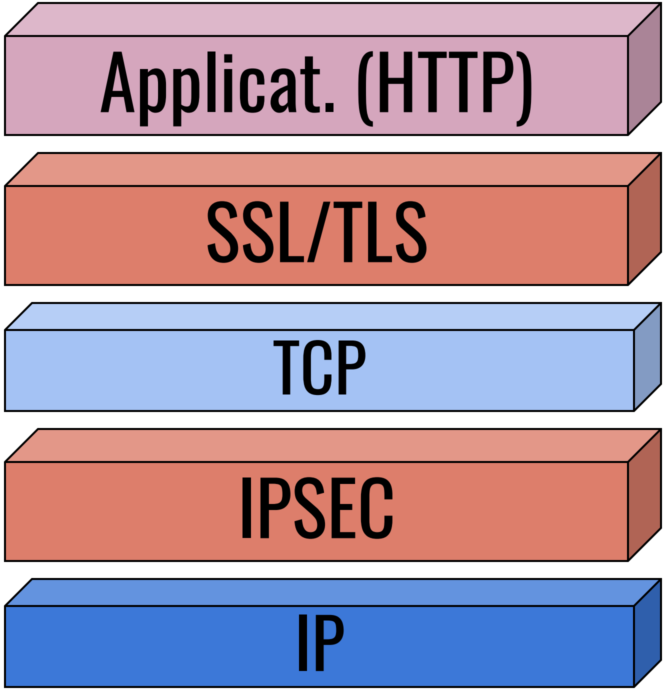
# IPSec

## Computer and Network Security

Emilio Coppa

# Security architecture and protocol stack




Approaches:

- Security in the applications: PGP, HTTPS, S-HTTP, SFTP.
- Security in the protocol stack:
  - SSL/TLS between TCP and application layer
  - IPSEC between IP and TCP

# Why (not) security on datagrams?

Idea: protect IP packets at each hop (there is a shared key among two routers that are connected by a link)

- Good:
  - all traffic is encrypted (including IP headers)
- Bad:
  - Cooperation among router is required
  - Significant computational effort (when a router receives a packet decodes it, then encodes it for next hop)

# IP Security

- there exist several application specific security mechanisms
  - e.g. S/MIME, PGP, Kerberos, SSL/HTTPS
- however there are security concerns that cut across protocol layers
- it is important to have a security protocol that can be used by all applications

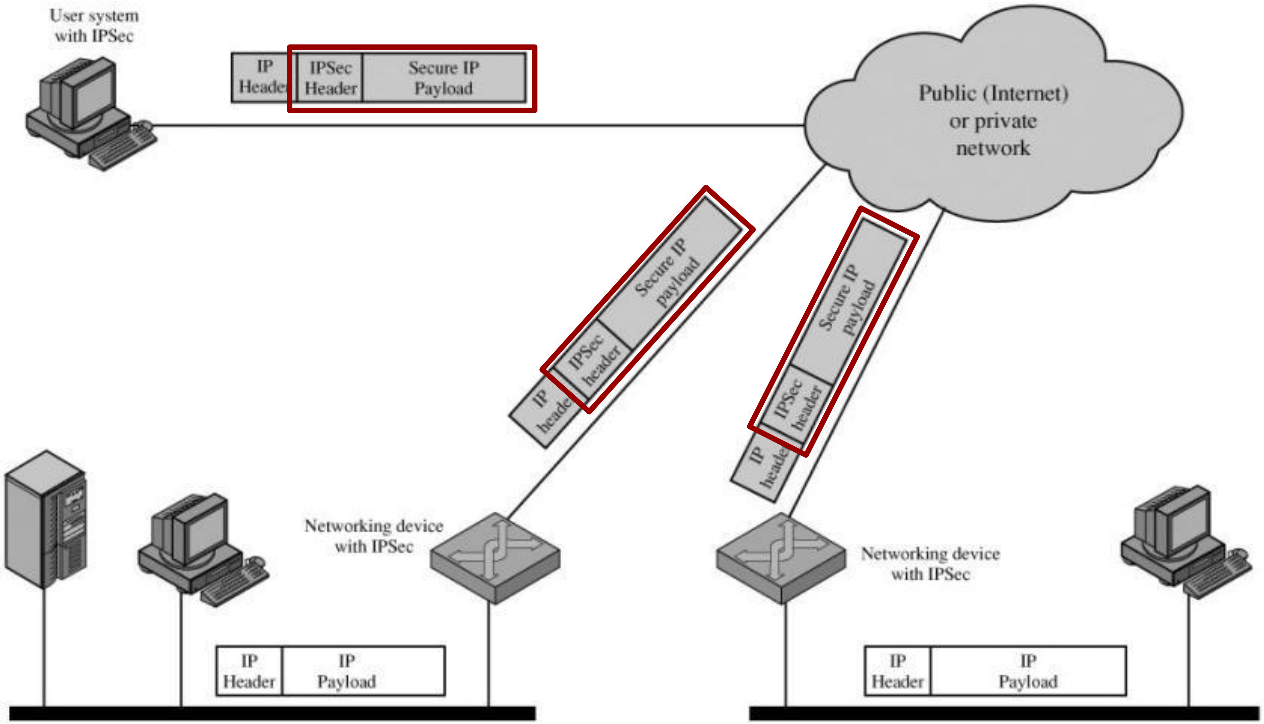
One solution: IP Security, which provides security between IP and TCP

# IPSec

- IP Security mechanism provides:
  - authentication
  - confidentiality
  - key management

- applicable to use over LANs, across public & private WANs & for the Internet
- Very complicated & articulated specification (many docs...). It was formerly mandatory in IPv6, then (2011) optional. Optional in IPv4.

