Module 5
IP SECURITY

IP-level security encompasses three functional areas:

- Authentication
- Confidentiality
- Key management.

5.1 IP SECURITY OVERVIEW

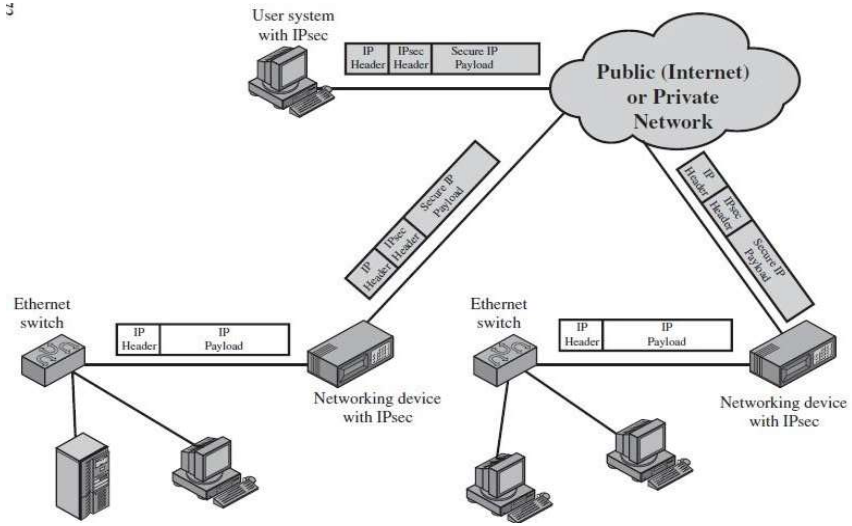
IPsec provides the capability to secure communications across a LAN, across private and public WANs, and across the Internet. Examples of its use include the following:

- ***Secure branch office connectivity over the Internet:*** A company can build a secure virtual private network over the Internet or over a public WAN. This enables a business to rely heavily on the Internet and reduce its need for private networks, saving costs and network management overhead.
- ***Secure remote access over the Internet*:** An end user whose system is equipped with IP security protocols can make a local call to an Internet Service Provider (ISP) and gain secure access to a company network. This reduces the cost of toll charges for traveling employees and telecommuters.
- ***Establishing extranet and intranet connectivity with partners:*** IPsec can be used to secure communication with other organizations, ensuring authentication and confidentiality and providing a key exchange mechanism.
- ***Enhancing electronic commerce security:*** Even though some Web and electronic commerce applications have built-in security protocols, the use of IPsec enhances that security. IPsec guarantees that all traffic designated by the network administrator is both encrypted and authenticated, adding an additional layer of security to whatever is provided at the application layer.

The below diagram shows typical scenario of IPsec usage.

- An organization maintains LANs at dispersed locations. Nonsecure IP traffic is conducted on each LAN.
- For traffic offsite, through some sort of private or public WAN, IPsec protocols are used.
- These protocols operate in networking devices, such as a router or firewall that connect each LAN to the outside world.
- The IPsec networking device will typically encrypt and compress all traffic going into the WAN and decrypt and decompress traffic coming from the WAN; these operations are transparent to workstations and servers on the LAN

- Secure transmission is also possible with individual users who dial into the WAN. Such user workstations must implement the IPsec protocols to provide security.



An IP Security Scenario

Benefits of IPsec

Some of the benefits of IPsec are:

- When IPsec is implemented in a firewall or router, it provides strong security that can be applied to all traffic crossing the perimeter.
- IPsec in a firewall is resistant to bypass if all traffic from the outside must use IP and the firewall is the only means of entrance from the Internet into the organization.
- IPsec is below the transport layer (TCP, UDP) and so is transparent to applications.
- IPsec can be transparent to end users. There is no need to train users on security mechanisms, issue keying material on a per-user basis, or revoke keying material when users leave the organization.
- IPsec can provide security for individual users if needed.

Routing Applications

IPsec can assure that

- A router advertisement comes from an authorized router.
- A neighbor advertisement comes from an authorized router.
- A redirect message comes from the router to which the initial IP packet was sent.
- A routing update is not forged.

5.2 IP SECURITY ARCHITECTURE

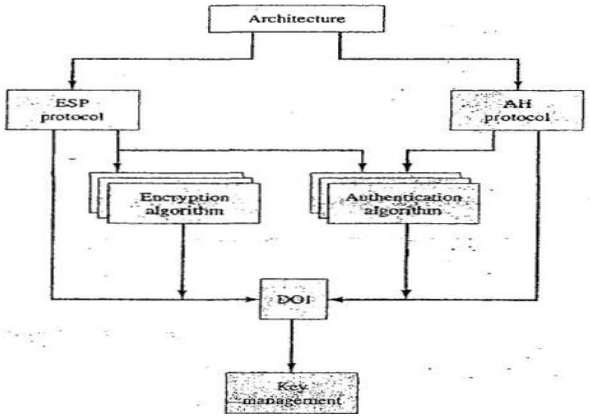
IPsec Documents :

- ✓ IPsec encompasses three functional areas: authentication, confidentiality, and key management. The best way to grasp the scope of IPsec is to consult the latest version of the IPsec document roadmap, which as of this writing is [FRAN09].

The documents can be categorized into the following groups.

