IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501
Vol.2, No6, December 2012

Internet Protocol Security(IPSec)

Ajit Singh
Professor in CSE department,SES
BPSMV, Khanpur Kalan
Sonepat, India
ghanghas_ajit@rediffmail.com

Meenakshi Gahlawat
Student in CSE department ,SES
BPSMV, Khanpur Kalan
Sonepat, India
cse07331.sbit@gmail.com

***Abstract*— The standard Internet communication protocol is completely unprotected, allowing hosts to inspect or modify data which is in transit. Adding IPSec to systems will overcome this limitation by providing strong encryption, integrity, authentication and replay protection. This paper describes IP security in details and explains theory, its mode of operation, security protocols and various services been provided, its application area along with various advantages and disadvantages.**

Keywords- Authentication Header, Encapsulating Security Payload, Security Association, Tunnel mode, Transport mode, Internet Key Exchange.

I. INTRODUCTION

Internet communication has no data security built-in, i.e. the protocol is completely unprotected. The user data is been sent in clear text form, hence all the information can be seen by any person, organization, competitor etc. For example, the passwords are sent in the open and can be seen and used to hack the system. The contents of the IP packets can be modified without the possibility of being detected. This matters when one does not care if anyone sees his/her information, but would certainly care if someone alters it. Since packets can be forged, altered etc. Moreover it is possible to pose as someone or something else on the Internet. For example, you may only permit your operators to manage your systems, but without protection anyone could possibly do it. This is been known as Identity Spoofing, i.e. pretending to be someone else by creating IP packets with fake source address. So to overcome all these threats we need to add IPSec to our system**. Internet Protocol Security** (**IP sec**) is a collection of protocols designed by the Internet Engineering Task Force to provide security for a packet at the network layer. IPSec is an end-to-end security scheme operating in the Internet Layer of the Internet Protocol Suite. It 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*). IPSec helps to create authenticated and confidential packet for the IP layer. [1, 3]

Conceptual IPSec positioning in the TCP/IP protocol stack is as shown in figure:

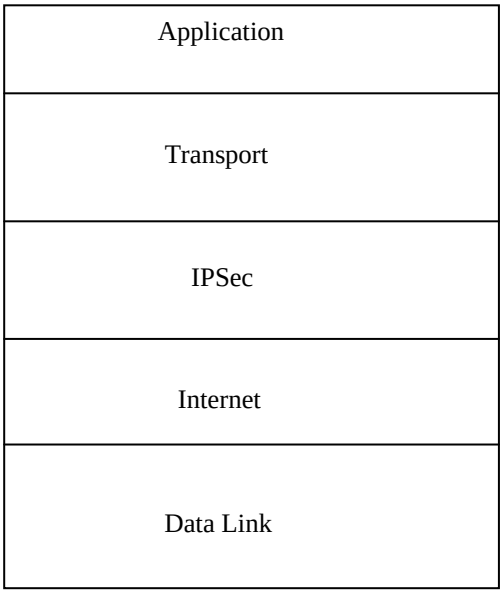

Figure 1.Conceptual IPSec positioning in TCP/IP protocol stack

II. IP SEC SECURITY PROTOCOLS

IPSec has two protocols: Authentication Header and Encapsulating Security Payload. These two protocols together provide authentication and/or encryption for packets at the IP level.

A. Authentication Header

The authentication header provides support for data integrity and authentication of IP packets. The data integrity service ensures that data inside IP packets is not altered durig transit. The authentication service enables an end user or computer system to authenticate the user or application at other end and decide whether to accept or reject packets accordingly. It also prevents the address spoofing attacks observed in today's Internet. The AH also guards against the replay attacks. Authentication is based on the use of a Message Authentication Code (MAC) which means the two parties must share a secret key.

