Network-Layer Security: IPsec

Network layer security controls have been used frequently for securing communications, particularly over shared networks such as the Internet because they can provide protection for many applications at once without modifying them. In 1992, the Internet Engineering Task Force (IETF) began to define a standard 'IPsec'.

Security in Network Layer

The popular framework developed for ensuring security at network layer is Internet Protocol Security (IPsec). The **IP security** protocol, more commonly known as IPsec, is a suite of protocols that provides security at the network layer.

- **Features of IPsec**
  - IPsec is **not** designed 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.
  - IPsec protects the entire packet presented to IP layer including higher layer headers.
  - Since higher layer headers are hidden which carry port number, traffic analysis is more difficult.
  - IPsec works from one network entity to another network entity, not from application process to application process. Hence, security can be adopted without requiring changes to individual user computers/applications.
  - Tough widely used to provide secure communication between network entities, IPsec can provide host-to-host security as well.
  - The most common use of IPsec is 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).
- **Security Functions (IPsec Services)**

  The important security functions provided by the IPsec are as follows −

  1) Confidentiality
    - Enables communicating nodes to encrypt messages.
    - Prevents eavesdropping by third parties.

2) ***Origin authentication and data integrity***.

- Provides assurance that a received packet was actually transmitted by the party identified as the source in the packet header.
- Confirms that the packet has not been altered or otherwise.

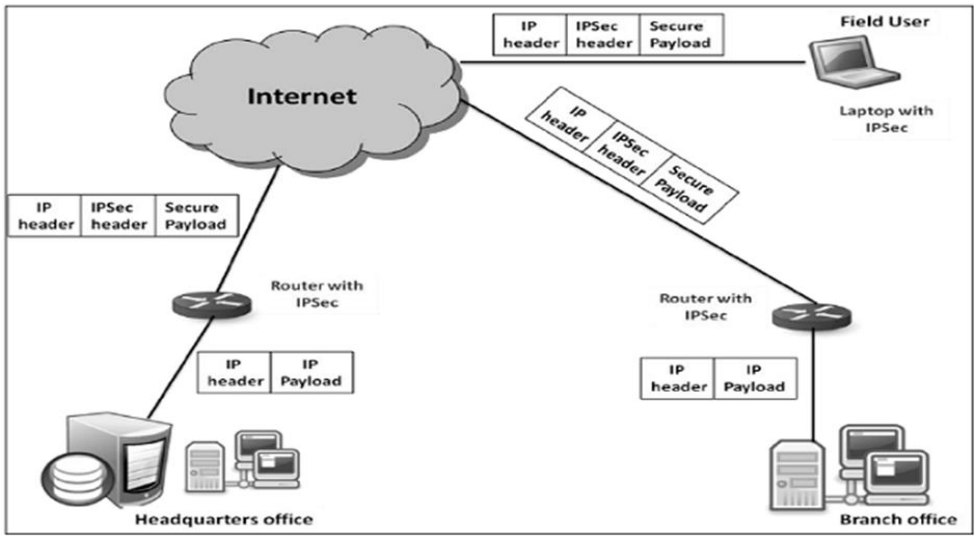
3) Key management.

- Allows secure exchange of keys.
- Protection against certain types of security attacks, such as replay attacks.

Virtual Private Network

Ideally, any institution would want its own private network for communication to ensure security. However, it may be very **costly** to establish and maintain such private network over geographically dispersed area. It would require to manage complex infrastructure of communication links, routers, DNS, etc.

IPsec provides an easy mechanism for implementing Virtual Private Network (VPN) for such institutions. ***VPN technology*** allows institution's inter-office traffic to be sent over public Internet **by** encrypting traffic before entering the public Internet and logically separating it from other traffic.



Operations within IPsec

The IPsec suite can be considered to have two separate operations, ***IPsec Communication*** and ***Internet Key Exchange***.

