IP SECURITY

Group 1

DAVID TUGUME	DENIS MBABAZI	SEBULIME STUART MCCARTHY	OBURA JULIUS

Content

- ❏ IP Security
  - ❏ IP Security Overview
  - ❏ IP Security Policy
- ❏ Encapsulating Security Payload
- ❏ Combining Security Associations
- ❏ Internet Key Exchange,
- ❏ Cryptographic Suites.

IP Security Overview

- Applications of IPsec
- Benefits of IPsec
- Routing Applications
- IPsec Documents
- IPsec Services
- Transport and Tunnel Modes

Applications of IPsec

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

- Secure branch office connectivity over the Internet: *An institution can rely mainly on Internet and reduce the need for private networks hence saving costs.*
- Secure remote access over the Internet: *This reduces the cost of toll charges for traveling employees and telecommuters.*
- Establishing extranet and intranet connectivity with partners: *Secures communication with other organizations.*
- Enhancing electronic commerce security: *IPsec guarantees additional layer of security at the application layer.*

The principal feature of IPsec is that it can encrypt and or authenticate all traffic at the IP level.

- Thus all distributed applications (remote logon, client/server, email, file transfer, Web access) can secured

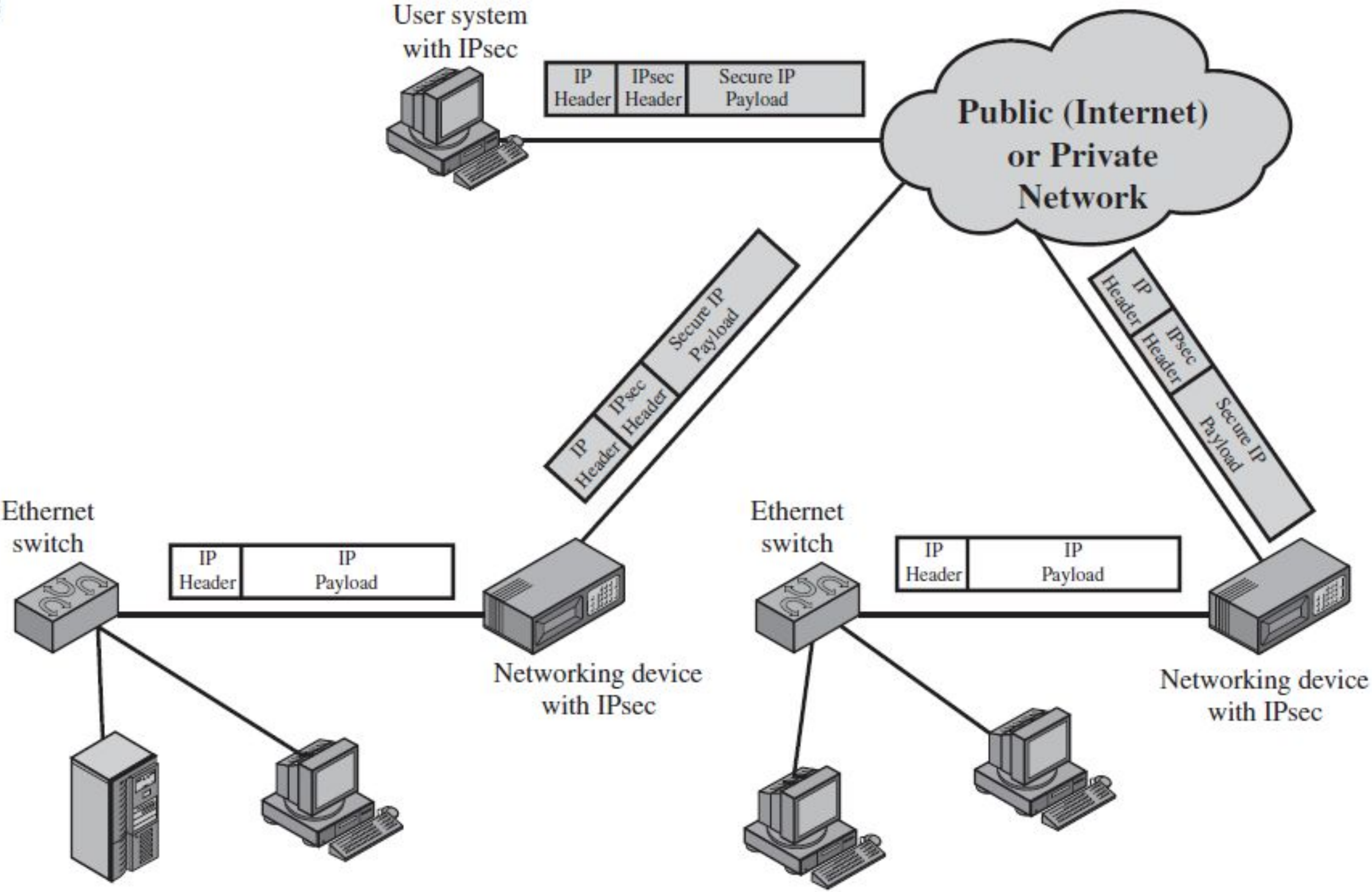


Figure 8.1 An IP Security Scenario

Benefits of IPsec

- When IPsec is implemented in a firewall or router, it provides strong security that can be applied to all traffic crossing the perimeter.
    - Traffic within a company or workgroup does not incur the overhead of security-related processing.
- 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.
    - There is no need to change software on a user or server system when IPsec is implemented in the firewall or router.
- 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.
    - This is useful for offsite workers and for setting up a secure virtual subnetwork within an organization for sensitive applications.

Routing Applications

- ❑ IPsec can play a vital role in the routing architecture required for internetworking.
- ❑ IPsec can ensure that:
    - ❑ A router advertisement (a new router advertises its presence) comes from an authorized router.
    - ❑ A neighbor advertisement (a router seeks to establish or maintain a neighbor relationship with a router in another routing domain) 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.

IPsec Documents

The documents can be categorized into the following groups.

- ❏ Architecture: *Covers the general concepts, security requirements, definitions, and mechanisms defining IPsec technology.*
- ❏ Authentication Header (AH): *An extension header to provide message authentication.*
- ❏ Encapsulating Security Payload (ESP): *ESP consists of an encapsulating header and trailer used to provide encryption.*
- ❏ Internet Key Exchange (IKE): *This is a collection of documents describing the key management schemes for use with IPsec.*
- ❏ Cryptographic algorithms: *Documents that define and describe cryptographic algorithms for encryption, message authentication and cryptographic key exchange.*
- ❏ Other: There are a variety of other IPsec-related RFCs, including those dealing with security policy and management information base (MIB) content.

IP Security Policy

- IP Security Policy deals with the security policy applied to each ip packet that transmits from source to destination.
- Security Associations: *Appears in both the authentication and confidentiality mechanisms for IP.*
- Security Association Database: *For IPsec implementation, it defines the parameters associated with each Security Associations (SA).*
- Security Policy Database: *The means by which IP traffic is related to specific SA or no SA in the case of traffic allowed to bypass IPsec.*
- IP Traffic Processing: *IPsec is executed on a packet-by-packet basis.*

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.
- RFC 4301 lists the following services:
  - Access control
  - Data origin authentication
  - Rejection of replayed packets(a form of partial sequence integrity)
  - Confidentiality(encryption)
  - Limited traffic flow confidentiality