- **Architecture:**
  Covers the general concepts, security requirements, definitions, and mechanisms defining IPsec technology.
- **Encapsulating Security Payload (ESP):**
  ESP consists of an encapsulating header and trailer used to provide encryption or combined encryption/authentication.
- **Authentication Header (AH):**
  AH is an extension header to provide message authentication. **Encryption Algorithm:** A set of documents that describe how various encryption algorithms are used for ESP
- **Authentication Algorithm:**
  A set of documents that describe how various authentication algorithms are used for AH and for the authentication option of ESP
- **Key Management:** document that describes key management schemes.
- **Domain of Interpretation(DOI):** contains values needed for the other documents to relate to each other.

The below diagram shows this concept



IPSec Document Overview

IPsec Services

- ✓ IPsec provides security services at the IP layer by enabling a system to select required security protocols, determine the algorithm(s) to use for the service(s), and put in place any cryptographic keys required to provide the requested services.
- ✓ Two protocols are used to provide security:
  - An authentication protocol designated by the header of the protocol, Authentication Header (AH)
  - A combined encryption/ authentication protocol designated by the format of the packet for that protocol, Encapsulating Security Payload (ESP).
- ✓ The services are:
  - Access control
  - Connectionless integrity
  - Data origin authentication
  - Rejection of replayed packets (a form of partial sequence integrity)
  - Confidentiality (encryption)
  - Limited traffic flow confidentiality

Security Associations

- ✓ An association is a one-way logical connection between a sender and a receiver that affords security services to the traffic carried on it.
- ✓ Security association (SA) is the key concept for both authentication and confidentiality mechanism for IP.
- ✓ A security association is uniquely identified by three parameters.
  - **Security Parameters Index (SPI):** A bit string assigned to this SA and having local significance only. The SPI is carried in AH and ESP headers to enable the receiving system to select the SA under which a received packet will be processed.
  - **IP Destination Address:** This is the address of the destination endpoint of the SA, which may be an end-user system or a network system such as a firewall or router.
  - **Security Protocol Identifier:** This field from the outer IP header indicates whether the association is an AH or ESP security association.

SA Parameter(Security Association Database)

- ✓ A security association is defines the parameter associated with SA.
- ✓ A security association is normally defined by the following parameters in an SAD entry.
  - **Security Parameter Index:** A 32-bit value selected by the receiving end of an SA to uniquely identify the SA.
  - **Sequence Number Counter:** A 32-bit value used to generate the Sequence Number field in AH or ESP headers.

- **Sequence Counter Overflow:** A flag indicating whether overflow of the Sequence Number Counter should generate an auditable event and prevent further transmission of packets on this SA
- **Anti-Replay Window:** Used to determine whether an inbound AH or ESP packet is a replay.
- **AH Information:** Authentication algorithm, keys, key lifetimes, and related parameters being used with AH
- **ESP Information:** Encryption and authentication algorithm, keys, initialization values, key lifetimes, and related parameters being used with ESP
- **Lifetime of this Security Association:** A time interval or byte count after which an SA must be replaced with a new SA or terminated, plus an indication of which of these actions should occur.
- **IPsec Protocol Mode:** Tunnel, transport, or wildcard.
- **Path MTU:** Any observed path maximum transmission unit and aging variables

SA Selectors (Security Policy Database)

- ✓ IPSec provides the user with considerable flexibility in the way in which IPSec services are applied.
- ✓ IP traffic is related to specific SAs (or no SA in the case of traffic allowed to bypass IPsec) is the nominal Security Policy Database (SPD).
- ✓ In its simplest form, an SPD contains entries, each of which defines a subset of IP traffic and points to an SA for that traffic.
- ✓ In more complex environments, there may be multiple entries that potentially relate to a single SA or multiple SAs associated with a single SPD entry.
- ✓ Each SPD entry is defined by a set of IP and upper-layer protocol field values, called *selectors*.
- ✓ These selectors are used to filter outgoing traffic in order to map it into a particular SA.

Outbound processing obeys the following general sequence for each IP packet:

1. Compare the values of the appropriate fields in the packet (the selector fields) against the SPD to find a matching SPD entry, which will point to zero or more SAs.
2. Determine the SA if any for this packet and its associated SPI.
3. Do the required IPsec processing (i.e., AH or ESP processing).

The following selectors determine an SPD entry:

- **Remote IP Address (destination IP address):** This may be a single IP address, an enumerated list or range of addresses, or a wildcard (mask) address.
- **Source IP Address:** This may be a single IP address, an enumerated list or range of addresses, or a wildcard (mask) address.
- **UserID:** a user identifier from the operating system

- **Data sensitivity level:** used for systems providing information flow security
- **Transport layer protocol:** this may be an individual protocol number, a list of protocol numbers, or a range of protocol numbers
- **Source and Destination ports:** these may be individual TCP or UDP port values, an enumerated list of ports or a wildcard port

Transport and Tunnel Modes

- ✓ Both AH and ESP support two modes of use
  - Transport mode
  - Tunnel mode
- ✓ The below table shows the functionality of transport mode and tunnel mode

Tunnel Mode and Transport Mode Functionality

	Transport Mode SA	Tunnel Mode SA
AH	Authenticates IP payload and selected portions of IP header and IPv6 extension headers.	Authenticates entire inner IP packet (inner header plus IP payload) plus selected portions of outer IP header and outer IPv6 extension headers.
ESP	Encrypts IP payload and any IPv6 extension headers following the ESP header.	Encrypts entire inner IP packet.
ESP with Authentication	Encrypts IP payload and any IPv6 extension headers following the ESP header. Authenticates IP payload but not IP header.	Encrypts entire inner IP packet. Authenticates inner IP packet.