# IPSec



User system
with IPSec
IP
Header
IPSec
Header
Secure IP
Payload
Public (Internet)
or private
network
IP
header
IPSec
header
Secure IP
payload
IP
header
IPSec
header
Secure IP
payload
Networking device
with IPSec
Networking device
with IPSec
IP
Header
IP
Payload
IP
Header
IP
Payload

# Benefits of IPSec

- a firewall/router provides strong security to all traffic crossing the perimeter
- is resistant to bypass
- is below transport layer, hence transparent to applications
- can be transparent to end users (allows to realize Virtual Private Networks)
- can provide security for individual users if desired

# Practical applications of IPSec

- Secure branch office connectivity over the Internet
  - A company can build a secure virtual private network over the Internet or over a public WAN
- 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

# Practical applications of IPSec (2)

- 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

# Practical applications of IPSec (3)

- The principal feature of IPSec that enables it to support these varied applications is that it can encrypt and/or authenticate all traffic at the IP level

- All distributed applications, including remote login, client/server, e-mail, file transfer, Web access, and so on, can be secured
    - also routing protocols could benefit

# Security features

Implemented as extension headers that follow the main IP header:

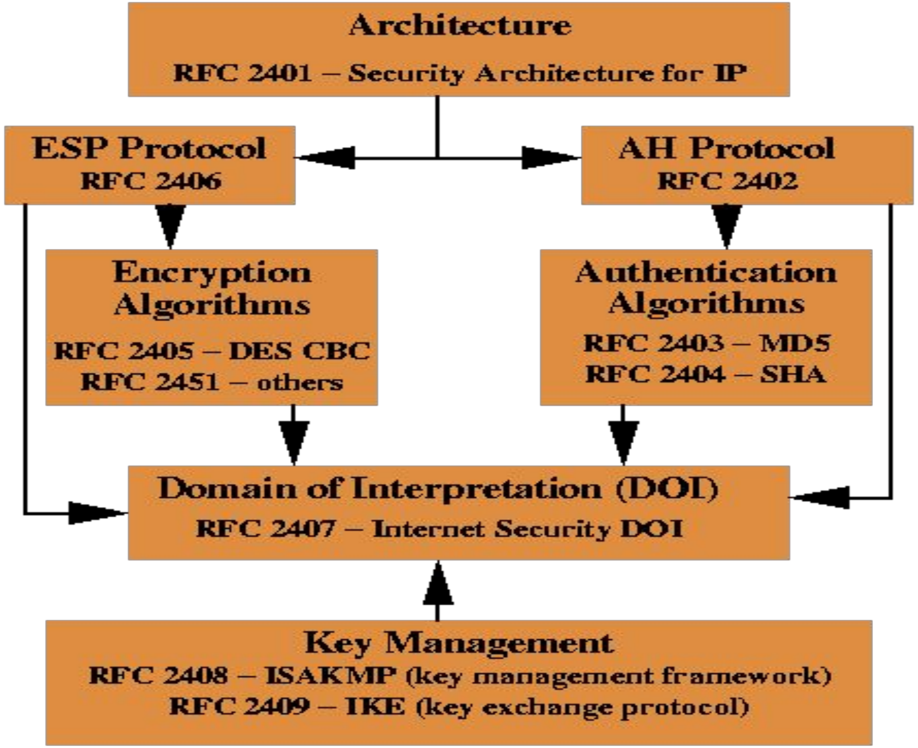
- Authentication Header (AH) is the extension header for <u>authentication</u> and <u>integrity</u>
- Encapsulating Security Payload (ESP) is the extension header for <u>encryption</u>

# IPSec Documents

The most important (1998):

- RFC 2401: An overview of a security architecture
- RFC 2402: Description of a packet authentication extension to IPv4 and IPv6
- RFC 2406: Description of a packet encryption extension to IPv4 and IPv6
- RFC 2408: Specification of key management capabilities

# IPsec Document Roadmap



# IPSec Services

- Access control
  - prevents unauthorized use of a resource (computing cycles, data, network, bandwidth etc.)
- Connectionless integrity
  - detects modification of an individual IP datagram
- Data origin authentication
  - verifies the identity of the claimed source of data
- Rejection of replayed packets
  - a form of partial sequence integrity
- Confidentiality (encryption)
- Limited traffic flow confidentiality
  - *traffic flow confidentiality* = concealing source and destination addresses, message length, or frequency of communication

# IPSec Architecture

Based on three main concepts:

- Security Association (SA): provides the bundle of algorithms and data that provide the parameters necessary for IPSec operations. Internet Security Association and Key Management Protocol (ISAKMP) has been defined to establish SA.
- Authentication Headers provides connectionless data integrity and data origin authentication for IP datagrams and provides protection against replay attacks.
- Encapsulating Security Payload (ESP) provides confidentiality, connectionless data integrity, data-origin authentication, an anti-replay service (a form of partial sequence integrity), and limited traffic-flow confidentiality.

# Services provided by AH and ESP protocols

- For ESP, two cases: with and without the authentication option
- Both AH and ESP are vehicles for access control, based on the distribution of cryptographic keys and the management of traffic flows relative to these security protocols

| | AH | ESP (encryption only) | ESP (encryption plus authentication) |
|---|---|---|---|
| Access control | ✔ | ✔ | ✔ |
| Connectionless integrity | ✔ | | ✔ |
| Data origin authentication | ✔ | | ✔ |
| Rejection of replayed packets | ✔ | ✔ | ✔ |
| Confidentiality | | ✔ | ✔ |
| Limited traffic flow confidentiality | | ✔ | ✔ |

Remark. ESP does not allow inspection of inner data (which can useful in, e.g., firewalls)

# Security Associations

A Security Association (SA) is a <u>one-way</u> cryptographically protected connection:


Remark. A SA is an unidirectional “channel”. Hence, if a bi-directional channel is needed, then two SAs must be established, i.e., SA(A, B) and SA(B, A).

# Security Associations (2)

Each SA is identified by three main parameters:

1. Security Parameters Index (SPI)
2. IP Destination Address
3. Security Protocol Identifier (AH or ESP)

This data, as well other details about SAs, are stored into a Security Association Database (SADB). RFC 2401 requires two databases, one for inbound connections and one for outbound connections.

# Security Association Database (SADB)

For each SA, it stores:

- Security Parameters Index (SPI): unique identifier, conceptually similar to TCP port number; it enables the receiving system to select the SA under which a received packet will be processed
- IP Destination Address
- Security Protocol Identifier (AH or ESP)
- Sequence Number Counter: 32-bit value used to generate the Sequence Number field in AH or ESP headers

# Security Association Database (2)

- Sequence Counter Overflow: 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

# Security Association Database (3)

- Lifetime: a time interval or byte count after which an SA must be replaced with a new SA (and new SPI) 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 (maximum size of a packet that can be transmitted without fragmentation) and aging variables

# Multicast SA

- For multicast, SA is provided for the group, and is duplicated across all authorized receivers of the group.
- There may be more than one SA for a group, using different SPIs, thereby allowing multiple levels and sets of security within a group.
- Note that the relevant standard does not describe how the association is chosen and duplicated across the group; it is assumed that a responsible party will have made the choice.