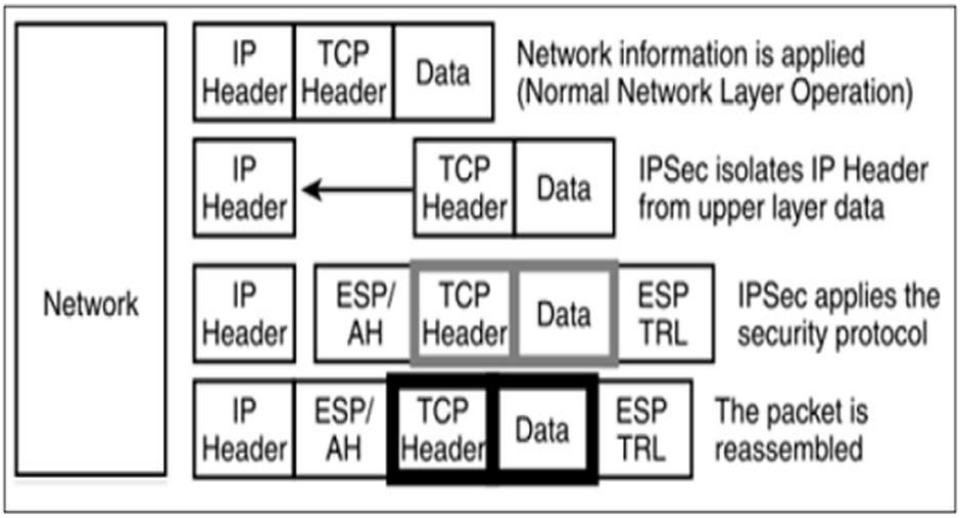
- ***IPsec Communication***
  - It is typically associated with standard IPsec functionality. It involves ***encapsulation***, ***encryption***, and ***hashing*** the IP datagrams and ***handling*** all packet processes.
  - It is responsible for managing the communication according to the available Security Associations (SAs) established between communicating parties.
  - It uses security protocols such as Authentication Header (AH) and Encapsulated SP (ESP).
- ***Internet Key Exchange***
  - ***IKE*** is the automatic key management protocol used for IPsec.
  - Technically, key management is not essential for IPsec communication and the keys can be manually managed. However, manual key management is not ***desirable*** for large networks.
  - ***IKE*** is responsible for creation of keys for IPsec and providing authentication during key establishment process.
  - ***IKE*** defines ***two*** protocols (Oakley and SKEME) to be used with already defined key management framework ***Internet Security Association Key Management Protocol (ISAKMP).***
  - ***ISAKMP*** is ***not IPsec specific***, but provides the framework for creating ***SAs*** for any protocol.

IPsec Communication Modes

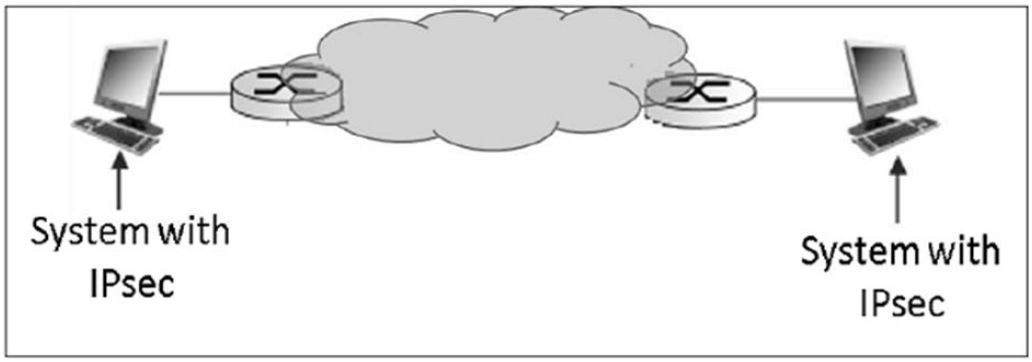
IPsec Communication has two modes of functioning; ***transport*** and ***tunnel*** modes. These modes can be used in combination or used individually depending upon the type of communication desired.

1) Transport Mode

- IPsec does not encapsulate a packet received from upper layer.
- **AH** is inserted **after** the IP header and **before** an upper layer protocol (i.e. TCP) or other IPSEC headers have been inserted.
- The following diagram shows the data flow in the protocol stack.