Transport Mode:

- ✓ Transport mode provides protection primarily for upper-layer protocols.
- ✓ Transport mode protection extends to the payload of an IP packet.

Example: TCP or UDP segment or an ICMP packet

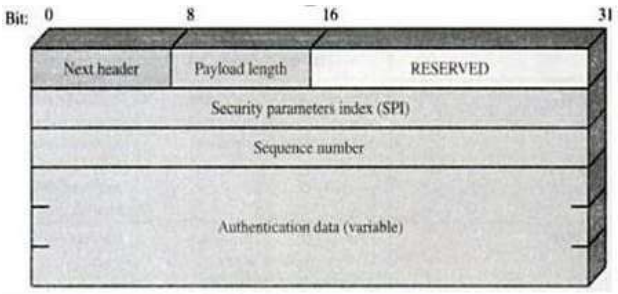
- ✓ Transport mode is used for end-to-end communication between two hosts (e.g., a client and a server, or two workstations).
- ✓ When a host runs AH or ESP over IPv4, the payload is the data that normally follow the IP header.
- ✓ For IPv6, the payload is the data that normally follow both the IP header and any IPv6 extensions headers that are present, with the possible exception of the destination options header, which may be included in the protection.
- ✓ ESP in transport mode encrypts and optionally authenticates the IP payload but not the IP header.
- ✓ AH in transport mode authenticates the IP payload and selected portions of the IP header.

Tunnel Mode:

- ✓ Tunnel mode provides protection to the entire IP packet. To achieve this, after the AH or ESP fields are added to the IP packet, the entire packet plus security fields is treated as the payload of new outer IP packet with a new outer IP header.
- ✓ The entire original, inner, packet travels through a tunnel from one point of an IP network to another; no routers along the way are able to examine the inner IP header.
- ✓ Because the original packet is encapsulated, the new, larger packet may have totally different source and destination addresses, adding to the security.
- ✓ Tunnel mode is used when one or both ends of a security association (SA) are a security gateway, such as a firewall or router that implements IPsec.

5.3 AUTHENTICATION HEADER

- ✓ The Authentication Header provides support for data integrity and authentication of IP packets
- ✓ The data integrity feature ensures that undetected modification to a packet's content in transit is not possible
- ✓ The authentication feature enables an end system or network device to authenticate the user or application and filter traffic accordingly
- ✓ It also prevents the address spoofing attacks and guards against the replay attack.
- ✓ The below diagram shows IPSec authentication header



IPSec Authentication Header

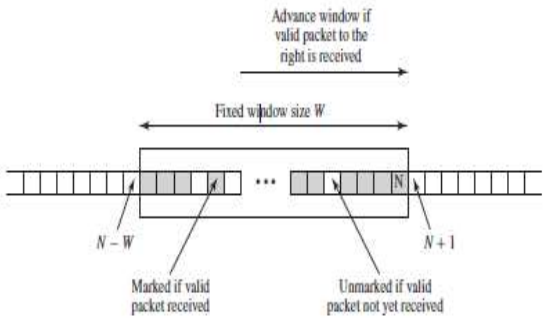
The authentication header consists of the following fields:

- ✓ **Next Header (8 bits):** Identifies the type of the header immediately following this header.
- ✓ **Payload Length(8 bits):** Length of authentication header in 32-bit words, minus 2.
- ✓ **Reserved(16 bits):** For future use.
- ✓ **Security Parameters Index(32 bits):** Identifies a security association.

- ✓ **Sequence Number(32 bits):** A monotonically increasing counter value
- ✓ **Authentication Data(variable):** A variable-length field that contains the Integrity Check value(ICV),or MAC for the packet.

Anti-Replay service

- ✓ A replay attack is one in which an attacker obtains a copy of an authenticated packet and later transmits it to the intended destination
- ✓ The sequence number field is designed to thwart such attacks
- ✓ When a new SA is established, the sender initializes a sequence number counter to 0
- ✓ Each time a packet is sent on this SA, the sender increments the counter and places the value in sequence number field .Thus, the first value to be used is 1.
- ✓ If anti-replay is enabled, the sender must not allow the sequence number to cycle past $2^{32} - 1$ back to 0 otherwise, there would be multiple valid packets with the same sequence number.
- ✓ If the limit of 232 – 1 is reached, the sender should terminate this SA and negotiate a new SA with a new key.
- ✓ Because IP is a connectionless, unreliable service, the protocol does not guarantee that packets will be delivered in order and does not guarantee that all packets will be delivered.
- ✓ The IPSec authentication document dictates that the receiver should implement a window of size W with a default of W=64.
- ✓ The right edge of the window represents the highest sequence number, , so far received for a valid packet.
- ✓ For any packet with a sequence number in the range from to that has been correctly received (i.e., properly authenticated), the corresponding slot in the window is marked .