# Security Policy Database (SPDB)

The Security Policy Database (SPD) contains a set of rules that determines whether a packet is subject to IPsec processing and governs the processing details. Each entry in the SPD represents a policy that defines how the set of traffic covered under the policy will be processed. Any inbound or outbound packet is processed in one of three ways:

- discard
- perform IPsec processing
- bypass IPsec processing.

# Security Policy Database (SPDB) and SA selectors

To match a packet with SA, SPDB uses SA selectors:

1. Compare the values of the appropriate fields in the packet (the selector fields) against the SPDB 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)

# SA selectors

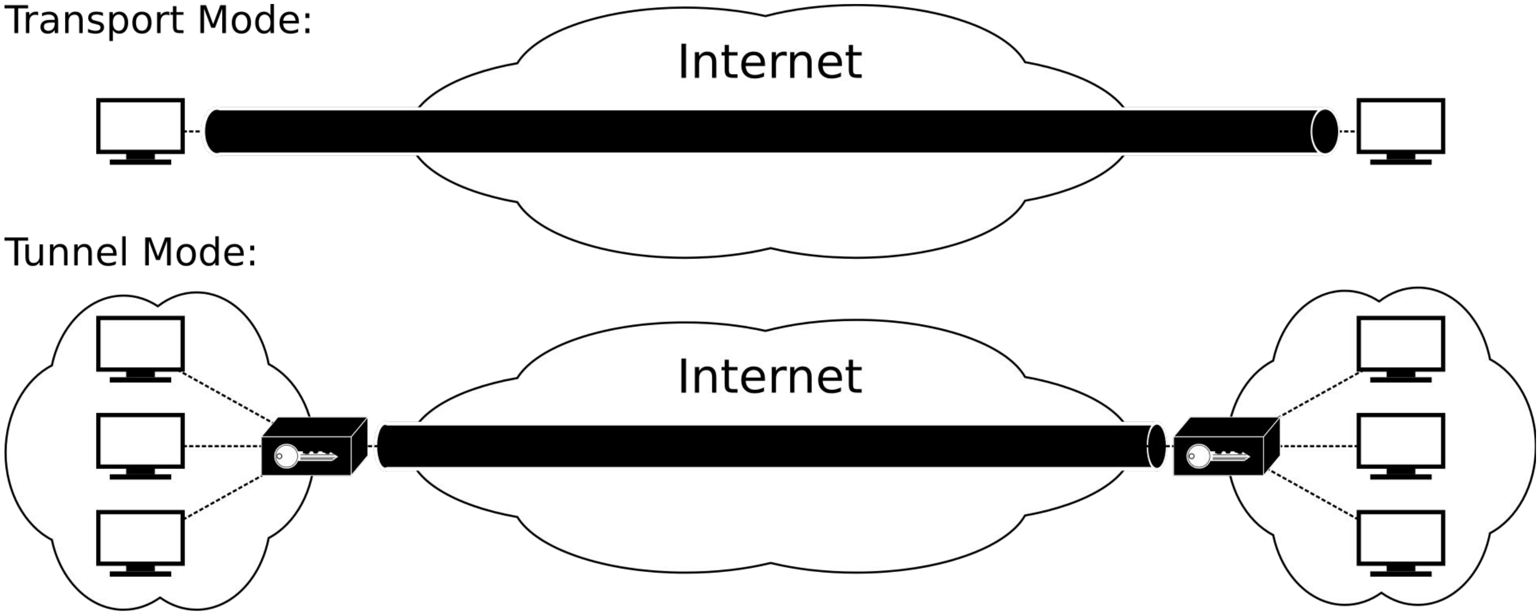
- Destination IP Address: a single IP address, an enumerated list or range of addresses, or a wildcard (mask) address
- Source IP Address: a single IP address, an enumerated list or range of addresses, or a wildcard (mask) address
- UserID: a user identifier from the operating system; not a field in the IP or upper-layer headers but is available if IPSec is running on the same operating system as the user
- Data Sensitivity Level: used for systems providing information flow security (e.g., *secret* or *unclassified*)
- Transport Layer Protocol: from IPv4 or IPv6, may be an individual protocol number, a list of protocol numbers, or a range of protocol numbers
- Source and Destination Ports: may be individual TCP/UDP port values, an enumerated list of ports, or a wildcard port

# SADB vs SPDB

- SPDB specifies the policies that determine the disposition of all IP traffic inbound or outbound from a host or a security gateway
- SADB is a security association table, containing parameters of the security associations

# Transport vs Tunnel Mode

Transport mode is often used for end-to-end security




Tunnel mode is often used for building a secure tunnel between two networks

# Transport vs tunnel mode (2)

# Transport mode

Original IP header not touched. IPsec information added between IP header and packet body:

IP header | IPsec | [ packet ]

$\underbrace{\text{[ packet ]}}_{\text{protected}}$

Most logical when IPsec used end-to-end

# Transport mode (2)

- Used for host-to-host communications
- Only payload (the data you transfer) of IP packet is encrypted and/or authenticated
- Routing is intact, since the IP header is neither modified nor encrypted
  - however, when the authentication header is used, the IP addresses cannot be translated (NAT), as this will invalidate the hash value

# Transport mode (3)

- Transport and application layers are always secured by hash, so they cannot be modified in any way (for example by translating the port numbers)
- A means to encapsulate IPsec messages for NAT traversal has been defined (see RFCs 3715, 3947, 3948), describing the NAT-T mechanism

# Tunnel mode

Keep original IP packet intact but protect it; add new header information outside:

New IP header | IPsec | [ old IP header | packet ]

encrypted

authenticated

Can be used when IPSec is applied at intermediate point along path (e.g., for firewall-to-firewall traffic) and treat the link as a secure tunnel.