Transport and Tunnel Modes

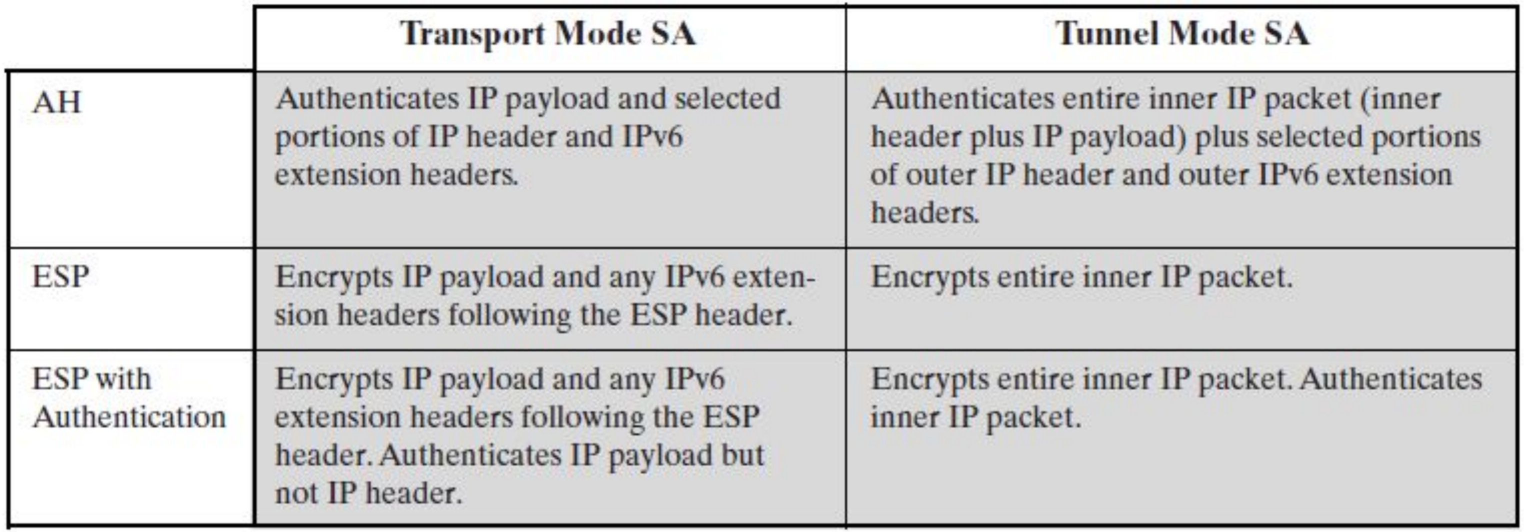
TRANSPORT MODE

- Transport mode provides protection primarily for upper-layer protocols.
- Examples include a TCP or UDP segment or an ICMP packet
- Typically used for end-to-end communication between two hosts
- 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.
- is used when one or both ends of a security association (SA) are a security gateway
- a number of hosts on networks behind firewalls may engage insecure communications without implementing IPsec.
- ESP in tunnel mode encrypts and optionally authenticates the entire inner IP packet, including the inner IP header.
- AH in tunnel mode authenticates the entire inner IP packet and selected portions of the outer IP header.

Table 8.1 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.

Security Associations

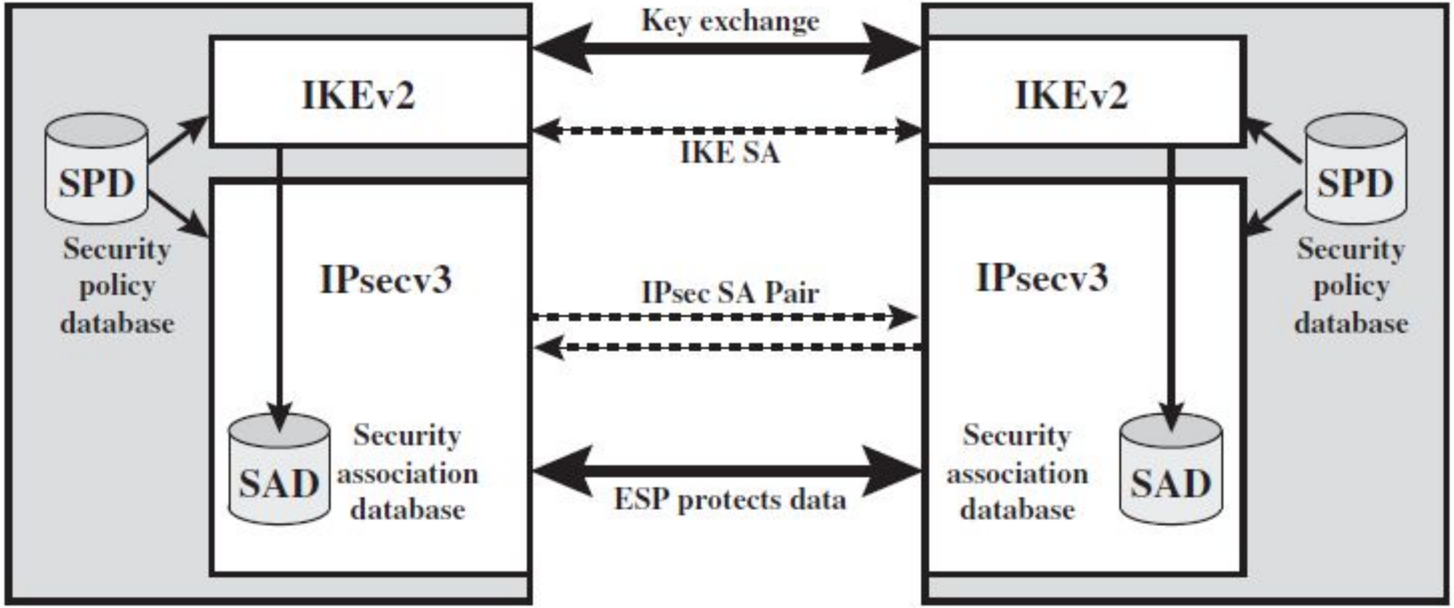


Figure 8.2 IPsec Architecture

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.
- In any IP packet, the SA is uniquely identified by the Destination Address in the IPv4 or IPv6 header and the SPI in the enclosed extension header(AH or ESP).
- 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.
  - 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.

Security Association Database

- Defines the parameters associated with each SA
- Normally defined by the following parameters in an SAD entry.
  - Security Parameter Index:
  - Sequence Number Counter:
  - Sequence Counter Overflow:
  - Anti-Replay Window:
  - AH Information
  - ESP Information:
  - Lifetime of this Security Association
  - IPsec Protocol Mode: Tunnel, transport, or wildcard.
  - Path MTU:

Security Policy Database

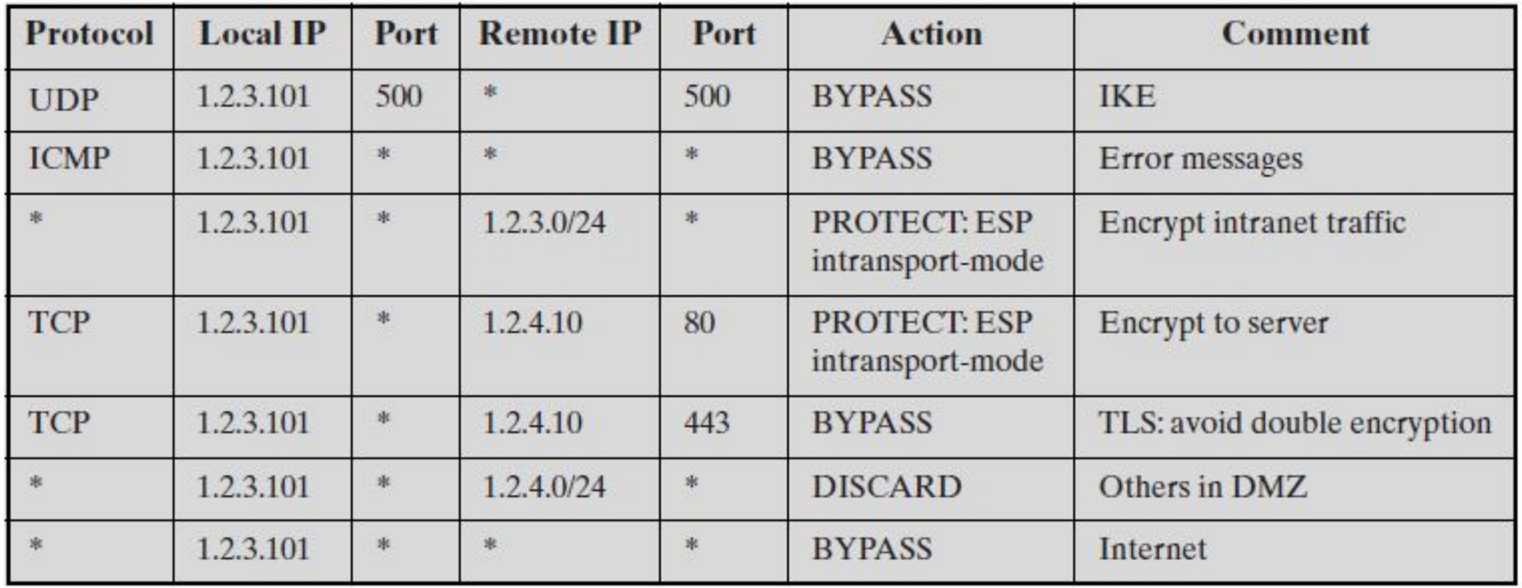
- The means by which IP traffic is related to specific SAs
- Contains entries, each of which defines a subset of IP traffic and points to an SA for that traffic.
- In more complex environments, there may be multiple entries that potentially relate to a single SA or multiple SAs associated with a single 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