Anti-replay Mechanism

- ✓ Inbound processing proceeds as follows when a packet is received:

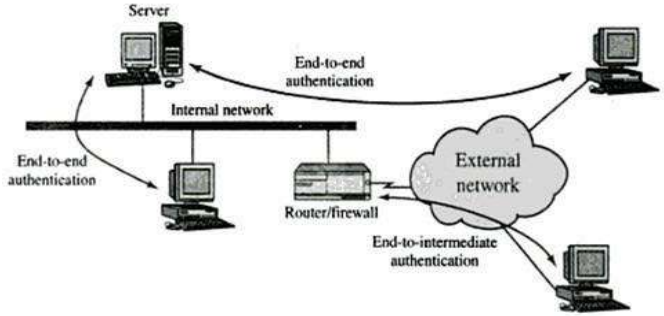
1. If the received packet falls within the window and is new, the MAC is checked. If the packet is authenticated, the corresponding slot in the window is marked.
2. If the received packet is to the right of the window and is new, the MAC is checked. If the packet is authenticated, the window is advanced so that this sequence number is the right edge of the window, and the corresponding slot in the window is marked.
3. If the received packet is to the left of the window, or if authentication fails, the packet is discarded; this is an auditable event.

Integrity Check Value

- ✓ The ICV is a message authentication code or truncated version of a code produced by a MAC algorithm.
- ✓ The MAC is calculated over
  1. IP header fields that either do not change or that are predictable in value upon arrival at the endpoint for the AH SA>
  2. The AH header other than the authentication data field.
  3. The entire upper-level protocol data, which is assumed to be immutable in transit.

Transport and Tunnel Modes

- ✓ The below diagram shows two ways in which the IPSec authentication service can be used.



End-to-End versus End-to-Intermediate Authentication

Transport Mode:

- ✓ In this case authentication is provided directly between a server and client workstations; the workstations can be either on the same network as the server or on an external network.

- ✓ As long as the workstation and the server share a protected secret key, the authentication process is secure.

Tunnel Mode:

- ✓ In this case a remote workstation authenticates itself to the corporate firewall, either for access to the entire internal network or because the requested server does not support the authentication feature.
- ✓
- ✓ For **transport mode** AH using IPv4, the AH is inserted after the original IP header and before the IP payload
- ✓ Authentication covers the entire packet, excluding mutable fields in the IPv4 header that are set to zero for MAC calculation
- ✓ For **tunnel mode** AH, 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 carries the ultimate source and destination address
- ✓ The outer IP header may contain different IP addresses
- ✓ The below diagram shows Scope of AH Encryption and Authentication scheme

Original IPv4 Header (any options)	TCP	Data

IPv4----After applying AH (transport mode)

Original IPv4 Header (any options)	AH	TCP	Data

IPv4----After applying AH (tunnel mode)

New IPv4 Header (any options)	AH	Orig IPv4 Header (any options)	TCP	Data

(a)

IPv6----Before applying AH

Original IPv6 Header	Extension Header if present	TCP	Data

IPv6----After applying AH (transport mode)

Original IPv6 Header	Extension Header if present *	AH	Dest. *	TCP	Data

*: If destination extension header presents, it could be before AH, after AH or both

IPv6----After applying AH (tunnel mode)

New IPv6 Header	New Extension Headers if present	AH	Orig IPv6 Header	Extension Headers if present	TCP	Data

(b)

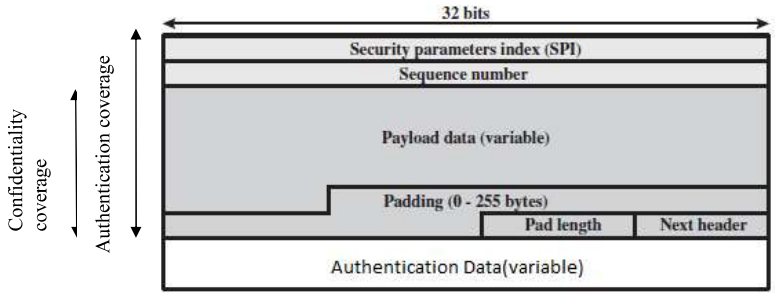
Scope of AH Authentication

5.4 ENCAPSULATING SECURITY PAYLOAD(ESP)

- ✓ ESP can be used to provide confidentiality, data origin authentication, connectionless integrity, an anti-replay service (a form of partial sequence integrity), and (limited) traffic flow confidentiality
- ✓ The set of services provided depends on options selected at the time of Security Association (SA) establishment and on the location of the implementation in a network topology.
- ✓ ESP can work with a variety of encryption and authentication algorithms, including authenticated encryption algorithms such as GCM.

ESP Format

In below Figure shows the format of an ESP packet. It contains the following fields.



- **Security Parameters Index (32 bits):** Identifies a security association.
- **Sequence Number (32 bits):** A monotonically increasing counter value; this provides an anti-replay function, as discussed for AH.
- **Payload Data (variable):** This is a transport-level segment (transport mode) or IP packet (tunnel mode) that is protected by encryption.
- **Padding (0–255 bytes):** The purpose of this field is discussed later.
- **Pad Length (8 bits):** Indicates the number of pad bytes immediately preceding this field.
- **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 that contains Integrity Check value computed over the ESP Packet minus the Authentication Data field.