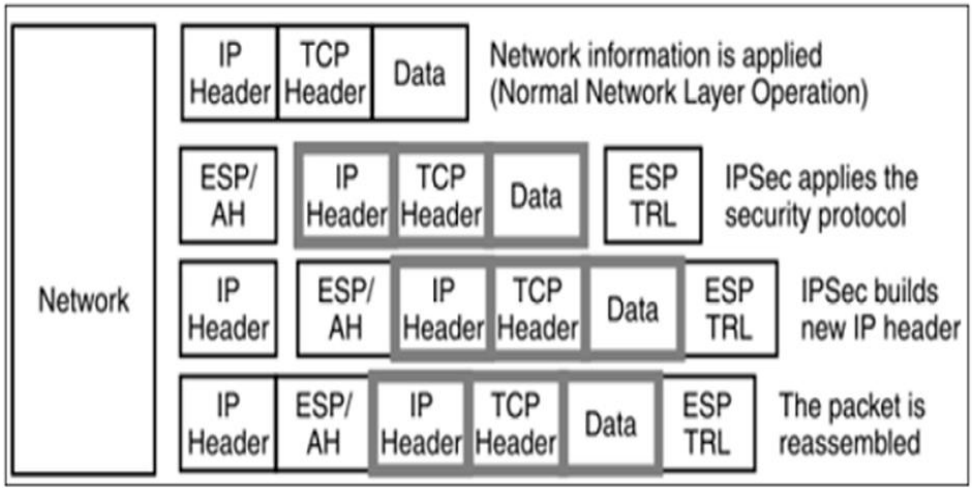
- The limitation of transport mode is that ***no gateway services*** can be provided. It is reserved for ***point-to-point*** communications as depicted in the following image.



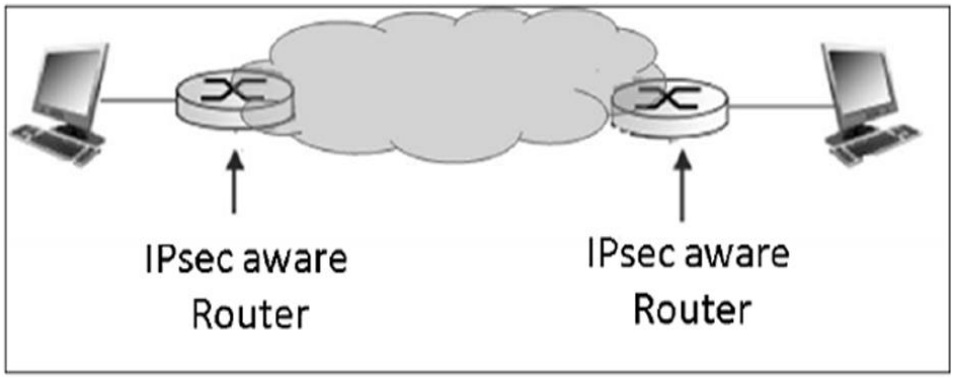
2) Tunnel Mode

- This mode of IPsec provides ***encapsulation*** services along with other security services.

- In tunnel mode operations, the entire packet from upper layer is ***encapsulated*** before ***applying security protocol***. ***New IP header*** is added.
- The following diagram shows the data flow in the protocol stack.



- Tunnel mode is typically associated with ***gateway*** activities. The encapsulation provides the ability to send several sessions through a ***single gateway***. Using IPsec, the tunneling mode can be established between the **gateway** and **individual end system** as well. Tunnel mode is used to form a traditional VPN, as it provides a ***virtual secure tunnel*** across an untrusted Internet.
- In tunnel-mode, the ***inner IP header*** carries the ultimate source and destination ***address*** while an ***outer*** IP header contains the address of the security gateway.
- The typical tunnel mode communication is as depicted in the following diagram.