Results in slightly longer packet

# Tunnel mode (2)

- The entire IP packet (data and IP header) is encrypted and/or authenticated. It is then encapsulated into a new IP packet with a new IP header.
- Tunnel mode is used to create Virtual Private Networks (VPN) for network-to-network communications (e.g. between routers to link sites), host-to-network communications (e.g. remote user access), and host-to-host communications (e.g. private chat)

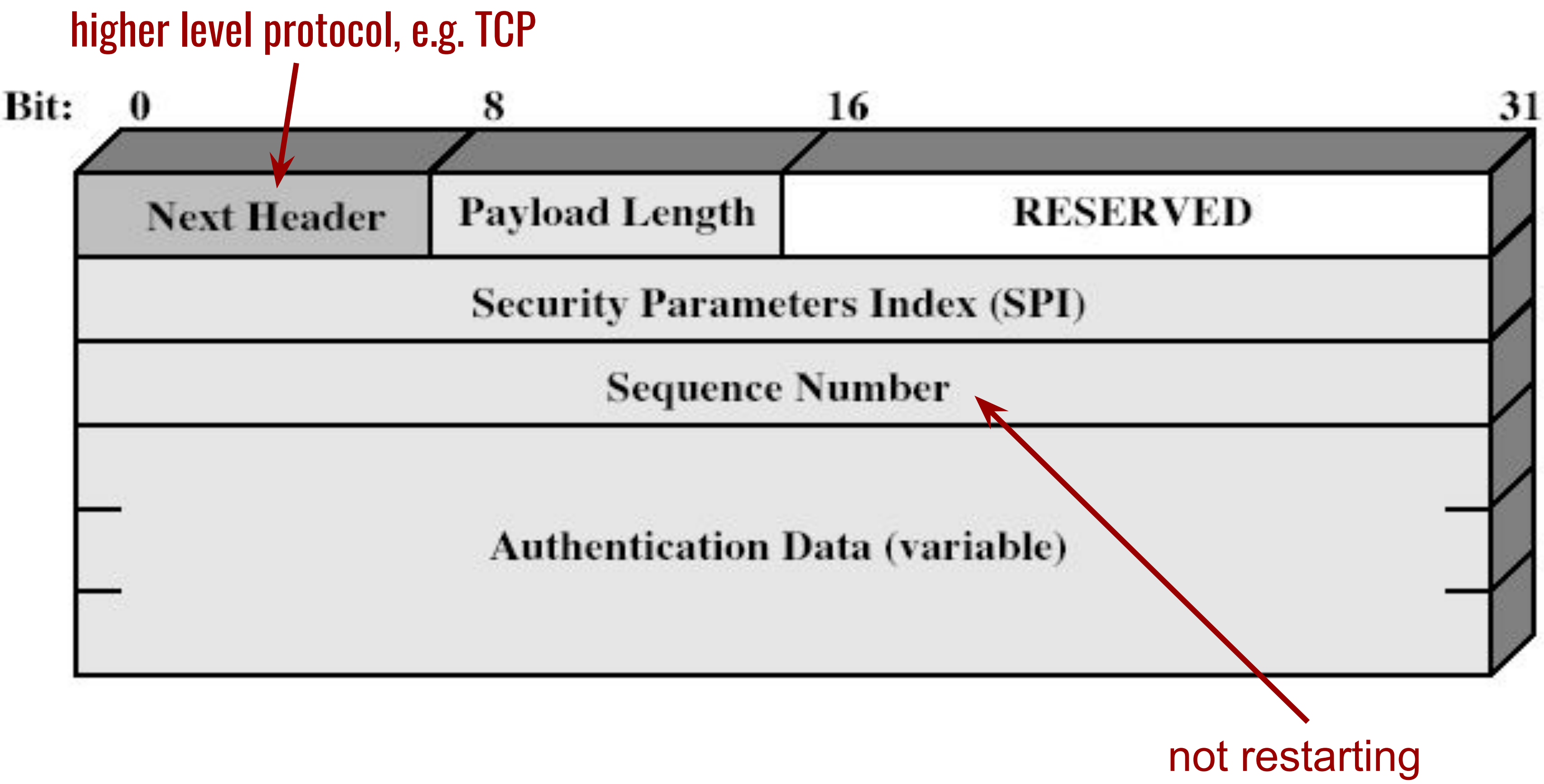
# Tunnel & Transport Mode Functionality

| | 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. |

# Authentication Header (AH)

- provides support for data integrity & authentication of IP packets
  - end system/router can authenticate user/app
  - prevents address spoofing attacks by tracking sequence numbers
- does not provide support for confidentiality
- based on use of a MAC
  - HMAC-MD5-96 or HMAC-SHA-1-96 (160 bits truncated to 96)
- users must share a secret key

# Authentication Header



# AH protocol

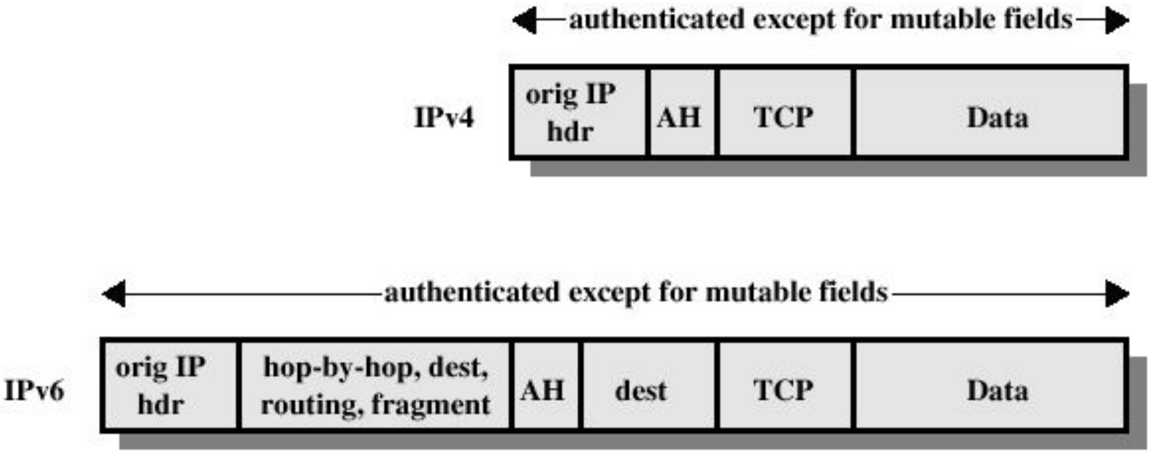
- AH protects the IP payload and all header fields of an IP datagram except for mutable fields
  - In IPv4, mutable (and therefore unauthenticated) IP header fields include TOS, Flags, Fragment Offset, TTL and Header Checksum.
- AH operates directly on top of IP, using IP protocol number 51

