Network Security

Asim Rasheed

Where we are …

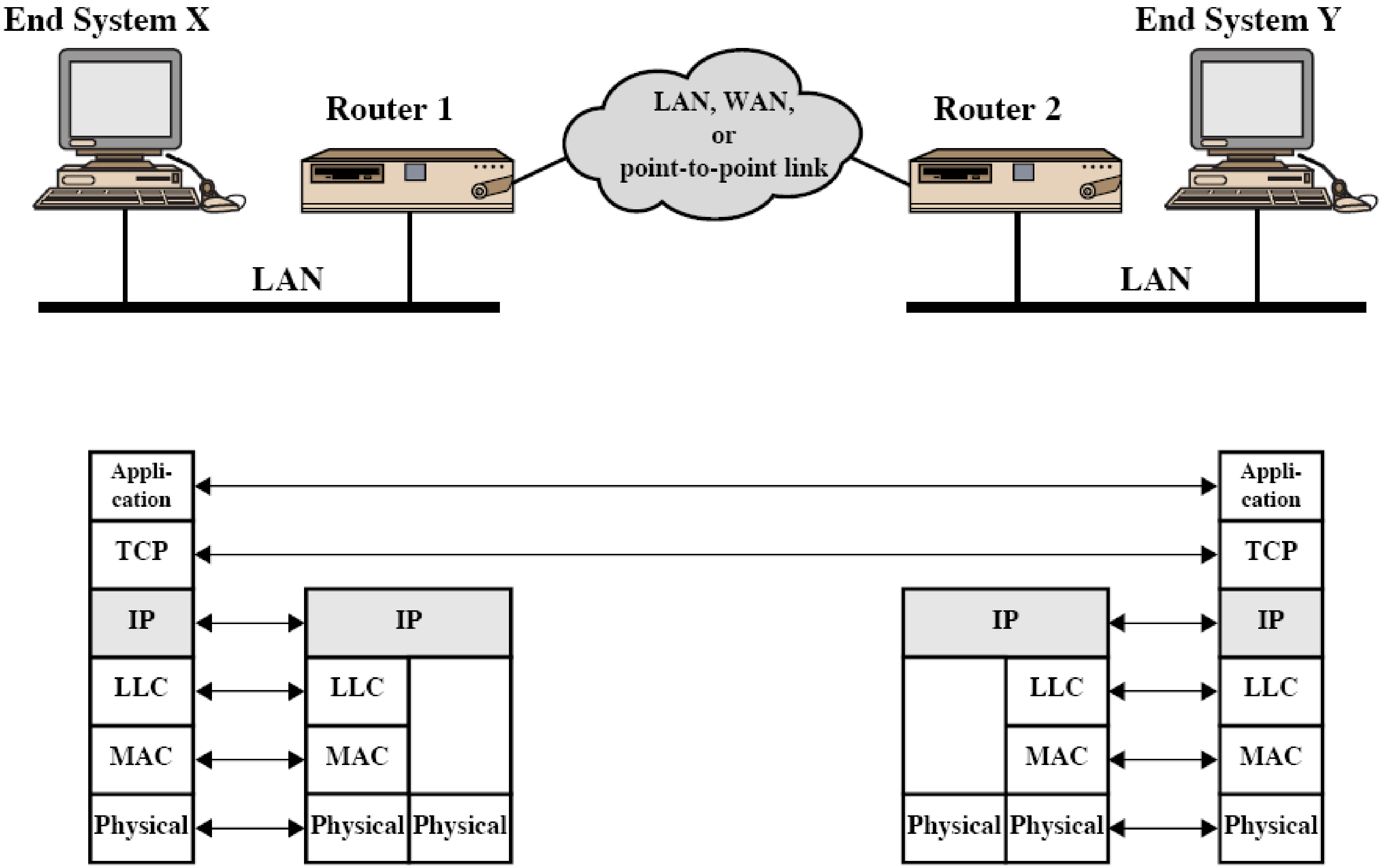
- Introduction to network security
- Vulnerabilities in IP
- I. CRYPTOGRAPHY
  - Symmetric Encryption and Message Confidentiality
  - Public-Key Cryptography and Message Authentication
- II. NETWORK SECURITY APPLICATIONS
  - Authentication Applications (Kerberos, X.509)
  - Electronic Mail Security (PGP, S/MIME)
  - IP Security (IPSec, AH, ESP, IKE)
  - Web Security (SSL, TLS, SET)
- III. SYSTEM SECURITY
  - Intruders and intrusion detection
  - Malicious Software (viruses)
  - Firewalls and trusted systems

Network Layer Security: IPSec

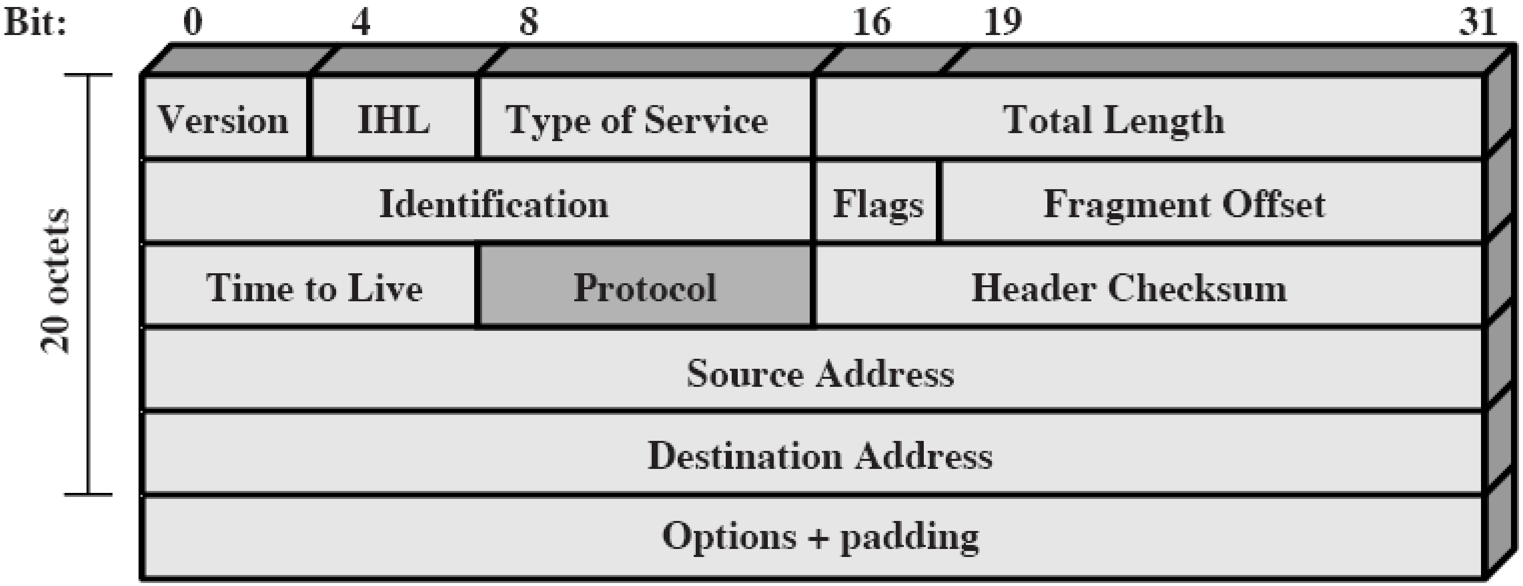
IP Security

- have a range of application specific security mechanisms
  - eg. S/MIME, PGP, Kerberos, SSL/HTTPS
- however there are security concerns that cut across protocol layers
- would like security implemented by the network for all applications

Configuration for TCP/IP Example



IPv4 Headers



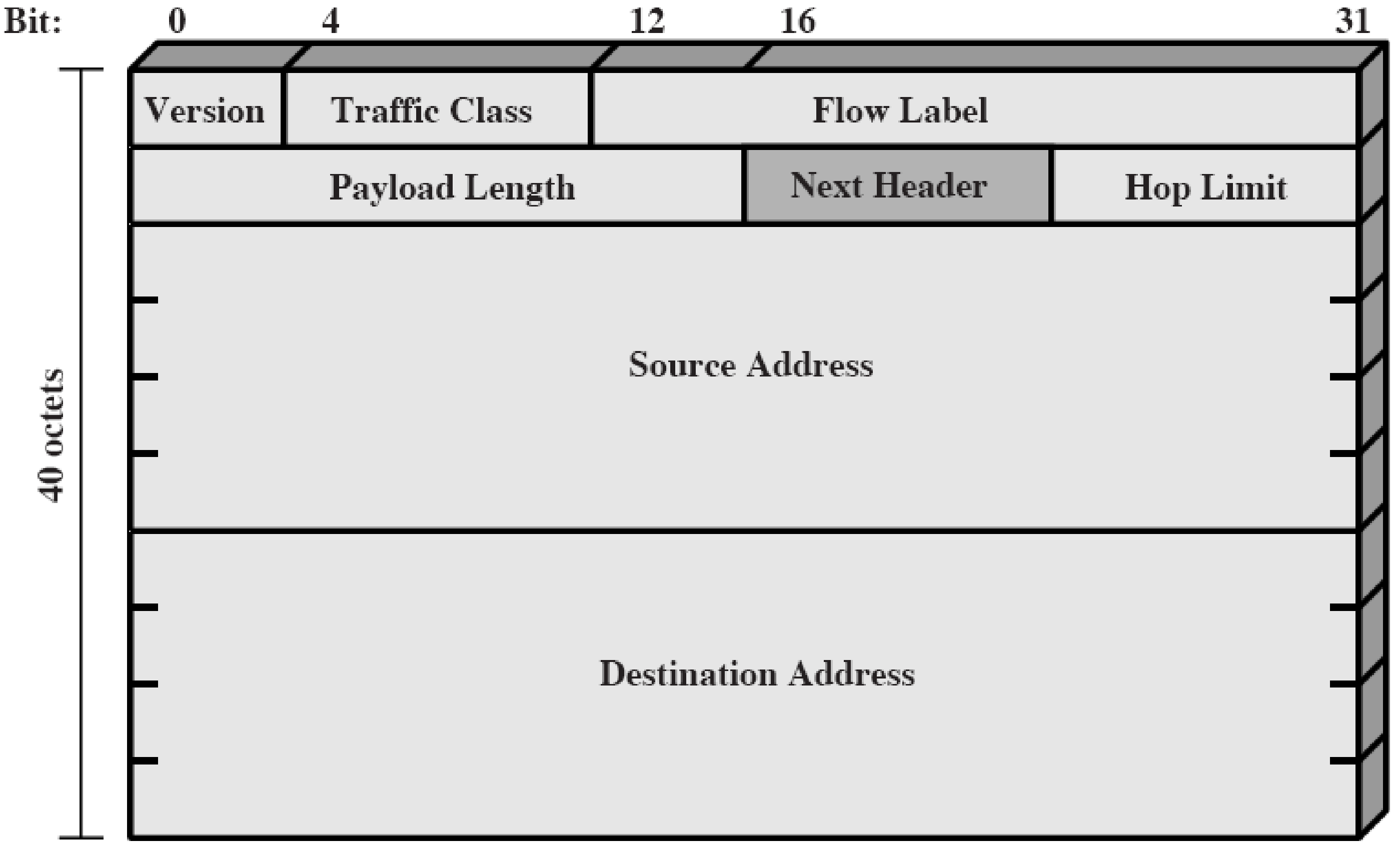
Bit: 0 4 8 16 19 31

20 octets

Version	IHL	Type of Service	Total Length	
Identification			Flags	Fragment Offset
Time to Live		Protocol	Header Checksum	
Source Address				
Destination Address				
Options + padding				