IPsec Protocols

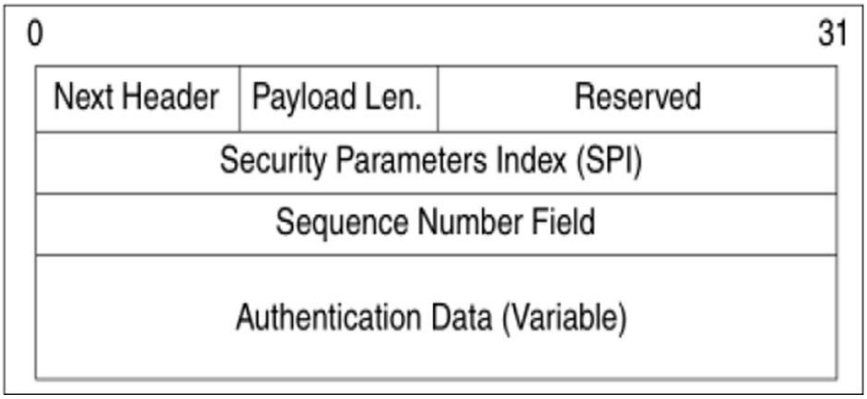
There are two security protocols defined by IPsec: ***Authentication Header (AH)*** and ***Encapsulating Security Payload (ESP).***

1) Authentication Header (AH)

The AH protocol provides service of ***data integrity*** and ***origin authentication***. It optionally caters for message replay resistance. However, it does not provide any form of confidentiality. AH is a protocol that provides authentication of either all or part of the contents of a datagram by the addition of a header. The place of the header depends on the mode cooperation (tunnel or transport).

AH uses special ***hashing*** algorithm and a ***secret key*** known only to the communicating parties. 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 available 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:-



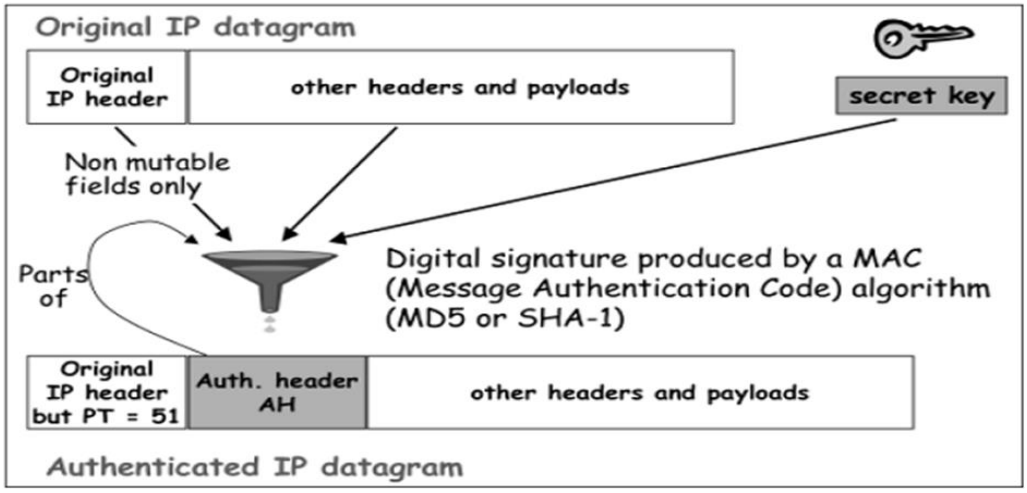
AH Format

The fields of the Authentication Headers are as follows: ·

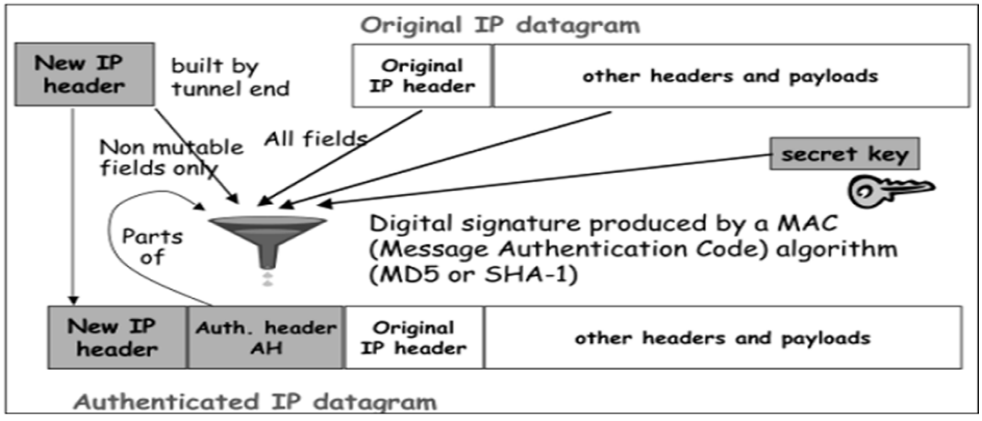
- ***Next Header***: **8 bit** field which specifies the protocol of packet following AH header.
- ***Payload Length*** - **8 bit** field which specifies the length of the AH in 32 bit words ·
- ***Reserved*** - **16 bit** field which must be set to zero ·