# HMAC (from RFC 2104)

- $H(\cdot)$ be a cryptographic hash function: e.g., MD5, SHA-1
- K be a secret key padded to the right with extra zeros to the block size of the hash function
- m be the message to be authenticated
- // denote concatenation, $\oplus$ denote exclusive or (XOR)
- opad be the outer padding (0x5c5c5c…5c5c, one-block-long hexadecimal constant)
- ipad be the inner padding (0x363636…3636, one-block-long hexadecimal constant)

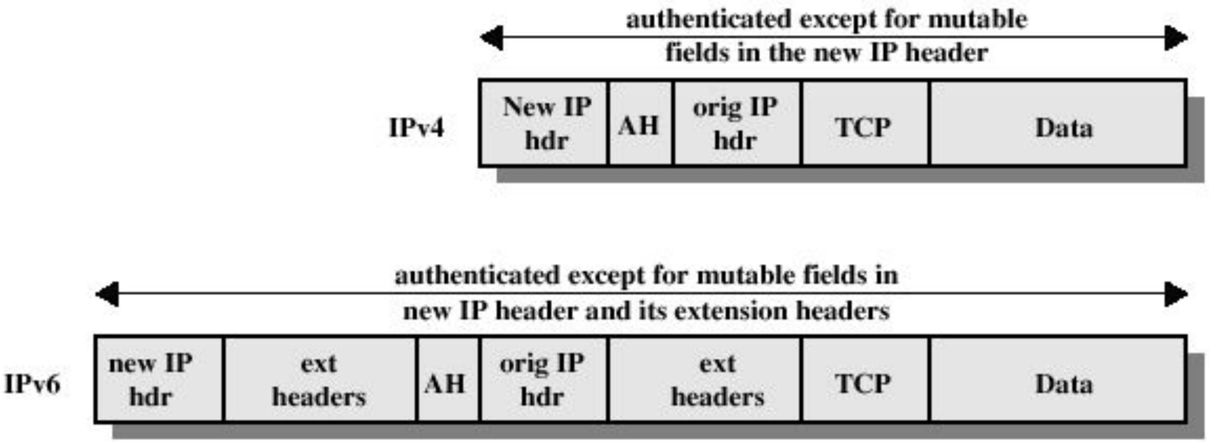
$$HMAC(K,m) = H((K \oplus opad)\ //\ H((K \oplus ipad)\ //\ m))$$

