there is no effective solution. IV is encrypted using the ECB mode and the ESP payload contained therein, and IV by applying the message authentication, and data integrity checking method IV is also presented. Therefore, this research will be able to contribute for building secure communication by using a IPSec protocol.

ACKNOWLEDGMENT

This research is supported by 2014 Baekseok University research fund.

REFERENCES

[1] Kent, S.; Atkinson, R.. IP Encapsulating Security Payload (ESP). IETF. RFC 2406, November 1998.

[2] Juhyuk Kim; Myungmook Han. "A Study of the NATted Host Identification Algorithm Using Pattern Analysis from Extended IP Header Information". Proceedings of KIIS spring Conference 2011 Vol.21. No.1. pp. 42-43. Apr. 2011

[3] TaeSeok Jin, "Protocol and Algorithm Trend for IPSec Technology", 2011 spring conference proceedings of 'Korean Institue of Intelligent Systems' Vol.21, No.1, pp.221-224, Apr. 2011

[4] Myunghee Kang; Hwangbin Ryou; Future System, Inc; Kwangwoon University. "An User Authorization Mechanism using an Attribute Certificate in the IPSec-VPN System". Institute of Information Security Vol.14. No.5. pp.11-21. Oct. 2004

[5] Junghym kim; Youjip Won; Eulgyu Im, "A security problem and its solurion in IPSec", 2006 summer conference of The Institute of Electronics Engineers of Korea Vol. 29, No. 1, pp.57-58, 2006

[6] Youngji Lee; Taiyun kim, "The problem resolution algorithm in ESP protoco", The KIPS transactions. Part C Part C c9(2), pp. 189-196, 2002

[7] A. Nascimento et al., "Can I Add a Secure VoIP Call?" Proc. 13th IEEE Int'l Conf. Networks, vol. 1, 2005, pp. 151 - 155.

[8] R. Rajavelsamy et al., "Performance Evaluation of VoIP over 3G-WLAN Interworking System," Proc. IEEE WCNC, vol. 4, 2005, pp. 2312 - 2317.

[9] D.P. Hole and F.A. Tobagi, "Capacity of an IEEE 802.11b Wireless LAN Supporting VoIP," Proc. IEEE Int'l Conf. Comm., vol. 1, 2004, pp. 196 - 201.

[10] W. Wang, S.-C. Liew, and V.O.K. Li, "Solutions to Performance Problems in VoIP over a 802.11 Wireless LAN," IEEE Trans. Vehicular Technology, vol. 54, no. 1, 2005, pp. 366 - 384.

[11] doi: 10.1109/ACCT.2012.64

[12] doi: 10.1109/LCN.2007.103

홍 성 혁(Hong, Sunghyuck)

- 1995년 2월 : 명지대학교 컴퓨터공학과 (공학사)
- 2007년 8월 : Texas Tech University, Computer Science (공학박사)
- 2012년 3월 ~ 현재 : 백석대학교 정보통신학부 교수
- 관심분야 : 네트워크 보안
- E-Mail : shong@bu.ac.kr