- ***Security Parameters Index (SPI)*** - Arbitrary 32 bit value that in combination with the destination address identifies the Security Association for the datagram, (i.e. it is obtained from SA existing between communicating parties).
- ***Sequence Number Field*** - Unsigned 32 bit field contains a monotonically increasing counter value for defense against replay attacks ·
- ***Authentication Data*** - Variable length field that is calculated differently depending upon the communication mode:

A) **In transport mode**, the calculation of authentication data and assembling of final IP packet for transmission is depicted in the following diagram. In original IP header, change is made only in protocol number as 51 to indicated application of AH.

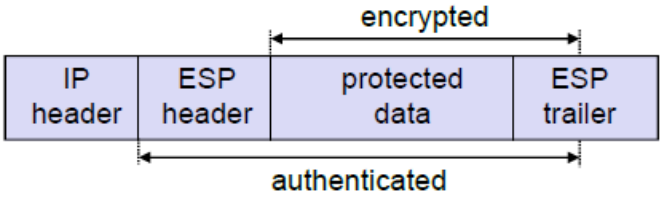


B) **In Tunnel mode**, the above process takes place as depicted in the following diagram.



2) *Encapsulating Security Payload (ESP)*

- ESP provides security services such as ***confidentiality***, ***integrity***, ***origin authentication***, and optional ***replay resistance***. The set of services provided depends on options selected at the time of ***Security Association*** (SA) establishment.
- Is realized with a header and a trailer encapsulating the data to be protected



Security Associations (SA) in IPsec

Security Association (SA) is the foundation of an IPsec communication. It provides the bundle (حزمة) of algorithms and data that provide the parameters necessary for AH and/or ESP operations. The features of SA are:

- Before sending data, a virtual connection is established between the ***sending*** entity and the ***receiving*** entity, called "***Security Association (SA)***".
- **SA** is simple in nature and hence two SAs are required for bi-directional communications.
- **SAs** are identified by a ***Security Parameter Index (SPI) number*** that exists in the security protocol header.
- Both ***sending*** and ***receiving*** entities ***maintain state information*** about the SA. It is similar to TCP endpoints which also maintain state information. ***IPsec*** is ***connection-oriented*** like TCP.
- An SA can be set up between the following peers :
  - ✓ Host ↔Host
  - ✓ Host ↔Gateway (or vice versa)
  - ✓ Gateway ↔Gateway