# Authentication Header (AH): transport mode




Note that only part of the header is authenticated

# Authentication Header (AH): tunnel mode

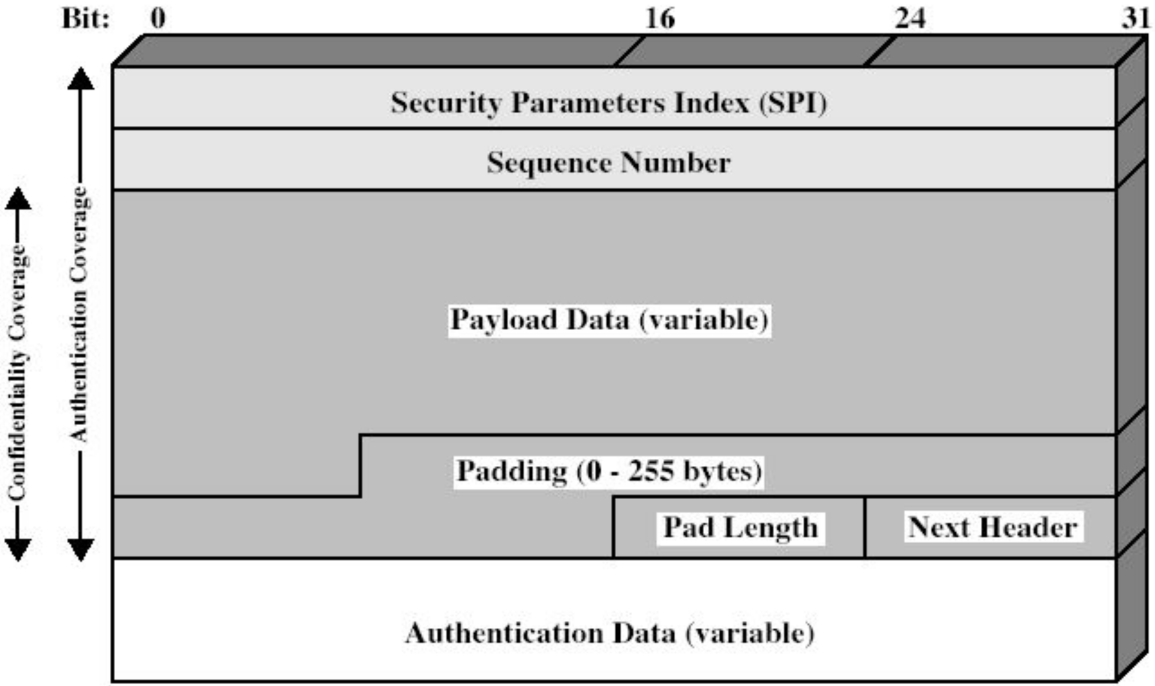



Note that only part of the header is authenticated

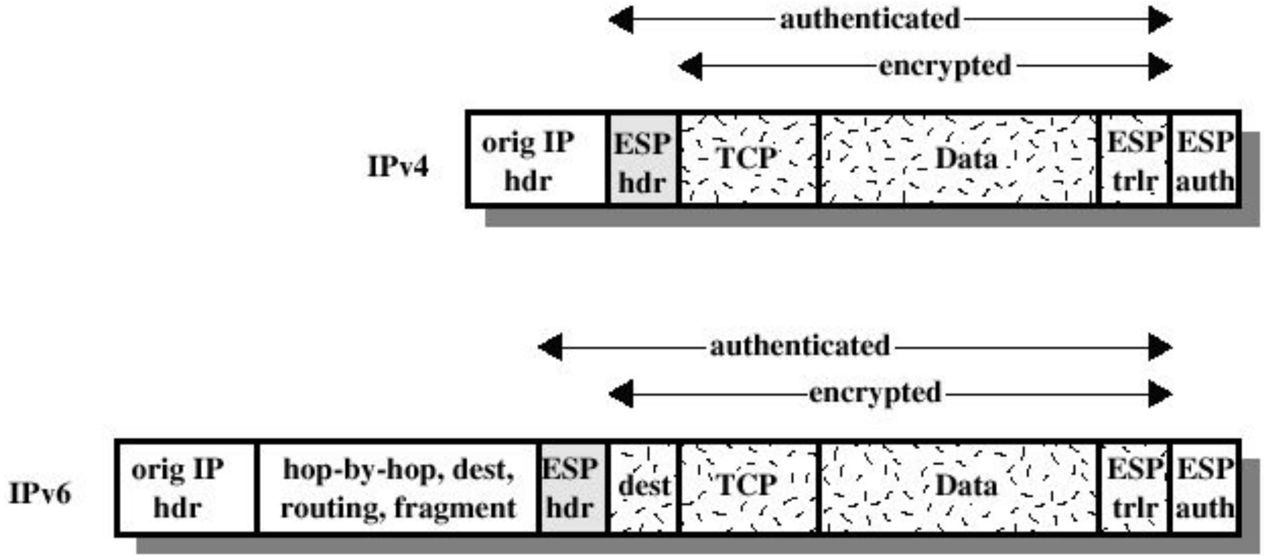
# Encapsulating Security Payload (ESP)

- provides message content confidentiality & limited traffic flow confidentiality
- can optionally provide the same authentication services as AH
- supports range of ciphers, modes, padding
  - AES, DES, Triple-DES, Blowfish etc
  - CBC most common
  - padding to meet blocksize of the packet
  - HMAC (same as AH)

# Encapsulating Security Payload

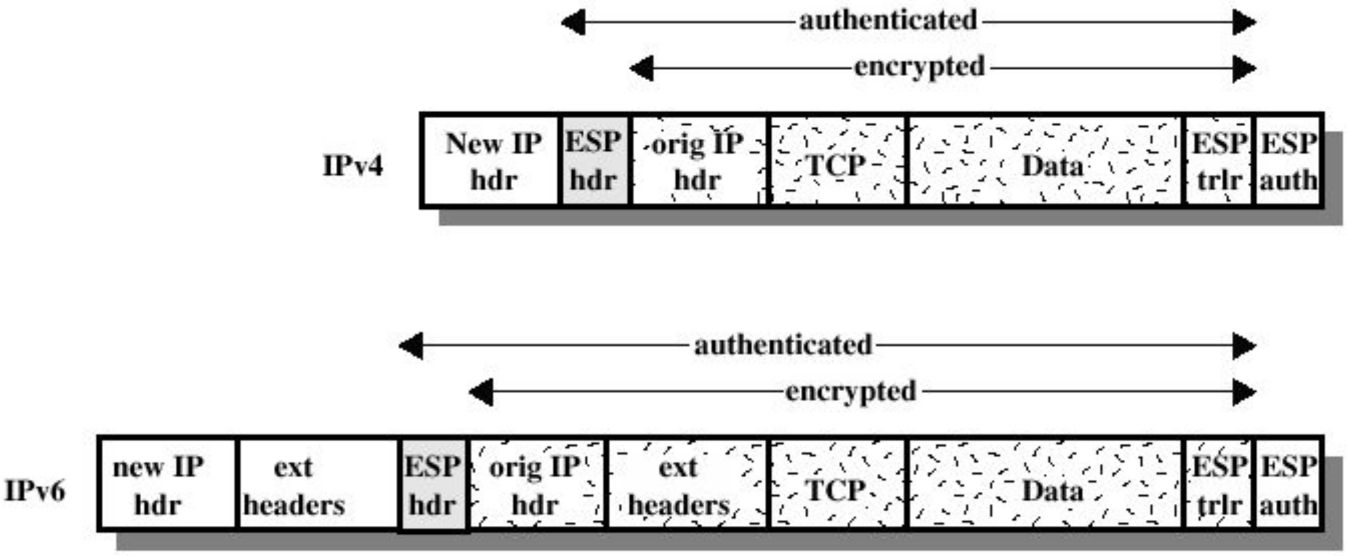


# ESP (encryption and authentication): transport mode




(a) Transport Mode

# ESP (encryption and authentication): tunnel mode




(b) Tunnel Mode

# Transport vs Tunnel Mode ESP

- transport mode is used to encrypt & optionally authenticate IP data
  - data protected but header left in clear
  - adversary can try traffic analysis
  - good for host to host traffic

- tunnel mode encrypts entire IP packet
  - add new header for next hop
  - slow
  - good for VPNs (Virtual Private Networks, gateway to gateway security)

# Combining Security Associations

- Because an ESP header cannot authenticate the outer IP header, it is useful to combine an AH and an ESP. SAs can implement either AH or ESP
- to implement both need to combine SAs and form a security bundle; two ways:
    - transport adjacency
        - applying more than one protocol to same IP packet, without tunneling
        - only one level of combination, further nesting yields no added benefit
    - iterated tunneling
        - application of multiple layers of security effected through IP tunneling
        - allows for multiple levels of nesting, since each tunnel can originate or terminate at a different IPsec site along the path
- 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

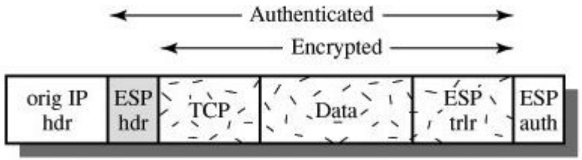
Encryption and authentication can be combined in order to transmit a packet that has both confidentiality and authentication.

