International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 4 Issue 4, June 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Working Survey of Authentication Header and Encapsulating Security Payload

Er. Komalpret Kaur[1], Rajwinder Kaur[2], Arpan Chadak[2]

[1]Assistant Professor, [2]Student,
[1,2]Computer Science & Engineering Department,
[1,2]Swami Sarvanand Group of Institutes, Dinanagar, Punjab, India

ABSTRACT

In this paper we are discuss about IP security in AH and ESP. Internet Protocol suit is used to provide separation and Authentication services at the IP layer by authenticating and encrypting method. It is a collective of authentication between nodes at the starting session and transaction of cryptographic keys to be used during the session. Internet Protocol address is also known as IP address and IP suit. Internet Protocol Security (IP sec) functionality is based on two main techniques i.e. Protocol to exchange security parameters (IKE) and IP header extensions to carry the cryptographic information. (AH/ESP). IKE protocol aims for end-points to exchange security parameters or proposals each of the service that is Authentication Header (AH) or Encapsulation Header (ESP) and the type of operation mode: Tunnel mode or Transport mode. Now we are discuss two types of security protocols defined by IP sec i.e. Authentication Header (AH) and Encapsulating Security Payload (ESP). Encapsulating Security Payload (ESP) protocol is to contribute confidentiality by specifying how to encrypt the data that is to be sent and Authentication Header (AH) service provides integrity protection, authentication of origin and anti-replay attacks and does not offer encryption services to the payload portion of the packet. It also provides service of data integrity and origin authentication. Now we are discuss briefly implementation of AH and ESP in IP Suit.

KEYWORDS: *IP Security, IP Sec Suit, AH, ESP, IPV4, IPV6*

How to cite this paper: Er. Komalpret Kaur | Rajwinder Kaur | Arpan Chadak "Working Survey of Authentication Header and Encapsulating Security Payload" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-4 | Issue-4, June 2020, pp.632-636, URL: www.ijtsrd.com/papers/ijtsrd31122.pdf

IJTSRD31122

INTRODUCTION TO IP SECURITY

Protocol suit is used to provide separation and Authentication services at the IP layer by authenticating and encrypting in each IP packet of a communication session. It also includes protocols for establishing collective authentication between nodes at the starting of the session and transaction of cryptographic keys to be used during the session. Internet Protocol address is also known as IP address. It is a numerical label which assigned to each device connected to a computer network used the IP communication. IP address act as an identifier for a specific machine on a particular network. The IP address is also called IP number and internet address. IP address specifies the technical format of the addressing and packets scheme. Widely networks combine IP with a TCP (Transmission Control Protocol). It also allows developing a virtual connection between a destination and a source. The main advantage of IP sec over other security protocols resides on its characteristic of transparent implementation for end users since it does not require any modification at the application level. This means that IP sec is capable to protect any protocol consist above IP regardless the basic medium supporting IP. This characteristic is special interest given the introduction of heterogeneous environment enabled by an all-IP approach. IP sec protocol suite robustness offers comprehensive security solutions. Diverse configuration settings enable unique possibilities for security schemes. In order to implement a common explanation enables interoperability.

Extensively used and very important security technology is Internet Protocol Security (IPsec) [6]. It is used in the authentication and encryption in the public internet to provide the secure access. The IPsec is a set of protocols whose function is to secure communications over the Internet Protocol (IP) by authenticating or encrypting each IP packet in a data stream. IPsec also includes protocols for establishing encryption keys [11]. IPsec protocols act on the network layer, Layer 3 of the OSI model. Other extended Internet security protocols such as SSL, TLS and SSH operates from the application layer (Layer 7 of the OSI model). This makes IPsec more edible because it can be used to protect Layer 4 protocols, including TCP and UDP [5, 15]. In addition, the feature of IPSec is its open standard nature. It complements perfectly with the PKI technology and, although it establishes certain common algorithms, for interoperability reasoning allows to integrate more robust algorithms cryptographic that can be de- signed in the future [14]. Among the provided by IPSec, it should be noted that [12]:

- It enables current applications such as secure and transparent access to a remote IP node.

- Facilitates business-to-business e-commerce by providing a secure infrastructure on which to conduct transactions using any application. Extranets are an example.
- It allows building a secure corporate network over public networks, eliminating the management and cost of dedicated lines.
- It offers the telegram worker the same level of confidentiality that would have in the local network of his company, being not required the limitation of access to the tricky information by problems of privacy in alteration
- It is important to note that when we cite the word "secure" we do not refer only to the confidentiality of the communication, we are also referring to the probity of the data, which for many companies and business environments may be a much more critical demand than Confidentiality. This probity is `provided by IP sec as a service added to data encryption or as an independent service. Within IP sec the following peripheral are distinguished [16]
- Two security protocols: IP Authentication Header (AH) and IP Encapsulating Security Payload (ESP) that provide security mechanisms to protect IP.
- An Internet Key Exchange (IKE) key management protocol that allows two nodes to negotiate the keys and all the parameters necessary to establish an AH or ESP connection.