SPD ENTRIES

The following selectors determine an SPD entry:

- **Remote IP Address:** This may be a single IP address, an enumerated list or range of addresses, or a wildcard (mask) address.The latter two are required to support more than one destination system sharing the same SA (e.g., behind a firewall).
- **Local IP Address:** This may be a single IP address, an enumerated list or range of addresses, or a wildcard (mask) address. The latter two are required to support more than one source system sharing the same SA (e.g., behind a firewall).
- **Next Layer Protocol:** The IP protocol header (IPv4, IPv6, or IPv6 Extension) includes a field that designates the protocol operating over IP.
- **Name:** A user identifier from the operating system.This is not a field in the IP or upper-layer headers but is available if IPsec is running on the same operating system as the user.
- **Local and Remote Ports:** These may be individual TCP or UDP port values, an enumerated list of ports, or a wildcard port.

Table 8.2 Host SPD Example



Protocol	Local IP	Port	Remote IP	Port	Action	Comment
UDP	1.2.3.101	500	*	500	BYPASS	IKE
ICMP	1.2.3.101	*	*	*	BYPASS	Error messages
*	1.2.3.101	*	1.2.3.0/24	*	PROTECT: ESP intransport-mode	Encrypt intranet traffic
TCP	1.2.3.101	*	1.2.4.10	80	PROTECT: ESP intransport-mode	Encrypt to server
TCP	1.2.3.101	*	1.2.4.10	443	BYPASS	TLS: avoid double encryption
*	1.2.3.101	*	1.2.4.0/24	*	DISCARD	Others in DMZ
*	1.2.3.101	*	*	*	BYPASS	Internet