(a) IPv4 Header

IPv6 Headers



(b) IPv6 Header

Overview

- important RFCs
  - RFC 2401: an overview of the IPSec security architecture
  - RFC 2402: specification of AH
  - RFC 2406: specification of ESP
  - RFC 2408: specification of ISAKMP
  - RFC 2412: specification of Oakley
- IPSec is mandatory for IPv6 and optional for IPv4

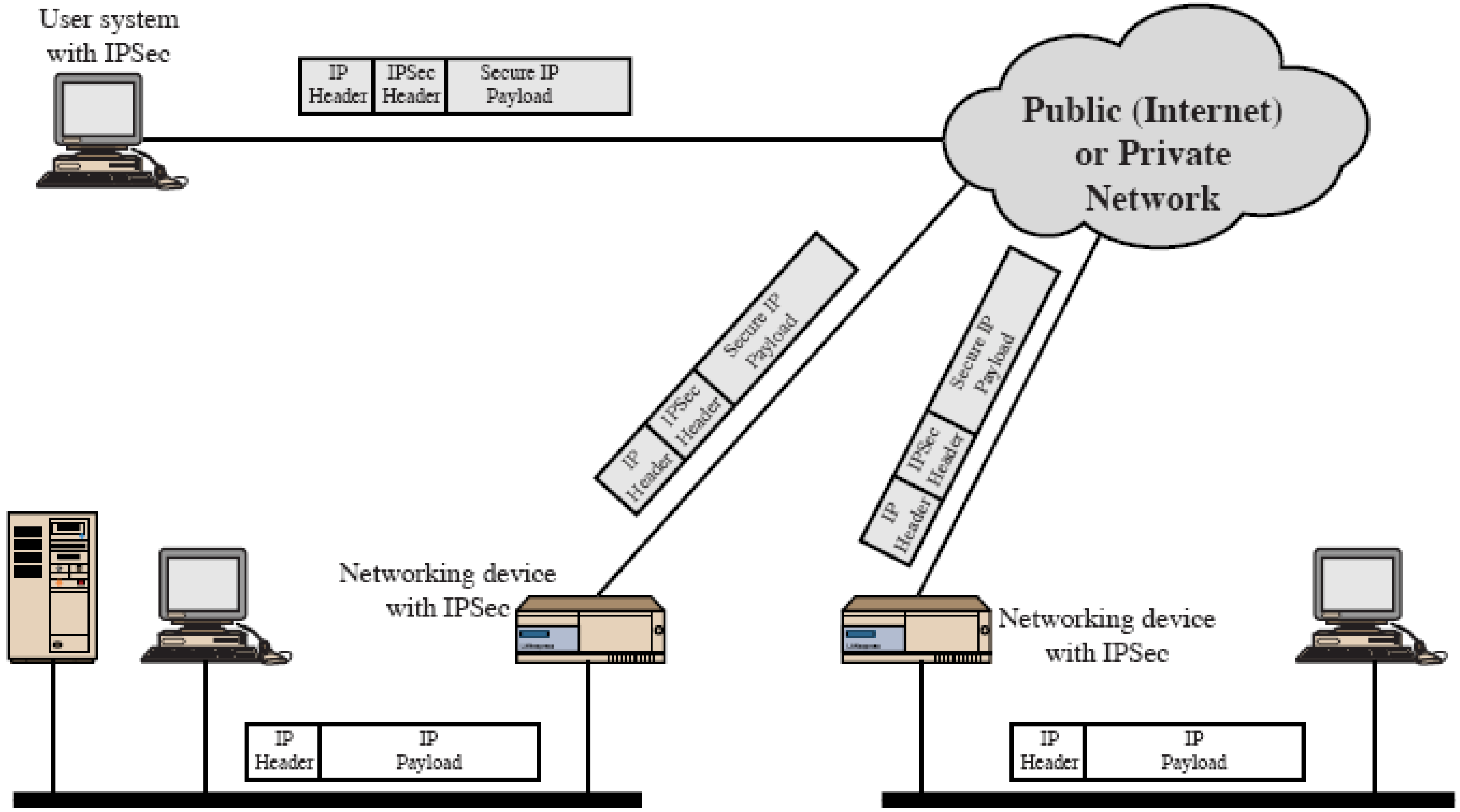
Design

- IPSec is an Internet standard for network layer security
- components:
  - an authentication protocol (Authentication Header – AH)
  - a combined encryption and authentication protocol (Encapsulated Security Payload – ESP)
  - key management protocols (the default is ISAKMP/Oakley)

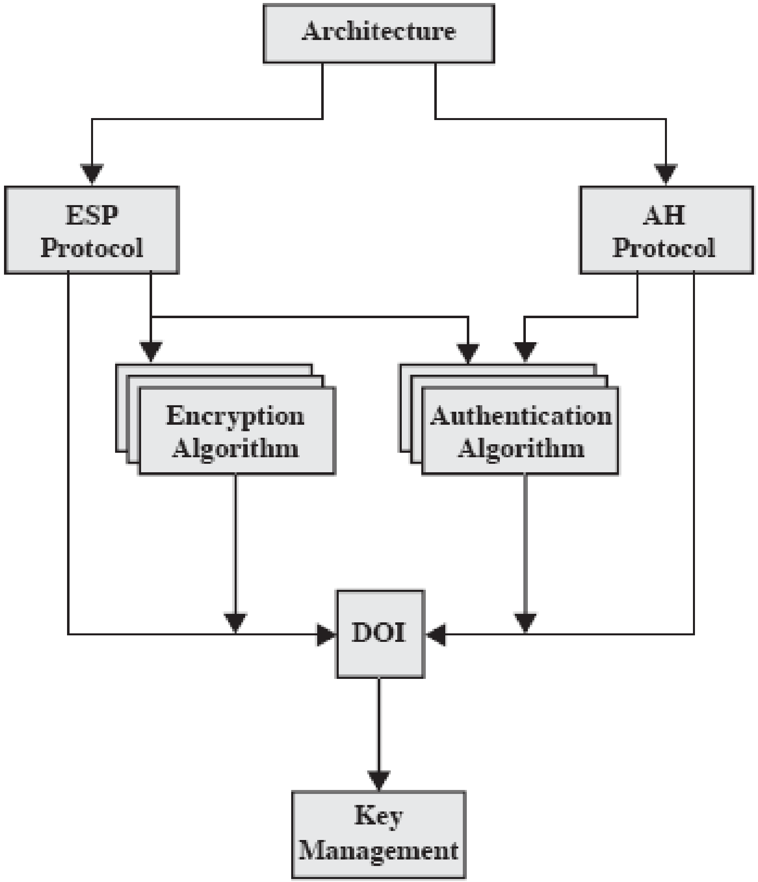
IPSec

- General IP Security mechanisms
- Provides
  - authentication
  - confidentiality
  - key management
- applicable to use over LANs, across public & private WANs, & for the Internet

