Research on Network Security Based on IPSec

Yanru Liu

Information Technology and Media Department of Beihua University in Jilin

2268723407@qq.com

Keywords: IPSec; Network security; IPV6; Security protocol; Communication

Abstract. With the development of information technology, Network security issues are very prominent, Network security incidents occur frequently. In order to enhance network security, we must take certain measures that are the use of IP protocol. IP protocol also called Internet Protocol. As defined in the network layer in the internet important agreement, is the current implementation of the network communication between the computer requirements. As a security model, IPSec is based on end-to-end trust and security between the source IP address and the destination IP address. IPSec network transmission protocol is developed mainly to solve the network layer security issues, and IP protocol to improve the confidentiality and integrity. It is necessary to apply the IPSec to the new IPv6 network protocol. Through the use of IPSec, you can build a more secure and reliable network environment, which provides more spaces for the development of the Internet and e-commerce.

The Importance of Network Security

From the 1998, the period of rapid development of the Internet to the present, with the constant development of information technology, Network information security has become a hot topic in the 21st century. Network security issues emerge in an endless stream, such as in August 2003, the virus of worms make use of Microsoft's system vulnerabilities attack 80% of the global Windows users. There are many examples in China, such as Panda case. In the *2015 China Internet Network Security Report* that published in May 25 2015, network security incidents up to 12,616, that’s a 125.9% increase on last year. At present, the Internet develops rapidly, but the corresponding speed of security measures cannot keep up. Network security incidents occur frequently; we should realize the seriousness of this problem and strengthen the research of Network Security.

Using IPSec to guarantee network security. The full name of IPSec is Internet Protocol Security. It is an effective method to solve the network security problems. IPSec can provide a variety of security services, mainly includes the following aspects: data privacy, data integrity based on a connectionless, packet source authentication, access control, anti-retry attacks, privatization and some degree of data traffic. The above-mentioned security services are mainly achieved through the two security protocols, ESP (Encapsulating Security Payload) and AH (Authentication Header).

There are two ways to implement Internet protocol security. The first one is to achieve in the gateway. The second one is to implement on the host. However, regardless of which method to implement IPSec, when the IPSec interface has an IP packet to enter or leave, IPSec will take different treatment to this package based on the SPD (Security Policy Database). There are three kinds of IP packet processing in IPSec: drop, bypass, and IPSec processing according to the security association. It is particularly easy to implement for the access control security of the firewall in IPv4. When an IP packet is sent to an interface, the first step is to look at the properties of the IP packet and the associated security settings. And then to find the appropriate security settings in the SAD (Security Association Database), decode this IP packet, then you can find the corresponding security policy stored in the SPD. Then you can find the corresponding security policy stored in and SPD. If the security policy of IP packet can be found in SPD, we should deal with the IP packet in accordance with the provisions of security policy, generally divided into three cases, the first way is discarded. It means that deal with the package in accordance with the regulation, at the same time, logs are also logged. The second way is bypassed. The so-called bypass is to let the IP packet through, and don’t do other processing. The third way is IPSec processing. The main dealing way is to find the corresponding security association (SA) in the SAD by one or more security association pointers of the corresponding packet, and then according to the SA corresponding to the operation of the IP packet processing. Of course, if the corresponding security policy is not found in the SPD, it will directly discard the IP packet and record the log.

The basic structure of IPSec is use Authentication Header (AH) and Encapsulated Security Payload (ESP) to achieve data authentication and encryption. The former is used to achieve data integrity; the latter is used to achieve data confidentiality. At the same time, the data transmission provides two modes: transmission mode and tunnel mode. In the transfer mode, a new IPSec header (AH or ESP) is embedded between the IP header and the upper protocol header. In the channel mode, the entire IP packet that to be protected is encapsulated in another IP packet, while embedding a new IPSec header between the external and internal IP headers. Both IPSec headers can operate both in transport mode and in tunnel mode.

Working Mode of IPSec under the Agreement of IPv6

The Use of AH. AH（Authentication Header） agreement, which is what we called IPsec Authentication Header. Its main function is to protect the content of the data packet, so that the contents of the packet are not easy to tamper, but will not prevent eavesdropping. It is possible to transmit the non-confidential data. The working principle of AH is mainly operating the data packet, it will add an AH packet header in the packet. The main content of packet header is hash; the hash is a secret key. Its calculation method uses the entire data packet, if the hacker modifies the data packet, the content of hash and packet is inconsistent, it will result that data packets will not be accepted and the security of network can be protected. The security model it provided is mainly used for data authentication, and will not encrypt the data, detection of data integrity testing to prevent the replay of the situation.