FEATURES OF IP SEC

- IP sec is not form to work only with TCP as a transport protocol. It works with UDP as well as any other protocol above IP such as ICMP, OSPF etc.
- IP sec protects the entire packet presented to IP layer including higher layer headers.
- Since higher layer headers are invisible which give port number, traffic analysis is more difficult.
- IP sec works from one network entity to another network entity, not from application process to application process. Security can be adopting without requiring the variation to individual user computers applications.
- Widely used to provide secure communication between network entities, IPsec can provide host-to-host security as well.
- IP sec is most use to provide a Virtual Private Network (VPN), either between two locations (gateway-to-gateway) or between a remote user and an enterprise network (host-to-gateway).

IP SEC SUITE ARCHITECTURE

Internet Protocol Security (IP sec) functionality is based on two main aspects, namely:

1. Protocol to exchange security parameters (IKE)
2. IP header extensions to carry the cryptographic information (AH/ESP)

The IP sec operates as follows to create a cryptographically protected connection between two end-points session key must be established between an author and a responder side by means of the Internet Key Exchange Protocol (IKE). IKE protocol aims for end-points to exchange security parameters or proposals each of them support including the type of service that is Authentication Header (AH) or Encapsulation Header (ESP) and the type of operation mode: Tunnel mode or Transport mode. Once both entities agree on the security features, they establish an active IPsec connection for the secured data.[11]

OPERATION MODES IN INTERNET PROTOCOL SECURITY (IPSEC)

IP sec services can be implemented either as a combination of both services or only one single service. Once the desired security level is selected, the actual transit of the data bring place according to the following connection modes.

- Transport Mode- In transport mode, the original IP packet is division to allocate IP sec information between the IP header and the rest of the data packet. Represents the application of transport mode for both types of services. As the same figure shows Transport mode protects the entire data packet. Because of this transport mode is more relevant for end-to-end communications.
- Tunnel Model- In comparison with transport mode, Tunnel mode does not alter the original packet. In the adverse it only adds a current IP header and IPsec information allocation at the opening of the IP packet. Therefore, tunnel mode is more suitable for connection between two networks or security gateways.

OPERATIONS WORKING IN IP SEC

The IP sec suit can be considered to have two separate operations when performed in unison, providing a complete set of security services. These two operations are IP sec Communication and Internet Key Exchange.[11]

IP sec Communication	**Internet Key Exchange (IKE)**
1. It is typically combine with standard IP sec functionality. It involves encapsulation, encryption, and hashing the IP data grams and handling all packet processes. 2. It is answerable for managing the communication according to the available Security Associations (SAs) established between communicating parties. 3. It uses security protocols such as Authentication Header (AH) and Encapsulated SP (ESP). 4. IP sec communication is not involved in the establishment of keys or their management. 5. IP sec communication operation itself is commonly referred to as IP sec.	1. IKE is the automatic key management protocol used for IP sec. 2. Technically, key management is not essential for IP sec communication and the keys can be manually managed. However, guide key management is not desirable for large networks. 3. IKE is responsible for guide of keys for IP sec and providing authentication during key establishment development. Though, IP sec can be used for any other key management protocols, IKE is used by default. 4. IKE defines Protocol (Oakley and SKEME) to be used with already defined key management framework Internet Security Association Key Management Protocol (ISAKMP). 5. ISAKMP is not IP sec specific, but provides the framework for creating SAs for any protocol.

INTRODUCTION TO IP SEC PROTOCOLS

It uses the security protocols to provide crave security services. These protocols are the heart of IP sec operations and everything else is designed to the protocol in IP sec. Security associations between the communicating entities are established and manage by the security protocol used. There are two security protocols defined by IP sec Authentication Header (AH) and Encapsulating Security Payload (ESP).[11]

IPV4

IPv4 was the first version of IP. It was utilize for production in the ARPANET in 1983. Today it is most universally used IP version. It is used to identify devices on a network using an addressing system. The IPv4 uses a 32-bit address scheme allowing to store 2^32 addresses which is more than 4 billion addresses. Till date, it is considered the prime Internet Protocol and carries 94% of Internet traffic.