An IP Security Scenario



IPSec Document Overview



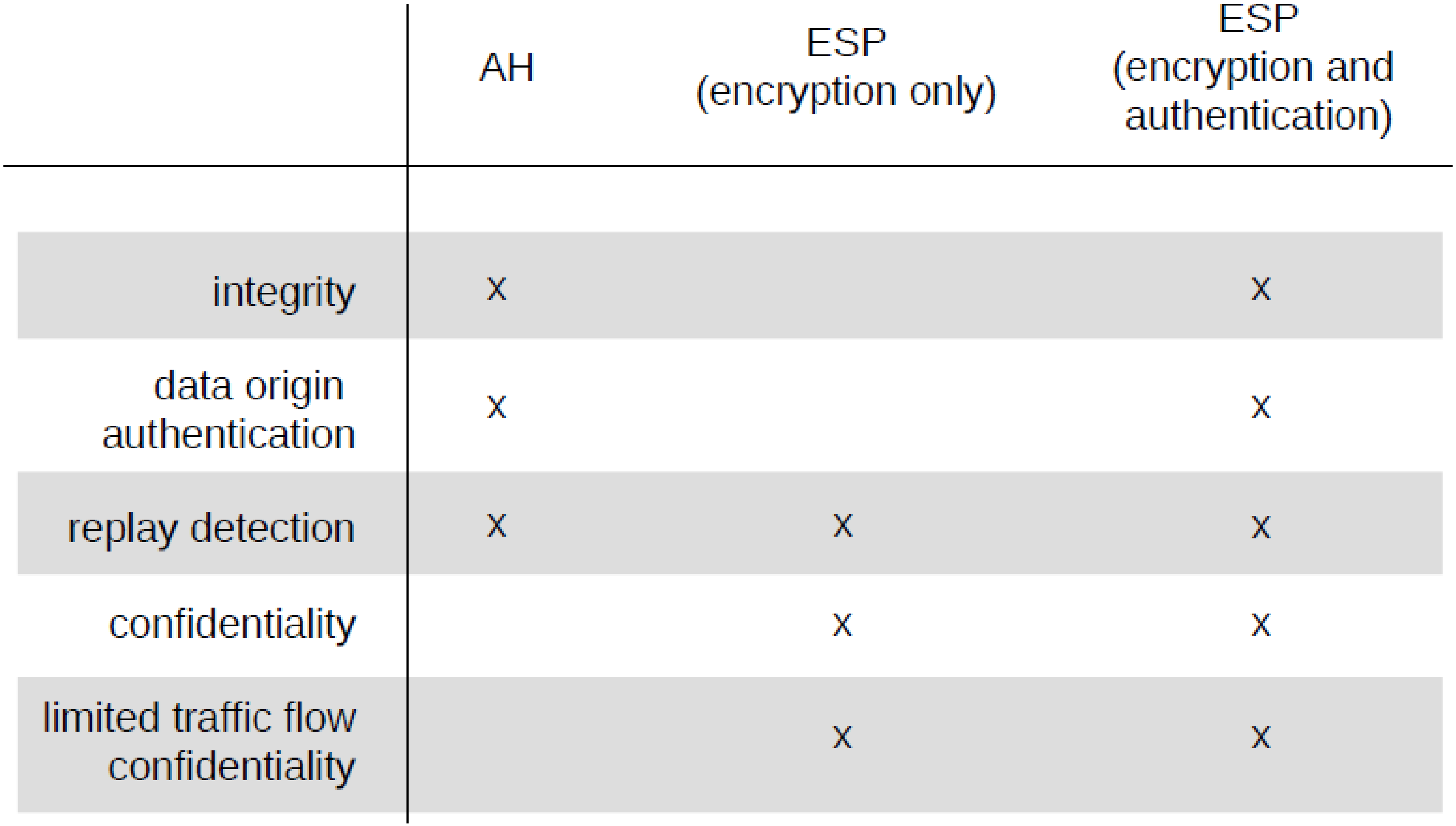
Benefits of IPSec

- in a firewall/router provides strong security to all traffic crossing the perimeter
- in a firewall/router is resistant to bypass
- is below transport layer, hence transparent to applications
- can be transparent to end users
- can provide security for individual users
- secures routing architecture

Benefits of IPSec

- IPSec can assure that:
  - A router or neighbor advertisement comes from an authorized router
  - A redirect message comes from the router to which the initial packet was sent
  - A routing update is not forged

IPSec services



	AH	ESP (encryption only)	ESP (encryption and authentication)
integrity	X		X
data origin authentication	X		X
replay detection	X	X	X
confidentiality		X	X
limited traffic flow confidentiality		X	X

Modes of operation

- Transport Mode
- Tunnel Mode

What is a tunnel?

- A tunnel identifies packets in a data stream
    - Identify by encapsulation (new header possibly new trailer)
    - Identify by labeling.
- Entry into a tunnel gives the data stream different characteristics
- E.g., Privacy, authentication, different routing characteristics
- Security is not always the goal of the tunnel

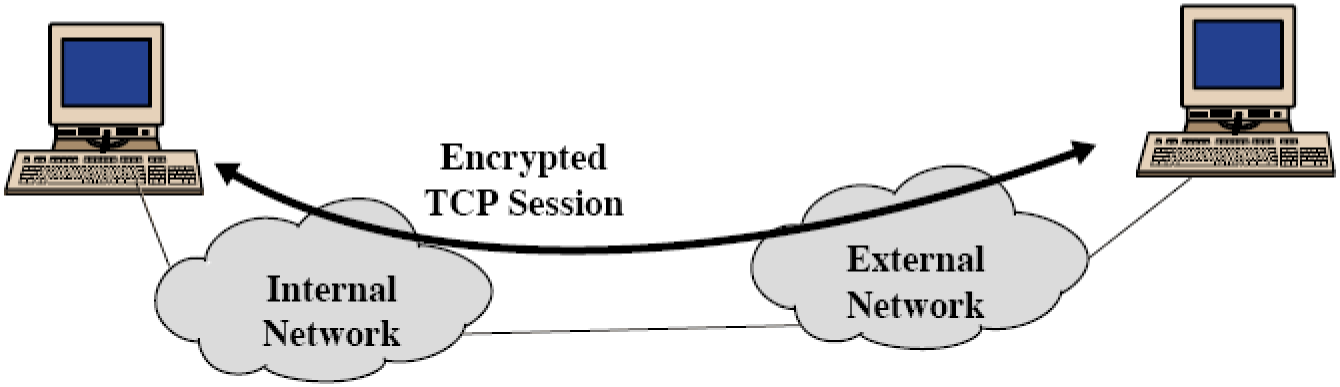
Tunnel Protocols for all Levels

- Layer 2
  - ▫ 802.1Q VLANs – labels Ethernet frames for traffic separation
  - ▫ Proprietary link encryption
- Layer 3
  - ▫ IPSec
  - ▫ IPv6 in IPv4 – Carry IPv6 traffic over IPv4 networks
  - ▫ Generic Routing Encapsulation (GRE)
  - ▫ Multiprotocol Label Switching (MPLS) – uses labels to implement circuit switching at layer 3

Tunnel Protocols for all Levels

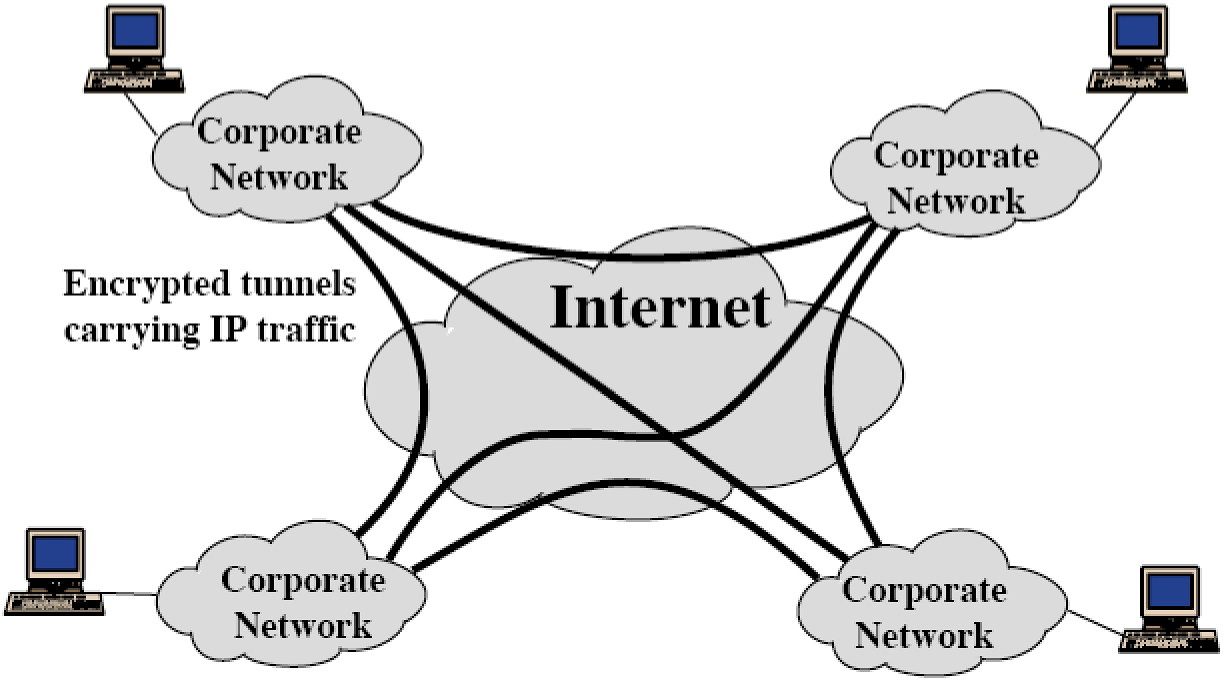
- Layer 4
  - SSL/TLS
- Layer 7
  - SMIME
  - DNSSec

Transport Level Security



(a) Transport-level security

Tunnel Mode Security



(b) A virtual private network via Tunnel Mode

Modes of operation

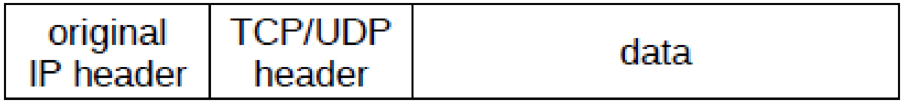
- Transport mode
  - provides protection primarily for upper layer protocols
  - protection is applied to the payload of the IP packet
- ESP in transport mode encrypts and optionally authenticates the IP payload but not the IP header
- AH in transport mode authenticates the IP payload and selected fields of the IP header
  - usually used between end-systems

Modes of operation

- Tunnel mode
  - provides protection to the entire IP packet
  - the entire IP packet is considered as payload and encapsulated in another IP packet (with potentially different source and destination addresses)
- ESP in tunnel mode encrypts and optionally authenticates the entire inner IP packet
- AH in transport mode authenticates the entire inner IP packet & selected fields of outer IP header
  - usually used between security gateways (routers, firewalls)

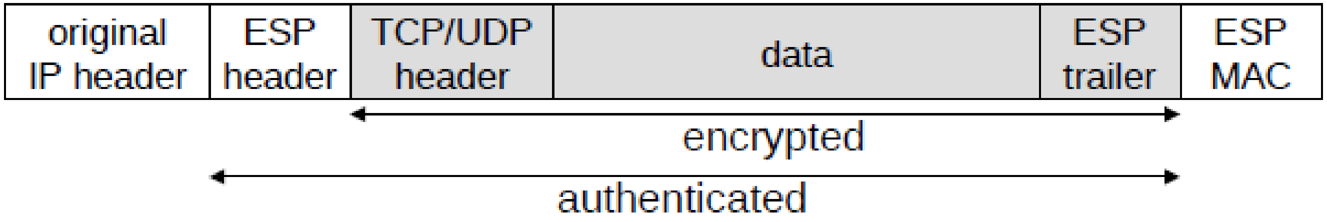
ESP in transport and tunnel mode

original IPv4 packet



original IP header	TCP/UDP header	data

ESP in transport mode

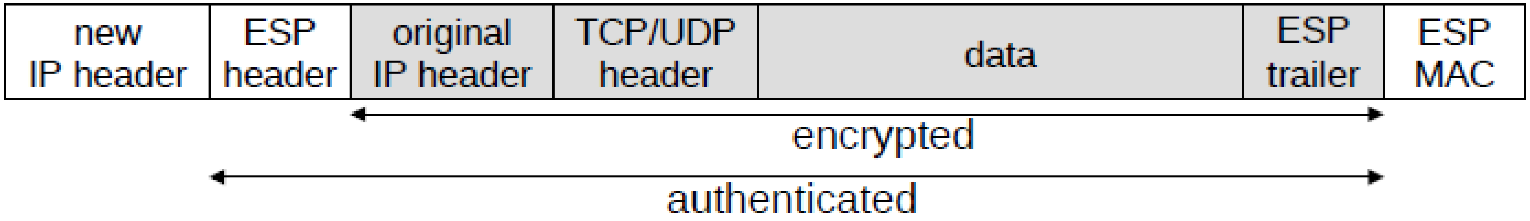


original IP header	ESP header	TCP/UDP header	data	ESP trailer	ESP MAC

encrypted

authenticated

ESP in tunnel mode



new IP header	ESP header	original IP header	TCP/UDP header	data	ESP trailer	ESP MAC