The AH structure is shown below:

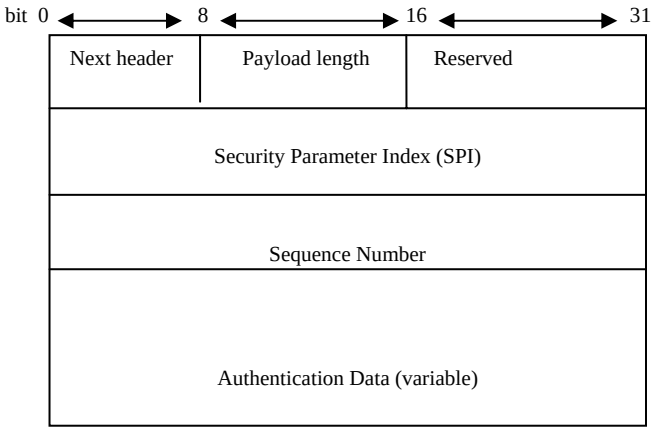

Figure 2.Authentication Header format

It contains following fields:

- **Next Header** (8 bits): This field identifies the type of header immediately following this header.
- **Payload Length** (8 bits): This field gives the length of the authentication header in 32-bit words, minus 2. For example, the default length of the authentication data field is 96 bits, or three 32-bit words. With a three-word fixed header, there are a total of six words in the header, and the Payload Length field has a value of 4.
- **Reserved** (16 bits): This field is reserved for future use.
- **Security Parameters Index** (32 bits): This field is used in combination with the source and destination addresses as well as the IPSec protocol used (AH or ESP) to uniquely identify the Security association for the traffic to which a datagram belongs.
- **Sequence Number** (32 bits): This field provides ordering information for a sequence of datagrams. The sequence prevent a playback.The sequence number is not repeated even if a packet is retransmitted.A sequence number does not wrap around after it reaches 232; a new connection must be established.
- **Authentication Data** (variable): This variable-length field .It is the result of applying a hash function to the entire IP datagram except for the fields that are changed during transit. [1,2]

B. Encapsulating Security Payload

The AH Protocol does not provide privacy only, but also source authentication and integrity of data. IPSec later defined an alternative protocol that provides source authentication, integrity, and privacy called Encapsulating Security Payload. ESP adds a header and trailer. ESP is based on symmetric key cryptography techniques. It can be used in isolation or can be combined with AH.

IPSec ESP Format is as shown:

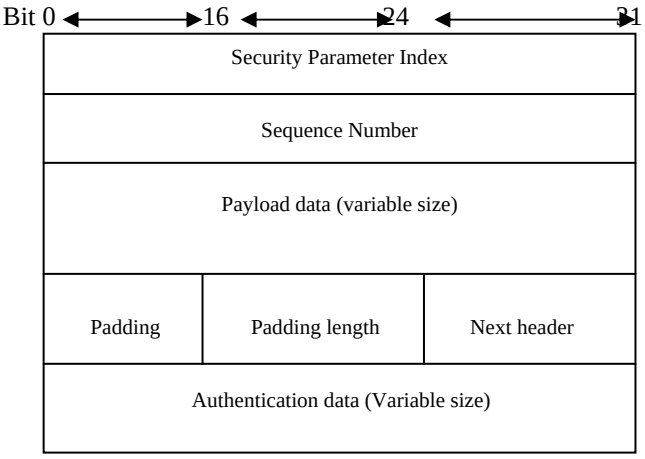

Figure 3.Encapsulating Security Payload format

It contains following fields:

- **Security Parameters Index** (32bits): Identifies a security association
- **Sequence Number** (32 bits): It is similar to that defined for AH protocol.
- **Padding** (0-255 bytes): Extra bytes that may be required if the encryption algorithm requires the plaintext to be a multiple of some number of octets
- **Pad Length** (8 bits): This field defines the number of padding bytes. The value is between 0 and 255; the maximum value is rare.
- **Next Header** (8 bits): Identifies the type of data contained in the payload data field by identifying the first header in that payload (for example, an extension header in IPv6, or an upper-layer protocol such as TCP)
- **Authentication Data** (variable): A variable-length field (must be an integral number of 32-bit words) that contains the integrity check value computed over the ESP packet minus the Authentication Data field. [1,2]

C. Supporting protocols

1)Internet Key Exchange(IKE) Protocol

Another supporting protocol is also used in IPSec. This protocol is used for the key management procedures and is called as Internet Key Exchange(IKE) protocol. IKE, it is used to negotiate the cryptographic algorithms to be later used by AH and ESP in the actual cryptographic operations. The IPSec protocols are designed to be independent of the actual lower-level cryptographic algorithms. Thus, IKE is the intial phase of IPSec, where the algorithms and keys are decided. After the IKE phase, the AH and ESP protocols take over.[2]

