© 2017 IJSRST | Volume 3 | Issue 6 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

Internet Protocol Security as the Network Cryptography System

Haryanto[1], Andysah Putera Utama Siahaan[2], Robbi Rahim[3], Mesran[4]
[1]*Faculty of Engineering, Universitas Pembanguan Panca Budi, Medan, Indonesia*
[2]*Faculty of Computer Science, Universitas Pembanguan Panca Budi, Medan, Indonesia*
[2]*Department of Health Information,, Akademi Perekam Medik dan Infokes Imelda, Medan, Indonesia*
[4]*Department of Computer Engineering, STMIK Budi Darma, Medan, Indonesia*
[2,3]*Ph.D. Student of School of Computer and Communication Engineering, Universiti Malysia Perlis, Kangar, Malaysia*

ABSTRACT

Internet Protocol Security (IP Security) is a security protocol that serves to secure information in the event of an exchange on the internet. It happens if there is a connection between private IP and public IP. This protocol will exchange packets on the IP layer safely. It provides two types of encryption options, transport, and tunnel. Transport mode will encrypt the data section without changing the packet header. The algorithm used to encrypt data is a symmetric cryptography algorithm. This protocol authenticates and encrypts every packet from a data transmission session. Also, it can generate keys between the sender and the recipient at the first time it is activated and can negotiate the cryptographic keys that will be used during the session. IP Security is an end-to-end cryptosystem that works at the internet layer of the Internet Protocol Suite. The protocol serves to protect the data flow in host-to-host, network-to-network, and network-to-host as well.

Keywords : Network Security, IP Security, Cryptography

I. INTRODUCTION

The first computer network was created to exchange data on internal connections only. Along with its development, computer network developed to be able to share information globally; then it is the creation of the internet. At the time of exchanging information in cyberspace, there are so many threats that occur; Data theft is one of the most frequent threats by wild parties. Currently, computer networks are used for various activities. Network traffic is often used to conduct online transactions so that security aspect becomes a problem that should get a big attention [8]. To secure the network traffic required a proper protocol. This protocol is capable of filtering incoming packets and may refuse instruction requests if suspected. In this study, the author tries to use the ability of IP Security. It is a protocol to secure TCP/IP transmissions. This protocol will be implemented at the transport layer in the OSI Reference Model to protect the IP by deploying security rules [1][2]. This rule can be set according to user requirements. Implementing this protocol is expected to avoid the threats that occur during the exchange of information on computer networks.

II. THEORIES

A protocol is a rule that defines functions contained in a network, such as sending messages, data, or information. It must be fulfilled by the sender and receiver so the communication can take place properly and correctly even though the system contained in the network is not similar [7]. At the time of activity in cyberspace, even the best network will always be unsafe. It requires additional software to protect information in the event of the exchange. This protocol provides source authentication, integrity checking, and content confidentiality. Data security is not a new thing applied. There are many ways to provide that security. Some applications ensure the safety services on the application layer including Secure Socket Layer (SSL) or Transport Layer Security (TLS). There are many conditions in the implementation of this security. This protocol makes calls to the underlying security provider to provide this service. IP Security eliminates this requirement by transferring security to the network layer. It provides the ability to authenticate, and encrypt data passing on the network. IP Security provides end-to-end encryption between computers and networks [3][4].

IP Security provides IP datagram security. It is end to end encyption; only the sender and receiver know about the security key. Devices between the two parties do not have to worry about encryption, secret keys, and so on, to forward the data together. The connection where the data flows may not be safely traveled. It means that in most cases, the underlying network infrastructure does not need to be modified. The application is fairly straightforward. Only hosts need to understand the protocol. Intermediary devices such as routers do not need IP Security aware [5].

However, it is important to note that firewalls and other devices that block certain types of traffic require special consideration and will be discussed later. The protocol works by identifying the traffic that needs to be secured and then applying a specified security level [6]. For example, the organization may identify traffic that meets certain criteria such as the source IP address or host name, and select the appropriate level of security based on that identification.

III. RESULT AND DISCUSSION

3.1 How IP Security Works

The security aspect is a significant concern in the protocol. Any information connected to the internet will be vulnerable to data theft. One way is to apply the security aspects of the application layer. End-to-end encryption can secure data security. Any attempt to access or change data in the data transmission process is preventable. It has a major effect that all built applications must be added to the security aspect to ensure the secure delivery of data.

IP Security can secure between certain hosts, network routers, firewalls or between hosts and routers or firewalls. The protocol uses some encryption algorithms. Each service has its authentication. It provides an approach to maintaining network traffic. There are two protocols protect the IP datagram, Authentication Header (AH) and Encapsulating Security Payload (ESP). AH is used to ensure data integrity, provide antireplay protection, and host authentication while ESP provides data confidentiality. There are no actual cryptographic algorithms in them.

The protocols, AH and ESP, work to provide authentication, integrity, and confidentiality. It can be configured to protect the entire IP payload or just the top layer protocol of the IP payload. Using protocols separately, or in combination, Banks can achieve simple authentication and integrity checking, as well as data encryption when sent over the wire. The AH header authentication, as defined by RFC 2402, provides the integrity of the data transmitted through typing hashing. It is needed to ensure the data is original. Hashing is a technology which is coded into several characters that create a digital signature from data. It is to verify that the message comes from the real source. Notice that the AH hash of the IP header and the load, but does not include any part of the allegedly changed datagram, such as hops. Because both headers and payloads are encrypted.