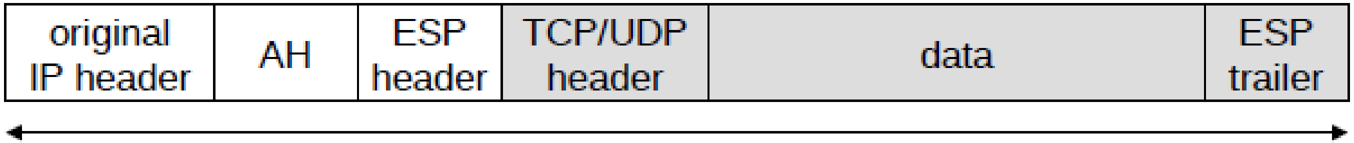
encrypted

authenticated

Combining security associations

basic ESP-AH combination

1. apply ESP in transport mode without authentication
2. apply AH in transport mode

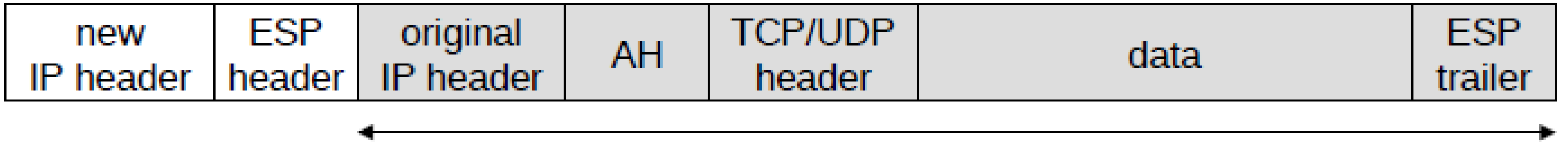


original IP header	AH	ESP header	TCP/UDP header	data	ESP trailer

authenticated except for mutable fields in the IP header

basic AH-ESP combination

1. apply AH in transport mode
2. apply ESP in tunnel mode without

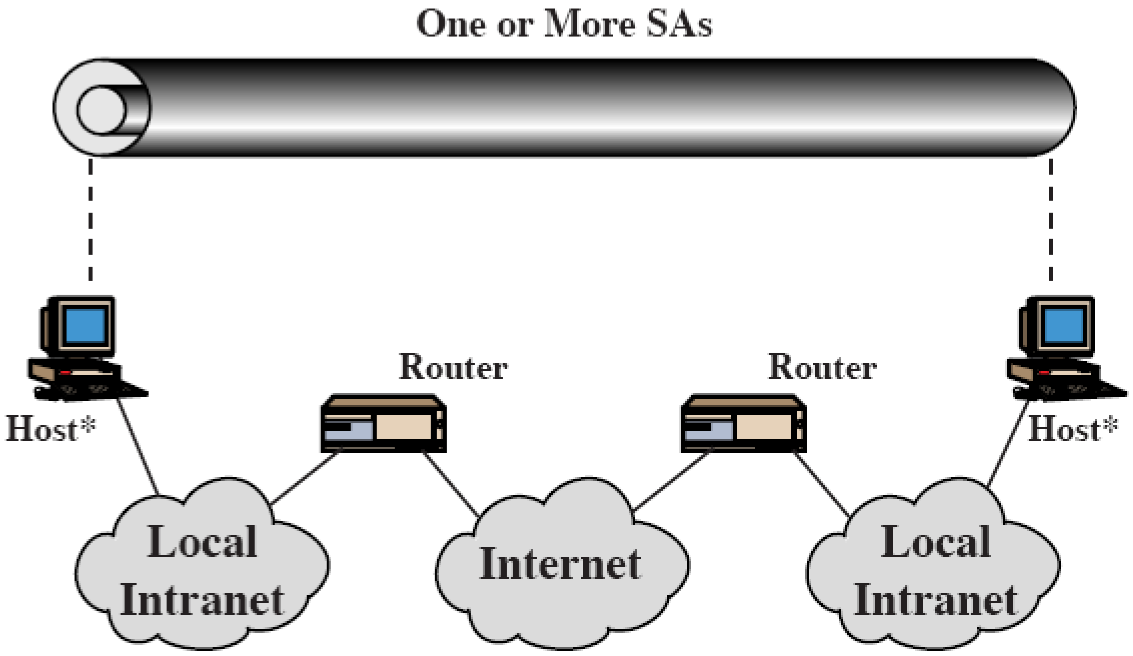


new IP header	ESP header	original IP header	AH	TCP/UDP header	data	ESP trailer

authenticated except for mutable fields in the inner IP header