IP Traffic Processing

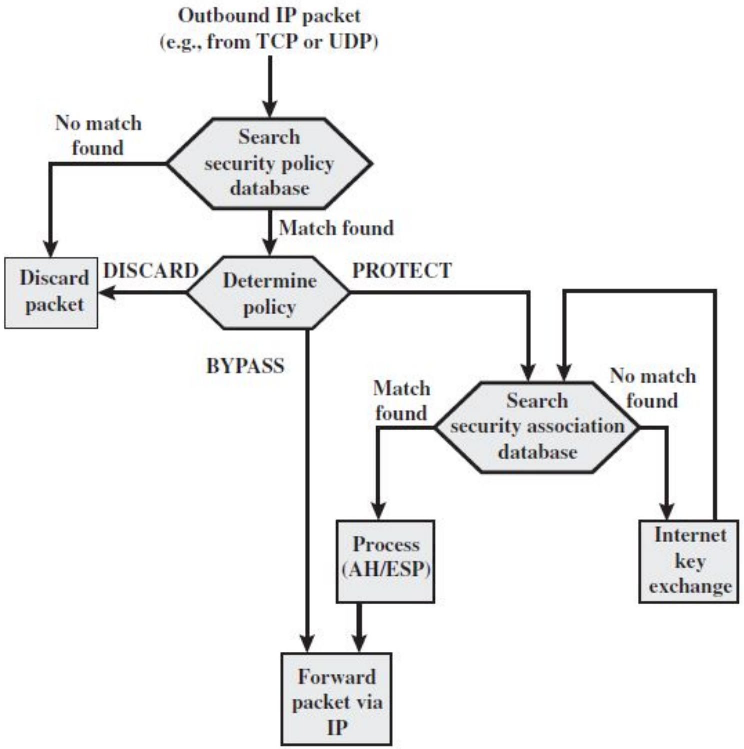


Figure 8.3 Processing Model for Outbound Packets

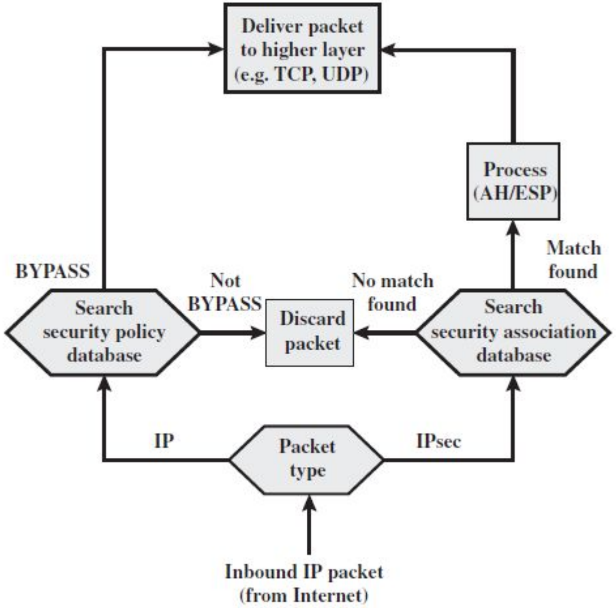


Figure 8.4 Processing Model for Inbound Packets

Encapsulating Security Payload

ESP Format

Encryption and Authentication Algorithms

Padding

Anti-Replay Service

Transport and Tunnel Modes

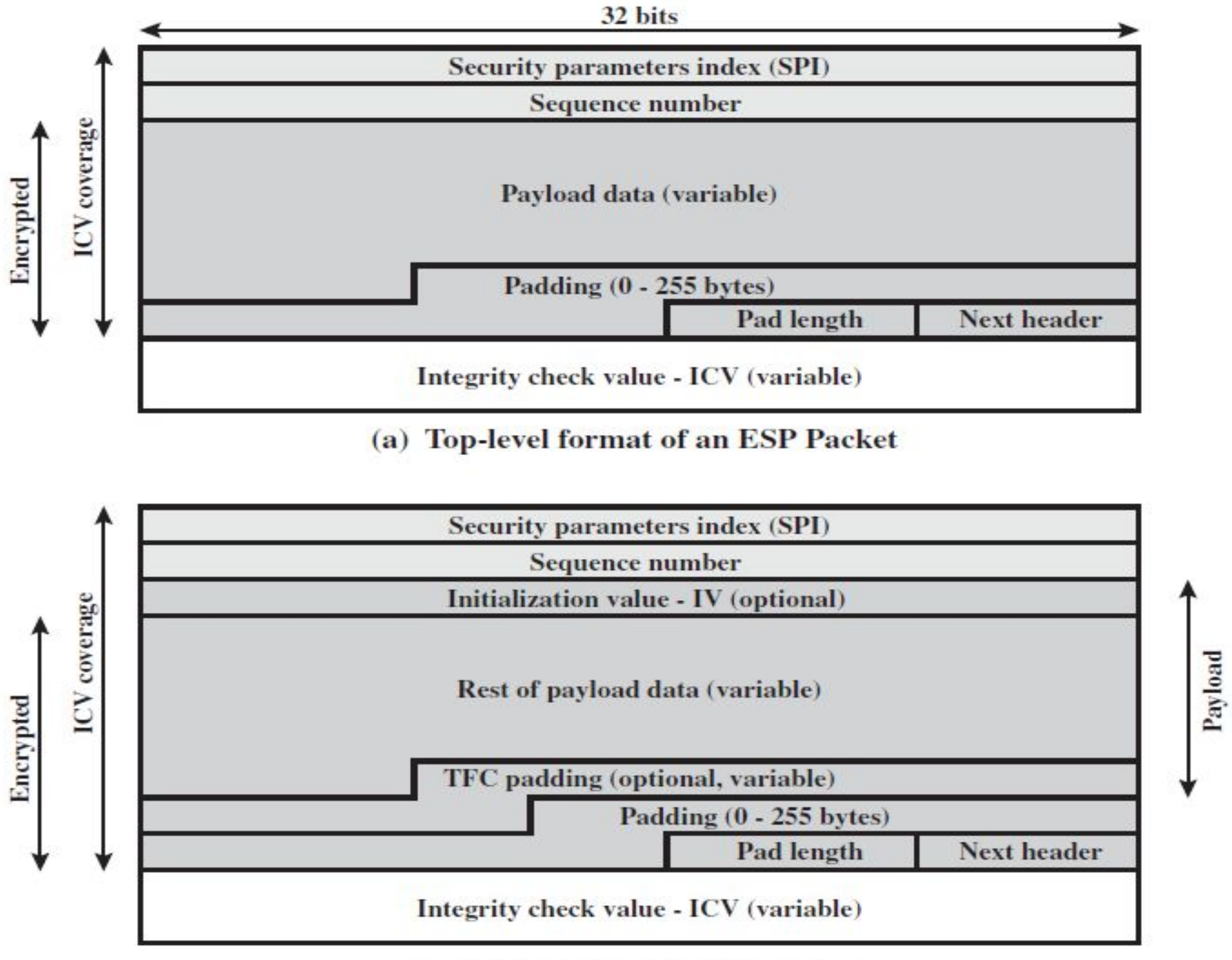
ENCAPSULATING SECURITY PAYLOAD

- 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

- Figure 8.5a shows the top-level 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
- 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):
- 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
- Integrity Check Value (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.

Fig 8.5a



32 bits

Encrypted

ICV coverage

Security parameters index (SPI)

Sequence number

Payload data (variable)

Padding (0 - 255 bytes)

Pad length

Next header

Integrity check value - ICV (variable)

(a) Top-level format of an ESP Packet

Encrypted

ICV coverage

Security parameters index (SPI)

Sequence number

Initialization value - IV (optional)

Rest of payload data (variable)

TFC padding (optional, variable)

Padding (0 - 255 bytes)

Pad length

Next header

Integrity check value - ICV (variable)

Payload

(b) Substructure of payload data

ESP FORMAT (cont’d)

•When any combined mode algorithm is employed, the algorithm itself is expected to return both decrypted plaintext and a pass/fail indication for the integrity check.

•For combined mode algorithms, the ICV that would normally appear at the end of the ESP packet (when integrity is selected) may be omitted.

•When the ICV is omitted and integrity is selected, it is the responsibility of the combined mode algorithm to encode within the Payload Data an ICV-equivalent means of verifying the integrity of the packet

•Two additional fields may be present in the payload (Figure 8.5b). An initialization value (IV), or nonce, is present if this is required by the encryption or authenticated encryption algorithm used for ESP.
If tunnel mode is being used, then the IPsec implementation may add traffic flow confidentiality (TFC) padding after the Payload Data and before the Padding field

Encryption and Authentication Algorithms

- The Payload Data, Padding, Pad Length, and Next Header fields are encrypted by the ESP service. If the algorithm used to encrypt the payload requires cryptographic synchronization data, such as an initialization vector (IV), then these data may be carried explicitly at the beginning of the Payload Data field.
- If included, an IV is usually not encrypted, although it is often referred to as being part of the ciphertext
- The ICV field is optional. It is present only if the integrity service is selected and is provided by either a separate integrity algorithm or a combined mode algorithm that uses an ICV

Encryption and Authentication Algorithms (cont'd)

- The ICV is computed after the encryption is performed.This order of processing facilitates rapid detection and rejection of replayed or bogus packets by the receiver prior to decrypting the packet, hence potentially reducing the impact of denial of service (DoS) attacks.
- It also allows for the possibility of parallel processing of packets at the receiver, i.e., decryption can take place in parallel with integrity checking

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. Equivalently, the ciphertext must be an integer multiple of 32 bits. The Padding field is used to assure this alignment.
- Additional padding may be added to provide partial traffic-flow confidentiality by concealing the actual length of the payload

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 receipt of duplicate, authenticated IP packets may disrupt service in some way or may have some other undesired consequence
- The Sequence Number field is designed to thwart such attacks
- In the next slide, I explain how sequence number is generated by the sender and how it’s processed by the recipient.

Anti-Replay Service (cont'd)

•When a new SA is established, the sender initializes a sequence number counter to 0. Each time that a packet is sent on this SA, the sender increments the counter and places the value in the Sequence Number field.

•Thus, the first value to be used is 1. If anti-replay is enabled (the default), the sender must not allow the sequence number to cycle past 232 – 1 back to zero.

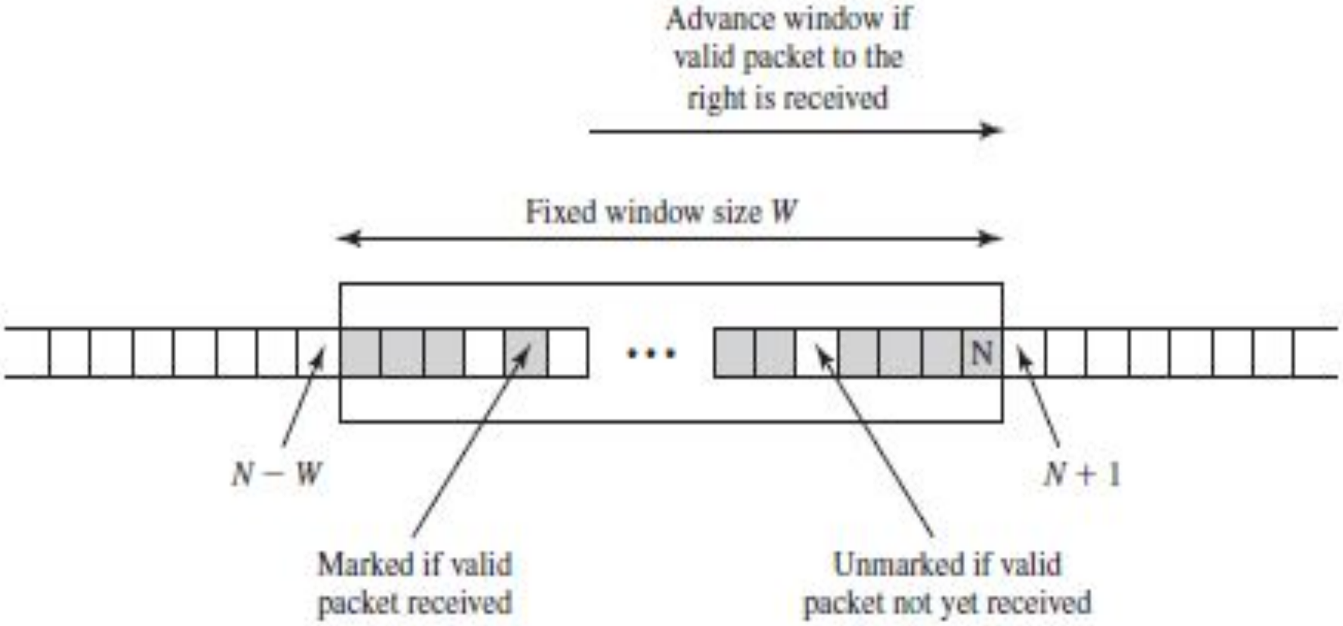
•Otherwise, there would be multiple valid packets with the same sequence number. If the limit of 232 – 1 is reached, the sender should terminate this SA and negotiate a new SA with a new key

•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. Therefore, the IPsec authentication document dictates that the receiver should implement a window of size , with a default of w= 64.