There are two working modes of the AH protocol, the first is transmission mode, the second is tunnel mode. The transmission mode structure of the AH protocol is shown in Table 1

Table 1 Transmission mode structure of IPv6 AH

IP header	Extended header	AH header	Destination Options	load

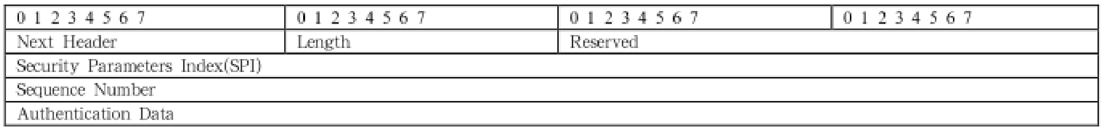
The second type is to encapsulate the original packet with a new packet, the original data packet become the load of a new packet. After these conversions, the resulting new packet is called a tunnel packet. Table 2 shows the tunnel mode packet structure.

Table 2 tunnel mode of IPv6 AH

New IP header	Extended header	AH header	The raw IP header	TCP	data

AH in the two modes of the header format is consistent with the structure shown in Table 3.

Table 3 Packet headers under AH protocol mode



0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7
Next Header	Length	Reserved	
Security Parameters Index(SPI)			
Sequence Number			
Authentication Data			

The most important component is the Security Parameters Index in the AH header format, also called SPI, which is combined with the IP address to identify the important parameters of security association, the number of bits is 32 bits. Authentication Date is the result of the authentication algorithm of the protected field after the AH protocol. Length is variable length and it is determined by the authentication algorithm. The function of Sequence Number is equivalent to a counter, mainly used to prevent replay.

AH does not provide encryption services, only provide certification. AH authentication almost protects the entire IP data packet, covering the basic packet header and packet header extension. There are also fields that may not change during transmission.

The Use of ESP. ESP, that is the package safety load, is similar to the AH protocol. The ESP protocol also provides the authentication function for packet contents. Compared to the AH protocol, it also add the function of encryption to prevent data packets tampering.

There are also two working principles of ESP. The first is the transmission mode, the second is the tunnel mode, AH protocol In the transmission mode. Its structure is shown in Table 4.

Table 4 IPv6 ESP transmission mode structure

IP header	Extended header	ESP header	Destination Options	TCP	data	ESP tail	ESP certification

In the transmission mode, encryption range of ESP is TCP, data, ESP tail. The authentication range is ESP header, TCP, data, ESP tail. It is different from the tunnel mode that in the transmission mode, IP header is invariable; the original IP header is unprotected, unauthenticated and unencrypted.

As same as AH, the tunneling mode encapsulates the data to be protected with a new packet. The original data as a new data packet load. A new packet is called a tunneled IP packet. The structure of ESP under IPv6 shown in Table 5.

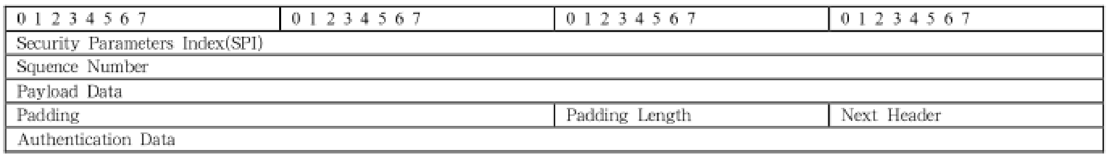
Table 5 Shows the ESP structure of IPv6

New IP header	New extension header	ESP header	The raw IP header	Raw Extension Header	TCP	data	ESP tail	ESP certification

But not the same as the transmission mode, in tunnel mode, encryption range of ESP includes the original IP header, that is to say, the encryption range is the original IP header, TCP header, data, ESP tail, its authentication range is ESP head, the original IP header, the original extension header, TCP, data, ESP tail ,The authentication function of ESP protects the original IP header, but the newly generated new IP header is not protected by authentication.

ESP protocol mode is more complex than AH protocol mode, ESP through the need to protect the data encryption to ensure the confidentiality of data and integrity, which used the secret key algorithm is a symmetric key encryption algorithm. This algorithm requires the sender and the receiver to use the same secret key to encrypt and decrypt the data. Its header format is shown in Table 6.