Features of IPv4

- Connectionless Protocol
- Allow creating a simple virtual communication layer over diversified devices
- It requires less memory, and ease of memorized addresses
- Already supported protocol by millions of devices
- Offers video libraries and conferences

IPV6

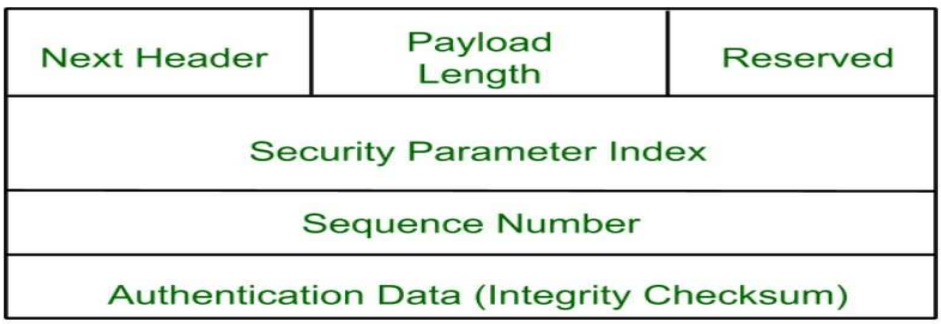
It is the most modern version of the Internet Protocol. Internet Engineer Taskforce initiated it in early 1994. The design and development of that suit now called IPv6. This modern IP address version is being utilize to fulfill the need for more Internet addresses. It was directed to resolve issues which are associated with IPv4. With 128-bit address space, it allows rare address space. IPv6 also called IPNG (Internet Protocol next generation).

Features of IPv6

- Hierarchical addressing and routing infrastructure
- State full and Stateless structure
- Support for quality of service (QOS)
- An standard protocol for neighboring node interaction

INTRODUCTION TO AUTHENTICATION HEADER (AH)

Authentication header contributes connectionless integrity, data origin authentication and an optional anti-replay service for IP datagrams. This dwell of the authentication data which is of variable length field that contains the integrity check value for this packet. The algorithms employed for integrity check value calculation are named by a security association of IPsec. For point-to-point communication keyed message authentication codes based on symmetric encryption algorithms or one way hash functions are used. For multicast communication one way hash algorithms mingled with asymmetric algorithms. Hashed based message authentication code has been mandatory to implement media access control for IPsec. Hash message authentication code is based on secure hash algorithm. It has been endorsed for message authentication in several network security protocols. The key acumen behind this are the free availability, flexibility of changing the hash function and reasonable speed, among others. The media access control based on the block ciphers due to the complexity of the encryption process. However, after selecting the AES encryption algorithm, this situation merits re-evaluation shows good performance in both hardware and software and it has sophisticated security features. It contributes the data integrity and the authentication to check and replay the protection. The Authentication header ensures the integrity and authentication of IP datagrams. That is, it provides a means to the receiver of the IP packets to authenticate the source of the data and to check that data has not been altered in transit. However, Authentication header does not provide any guarantee of confidentiality, that is the transmitted data can be viewed by third parties . It is inserted between the standard IP header (both IPv4 and IPv6) and the transported data, which can be TCP, UDP or ICMP message, or even a complete IP datagram.[7,10]



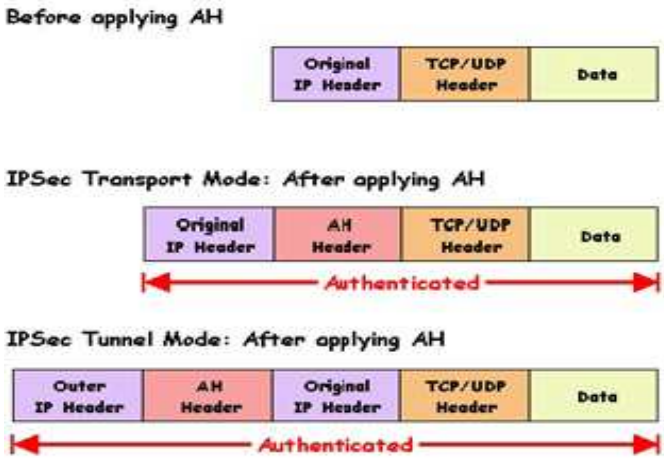
IMPLEMENTATION OF AH DATAGRAM

AH is actually a new IP protocol which is authorizes with decimal number 51. This means that the IP header contains the value 51, instead of the values 6 or 17 that are combined with TCP and UDP. Authentication Header (AH) service provides integrity protection, authentication of origin and anti-replay attacks. AH does not offer encryption services to the payload portion of the packet. It provides service of data integrity and origin authentication. It optionally caters for message replay resistance. However, it does not contribute any form of confidentiality. Authentication header provides authentication of either all or part

of the contents .The header is calculated based on the values in the datagram. The operation of the AH protocol is surprisingly simple. It can be treated similar to the algorithms used to calculate checksums or perform CRC checks for error detection. AH uses special hashing algorithm and a secret key. A security association between the two devices is set up that specifies these particulars.[8]