Several approaches:

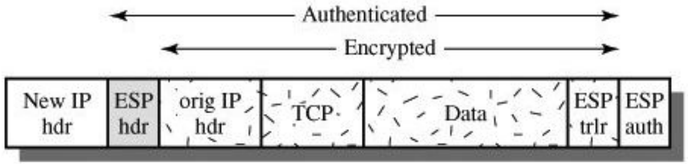
- ESP with authentication option
- Transport adjacency
- Transport-tunnel bundle

# ESP with authentication option

- User first applies ESP to data to be protected, then appends the authentication data field. Two subcases:
  - Transport mode ESP
    Authentication and encryption apply to IP payload delivered to the host, but IP header not protected




  - Tunnel mode ESP Authentication applies to entire IP packet delivered to outer IP destination address and authentication is performed at that destination. Entire inner IP packet is protected by the privacy mechanism, for delivery to the inner IP destination

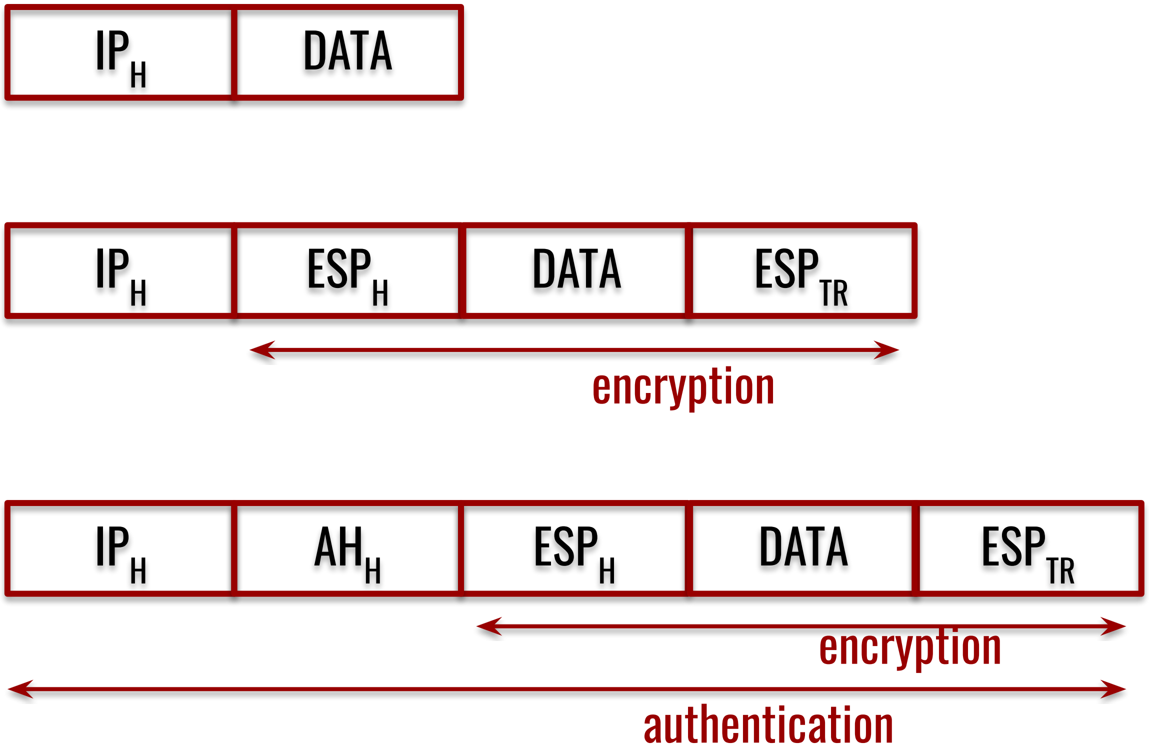



- For both cases, authentication applies to the ciphertext rather than the plaintext (authentication after encryption)

# Transport adjacency

- still authentication after encryption
- two bundled transport SAs
  - inner = ESP (no authentication)
  - outer = AH
- encryption is applied to IP payload and resulting packet is IP header + ESP
- AH is then applied in transport mode, so that authentication covers the ESP + original IP header (except for mutable fields)
- advantage over ESP + authentication: authentication covers more fields, including source and destination IP addresses
- disadvantage: overhead (two SAs versus one SA)

# Transport adjacency



# What about authentication first?

authentication prior to encryption:

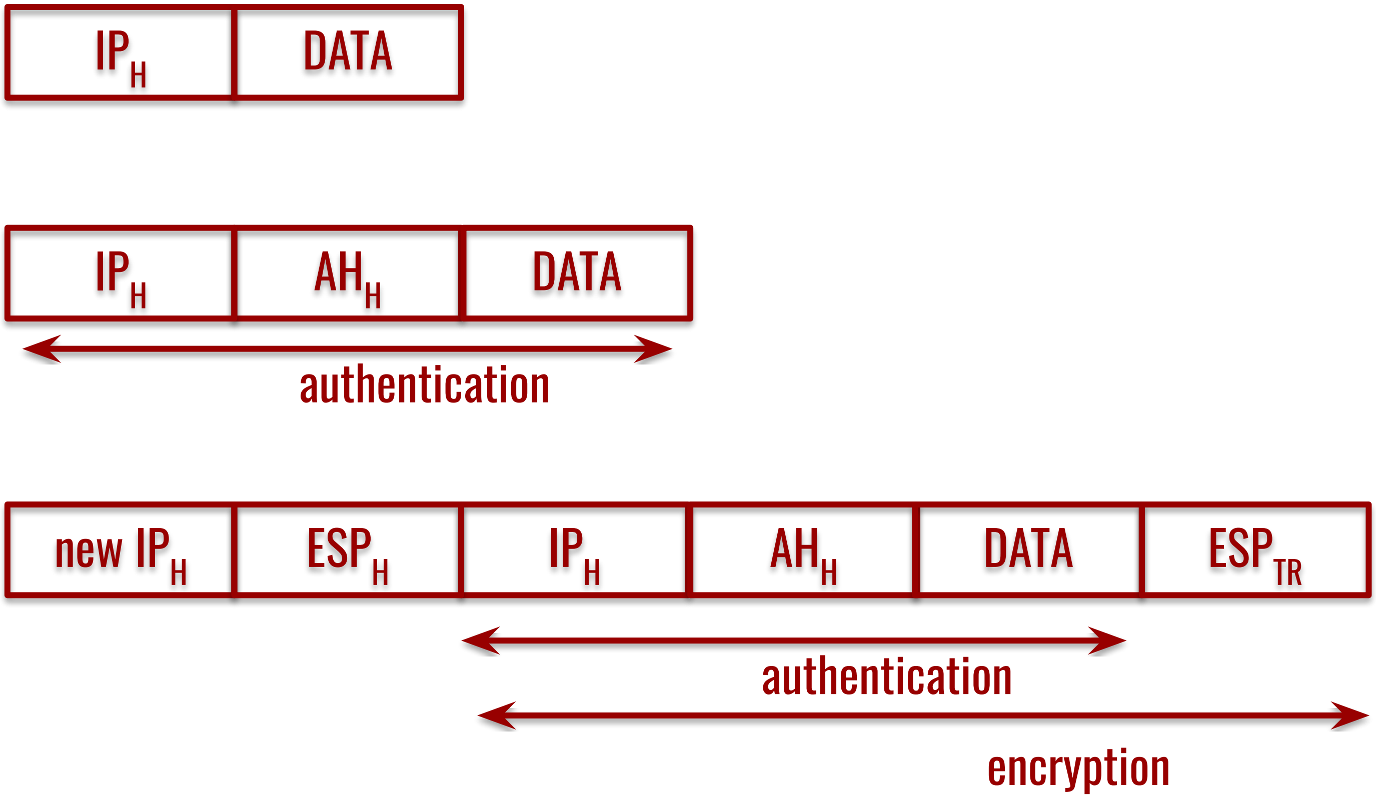
- since authentication data are protected by encryption, it is impossible to alter authentication data without decryption
- if message is stored as plaintext then verifying authentication data requires re-encryption