Table 6 Header format of ESP



0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7
Security Parameters Index(SPI)			
Squence Number			
Payload Data			
Padding		Padding Length	Next Header
Authentication Data			

ESP protocol also has Security Parameters Index as same as AH protocol, used to describe the header used by the encryption algorithm and secret key, Sequence Number as the anti-replay protection. The length of Authentication Date is also variable, and the integrity check value is stored. ESP encryption as long as it is for Payload Date, Padding, Padding Length and Next Header, Encryption is the first in the ESP, after encryption and other unencrypted part of the composition of the new IPv6 packets. ESP encryption and authentication functions are optional, but cannot choose not to encrypt and not certification, this is not allowed, encryption and authentication must choose either.

The Application of AH, ESP in PV6 Network. From the above content we can see, AH and ESP protocol common ownership of two modes, one is the transmission mode; the other one is the tunnel mode. AH transmission, AH tunnel, ESP transmission and ESP tunnel have different roles. AH, as the authentication header protocol, verifies the source and integrity of the packet, and does not provide the security service by encrypting the transmitted data. ESP not only provides the authentication function but also authenticates the data packets. Transmission mode and tunnel mode for IP header processing is different, the transport mode encapsulates the protocol header between the IP header and the upper layer protocol, encapsulates the data of the upper layer protocol and the load. The tunnel mode encapsulates the entire IP packet and generates a new IP header.

The advantage of the transmission mode is that the extra overhead is small, the efficiency of information processing is high, and the disadvantage is that the variable field cannot be protected. Tunnel mode can protect the variable field, but it is easy to cause IP packet is too long. Due to the different functions of the four working protocols, the application fields in IPv6 networks are different.

Security Association. We have realized the AH and ESP, So in practice, in the end is what determines whether we use the AH protocol or ESP protocol. It is SA that is security association.

SA is the foundation of network security. It encodes the protocol policy between two computers, prescribing algorithms and secret keys. SA related to the two databases of SPD and SADB. SPD is the security policy database and store IPSec policy. Each record of SPD corresponds to a security policy. Each IPSec policy corresponds to three types of processing: drop, bypass, IPSec is processed according to the security association. SADB is the security association database, which is composed of security association. Each SA contains the destination IP address, IPSec protocol, SPI triplet. Each record of the SA contains the following information:

Negotiated value that including the provisions of the IPSec mode of operation, that is, whether to select a transmission mode or a tunnel mode; whether the protocol selected by IPSec is AH protocol or ESP protocol; what is the encryption scheme and hash algorithm; the value of the security algorithm used.

Authentication and encryption keys

The integrity count value.

For processing of datagrams, the security policy database and the security association database are used in combination. When a device sends a datagram, firstly it should look up the policy to be used in the security policy database. If the policy requires IPSec processing, one or more security associations corresponding to the security association database are found by the pointer and the security is protected. Then send the datagram, after the datagram is received by the receiver, through the data reported in a number of column parameters to find the corresponding security association, and to make judgments on the data reported, including whether to see whether the data reported retransmission. If the packet is retransmitted, it will be discarded, if not retransmit the message, the message decryption and authentication. Through this security association, this model can guarantee data integrity and confidentiality.

Conclusion

IPSec as a security model based on end-to-end trust and security between the source IP address and the destination IP address, its role is not to be underestimated. Through the use of IPSec, you can build a more secure and reliable network environment, which provide more spaces for the development of the Internet and e-commerce.

References

[1] Y.J. Zhu, Z.H. Feng: The Principle and Application of IPSec .Computer Security.2008 (11).

[2] Y.F, H.J:The Latest Development of IPv6 Technology Standard ,Proceedings of the Conference on Next Generation Internet and Application (In Chinese ,2011).

[3] CF Xie, S.Q Zhao and H.L: From the evolution of the architecture of the Internet to see the development of IPv6, next-generation Internet and Applications Symposium (In Chinese, 2011).

[4] Q.F, H.G. Zhang: On the next generation of IPv6-based Internet security protection, the second national information security rating protection system construction Conference Proceedings (In Chinese, 2012).

[5] L.Z: IPv6 testing international certification and the latest progress, next-generation Internet and Application Symposium Proceedings (In Chinese, 2011).

[6] J.Y. Liu: Using IPSEC rules to create a secure network environment, Computer Knowledge and Technology: Experience, 2015 (9), P.116.

[7] L.G: IPSec protocol for the AES-128-CBC algorithm high-speed hardware design, Southeast University, (In Chinese, 2015).

[8] B.T.Liu: Based on IPSec network security protocol research and implementation. University of Electronic Science and Technology, (In Chinese, 2010).

[9] J.M.Lan, C.L: Analysis and suggestion of AH and ESP protocol in IPSec . Computer Technology and Development, (2009),P.15

[10] J.C. Cheng. IP packet network security analysis and IPSec technology. Computer and Network, 2010, 17: 42-43.