Combining security associations

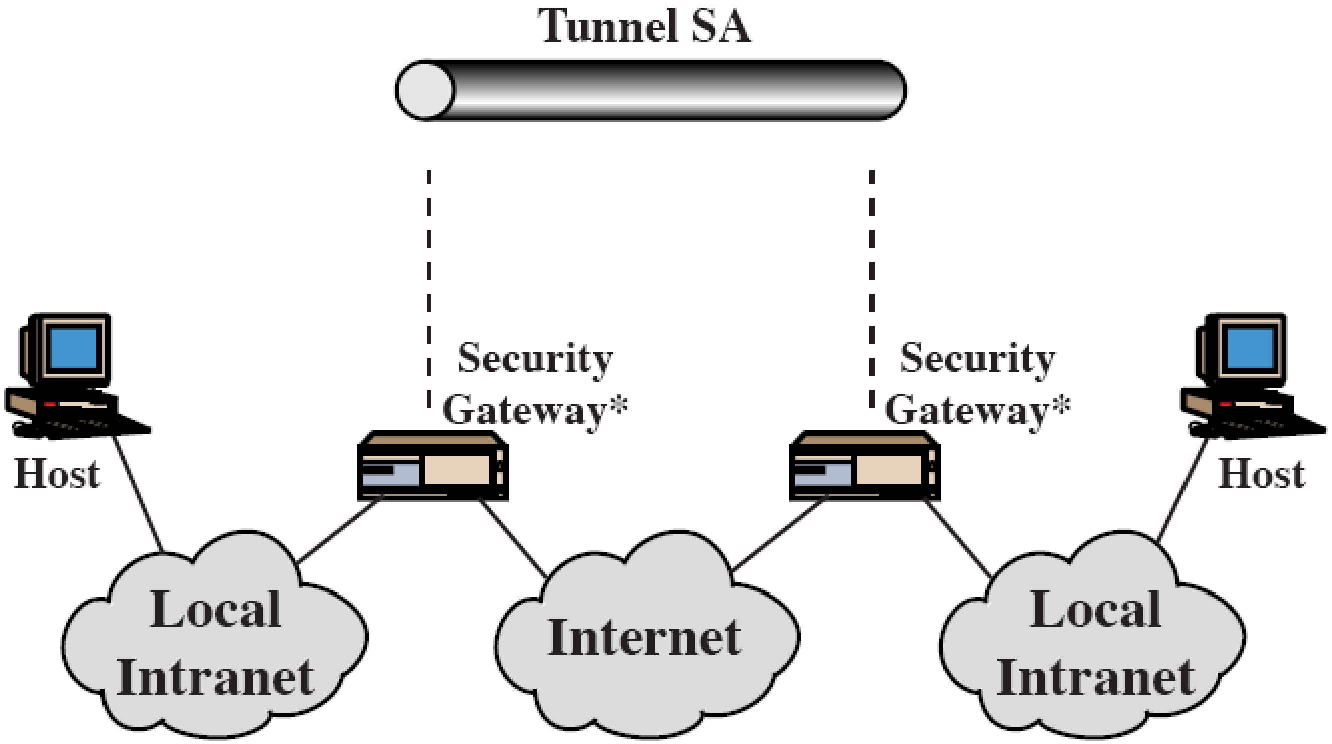
- Case 1: host-to-host security



(a) Case 1

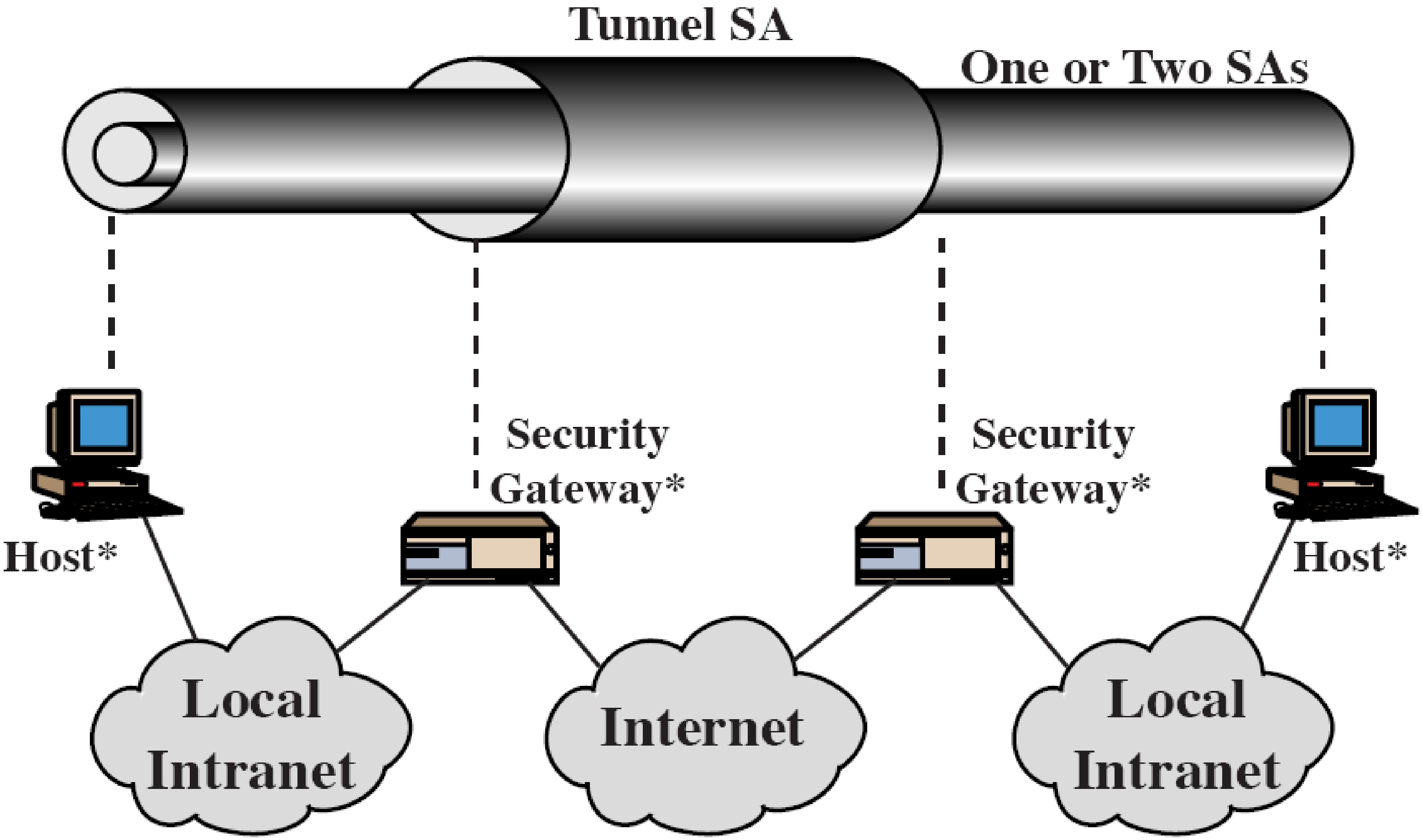
Combining security associations

- Case 2: gateway-to gateway security



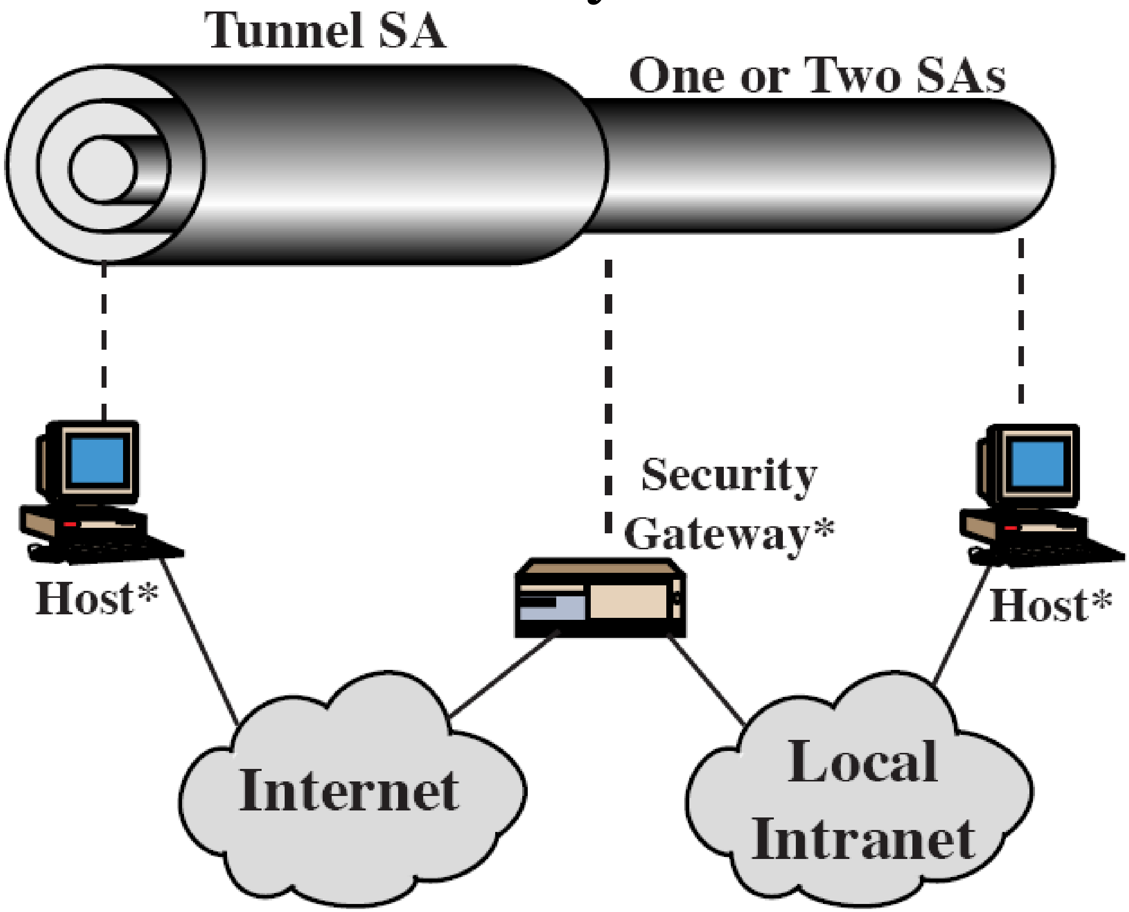
Combining security associations

- Case 3: host-to gateway security



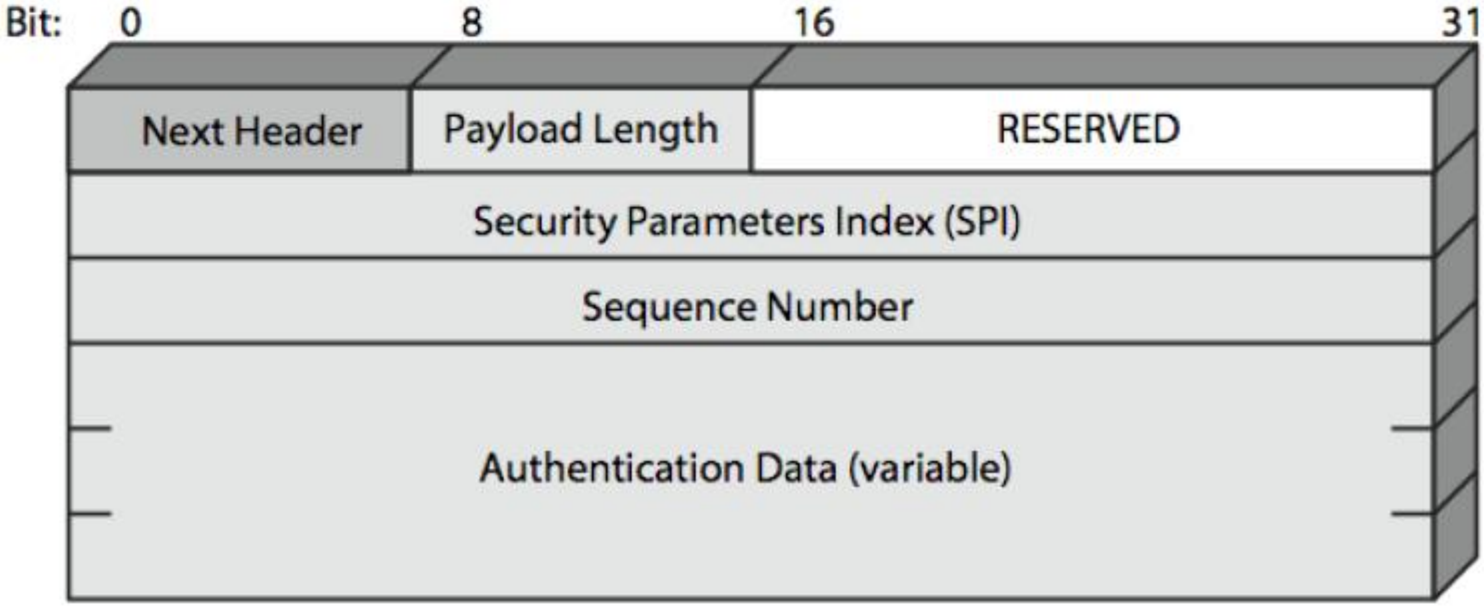
Combining security associations

- Case 3: Tunnel in Tunnel security



IPSec Authentication Header

- Provides support for data integrity and authentication (MAC code) of IP packets.
- Guards against replay attacks.