2)Security association

The output of the IKE phase is Security Association(SA). SA is an agreement between communicating parties about

factors such as the IPSec protocol in use, mode of operation, cryptographic algorithms, cryptographic keys, lifetime of keys, etc. As we know that the principal objective of the IKE protocol is to establish an SA between the two communicating parties. Once this is done, both major protocols of IPSec(AH and ESP) make use of SA for their actual operation. If both AH and ESP are used, each communicating party requires two sets of SA: one for AH and one for ESP. Moreover, SA is unidirectional. Therefore, at second level, we need two sets of SA per communicating party: one for incoming transmission and another for outgoing transmission. Thus, if the two communicating parties use both AH and ESP, each of them would require four sets of SA. Also both the parties must allocate some storage area for storing the SA information at their end. For this purpose, a standard storage area called as Security Association Database is pre-defined and used by IPSec. Thus, each communicating party requires maintaining its own SAD. [2]

III. IPSEC OPERATION MODES

Ipsec operates in one of two different modes:

- Transport mode
- Tunnel mode

A. *Transport mode:*

Transport mode is the default mode for IPSec, and it is used for end-to-end communications (for example, for communications between a client and a server). When transport mode is used, IPSec encrypts only the IP payload. Transport mode provides the protection of an IP payload through an AH or ESP header. Typical IP payloads are TCP segments (containing a TCP header and TCP segment data), a UDP message (containing a UDP header and UDP message data), or an ICMP message (containing an ICMP header and ICMP message data). IPSec in the transport mode does not protect the IP header; it only protects the information coming from the transport layer. This mode is normally used when we need host-to-host protection of data. [4]

Authentication Header transport mode:

In the transport mode, the position of the AH is between the original IP header and the original TCP header of the IP packet. [1]

Figure 4. Auhtentication Header for transport mode

Encapsulating Security Payload transport mode:

Encapsulating Security Payload provides confidentiality (in addition to authentication, integrity, and anti-replay protection) for the IP payload. ESP in transport mode does not sign the entire packet. Only the IP payload (not the IP header) is protected. ESP can be used alone or in combination with AH. [4]

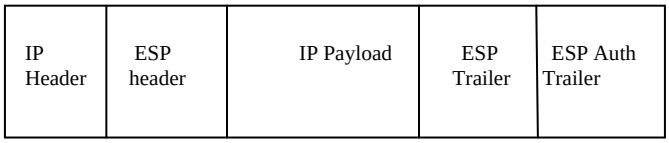

Figure 5. Encapsulating Security Payload Transport Mode

B. *Tunnel mode:*

In tunnel mode,IPSec protects the entire IP packet. It takes an IP packet,including the header,applies IPSec security methods to the entire packet,and then adds a new IP header.The tunnel mode is normally used between two routers,between a host and a router,or between a router and a host . When IPSec tunnel mode is used, IPSec encrypts the IP header and the payload, whereas transport mode only encrypts the IP payload. Tunnel mode provides the protection of an entire IP packet by treating it as an AH or ESP payload. With tunnel mode, an entire IP packet is encapsulated with an AH or ESP header and an additional IP header. The IP addresses of the outer IP header are the tunnel endpoints, and the IP addresses of the encapsulated IP header are the ultimate source and destination addresses.

IPSec tunnel mode is useful for protecting traffic between different networks, when traffic must pass through an intermediate, untrusted network. Tunnel mode is primarily used for interoperability with gateways, or end-systems that do not support L2TP/IPSec or PPTP connections. You can use tunnel mode in the following configurations: [5]

- Gateway-to-gateway
- Server-to-gateway
- Server-to-server

AH tunnel mode:

In the tunnel mode, the entire original IP packet is authenticated and the AH is inserted between the original IP header and a new outer IP header. The inner IP header contains the ultimate source and destination IP addresses, whereas outer IP header possibly contains different IP addresses. [2]