Parameters of SA

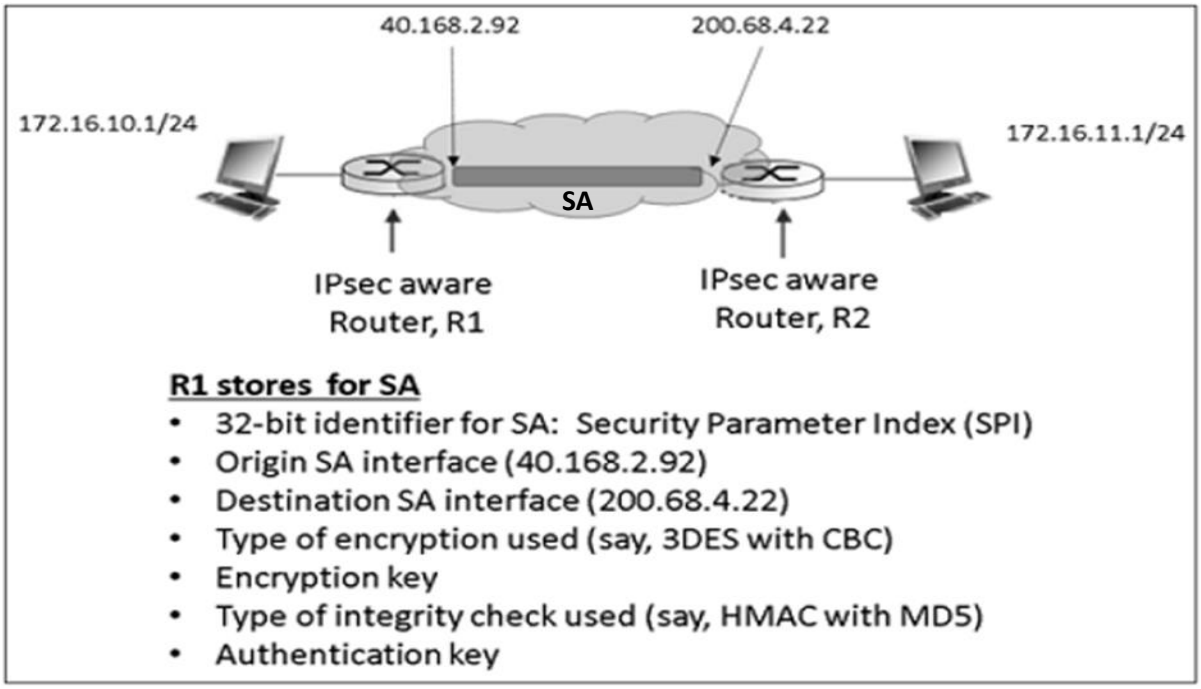
Any SA is uniquely identified by the following three parameters −

- ***Security Parameters Index (SPI).***

- It is a 32-bit value assigned to SA. It is used to distinguish among different SAs terminating at the same destination and using the same IPsec protocol.
- Every packet of IPsec carries a header containing SPI field. The SPI is provided to map the incoming packet to an SA.
- The SPI is a random number generated by the sender to identify the SA to the recipient.

- ***Destination IP Address***: It can be IP address of end router.
- ***Security Protocol Identifier***: It indicates whether the association is an AH or ESP SA.

Example of SA between two routers (R1 and R2)



Security Association Database (SAD)

- In IPsec communication, endpoint holds **SA** state in Security Association Database (SAD).
- With n- salespersons, (2+2n) SAs in R1's SAD.
- When sending IPsec datagram, R1 access SAD to determine how to process datagram.
- When IPsec datagram arrives to R2, R2 examines SPI in IPsec datagram, indexes SAD with SPI, and process datagram accordingly.
- All SA entries in the SAD are indexed by the ***three*** SA parameters: ***Destination IP address***, ***Security Protocol Identifier***, and ***SPI***.

Summary

Network-Layer Security: IPsec

The **IP security** protocol, more commonly known as IPsec, is a suite of protocols that provides security at the network layer.

The IPsec is an open standard as a part of the IPv4 suite. IPsec uses the following protocols to perform various functions:

- **Authentication Headers (AH)** provides connectionless data integrity and data origin authentication for IP datagrams and provides protection against replay attacks.
- **Encapsulating Security Payloads (ESP)** provides confidentiality, connectionless integrity, data-origin authentication, an anti-replay service (a form of partial sequence integrity), and limited traffic-flow confidentiality.

- **Security Associations (SA)** provides the bundle of algorithms and data that provide the parameters necessary for AH and/or ESP operations. The Internet Security Association and Key Management Protocol (ISAKMP) provides a framework for authentication and key exchange, with actual authenticated keying material provided either by manual configuration with pre-shared keys, Internet Key Exchange (IKE and IKEv2), Kerberized Internet Negotiation of Keys (KINK), or IPSECKEY DNS records.

RFC 2401 defines the basic architecture of IPSec:

- Concepts:
  - Security association (SA), security association database (SADB)
  - Security policy, security policy database (SPD)
- Fundamental IPSec Protocols:
  - Authentication Header (AH)
  - Encapsulating Security Payload (ESP)
- Protocol Modes:
  - Transport Mode
  - Tunnel Mode
- Use of various cryptographic primitives with AH and ESP:
  - Encryption: DES-CBC, CBC mode cipher algorithms
  - Integrity: HMAC-MD5, HMAC-SHA-1, HMAC-RIPEMD-160
- Key Management Procedures: ISAKMP, IKE