Bit: 0	8	16	31
Next Header	Payload Length	RESERVED	
Security Parameters Index (SPI)			
Sequence Number			
Authentication Data (variable)			

Authentication Header – AH

- Next header
  - type of header immediately following this header
- Payload length
  - length of AH (in 32 bit words) minus 2
  - e.g., 4 if Authentication data is 3x32 bits long
- Security Parameters Index
  - identifies the SA used to generate this header
- Sequence number
  - sequence number of the packet
- Authentication data
  - a (truncated) MAC (default length is 3x32 bits)

Security associations (SA)

- an SA is a *one-way relationship between a* sender and a receiver system
- an SA is used either for AH or for ESP but never for both
- an SA is uniquely identified by three parameters
  - Security Parameters Index (SPI)
    - a bit string assigned to the SA
    - carried in AH and ESP headers to allow the receiving party to select the SA which must be used to process the packet

Security associations (SA)

- an SA is uniquely identified by three parameters …
  - IP destination address
    - address of an end-system or a network element (e.g., router)
  - security protocol identifier
    - indicates whether the SA is an AH or an ESP SA

SA parameters

- sequence number counter
  - counts the packets sent using this SA
- sequence counter overflow flag
  - indicates whether overflow of the sequence number
  - counter should prevent further transmission using this SA
- anti-replay window
  - used to determine whether an inbound AH or ESP packet is a replay

SA parameters

- AH / ESP information
  - algorithm, key, and related parameters
- Lifetime
  - a time interval or byte count after which this SA must be terminated
- protocol mode
  - tunnel or transport mode
- path MTU
  - any observed maximum transmission unit

SA selectors

- Security Policy Database (SPD)
  - each entry defines a subset of IP traffic and points to the SAs to be applied to that traffic
  - subset of IP traffic is defined in terms of selectors
- destination IP address (single, enumerated list, range, or mask)
- source IP address (single, enumerated list, range, or mask)

SA selectors

- transport layer protocol (single, enumerated list, or range)
- destination port (single, enumerated list, range, or wildcard)
- outbound processing
  - compare the selector fields of the packet to the values in the SPD
  - determine which SAs should be used for the packet and their SPIs
  - do the required IPSec processing

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.
- When a new SA is established, the sender initializes a sequence number counter to zero

Anti-Replay Service

- 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 $2^{32} – 1$ back to zero
  - Otherwise, there would be multiple valid packets with the same sequence number
- If the limit of $2^{32} – 1$ is reached, the sender should terminate this SA, and negotiate a new SA with a new key

Anti-Replay Service

- 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 W, with a default of W = 64
- The protocol describes means to determine that a sequence number is correct in respect to it's position in or above the window

Replay detection

- replay: the attacker obtains an authenticated packet and later transmits (replays) it to the intended destination
- receiver has an anti-replay window of default size W = 64

Outbound Processing

- Outbound Processing
  - ▫ Security Association Lookup
  - ▫ Sequence Number Generation
  - ▫ Integrity Check Value Calculation
  - ▫ Fragmentation

Security Association Lookup – Outbound Proc

- AH is applied to an outbound packet only after an IPsec implementation determines that the packet is associated with an SA that calls for AH processing

Sequence Number Generation – Outbound Proc

- The sender's counter is initialized to zero when an SA is established. The sender increments the Sequence Number for this SA and inserts the new value into the Sequence Number Field.
- If anti-replay is enabled (the default), the sender checks to ensure that the counter has not cycled before inserting the new value in the Sequence Number field

Sequence Number Generation – Outbound Proc

- The sender assumes anti-replay is enabled as a default, unless otherwise notified by the receiver. Thus, if the counter has cycled, the sender will set up a new SA and key (unless the SA was configured with manual key management)
- If anti-replay is disabled, the sender does not need to monitor or reset the counter

Integrity Check Value Calculation-Outbound Proc

- The AH ICV is computed over:
  - IP header fields that are either immutable in transit or that are predictable in value upon arrival at the endpoint for the AH SA
  - the AH header (Next Header, Payload Len, Reserved, SPI, Sequence Number, and the Authentication Data (which is set to zero for this computation), and explicit padding bytes (if any))
  - the upper level protocol data, which is assumed to be immutable in transit

Integrity Check Value Calculation-Outbound Proc

- The IPv4 base header fields are classified as
  - Immutable
    - Version
    - Internet Header Length
    - Total Length
    - Identification Protocol (This should be the value for AH.)
    - Source Address Destination Address (without loose or strict source routing) Mutable but predictable Destination Address (with loose or strict source routing)

Integrity Check Value Calculation-Outbound Proc

- …..
  - Mutable (zeroed prior to ICV calculation)
    - Type of Service (TOS)
    - Flags
    - Fragment Offset
    - Time to Live (TTL) Header Checksum

Integrity Check Value Calculation-Outbound Proc

- The IPv6 base header fields are classified as
  - Immutable
    - Version
    - Payload Length
    - Next Header (This should be the value for AH.)
    - Source Address Destination Address (without Routing Extension Header) Mutable but predictable
    - Destination Address (with Routing Extension Header)

Integrity Check Value Calculation- Outbound Proc

- …..
  - Mutable (zeroed prior to ICV calculation)
    - Class
    - Flow Label
    - Hop Limit

MAC

- implementations must support
  - HMAC-MD5-96
  - HMAC-SHA1-96
- the MAC is calculated over
  - IP header fields that do not change in transit
  - the AH header fields except Authentication data field
  - entire upper layer protocol data
- the fields not covered by the MAC are set to zero for the calculation

Fragmentation – Outbound Processing

- If required, IP fragmentation occurs after AH processing within an IPSec implementation.
- An IP packet to which AH has been applied may itself be fragmented by routers en-route, and such fragments must be reassembled prior to AH processing at a receiver.
- In tunnel mode, AH is applied to an IP packet, the payload of which may be a fragmented IP packet

AH – Inbound processing

- If there is more than one IPSec header / extension present, the processing for each one ignores (does not zero, does not use) any IPSec headers applied subsequent to the header being processed
    - Reassembly
    - Security Association Lookup
    - Sequence Number Verification
    - Integrity Check Value Verification

Reassembly – Inbound processing

- If required, reassembly is performed prior to AH processing
- If a packet offered to AH for processing appears to be an IP fragment, i.e., the OFFSET field is non-zero or the MORE FRAGMENTS flag is set, the receiver MUST discard the packet

Reassembly – Inbound processing

- NOTE….:
  - For packet reassembly, the current IPv4 spec does NOT require either the zero'ing of the OFFSET field or the clearing of the MORE FRAGMENTS flag.
  - In order for a reassembled packet to be processed by IPsec (as opposed to discarded as an apparent fragment), the IP code must do these two things after it reassembles a packet

Security Association Lookup – Inbound Proc

- Upon receipt of a packet containing an IP Authentication Header, the receiver determines the appropriate (unidirectional) SA, based on the destination IP address, security protocol (AH), and the SPI
- If no valid Security Association exists for this session (e.g., the receiver has no key), the receiver MUST discard the packet

Sequence Number Verification – Inbound Proc

- If the receiver does not enable anti-replay for an SA, no inbound checks are performed on the Sequence Number
- If the receiver has enabled the anti-replay service for this SA, the receiver packet counter for the SA must be initialized to zero when the SA is established

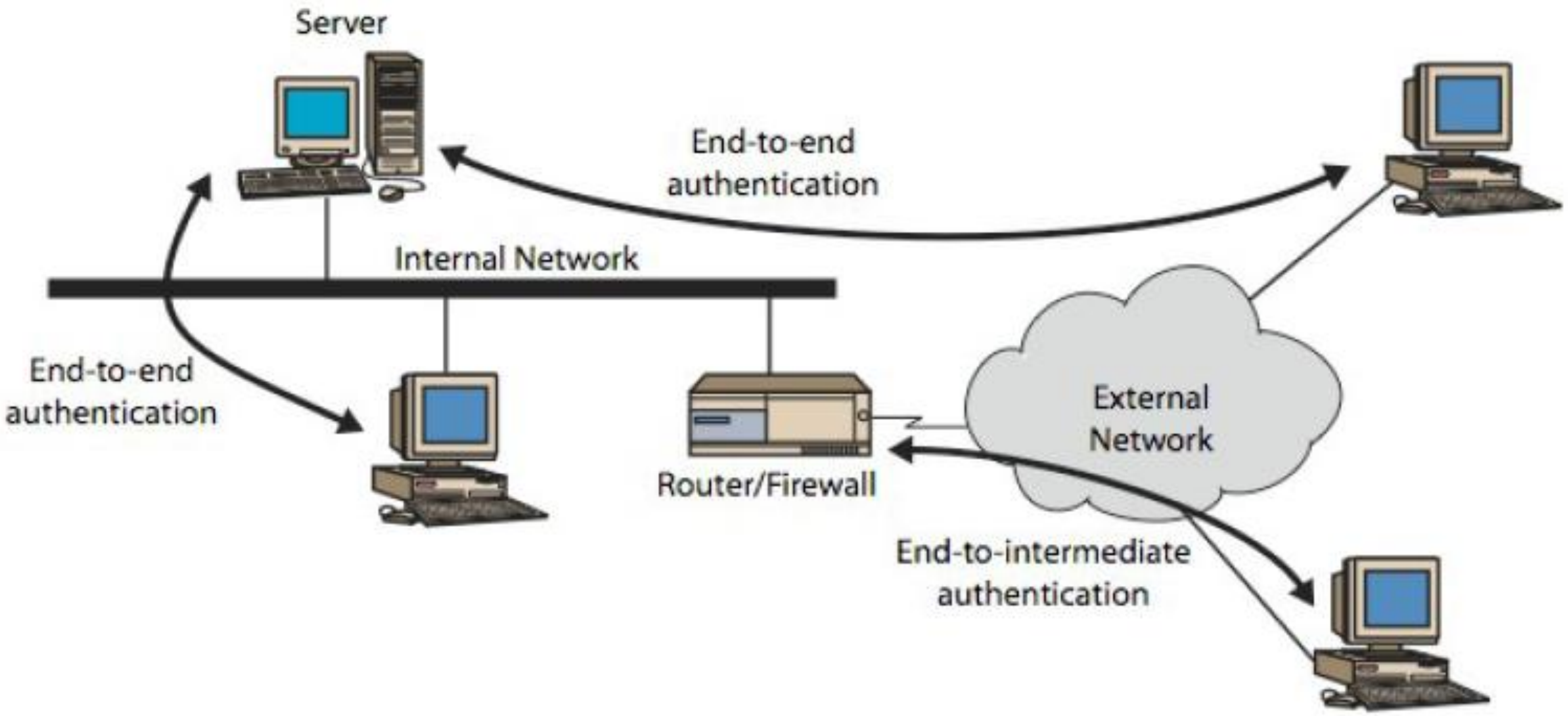
Sequence Number Verification – Inbound Proc

- For each received packet, the receiver must verify that the packet contains a Sequence Number that does not duplicate the Sequence Number of any other packets received during the life of this SA
- Duplicates are rejected through the use of a sliding receive window

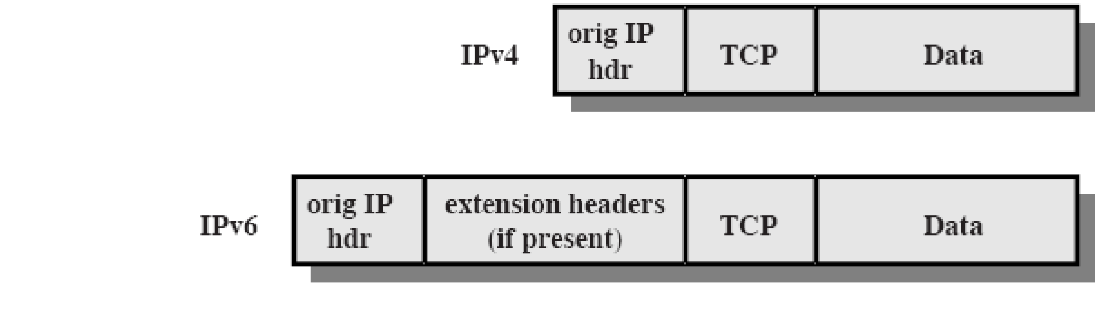
Integrity Check Value Verification

- The receiver computes the ICV over the appropriate fields of the packet, using the specified authentication algorithm, and verifies that it is the same as the ICV included in the Authentication Data field of the packet.
- If the computed and received ICV's match, then the datagram is valid, and it is accepted. If the test fails, then the receiver MUST discard the received IP datagram as invalid.