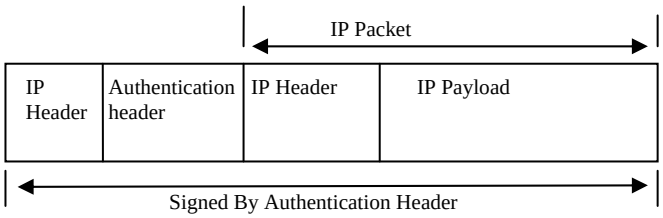

Figure 6. AH tunnel mode

ESP tunnel mode:

The tunnel mode ESP encrypts an entire IP packet.Here,the ESP header is pre-fixed to the packet and then

the packet along with the ESP trailer is encrypted.As we know,the IP header contains the destination address as well as intermediate routing information. Therefore,this packet cannot be transmitted as it is. Otherwise,the delivery of the packet would be impossible. Therefore,a new IP header is added,which contains sufficient information for routing. [2]

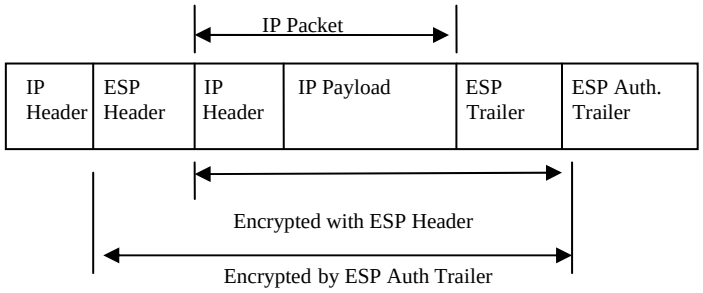

Figure 7. ESP Tunnel Mode

IV. IPSEC KEY MANAGEMENT

Apart from the two core protocols(AH and ESP), the third most significant aspect of IPSec is key management. Without a proper key management set up, IPSec cannot exist. This key management in IPSec consists of two aspects: key agreement and distribution. As we known,we require four keys if we want to make use of both AH and ESP: two keys for AH(one for message transmissions,one for message receiving) and two keys for ESP(one for message transmission,one for message receiving). The protocol used in IPSec for key management is called as ISAKMP. The Internet Security Association and Key Management Protocol (ISAKMP) defines procedures and packet formats to establish, negotiate, modify and delete Security Associations (SAs). SAs contain all the information required for execution of various network security services, such as the IP layer services (such as header authentication and payload encapsulation), transport or application layer services, or self-protection of negotiation traffic. ISAKMP defines payloads for exchanging key generation and authentication data. These formats provide a consistent framework for transferring key and authentication data independent of the key generation technique, encryption algorithm and authentication mechanism.

ISAKMP is distinct from key exchange protocols in order to cleanly separate the details of security association management (and key management) from the details of key exchange. There may be many different key exchange protocols, each with different security properties. However, a common framework is required for agreeing to the format of SA attributes and for negotiating, modifying and deleting SAs. ISAKMP serves as this common framework.

Separating the functionality into three parts adds complexity to the security analysis of a complete ISAKMP implementation. However, the separation is critical for interoperability between systems with differing security requirements and should also simplify the analysis of further evolution of an ISAKMP server.

ISAKMP is intended to support the negotiation of SAs for security protocols at all layers of the network stack (e.g., IPSEC, TLS, TLSP, OSPF, etc). By centralizing the management of the security associations, ISAKMP reduces the amount of duplicated functionality within each security protocol. ISAKMP can also reduce connection setup time by negotiating a whole stack of services at once. [2,6]

V. SERVICES PROVIDED BY IPSEC

- **Access Control**: IPSec provides access control by using a security association database. When a packet arrives at a destination, and there is no security association already established for this packet, the packet is discarded.
- **Message Authentication**: The integrity of the message is preserved in both AH and ESP by using authentication data. A digest of data is created and sent by the sender to be checked by the receiver.
- **Entity Authentication**: The security association and the key-hashed digest of the data sent by the sender authenticate the sender of the data in both AH and ESP.
- **Confidentiality**: The encryption of the message in ESP provides confidentiality. AH, however, does not provide confidentiality. If confidentiality is needed, one should use ESP instead of AH. [1]