Anti-Replay Service (cont’d)

- 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 (Figure 8.6).

Fig 8.6 : Anti-Replay mechanism



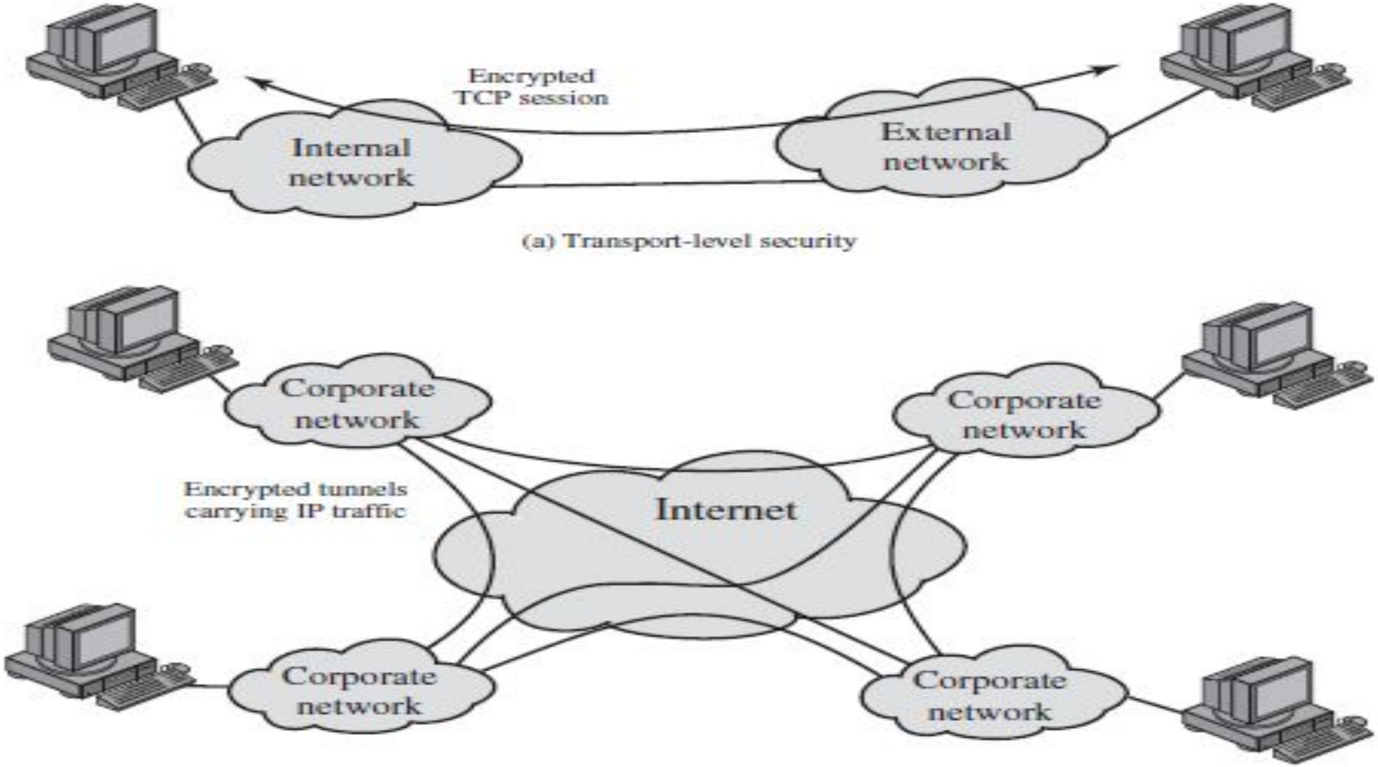
Anti-Replay Service (cont'd)

- 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.

Transport and Tunnel Modes

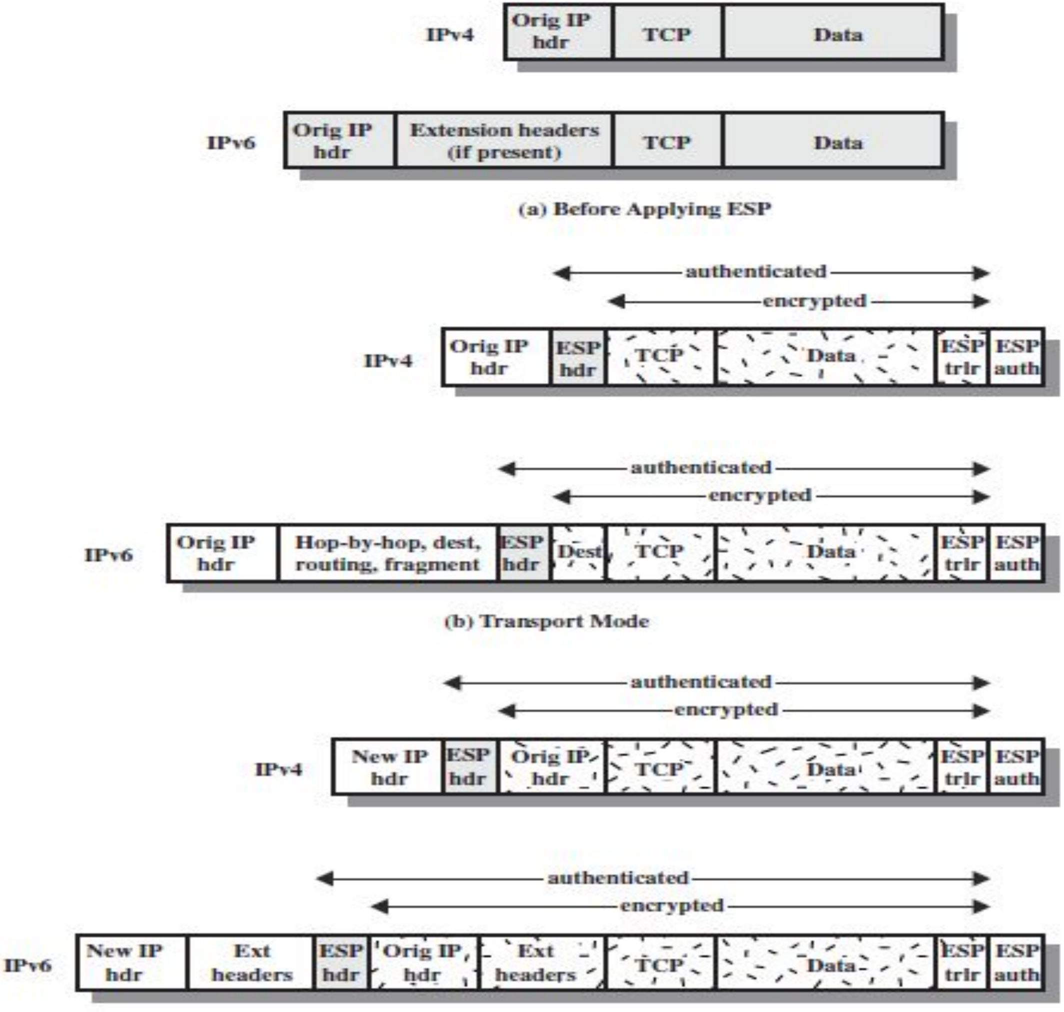
- Figure 8.7 shows two ways in which the IPsec ESP service can be used.
- In the upper part of the figure, encryption (and optionally authentication) is provided directly between two hosts.
- Figure 8.7b shows how tunnel mode operation can be used to set up a virtual private network

Figure 8.7 Transport-Mode versus Tunnel-Mode Encryption



TRANSPORT MODE ESP

- Transport mode ESP is used to encrypt and optionally authenticate the data carried by IP (e.g., a TCP segment), as shown in Figure 8.8b