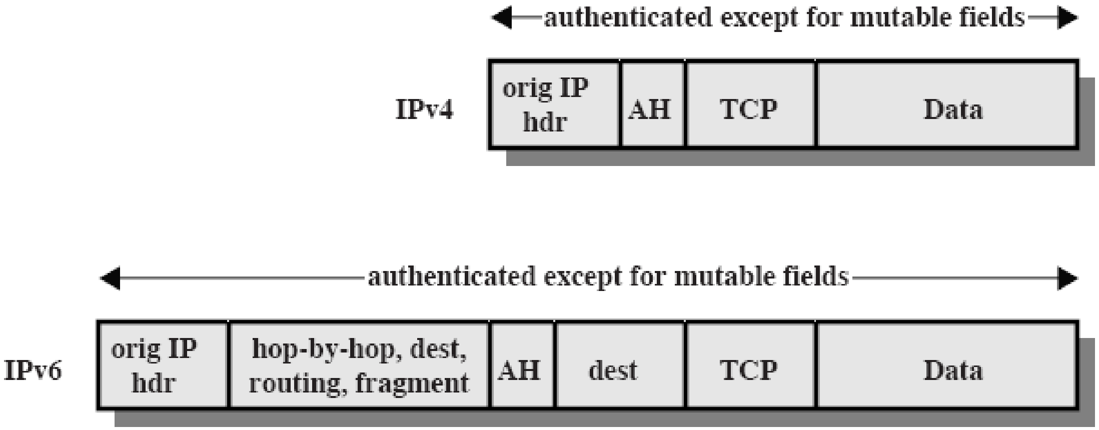
End to End versus End to Intermediate Authentication


Server
End-to-end authentication
Internal Network
End-to-end authentication
Router/Firewall
External Network
End-to-intermediate authentication

Scope of AH Authentication

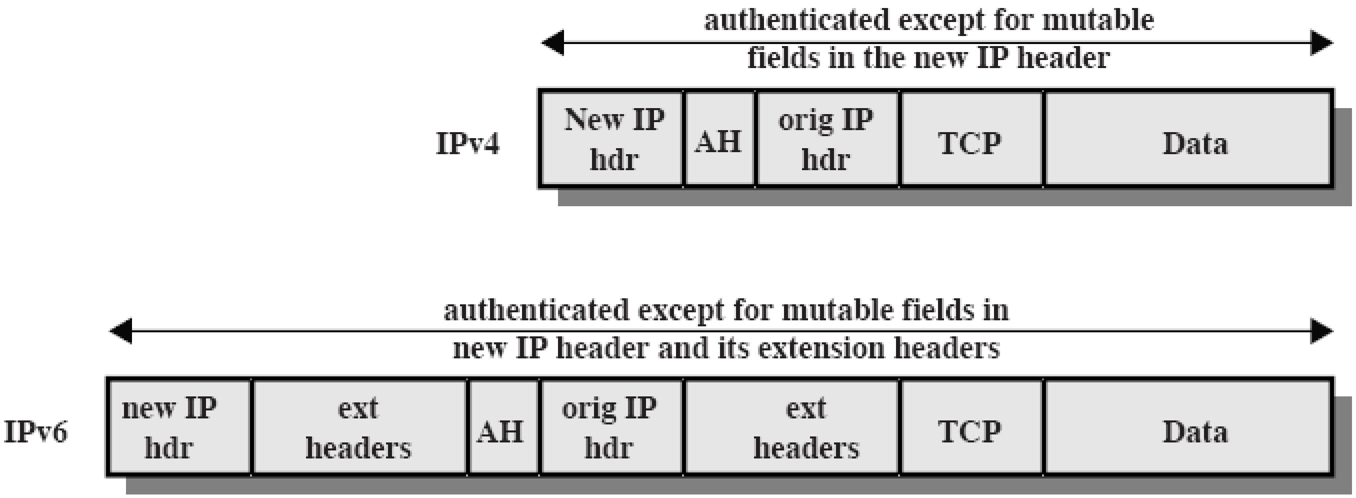


(a) Before Applying AH


authenticated except for mutable fields
IPv4
orig IP hdr
AH
TCP
Data
authenticated except for mutable fields
IPv6
orig IP hdr
hop-by-hop, dest, routing, fragment
AH
dest
TCP
Data

(b) Transport Mode

Cont..

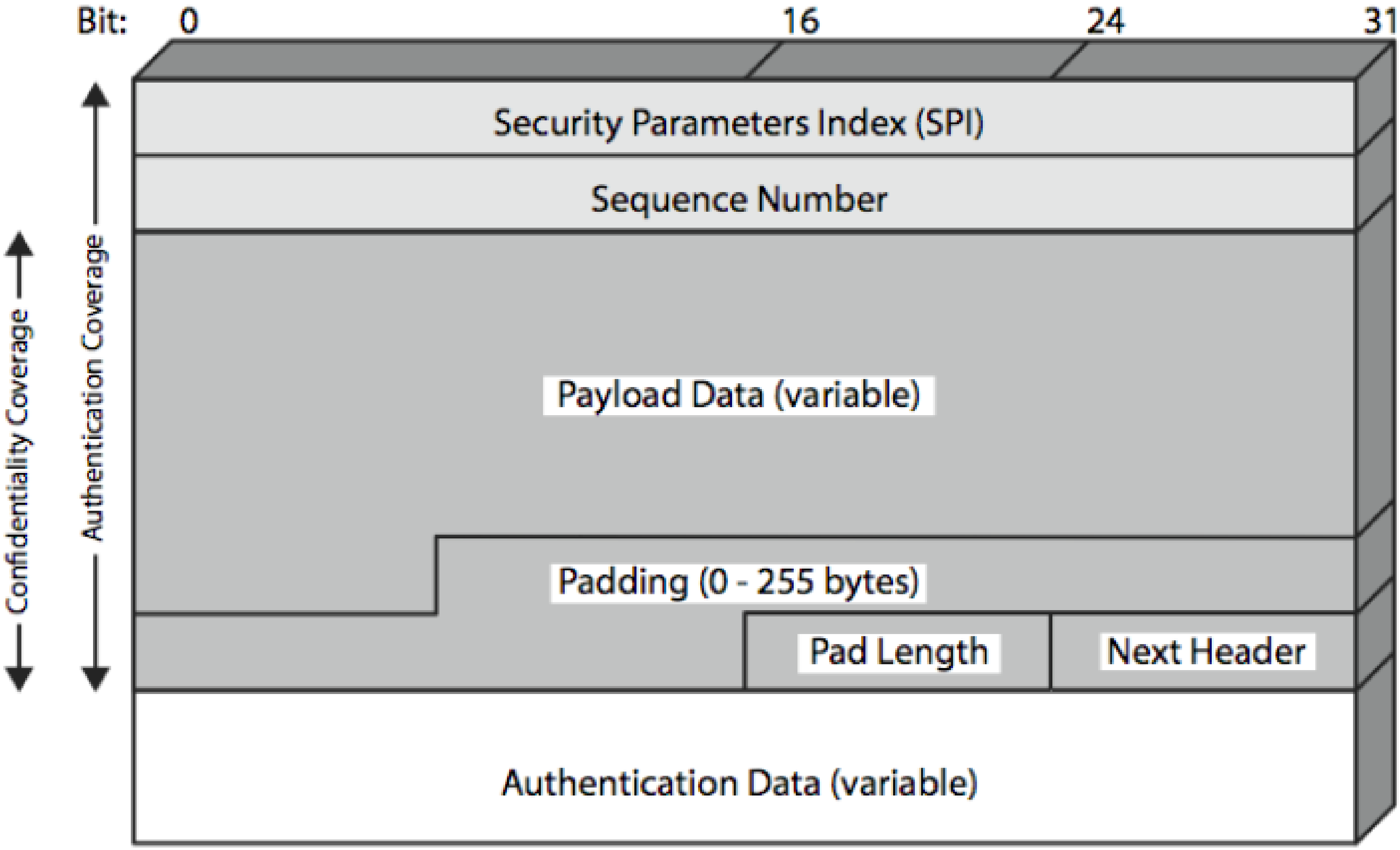

authenticated except for mutable
fields in the new IP header
IPv4
New IP hdr
AH
orig IP hdr
TCP
Data
authenticated except for mutable fields in
new IP header and its extension headers
IPv6
new IP hdr
ext headers
AH
orig IP hdr
ext headers
TCP
Data

(c) Tunnel Mode

Encapsulating Security Payload (ESP)

- provides message content confidentiality & limited traffic flow confidentiality
- can optionally provide the same authentication services as AH
- supports range of ciphers, modes, padding
  - incl. DES, Triple-DES, RC5, IDEA, CAST etc
  - CBC & other modes
  - padding needed to fill block size, fields, for traffic flow

IPSec ESP Format



Bit: 0 16 24 31

Security Parameters Index (SPI)

Sequence Number

Payload Data (variable)

Padding (0 - 255 bytes)

Pad Length

Next Header

Authentication Data (variable)

Confidentiality Coverage

Authentication Coverage

Encapsulating Security Payload (ESP)

- Security Parameters Index
  - identifies the SA used to generate this encrypted packet
- Sequence number
- Payload
  - transport level segment (transfer mode) or encapsulated IP packet (tunnel mode)
- Padding
  - variable length padding
- Pad length

Encapsulating Security Payload (ESP)

- Next header
  - identifies the type of data contained in the header
- Authentication data
  - a (truncated) MAC computed over the ESP packet (SPI … Next Header)

Encapsulating Security Payload (ESP)

- Security Parameters Index (32bits)
- Sequence Number (32 bits)
- Payload Data (variable)
- Padding (0–255 bytes)
- Pad Length (8 bits)
- Next Header (8 bits)
- Authentication Data (variable)
- Security Parameters Index (32bits)
    - ▫ Identifies a security association
- Sequence Number (32 bits)
    - ▫ A monotonically increasing counter value.