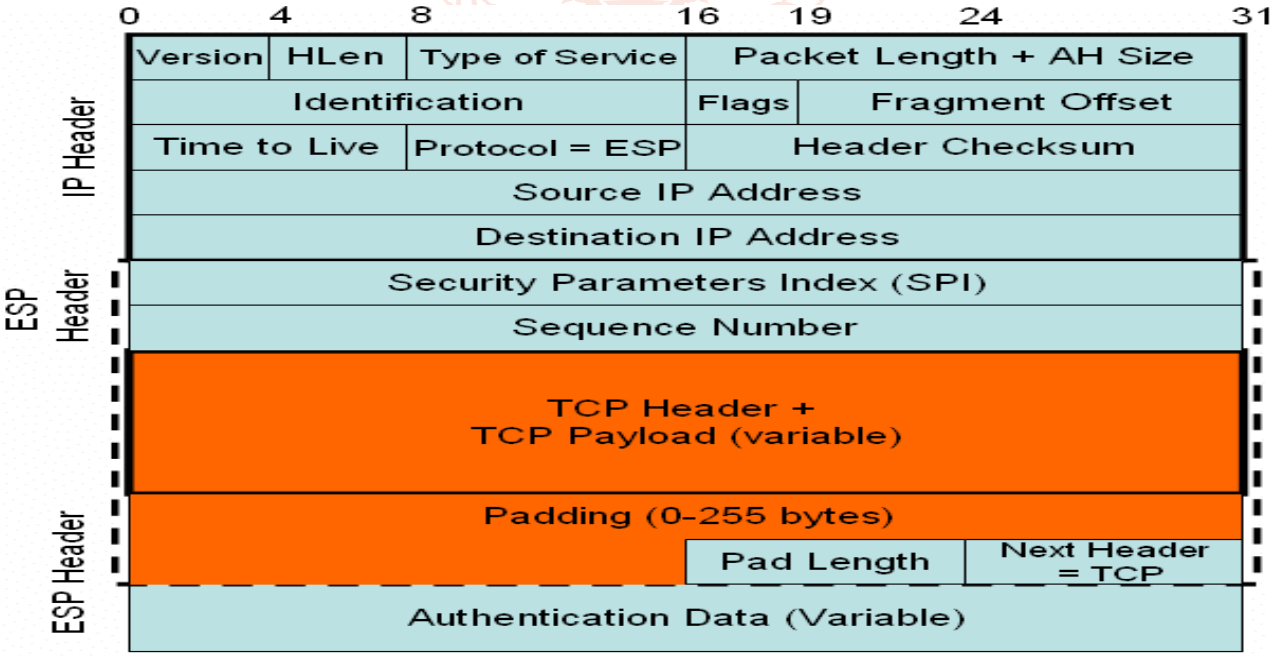
The process of AH goes through the following phases.

- When IP packet is received from upper protocol stack, IPsec determine the associated Security Association (SA) from feasible information in the packet; for example, IP address (source and destination).
- From SA, once it is identified that security protocol is AH, the parameters of AH header are calculated. The AH header consists of the following parameters –
- **The header field** specifies the protocol of Security Association packet following AH header. Sequence Parameter Index (SPI) is obtained from existing between communicating parties.
- **Sequence Number** is calculated and inserted. These numbers provide optional capability to AH to resist replay attack.
- **Authentication data** is figured differently depending upon the communication mode.
- In transport mode, the calculation of authentication data and assembling of final IP packet for transmission is depicted in the following diagram.
- In Tunnel mode, the above process takes place as depicted in the following diagram.