(a) Before Applying ESP

(b) Transport Mode

(c) Tunnel Mode

TRANSPORT MODE ESP (cont’d)

- For this mode using IPv4, the ESP header is inserted into the IP packet immediately prior to the transport-layer header (e.g., TCP, UDP, ICMP), and an ESP trailer (Padding, Pad Length, and Next Header fields) is placed after the IP packet.
- If authentication is selected, the ESP Authentication Data field is added after the ESP trailer. The entire transport-level segment plus the ESP trailer are encrypted. Authentication covers all of the ciphertext plus the ESP header

TRANSPORT MODE ESP (cont’d)

- In the context of 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.
- The destination options extension header could appear before or after the ESP header, depending on the semantics desired.
- For IPv6, encryption covers the entire transport-level segment plus the ESP trailer plus the destination options extension header if it occurs after the ESP header.
- Again, authentication covers the ciphertext plus the ESP header

TRANSPORT MODE ESP (cont’d)

- Transport mode operation provides confidentiality for any application that uses it, thus avoiding the need to implement confidentiality in every individual application.
- One drawback to this mode is that it is possible to do traffic analysis on the transmitted packets

TUNNEL MODE ESP

•Tunnel mode ESP is used to encrypt an entire IP packet (Figure 8.8c). 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.

•Because the IP header contains the destination address and possibly source routing directives and hop-by-hop option information, it is not possible simply to transmit the encrypted IP packet prefixed by the ESP header.

•Intermediate routers would be unable to process such a packet.

Therefore, it is necessary to encapsulate the entire block (ESP header plus ciphertext plus Authentication Data, if present) with a new IP header that will contain sufficient information for routing but not for traffic analysis

TUNNEL MODE ESP (cont’d)

- Whereas the transport mode is suitable for protecting connections between hosts that support the ESP feature, the tunnel mode is useful in a configuration that includes a firewall or other sort of security gateway that protects a trusted network from external networks,
- In this latter case, encryption occurs only between an external host and the security gateway or between two security gateways.
- This relieves hosts on the internal network of the processing burden of encryption and simplifies the key distribution task by reducing the number of needed keys. Further, it thwarts traffic analysis based on ultimate destination.

COMBINING SECURITY ASSOCIATIONS

- An individual SA can implement either the AH or ESP protocol but not both. Sometimes a particular traffic flow will call for the services provided by both AH and ESP.
- Further, a particular traffic flow may require IPsec services between hosts and, for that same flow, separate services between security gateways, such as firewalls. In all of these cases, multiple SAs must be employed for the same traffic flow to achieve the desired IPsec services.
- 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

COMBINING SECURITY ASSOCIATIONS (cont’d)

- 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
- Iterated tunneling: Refers to the application of multiple layers of security protocols effected through IP tunneling
- The two approaches can be combined, for example, by having a transport SA between hosts travel part of the way through a tunnel SA between security gateways.

Authentication Plus Confidentiality

- Encryption and authentication can be combined in order to transmit an IP packet that has both confidentiality and authentication between hosts.
- We look at several approaches

ESP WITH AUTHENTICATION OPTION

- In this approach, the user first applies ESP to the data to be protected and then appends the authentication data field.
- There are actually 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: Authentication applies to the entire IP packet delivered to the outer IP destination address (e.g., a firewall), and authentication is performed at that destination
- For both cases, authentication applies to the ciphertext rather than the plaintext.

TRANSPORT ADJACENCY

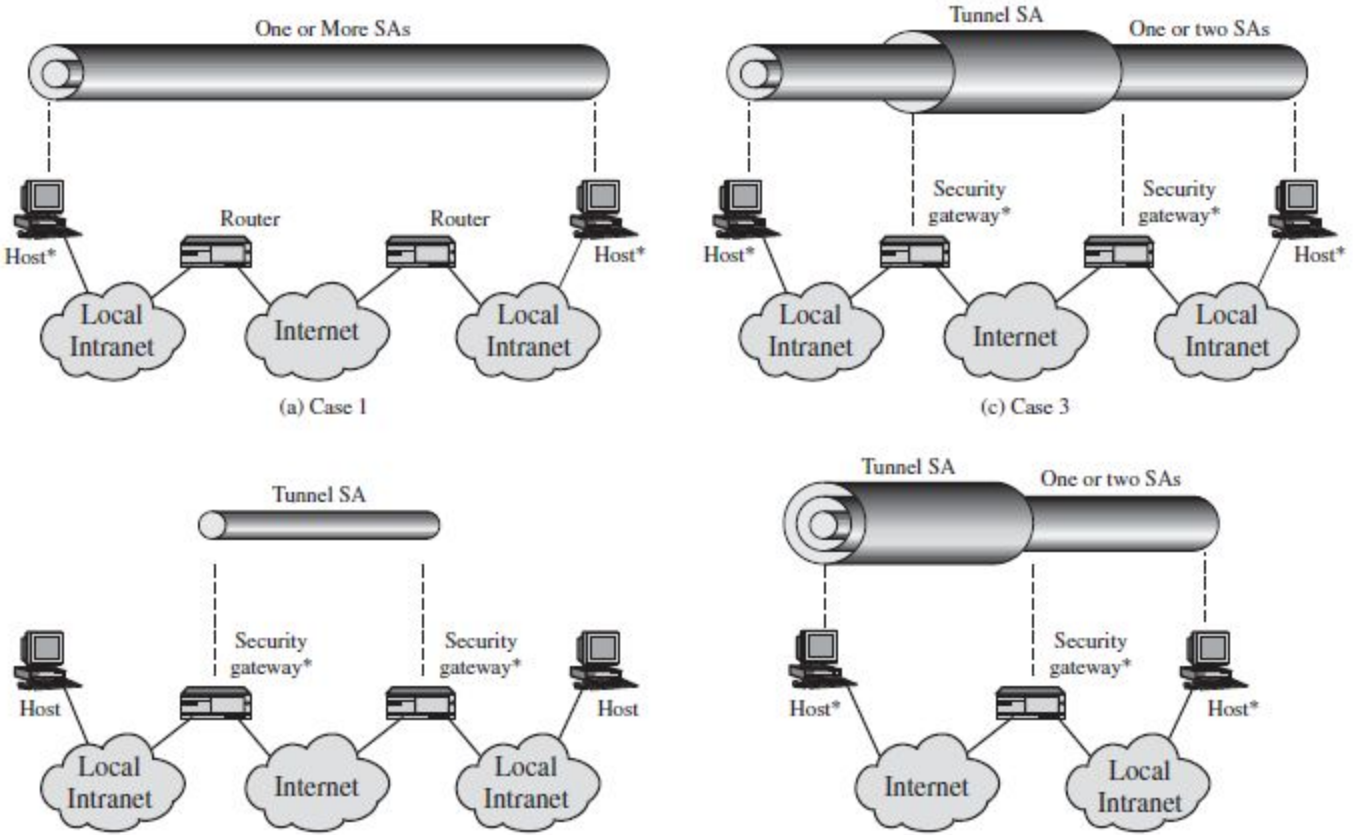
- Another way to apply authentication after encryption is to use two bundled transport SAs, with the inner being an ESP SA and the outer being an AH SA.
- In this case, ESP is used without its authentication option. Because the inner SA is a transport SA, encryption is applied to the IP payload.
- The resulting packet consists of an IP header (and possibly IPv6 header extensions) followed by an ESP
- The advantage of 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.
- 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. First, because the authentication data are protected by encryption, it is impossible for anyone to intercept the message and alter the authentication data without detection
- Second, it may be desirable to store the authentication information with the message at the destination for later reference
- One approach to applying authentication before encryption between two hosts is to use a bundle consisting of an inner AH transport SA and an outer ESP tunnel SA.
- In this case, authentication is applied to the IP payload plus the IP header (and extensions) except for mutable fields
- The resulting IP packet is then processed in tunnel mode by ESP; the result is that the entire, authenticated inner packet is encrypted and a new outer IP header (and extensions) is added

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 Figure 8.10. 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.