3.2 IP Security Implementation

The packet data and headers to be sent are computed using cryptographic checksum techniques and change the IP packet header section using a secure hashing function in tunnel mode. It adds a new header containing the hash value so that the information provided in the normal package is authenticated in the recipient. It seems to create a special tunnel on a public network that is only accessible to certain people. Figure 1 illustrated the example of an IP Security usage diagram for building the secure communications using public networks.

The private network #1 and #2 use the local IP addresses, 192.168.10.1 and 192.168.20.1. Both gateways use public IP, and it can be accessed from any computer as long as they are connected to the internet. There are several steps to ping from internal network #1 to #2. Every packet sent to IP 192.168.20.1 must be wrapped into another packet so that the IP header that appears is public IP X.X.X.X Then it will be sent to public IP Y.Y.Y.Y through a gateway with IP header stating as if the packet came from IP X.X.X.X. The process is called encapsulation. The gateway must know the path to achieve IP 192.168.20.1. It must redirect the packet to IP 192.168.20.1. It creates a special tunnel between the two networks. Once the connection has been established, each network can communicate and ping. When the packets arriving at IP Y.Y.Y.Y, it must be

unencapsulated to obtain the actual packet and sent to IP address 192.168.20.1.

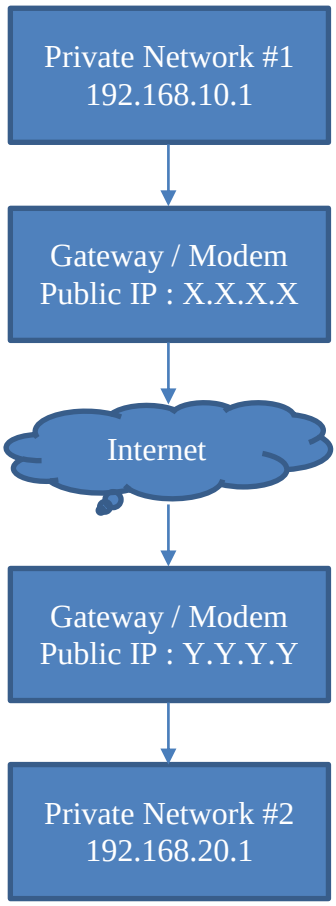

Figure 1. IP Security Implementation

3.2 The Advantages and Disadvantages

There are several advantages and disadvantages of using IP Security as a protocol of security protection on computer networks.

The advantages of IP Security:

- IP Security can protect any protocol that runs over IP and on any medium that IPs can use, so IPsec is a common method that can provide secure communications over a computer network.
- IP Security provides security in a transparent manner, so from the application side, the user does not need to be aware of its existence.
- IP Security is designed to meet the new IPv6 standard without forgetting which IPv4 is now in use.
- The design of IP Security does not require the use of certain encryption or hash algorithms so that if the frequently used algorithm has now been solved, its function can be replaced by other algorithms that are harder to solve.

The disadvantages of IP Security:

- IP Security too complex, provision of some additional features by adding unnecessary complexity.
- Some of the documentation still contains some errors, not explaining some essential and ambiguous explanations.
- Some of the default algorithms used in IP Security is now unsafe.

IV. CONCLUSION

IP Security is an important protocol for improving the security of computer networks. This protocol is in the network layer. It has some encryption features. If the data is successfully intercepted by a third party, the data is safe from theft. This protocol uses end-to-end encryption where the keys used are not mutually recognized by the recipient and the sender. The receiver does not know the sender's key and the sender does not know the recipient's key. IP Security protects communications by authentication and encrypts every IP packet from a communication session. Internet Protocol Security is used in protecting data flows between a pair of hosts, networks, or between security gateways and hosts. IP Security consists of two main parts of the protocol of adding headers to IP packets, AH and ESP. Cryptography is an IPsec technique used in providing security services Authentication, Data Integrity, and Confidentiality. Authentication and Data Integrity are provided by the AH and ESP protocols. The ESP protocol ensures confidentiality by using a cryptographic algorithm. IP Security is still considered the best solution in providing security in communication over computer networks, although it still has flaws.

V. REFERENCES

[1]. N. Ferguson and B. Schneier, "A Cryptographic Evaluation of IPSec, Counterpane," Counterpane Internet Security, Inc..

[2]. B. H. Kang and M. O. Balitanas, "Vulnerabilities of VPN using IPSec and Defensive Measures,"

International Journal of Advanced Science and Technology, vol. 8, no. 7, pp. 9-18, 2009.

[3]. H. Alshamrani, "Internet Protocol Security (IPSec) Mechanisms," International Journal of Scientific & Engineering Research, vol. 5, no. 5, pp. 85-87, 2014.

[4]. P. K. Singh and P. P. Singh, "A Novel Approach for the Analysis & Issues of IPsec VPN," International Journal of Science and Research, vol. 2, no. 7, pp. 187-189, 2013.

[5]. A. Singh and M. Gahlawat, "Internet Protocol Security (IPSec)," International Journal of Computer Networks and Wireless Communications, vol. 2, no. 6, pp. 717-721, 2012.

[6]. T. Sharma and S. Shiwani, "Statistical Results of IPSec in IPv6 Networks," International Journal of Computer Applications, vol. 79, no. 2, pp. 15-19, 2013.

[7]. R. Rahim and A. Ikhwan, "Study of Three Pass Protocol on Data Security," International Journal of Science and Research, vol. 5, no. 11, pp. 102-104, 2016.

[8]. A. Lubis and A. P. U. S. , "NetworkForensic Application in General Cases," IOSR Journal of Computer Engineering, vol. 18, no. 6, pp. 41-44, 2016.