Encryption and Authentication Algorithms

- ✓ The Payload Data, Padding, Pad Length, and Next Header fields are encrypted by the ESP service. These include:
  - ➢ Three-key triple DES
  - ➢ RC5
  - ➢ IDEA
  - ➢ Three-key triple IDEA
  - ➢ CAST
  - ➢ Blowfish

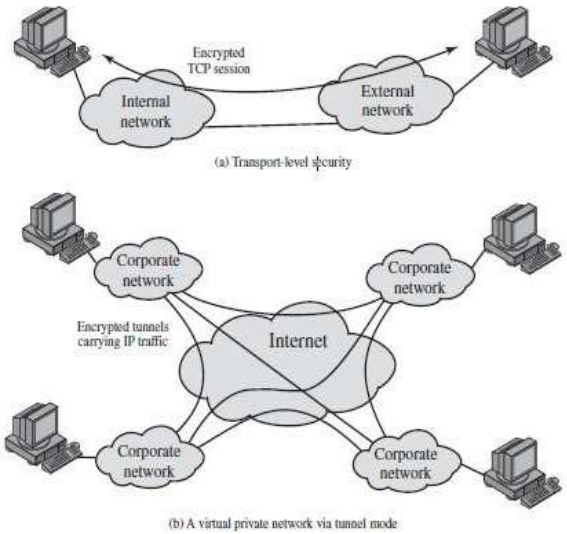
Padding

The Padding field serves several purposes:

- ➢ If an encryption algorithm requires the plaintext to be a multiple of some number of bytes, the Padding field is used to expand the plaintext to the required length.
- ➢ The ESP format requires that the Pad Length and Next Header fields be right aligned within a 32-bit word.
- ➢ Additional padding may be added to provide partial traffic-flow confidentiality by concealing the actual length of the payload.

Transport and Tunnel Modes

The below Figure shows two ways in which the IPSec ESP service can be used.



Transport-Mode versus Tunnel-Mode Encryption

- ✓ In Transport mode Encryption is provided directly between two hosts.
- ✓ In Tunnel mode operation can be used to set up a ***virtual private network***.
- ✓ In the above diagram, an organization has four private networks interconnected across the Internet. Hosts on the internal networks use the Internet for transport of data but do not interact with other Internet-based hosts. By terminating the tunnels at the security gateway to each internal network, the configuration allows the hosts to avoid implementing the security capability.

Transport Mode ESP

- ✓ Transport mode ESP is used to encrypt and optionally authenticate the data carried by IP.
- ✓ The IPv6, ESP is viewed as an end-to-end payload; that is, it is not examined or processed by intermediate routers.
- ✓ Therefore, the ESP header appears after the IPv6 base header and the hop-by-hop, routing, and fragment extension headers.

- ✓ Transport mode operation is summarized as follows.

  1. At the source, the block of data consisting of the ESP trailer plus the entire transport-layer segment is encrypted and the plaintext of this block is replaced with its ciphertext to form the IP packet for transmission. Authentication is added if this option is selected.

  2. The packet is then routed to the destination. Each intermediate router needs to examine and process the IP header plus any plaintext IP extension headers but does not need to examine the cipher text.

  3. The destination node examines and processes the IP header plus any plaintext IP extension headers.

Tunnel Mode ESP

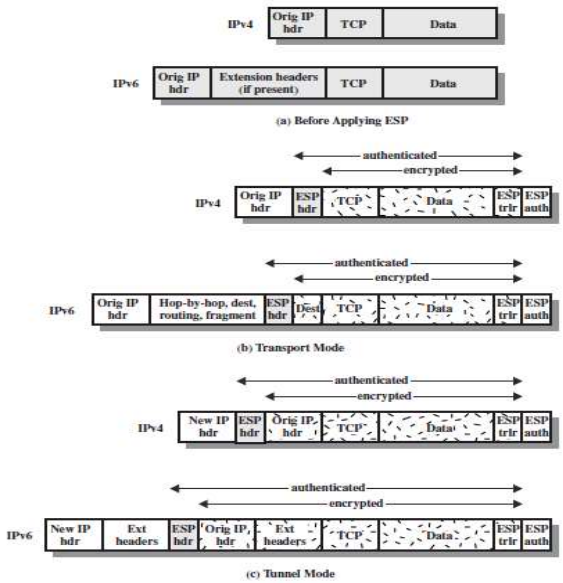
- ✓ Tunnel mode ESP is used to encrypt an entire IP packet. For this mode, the ESP header is prefixed to the packet and then the packet plus the ESP trailer is encrypted.
- ✓ This method can be used to counter traffic analysis.
- ✓ Tunnel mode ESP is used to encrypt an entire IP packet.
- ✓ The following steps occur for transfer of a transport layer segment from the external host to the internal host.

1. The source prepares an inner IP packet with a destination address of the target internal host.

2. The outer packet is routed to the destination firewall.

3. The destination firewall examines and processes the outer IP header plus any outer IP extension headers. This packet is then transmitted in the internal network.