VI. APPLICATIONS OF IPSEC

- **Secure branch office connectivity:** Rather than subscribing to an expensive leased line for connecting its branches across cities/countries,an organization can set up an IPSec-enabled network to securely connect all its branches over the internet.
- **Secure remote Internet access :** Using IPSec ,we can make a local call to an Internet Service Provider (ISP) so as to connect to our organization's network in secure fashion from our home or hotel.From there,we can access the corporate network facilities or access remote desktops/servers.
- **Set up communication with other organizations**: Just as IPSec allows connectivity between various branches of an organizations, it can also be used to connect the networks of different organizations together in a secure and inexpensive fashion. [2]

VII. BENEFITS OF IPSEC

The benefits of IPSec include*:*

- Traffic within a company or workgroup need not incur about the overhead of security-related processing because IPSec when implemented in a firewall or router, it provides strong security that can be applied to all traffic crossing the perimeter.
- IPSec is transparent to applications, so when it is implemented in the firewall or router,there is no need

to change software on a user or server system Even if IPSec is implemented in end systems, upper layer software, including applications, are not affected.

- IPSec can be transparent to end users. So there is no need of training users on the basis of security mechanisms, issue keying material on a per-user basis, or revoking of the keying material when users leave the organization.
- IPSec can be used to provide security for individual users when needed. This feature is beneficial for offsite workers and also for setting up a secure virtual subnetwork within an organization for sensitive applications. [7]

VIII. ADVANTAGES & DISADVANTAGES OF IPSEC

A. Advantages

- **Universality** - variety of different networks from around the world**.**
- **Scalability** - Through IP, IPSec can be integrated with the networks of all sizes ranging from LAN's to global networks.
- **Network Layer Security** - Since IPSec functions at low network level, factors such as users, applications, lower level data carrying protocols, and transport technology will not affect its performance.
- **Application Independence** - IPSec is not limited to specific applications. So traversing of a network is not application specific. However, it is guaranteed that they will be routed with IP, making them IPSec compatible. [8]

B. Disadvantages

- **Small Packets** – When small packets are been transmitted, a large overhead is generated due to encryption process of IPSec . This in turn diminishes the performance of the network.
- **Complexity** – Due to large number of features and options, IPSec becomes very complex. Complexity increases the probability of the presence of a weakness or hole. For example, IPSec is weak against replay attacks.
- **Firewall** - The purpose of a firewall is been defeated by the implementation of IPSec. This is because firewalls are based on preconfigured rules, which IPSec encrypts. This problem, however, can be avoided if the firewall is used along with the IPSec gateway, which is a decryption method. [8]

IX. ACKNOWLEDGMENT

I would like to give my sincere gratitude to my guide Dr. Ajit Singh who guided me throughout, to complete this topic.

References

[1] Behrouz A Forouzan (Fourth Edition), Data Communications and Networking
[2] Atul Kahate (2009), *Cryptography and Network Security*, second edition, McGraw-Hill.
[3] *www.interpeak.com/files/**ipsec**.**pdf***
[4] *technet.microsoft.com/en-us/library/cc739674(v=ws.10).aspx*
[5] *technet.microsoft.com/en-us/library/cc737154(v=ws.10).aspx*
[6] www.javvin.com/protocolISAKMP.html
[7] cs.iupui.edu/~durresi/CSC4601_07/16_4601_07_6.pdf - United States
[8] *nislab.bu.edu/sc546/sc441Spring2003/ip_sec/A&D.htm)*

AUTHORS PROFILE

Dr. Ajit Singh is presently working as Chairperson of School of Engineering & Sciences in BPSMV, Khanpur Kalan (Sonepat). He is also having the additional charge as a Director of University Computer Center (UGC). He posses qualifications of B.Tech, M.Tech, Ph.D. He is a member of BOG (Board of Governors) of Haryana State Counselling Society, Panchkula and also member of academic council in the University. He published approximate 20 papers in National/ International journals and conferences and holds a teaching experience of approximate 10 years. He holds the membership of Internal Quality Assurance cell, UG-BOS &PG-BOS and the NSS advisory committee. He is also an associate member of CSI & IETE. His research interests are in Network Security, Computer Architecture and Data Structure.

Ms. Meenakshi Gahlawat has completed her B.Tech degree in Computer Science from Maharishi Dayanand University, Rohtak in year 2011. She is pursuing M.Tech in Computer Science from BPSMV, Khanpur Kalan from June 2011. Her research interests are in Network Security and Computer Networks.