(a) Case 1

(c) Case 3

(b) Case 2

(d) Case 4

* = implements IPsec

Basic Combinations of Security Associations(cont’d)

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.

•**Case 1.** All security is provided between end systems that implement IPsec.

Case 2. Security is provided only between gateways (routers, firewalls, etc.)

and no hosts implement IPsec. This case illustrates simple virtual private network

Support

Case 3. This builds on case 2 by adding end-to-end security.The same combinations

discussed for cases 1 and 2 are allowed here.

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.

Internet Key Exchange

The key management portion of IPsec involves the determination and distribution of secret keys

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 protocols are referred to as ISAKMP/Oakley

Automated key management protocols

Oakley Key Distribution Protocol

- Based on Diffie Hellman algorithms
- Provided added security
- It is generic

Internet Security Association and Key Management Protocol (ISAKMP)

- Provides framework for internet Key management
- Provides the specific protocol support for negotiation of security attributtes

Key Determination Protocol

IKE key determination is a refinement of the **Diffie-Hellman key exchange algorithm** where advantages are retained while countering its weakenesses

- interaction between users A and B
- There is prior agreement on two global parameters: , a large prime number; and , a primitive root of q.
- A selects a random integer as its private key and transmits to B its public key . Similarly, B selects a random integer as its private key and transmits to A its public key .
- Computing the secret session key (K = (B) XA mod q = (A) XB mod q = aXAXB mod q)

he 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

Weaknesses to Diffie-Hellman

- It does not provide any information about the identities of the parties.

- 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.

man-in-the-middle attack

1. B sends his public key in a message addressed to A

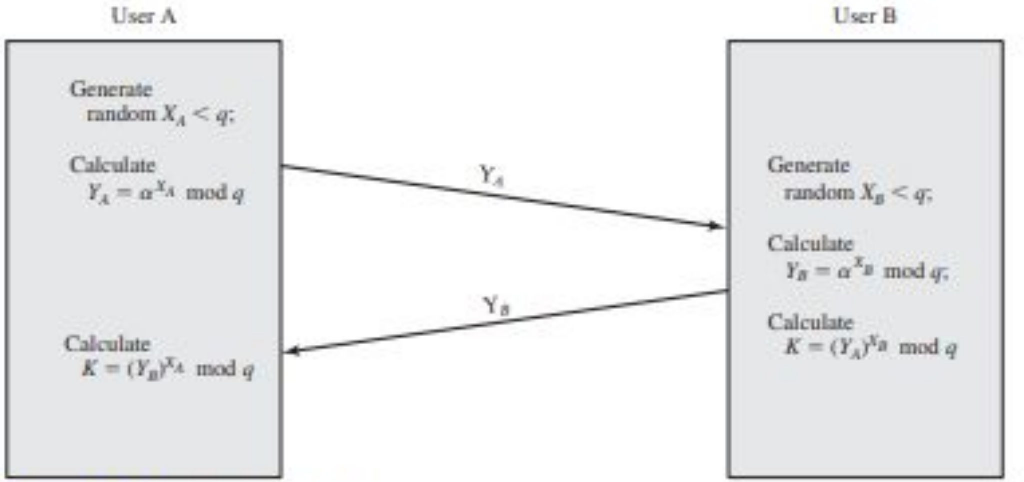

User A
Generate random $X_A < q$;
Calculate $Y_A = \alpha^{X_A} \bmod q$
Y_A
User B
Generate random $X_B < q$;
Calculate $Y_B = \alpha^{X_B} \bmod q$;
Calculate $K = (Y_A)^{X_B} \bmod q$
Y_B
Calculate $K = (Y_B)^{X_A} \bmod q$

Figure 3.13 Diffie-Hellman Key Exchange

weaknesses to Diffie-Hellman (Cont)

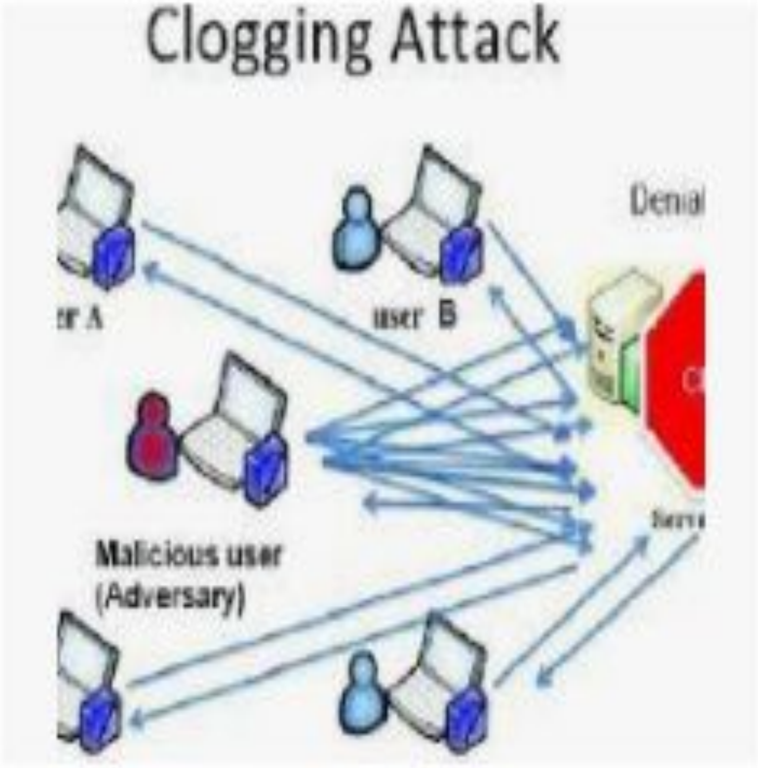
- It is computationally intensive.As a result, it is vulnerable to a clogging attack, in which an opponent requests a high number of keys.

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.

Cookies

- In this attack, an opponent forges the source address of a legitimate user and sends a public Diffie Hellman key to the victim
- The victim then performs a modular exponentiation to compute the secret key.
- Repeated messages of this type can clog the victim's system with useless work.



Cookies (Cont)

- The **cookie exchange** requires that each side send a pseudorandom number
- the cookie, in the initial message, which the other side acknowledges.
- acknowledgment must be repeated in the first message of the Diffie-Hellman key exchange
- If the source address was forged, the opponent gets no answer
- Thus, an opponent can only force a user to generate acknowledgments and not to perform the Diffie-Hellman calculation

IKE 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.

The recommended method for creating the cookie is to perform a fast hash (e.g., MD5) over the IP Source and Destination addresses, the UDP Source and Destination ports, and a locally generated secret value.

IKE key determination

The different authentication methods that can be used with IKE key determination:

- 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.

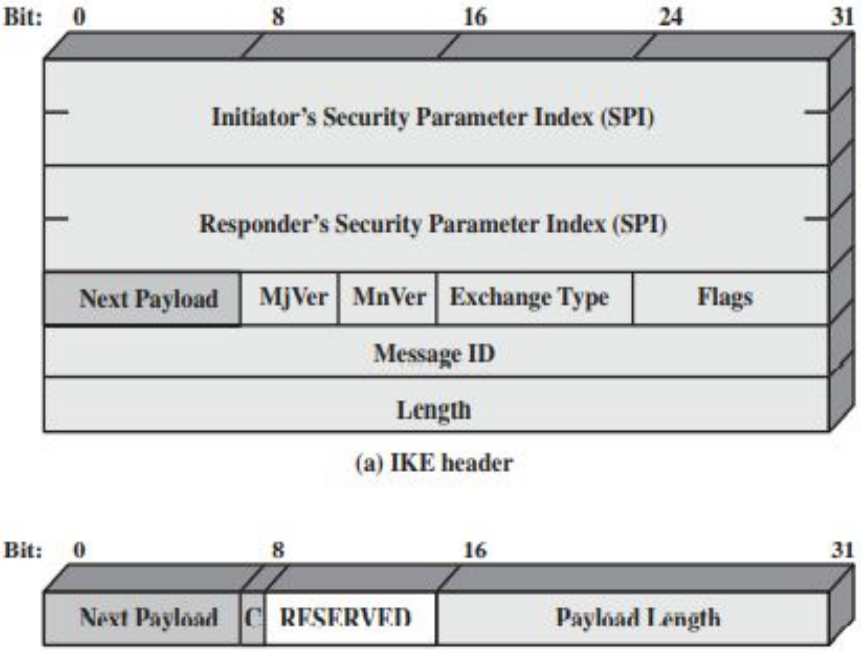
header format for an IKE message

It consists of the following fields.