4. The inner packet is routed through zero or more routers in the internal network to the destination host.



Scope of ESP Encryption and Authentication

5.5 COMBINING SECURITY ASSOCIATIONS

- ✓ The term security association bundle refers to a sequence of SAs through which traffic must be processed to provide a desired set of IPsec services.
- ✓ The SAs in a bundle may terminate at different endpoints or at the same endpoints. Security associations may be combined into bundles in two ways:
  - ➢ **Transport adjacency:** Refers to applying more than one security protocol to the same IP packet without invoking tunneling. This approach to combining AH and ESP allows for only one level of combination; further nesting yields no added benefit since the processing is performed at one IPsec instance: the (ultimate) destination.
  - ➢ **Iterated tunneling:** Refers to the application of multiple layers of security protocols effected through IP tunneling. This approach allows for multiple levels of nesting, since each tunnel can originate or terminate at a different IPsec site along the path.

Authentication Plus Confidentiality

Encryption and authentication can be combined in order to transmit an IP packet that has both confidentiality and authentication between hosts.

- ✓ **ESP with Authentication Option** There are two subcases:
  - ➢ **Transport mode ESP:** Authentication and encryption apply to the IP payload delivered to the host, but the IP header is not protected.
  - ➢ **Tunnel mode ESP:** The entire inner IP packet is protected by the privacy mechanism for delivery to the inner IP destination.

Transport Adjacency

- ✓ Another way to apply authentication after encryption is to use two bundled transport SAs, with the inner being an ESP SA and the outer being an AH SA
- ✓ Here ESP is used without its authentication option. Because the inner SA is a transport SA, encryption is applied to the IP payload.
- ✓ The resulting packet consists of an IP header followed by an ESP.
- ✓ AH is then applied in transport mode, so that authentication covers the ESP plus the original IP header except for mutable fields.

Advantage

- ➢ This approach over simply using a single ESP SA with the ESP authentication option is that the authentication covers more fields, including the source and destination IP addresses.

Disadvantage

- ➢ The disadvantage is the overhead of two SAs versus one SA.

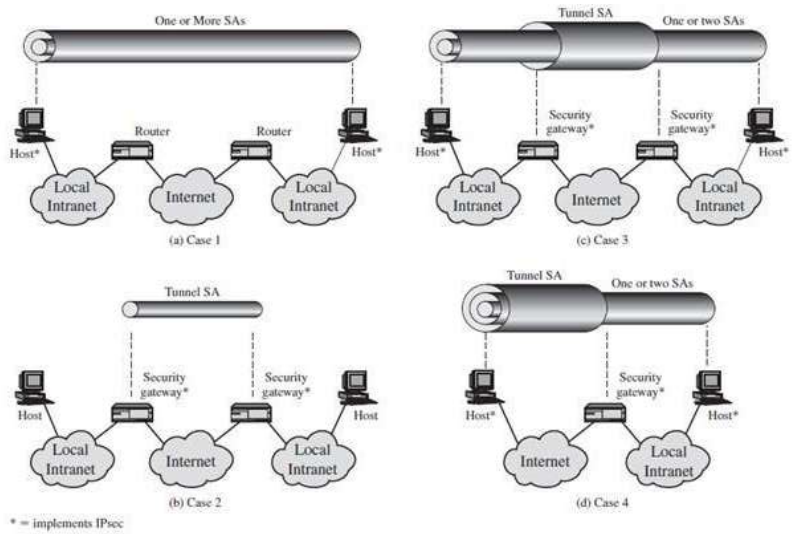
Transport-Tunnel Bundle

- ✓ The use of authentication prior to encryption might be preferable for several reasons.
  1. Because the authentication data are protected by encryption, it is impossible for anyone to intercept the message and alter the authentication data without detection.
  2. It may be desirable to store the authentication information with the message at the destination for later reference.

Basic Combinations of Security Associations

- ✓ The IPsec Architecture document lists four examples of combinations of SAs that must be supported by compliant IPsec hosts (e.g., workstation, server) or security gateways (e.g. firewall, router).

- ✓ These are illustrated in below Figure.



Basic Combinations of Security Associations

- ✓ The lower part of each case in the figure represents the physical connectivity of the elements; the upper part represents logical connectivity via one or more nested SAs.
- ✓ Each SA can be either AH or ESP. For host-to-host SAs, the mode may be either transport or tunnel; otherwise it must be tunnel mode.

Case 1.

- ➢ All security is provided between end systems that implement IPsec.
- ➢ For any two end systems to communicate via an SA, they must share the appropriate secret keys.
- ➢ Among the possible combinations are
  - **a.** AH in transport mode
  - **b.** ESP in transport mode
  - **c.** ESP followed by AH in transport mode (an ESP SA inside an AH SA)
  - **d.** Any one of a, b, or c inside an AH or ESP in tunnel mode

Case 2.

- ➢ Security is provided only between gateways (routers, firewalls, etc.) and no hosts implement IPsec.
- ➢ This case illustrates simple virtual private network support.
- ➢ The security architecture document specifies that only a single tunnel SA is needed for this case.
- ➢ The tunnel could support AH, ESP, or ESP with the authentication option.

- Nested tunnels are not required, because the IPsec services apply to the entire inner packet.

Case 3.

- This builds on case 2 by adding end-to-end security.
- The same combinations applies for cases 1 and 2 are allowed here.
- The gateway-to-gateway tunnel provides either authentication, confidentiality, or both for all traffic between end systems.
- When the gateway-to-gateway tunnel is ESP, it also provides a limited form of traffic confidentiality.
- Individual hosts can implement any additional IPsec services required for given applications or given users by means of end-to-end SAs.