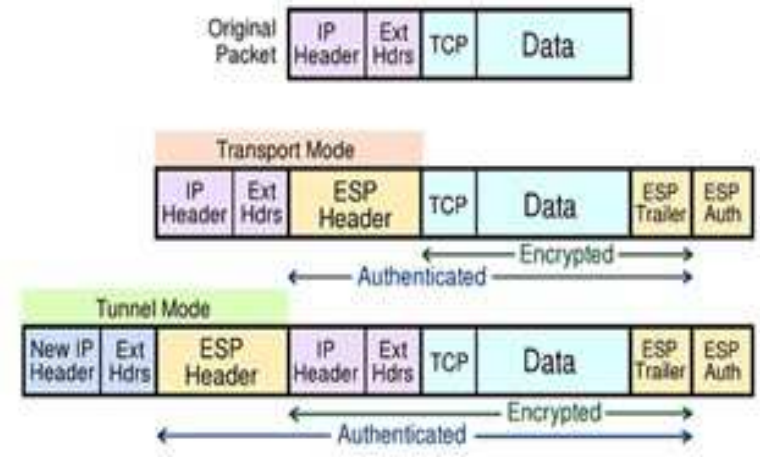
INTRODUCTION TO ENCAPSULATING SECURITY PAYLOAD (ESP)

The main objective of the Encapsulating Security Payload (ESP) protocol is to contribute confidentiality by specifying how to encrypt the data that is to be sent. In addition, it can grant data integrity and authentication services by incorporating a mechanism related to AH. It provides more functions than AH, the format of the header is more complex. This format consists of a header and tails that surround the data transported.



This data can be any IP protocol (for example, TCP, UDP or ICMP, or even a complete IP packet). The structure of an ESP datagram, which shows how the content or payload travels encrypted .In comparison to AH, Encapsulation Service Payload (ESP) not only contributes integrity protection, optional authentication and anti-replay attacks services but also confidentiality

by means of encryption. All services furnished by ESP are configurable meaning that offered services that can be activated or deactivated. A configuration mode of interest is ESP "Null Encryption" mode for which case confidentiality services are not offered. Under this configuration, ESP header has the same functionality as AH allows only integrity protection.[9,10]



CONCLUSION

This paper introduces the concept of IP Security, the basic model and its application in many fields. In this paper present the IP security in AH & ESP. Protocol suit is used to provide separation and Authentication services at the IP layer by authenticating and encrypting in each IP packet of a communication session. Now we are discussing implementation of AH & ESP. In comparison to AH, Encapsulation Service Payload (ESP) not only contributes integrity protection, optional authentication and anti-replay attacks services but also confidentiality by means of encryption. In this paper, we have a survey on IP Security, IPV4, IPV6, AH & ESP. Firstly, we discussed about IP Suit and its architecture, advantages, disadvantages. We have also defined how to works IP Security in AH and ESP. Thus in the end we have reviewed various type of know ledged about IP, AH, ESP.

REFERENCE

[1] www.google.com

[2] https://www.tutorialspoint.com/internet_technologies /internet_security_overview.htm

[3] https://www.guru99.com/difference-ipv4-vs-ipv6.html.

[4] A Review of the Adoption of IPSEC Concept in Securing Web Servers, International Journal of Research, Volume 03 Issue 12 August 2016.

[5] M. Balfaqih, et al., \Fast handover solution for network-based distributed mobility management in intelligent transportation systems," Telecommunication Systems, vol. 64, no. 2, pp. 325-346, 2017.

[6] S. Kent, IP Authentication Header, RFC 2402, 2005.

[7] S. Kent, R. Atkinson, IP Authentication Header, RFC 2402, 1998.

[8] S. Kent, IP Encapsulating Security Payload (ESP05), RFC 4303, 2005.

[9] C. Madson and R. Glenn, The Use of HMAC-MD5-96 within ESP and AH, RFC 1321, 1998.

[10] S. Frankel and S. Krishnan, IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap, RFC 6071, 2011.

[11] S. E. Frankel, et al., \Guide to IPsec VPNs: Recommendations of the national institute of standards and technology," NIST Special Publication, Special Publication (NIST SP)-800-77, 2005.

[12] A. J. Ghazali, et al., \Building IPv6 based tunneling mechanisms for VoIP security," in 13th International Multi-Conference on Systems, Signals and Devices (SSD'16), 2016.

[13] A. P. Hansen, Public Key Infrastructure (PKI) Inter-operability: A Security Services Approach to Support Transfer to Trust, Dissertations Monterey, California: Naval Postgraduate School, 1999.

[14] R. Hassan, A. A. Al-Khatib, and W. M. H. W. Hussain, \A framework of Universiti Kebangsaan Malaysia patent: UKM patent," in 19th International Conference on Advanced Communication Technology (ICACT'17), 2017.

[15] K. Seo, and S. Kent, Security Architecture for the Internet Protocol, RFC 2401, 2005.

[16] P. Jokela, J. Melen, and R. Moskowitz, Using the Encapsulating Security Payload (ESP) Transport Format with the Host Identity Protocol (HIP), RFC 7402, 2015.