- **Initiator SPI (64 bits):** A value chosen by the initiator to identify a unique IKE security association (SA).
- **Responder SPI (64 bits):** A value chosen by the responder to identify a unique IKE SA.
- **Next Payload (8 bits):** Indicates the type of the first payload in the message; payloads are discussed in the next subsection.
- **Major Version (4 bits):** Indicates major version of IKE in use.
- **Minor Version (4 bits):** Indicates minor version in use.

IKE Header and Formats

- **Exchange Type (8 bits):** Indicates the type of exchange
- **Flags (8 bits):** Indicates specific options set for this IKE 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



(a) IKE header

(b) Generic Payload header

Figure 8.12 IKE Formats

Cryptographic Suites

What is cryptographic suits? This is a set of cryptography instructions or algorithms that help secure network connections through the transport layer security.

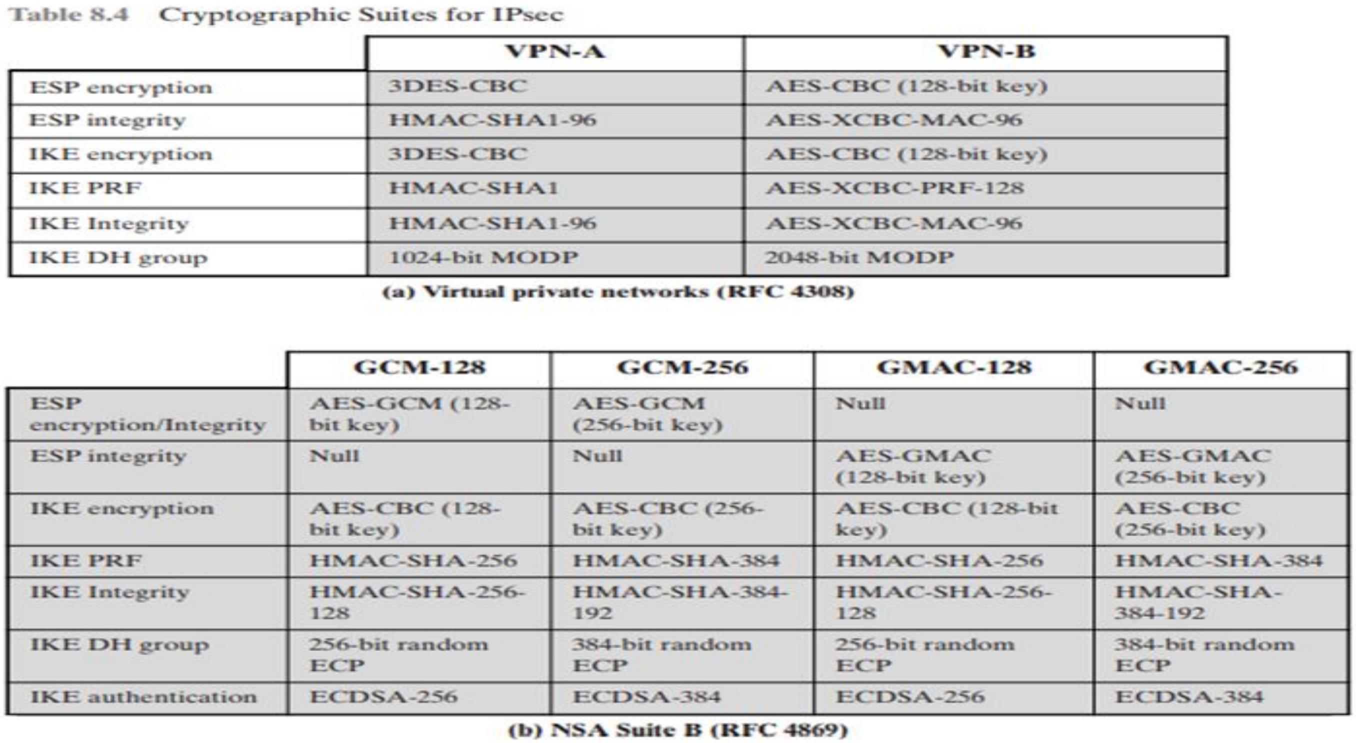


Table 8.4 Cryptographic Suites for IPsec

	VPN-A	VPN-B
ESP encryption	3DES-CBC	AES-CBC (128-bit key)
ESP integrity	HMAC-SHA1-96	AES-XCBC-MAC-96
IKE encryption	3DES-CBC	AES-CBC (128-bit key)
IKE PRF	HMAC-SHA1	AES-XCBC-PRF-128
IKE Integrity	HMAC-SHA1-96	AES-XCBC-MAC-96
IKE DH group	1024-bit MODP	2048-bit MODP

(a) Virtual private networks (RFC 4308)

	GCM-128	GCM-256	GMAC-128	GMAC-256
ESP encryption/Integrity	AES-GCM (128-bit key)	AES-GCM (256-bit key)	Null	Null
ESP integrity	Null	Null	AES-GMAC (128-bit key)	AES-GMAC (256-bit key)
IKE encryption	AES-CBC (128-bit key)	AES-CBC (256-bit key)	AES-CBC (128-bit key)	AES-CBC (256-bit key)
IKE PRF	HMAC-SHA-256	HMAC-SHA-384	HMAC-SHA-256	HMAC-SHA-384
IKE Integrity	HMAC-SHA-256-128	HMAC-SHA-384-192	HMAC-SHA-256-128	HMAC-SHA-384-192
IKE DH group	256-bit random ECP	384-bit random ECP	256-bit random ECP	384-bit random ECP
IKE authentication	ECDSA-256	ECDSA-384	ECDSA-256	ECDSA-384

(b) NSA Suite B (RFC 4869)

Cryptographic suits (cont)

- VPN-A relies on 3DES and while VPN-B relies exclusively on AES.

Three types of secret-key algorithms are used:-

- **Encryption:** For encryption, the cipher block chaining (CBC) mode is used.
- **Message authentication:** For message authentication, VPN-A relies on HMAC with SHA-1 with the output truncated to 96 bits. VPN-B relies on a variant of CMAC with the output truncated to 96 bits.
- **Pseudorandom function:** IKEv2 generates pseudorandom bits by repeated use of the MAC used for message authentication

As for the RFC 4308,three categories of secret key algorithms are listed:-

- **Encryption:** For ESP, authenticated encryption is provided using the GCM mode with either 128-bit or 256-bit AES keys. For IKE encryption, CBC is used, as it was for the VPN suites.
- **Message authentication:** For ESP, if only authentication is required, then GMAC is used. GMAC is a message authentication code algorithm based on the CRT mode of operation discussed in Chapter 2. For IKE, message authentication is provided using HMAC with one of the SHA-3 hash functions.
- **Pseudorandom function:** As with the VPN suites, IKEv2 in these suites generates pseudorandom bits by repeated use of the MAC used for message authentication

References

CHEN98 Cheng, P., et al. “A Security Architecture for the Internet Protocol.” IBM Systems Journal, Number 1, 1998.

FRAN05 Frankel, S., et al. Guide to IPsec VPNs. NIST SP 800-77, 2005.

PATE06 Paterson, K. “A Cryptographic Tour of the IPsec Standards.” “ Cryptology ePrint Archive: Report 2006/097, April 2006.

STAL07 Stallings, W. Data and Computer Communications, Eighth Edition. Upper Saddle River, NJ: Prentice Hall, 2007.