Case 4.

- This provides support for a remote host that uses the Internet to reach an organization's firewall and then to gain access to some server or workstation behind the firewall.
- Only tunnel mode is required between the remote host and the firewall.
- As in case 1, one or two SAs may be used between the remote host and the local host.

5.6 KEY MANAGEMENT

- ✓ The key management of IPsec involves the determination and distribution of secret keys.
- ✓ A typical requirement is four keys for communication between two applications; transmit and receive pairs for both integrity and confidentiality.
- ✓ The IPsec Architecture document mandates support for two types of key management:
  - **Manual:** A system administrator manually configures each system with its own keys and with the keys of other communicating systems.
  - **Automated:** An automated system enables the on-demand creation of keys for SAs and facilitates the use of keys in a large distributed system with an evolving configuration.
- ✓ The default automated key management protocol for IPsec is referred to as ISAKMP/Oakley and consists of the following elements:
  - **Oakley Key Determination Protocol:** Oakley is a key exchange protocol based on the Diffie-Hellman algorithm but providing added security. Oakley is generic in that it does not dictate specific formats.
  - **Internet Security Association and Key Management Protocol (ISAKMP):** ISAKMP provides a framework for Internet key management and provides the specific protocol support, including formats, for negotiation of security attributes.

Oakley Key Determination Protocol

- ✓ It is a refinement of the Diffie-Hellman key exchange algorithm.
- ✓ The Diffie-Hellman algorithm has two attractive features:

- Secret keys are created only when needed. There is no need to store secret keys for a long period of time, exposing them to increased vulnerability.
- The exchange requires no pre-existing infrastructure other than an agreement on the global parameters. The oakley key determination algorithm is characterized by five important features:

Disadvantages of Diffie-Hellman key exchange algorithm

1. It does not provide any information about the identities of the parties.
2. It is subject to a man-in-the-middle attack, in which a third party C impersonates B while communicating with A and impersonates A while communicating with B. Both A and B end up negotiating a key with C, which can then listen to and pass on traffic
3. B computes a secret key K_1 based on B's private key and Y_E. A computes a secret key K_2 based on A's private key and Y_E. E computes K_1 using E's secret key X_E and Y_B and computers K_2 using X_E and Y_A.
4. E is able to relay messages from A to B and from B to A, appropriately changing their encipherment en route in such a way that neither A nor B will know that they share their communication with E.

Features of Oakley

The IKE key determination algorithm is characterized by five important features:

1. It employs a mechanism known as cookies to thwart clogging attacks.
2. It enables the two parties to negotiate a *group*; this, in essence, specifies the global parameters of the Diffie-Hellman key exchange.
3. It uses nonces to ensure against replay attacks.
4. It enables the exchange of Diffie-Hellman public key values.
5. It authenticates the Diffie-Hellman exchange to thwart man-in-the-middle attacks.

ISAKMP mandates that cookie generation satisfy three basic requirements:

- The cookie must depend on the specific parties.
- It must not be possible for anyone other than the issuing entity to generate cookies that will be accepted by that entity
- The cookie generation and verification methods must be fast to thwart attacks intended to sabotage processor resources

Three different **authentication** methods can be used with Oakley:

- **Digital signatures:** The exchange is authenticated by signing a mutually obtainable hash; each party encrypts the hash with its private key. The hash is generated over important parameters, such as user IDs and nonces.
- **Public-key encryption:** The exchange is authenticated by encrypting parameters such as IDs and nonces with the sender's private key.

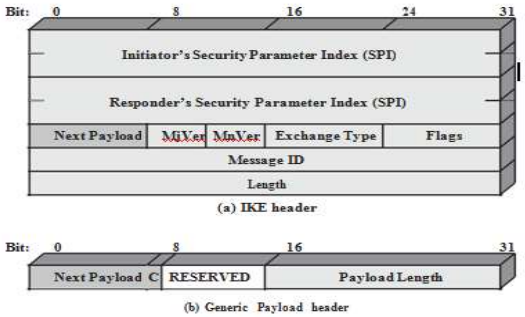
- **Symmetric-key encryption:** A key derived by some out-of-band mechanism can be used to authenticate the exchange by symmetric encryption of exchange parameters.

ISAKMP

- ✓ It defines procedures and packet formats to establish, negotiate, modify, and delete security associations.
- ✓ As part of SA establishment, IKE defines payloads for exchanging key generation and authentication data.
- ✓ These payload formats provide a consistent framework independent of the specific key exchange protocol, encryption algorithm, and authentication mechanism.

ISAKMP Header Format

- ✓ An ISAKMP message consists of an ISAKMP header followed by one or more payloads.
- ✓ All of this is carried in a transport protocol. The specification dictates that implementations must support the use of UDP for the transport protocol.
- ✓ The below Figure shows the header format for an ISAKMP message.



IKE Formats

- ✓ It consists of the following fields.
  - **Initiator SPI (64 bits):** A value chosen by the initiator to identify a unique ISAKMP security association (SA).
  - **Responder SPI (64 bits):** A value chosen by the responder to identify a unique ISAKMP SA.
  - **Next Payload (8 bits):** Indicates the type of the first payload in the message
  - **Major Version (4 bits):** Indicates major version of ISAKMP in use.