Encapsulating Security Payload (ESP)

- Payload Data (variable)
    - A transport level segment (transport mode) or IP packet (tunnel mode) that is protected by encryption.
- Padding (0–255 bytes)
    - Extra bytes that may be required if the encryption algorithm requires the plaintext to be a multiple of some number of octets
- Pad Length (8 bits)
    - Indicates the number of pad bytes immediately preceding this field

Encapsulating Security Payload (ESP)

- 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 upper layer protocol such as TCP)
- Authentication Data (variable)
  - A variable length field (must be an integral number of 32bit words) that contains the integrity check value computed over the ESP packet minus the Authentication Data field

Encryption & Authentication Algos

- The Payload Data, Padding, Pad Length, and Next Header fields are encrypted by the ESP service
- The current IPSec specification dictates that a compliant implementation must support the DES
- A number of other algorithms have been assigned identifiers and could, therefore, be used for encryption; These include
  - Three key Triple DES & Three key Triple IDEA
  - RC5
  - International Data Encryption Algorithm (IDEA)
  - CAST & Blowfish

Encryption and MAC algorithms

- encryption
  - applied to the payload, padding, pad length, and next header fields
  - if an IV is needed, then it is explicitly carried at the beginning of the payload data (the IV is not encrypted)
  - implementations must support DES-CBC
  - other suggested algorithms: 3DES, RC5, IDEA, 3IDEA, CAST, Blowfish

Encryption and MAC algorithms

- MAC
  - default length is 3x32 bits
  - implementations must support HMAC-MD5-96 and HMAC-SHA1-96
  - MAC is computed over the SPI, sequence number, and encrypted payload, padding, pad length, and next header fields
  - unlike in AH, here the MAC does not cover the preceding IP header

Outbound Packet Processing

- In transport mode, the sender encapsulates the upper layer protocol information in the ESP header/trailer, and retains the specified IP header (and any IP extension headers in the IPv6 context)
- If there is more than one IPSec header/extension required by security policy, the order of the application of the security headers must be defined by security policy

Outbound Packet Processing

- Processing involves
    - Security Association Lookup
    - Packet Encryption
    - Sequence Number Generation
    - Integrity Check Value Calculation
    - Fragmentation

Packet Encryption

- Accordingly, the sender:
  - encapsulates (into the ESP Payload field):
    - for transport mode - just the original upper layer protocol information.
    - for tunnel mode -- the entire original IP datagram.
  - Adds any necessary padding.
  - Encrypts the result (Payload Data, Padding, Pad Length, and Next Header) using the key, encryption algorithm, algorithm mode indicated by the SA and cryptographic synchronization data (if any)

Packet Encryption

- Accordingly, the sender…..:
  - If explicit cryptographic synchronization data, e.g., an IV, is indicated, it is input to the encryption algorithm per the algorithm specification and placed in the Payload field.
  - If implicit cryptographic synchronization data, e.g., an IV, is indicated, it is constructed and input to the encryption algorithm as per the algorithm specification

Packet Encryption

- If authentication is selected, encryption is performed first, before the authentication, and the encryption does not encompass the Authentication Data field
- 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 attacks

Packet Encryption

- It also allows for the possibility of parallel processing of packets at the receiver, i.e., decryption can take place in parallel with authentication
- Note that since the Authentication Data is not protected by encryption, a keyed authentication algorithm must be employed to compute the ICV

Sequence Number Generation

- The sender's counter is initialized to zero when an SA is established. The sender increments the Sequence Number for this SA and inserts the new value into the Sequence Number field.
- If anti-replay is enabled (the default), the sender checks to ensure that the counter has not cycled before inserting the new value in the Sequence Number field

Sequence Number Generation

- The sender assumes anti-replay is enabled as a default, unless otherwise notified by the receiver
- If anti-replay is disabled, the sender does not need to monitor or reset the counter, e.g., in the case of manual key management. However, the sender still increments the counter and when it reaches the maximum value, the counter rolls over back to zero

Integrity Check Value Calculation

- If authentication is selected for the SA, the sender computes the ICV over the ESP packet minus the Authentication Data
- For some authentication algorithms, the byte string over which the ICV computation is performed must be a multiple of a block size specified by the algorithm
- If the length of this byte string does not match block size requirements for the algo, implicit pad MUST be appended to the end of ESP packet, (after Next Header field) prior to ICV computation

Integrity Check Value Calculation

- The padding octets MUST have a value of zero.
- The block size (and hence the length of the padding) is specified by the algorithm specification. This padding is not transmitted with the packet. Note that MD5 and SHA-1 are viewed as having a 1-byte block size because of their internal padding conventions

Fragmentation

- If necessary, fragmentation is performed after ESP processing within an Ipsec implémentation. Thus, transport mode ESP is applied only to whole IP datagrams (not to IP fragments).
- An IP packet to which ESP has been applied may itself be fragmented by routers en route, and such fragments must be reassembled prior to ESP processing at a receiver.
- In tunnel mode, ESP is applied to an IP packet, the payload of which may be a fragmented IP packet

Inbound Packet Processing

- Involves
  - Reassembly
  - Security Association Lookup
  - Sequence Number Verification
  - Integrity Check Value Verification
  - Packet Decryption

Reassembly

- If required, reassembly is performed prior to ESP processing. If a packet offered to ESP for processing appears to be an IP fragment, i.e, OFFSET field is non-zero or MORE FRAGMENTS flag is set, the receiver MUST discard the packet.
  - NOTE: For packet reassembly, the current IPv4 spec does NOT require either the zero'ing of the OFFSET field or the clearing of the MORE FRAGMENTS flag. In order for a reassembled packet to be processed by IPsec (as opposed to discarded as an apparent fragment), the IP code must do these two things after it reassembles a packet

Security Association Lookup – in bound packet processing

- On receipt of a (reassembled) packet containing an ESP Header, the receiver determines the appropriate (unidirectional) SA, based on the destination IP address, ESP, and the SPI
- SA indicates whether the Sequence Number field will be checked, whether the Auth Data field should be present, and specify the algorithms and keys for decryption and ICV computations
- If no valid Security Association exists for this session (for example, the receiver has no key), the receiver must discard the packet

Sequence Number Verification

- All ESP implementations MUST support anti-replay service, though its use may be enabled or disabled by the receiver on a per-SA basis
  - ▫ This service MUST NOT be enabled unless the authentication service also is enabled for the SA, since otherwise the Sequence Number field has not been integrity protected.
  - ▫ (Note that there are no provisions for managing transmitted Sequence Number values among multiple senders directing traffic to a single SA (irrespective of whether the destination address is unicast, broadcast, or multicast)

Sequence Number Verification

- If the receiver does not enable anti-replay for an SA, no inbound checks are performed on the Sequence Number. However, from the perspective of the sender, the default is to assume that anti-replay is enabled at the receiver
- If the receiver has enabled the anti-replay service for this SA, the receive packet counter for the SA MUST be initialized to zero when the SA is established

Sequence Number Verification

- For each received packet, the receiver MUST verify presence of non duplicate Sequence Number received during the life of this SA. This SHOULD be the first ESP check applied to a packet after it has been matched to an SA
- Duplicates are rejected through the use of a sliding receive window. A MINIMUM window size of 32 MUST be supported; but a window size of 64 is preferred and SHOULD be employed as the default Another window size (larger than the MINIMUM) MAY be chosen by the receiver

Integrity Check Value Verification

- If authentication is selected, the receiver computes the ICV over the ESP packet minus the Auth Data using the specified auth algo and verifies that it is the same as the ICV included in the Auth Data field
- If the computed and received ICV's match, then the datagram is valid, and it is accepted. If the test fails, then the receiver MUST discard the received IP datagram as invalid; this is an auditable event
- The log data SHOULD include the SPI value, date/time received, Source Address, Destination Address, the Sequence Number, and (in IPv6) the clear text Flow ID.

Packet Decryption

Accordingly, the receiver:

- decrypts the ESP Payload Data, Padding, Pad Length, and Next Header using the key, encryption algo, algo mode, and cryptographic synchronization data (if any), indicated by the SA
  - If explicit cryptographic sync data, e.g., an IV, is indicated, it is taken from the Payload field and input to the decryption algo as per the algo spec.
  - If implicit cryptographic synchronization data, e.g., an IV, is indicated, a local version of the IV is constructed and input to the decryption algorithm as per the algorithm specification.

Packet Decryption

Accordingly, the receiver:

- Processes any padding as specified in the encryption algo spec. If the default padding scheme has been employed, the receiver SHOULD inspect the Padding field before removing the padding prior to passing data to the next layer.
- Reconstructs the original IP datagram from:
  - for transport mode -- original IP header + original upper layer protocol info in the ESP Payload field
  - for tunnel mode -- tunnel IP header + the entire IP datagram in the ESP Payload field.

IPSec challenges

- Scaling
  - Numerous security associations eat up too much memory for small routers
  - Configurations on the hub in a hub and spoke network grow n^2 in the number of spokes
    - Dynamic Multipoint VPN (DMVPN)
- Performance
  - Even symmetric encryption can be too much for high bandwidth environments

IPSec challenges

- Symmetry
  - ▫ Both sides must have a means to prove identity to each other
  - ▫ Implies the need for a PKI or other broad identity proof mechanism

Key management

- two types must be supported by implementations
  - manual
    - system administrator configures each system with the necessary keys
  - automated
    - on-demand creation of keys for SAs

Key management

- default automated method is ISAKMP/Oakley
  - Oakley key determination protocol
    - a key exchange protocol based on Diffie-Hellman
    - provides added security (e.g., authentication)
  - ISAKMP – Internet Security Association and Key Management Protocol
    - provides a framework for key exchange
    - defines message formats that can carry the messages of various key exchange protocols

Any question ?