  - **Minor Version (4 bits):** Indicates minor version in use. • Exchange Type (8 bits): Indicates the type of exchange
  - **Flags (8 bits):** Indicates specific options set for this ISAKMP exchange.
  - **Message ID (32 bits):** Used to control retransmission of lost packets and matching of requests and responses.
  - **Length (32 bits):** Length of total message (header plus all payloads) in octets.

ISAKMP Payload Types

- ✓ IKE payloads begin with the same generic payload header shown in Figure IKE Format(b).
- ✓ The Next Payload field has a value of 0 if this is the last payload in the message
- ✓ The Payload Length field indicates the length in octets of this payload, including the generic payload header.
- ✓ The critical bit is 0 if the sender wants the recipient to skip this payload if it does not understand the payload type code in the Next Payload field of the previous payload.
- ✓ It is set to 1 if the sender wants the recipient to reject this entire message if it does not understand the payload type.
- ✓ The below Table summarizes the payload types defined for IKE and lists the fields, or parameters, that are part of each payload.

IKE Payload Types

Type	Parameters
Security Association	Proposals
Key Exchange	DH Group #, Key Exchange Data
Identification	ID Type, ID Data
Certificate	Cert Encoding, Certificate Data
Certificate Request	Cert Encoding, Certification Authority
Authentication	Auth Method, Authentication Data
Nonce	Nonce Data
Notify	Protocol-ID, SPI Size, Notify Message Type, SPI, Notification Data
Delete	Protocol-ID, SPI Size, # of SPIs, SPI (one or more)
Vendor ID	Vendor ID
Traffic Selector	Number of TSs, Traffic Selectors
Encrypted	IV, Encrypted IKE payloads, Padding, Pad Length, ICV
Configuration	CFG Type, Configuration Attributes
Extensible Authentication Protocol	EAP Message

1. Security Association:

- ✓ The **SA payload** is used to begin the establishment of an SA. The payload has a complex, hierarchical structure.
- ✓ The payload may contain multiple proposals. Each proposal may contain multiple protocols.
- ✓ Each protocol may contain multiple transforms. And each transform may contain multiple attributes.
- ✓ These elements are formatted as substructures within the payload as follows.
  - ➢ **Proposal:** This substructure includes a proposal number, a protocol ID (AH, ESP, or IKE), an indicator of the number of transforms, and then a transform substructure.
  - ➢ **Transform:** The transforms are used primarily to define cryptographic algorithms to be used with a particular protocol.
  - ➢ **Attribute:** Each transform include attributes that modify or complete the specification of the transform. An example is key length.

2. Key Exchange payload:

- ✓ The **Key Exchange payload** can be used for a variety of key exchange techniques, including Oakley, Diffie-Hellman, and the RSA-based key exchange used by PGP.
- ✓ The Key Exchange data field contains the data required to generate a session key and is dependent on the key exchange algorithm used.

3. Identification Payload:

- ✓ The **Identification payload** is used to determine the identity of communicating peers and may be used for determining authenticity of information. Typically the ID Data field will contain an IPv4 or IPv6 address.

4. Certificate payload :

- ✓ The **Certificate payload** transfers a public-key certificate. The Certificate Encoding field indicates the type of certificate or certificate-related information, which include the following:
  - PKCS #7 wrapped X.509 certificate
  - PGP certificate
  - DNS signed key
  - X.509 certificate—signature
  - X.509 certificate—key exchange
  - Kerberos tokens
  - Certificate Revocation List (CRL)
  - Authority Revocation List (ARL)
  - SPKI certificate

5. Certificate Request:

- ✓ At any point in an IKE exchange, the sender may include a **Certificate Request** payload to request the certificate of the other communicating entity.

- ✓ The payload may list more than one certificate type that is acceptable and more than one certificate authority that is acceptable.

6. Authentication payload:

- ✓ The **Authentication** payload contains data used for message authentication purposes.The authentication method types so far defined are RSA digital signature, shared-key message integrity code, and DSS digital signature.

7. Nonce payload :

- ✓ The **Nonce** payload contains random data used to guarantee liveness during an exchange and to protect against replay attacks.

8. Notify payload:

- ✓ The **Notify** payload contains either error or status information associated with this SA or this SA negotiation.

9. Delete payload:

- ✓ The **Delete** payload indicates one or more SAs that the sender has deleted from its database and that therefore are no longer valid.

10. Vendor ID payload:

- ✓ The **Vendor ID** payload contains a vendor-defined constant. The constant issued by vendors to identify and recognize remote instances of their implementations. This mechanism allows a vendor to experiment with new features while maintaining backward compatibility.

11.Traffic Selector payload:

- ✓ The **Traffic Selector** payload allows peers to identify packet flows for processing by IPsec services.

12. Traffic Selector payload:

- ✓ The **Encrypted** payload contains other payloads in encrypted form. The encrypted payload format is similar to that of ESP. It may include an IV if the encryption algorithm requires it and an ICV if authentication is selected.

13.Configuration payload:

- ✓ The **Configuration** payload is used to exchange configuration information between IKE peers.

14.Extensible Authentication Protocol (EAP) payload: The **Extensible Authentication Protocol (EAP)** payload allows IKE SAs to be authenticated using EAP,