# Transport-tunnel bundle

Authentication before encryption between two hosts

- use a bundle consisting of an inner AH transport SA and an outer ESP tunnel SA
- authentication is applied to IP payload plus the IP header except for mutable fields
- resulting 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 is added

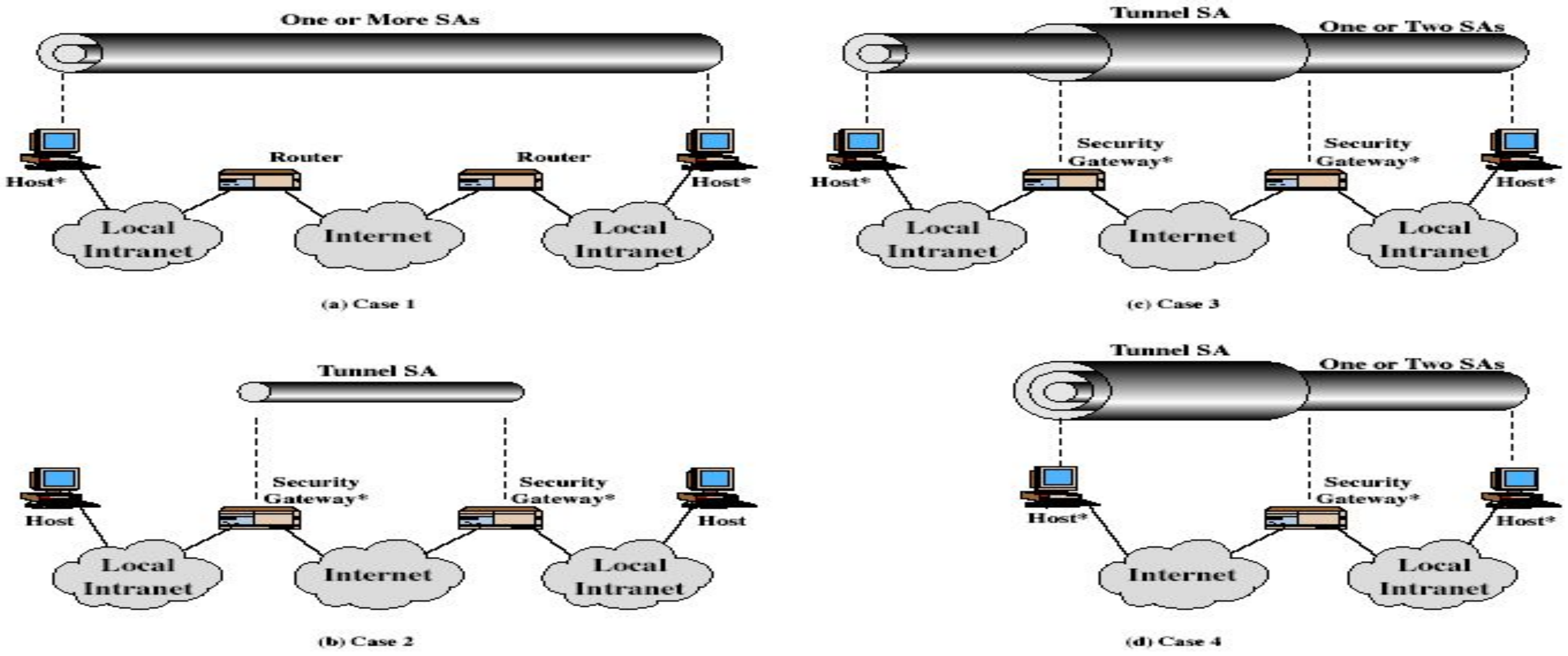
# Transport-tunnel bundle



# Combining Security Associations

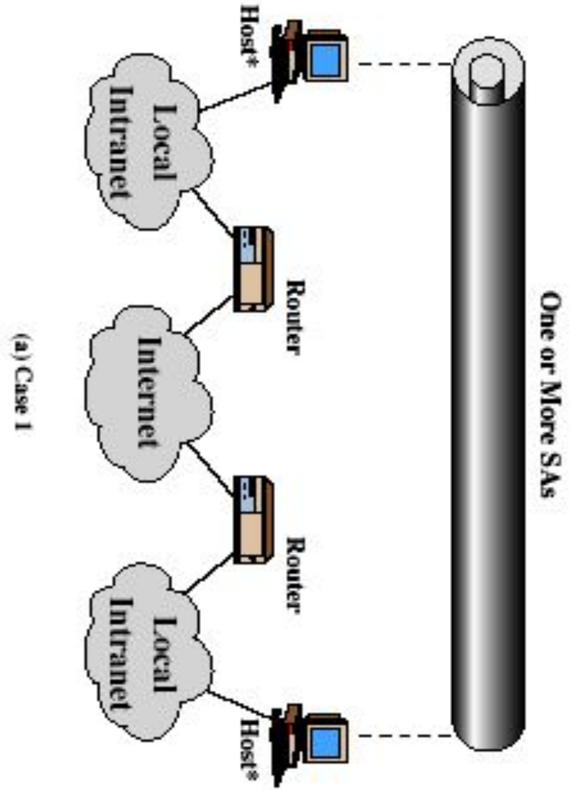
The IPSec Architecture document lists four examples of combinations of SAs that must be supported by compliant IPSec hosts (e.g., workstation, server) or security gateways (e.g. firewall, router)

# Combining Security Associations



# Case #1

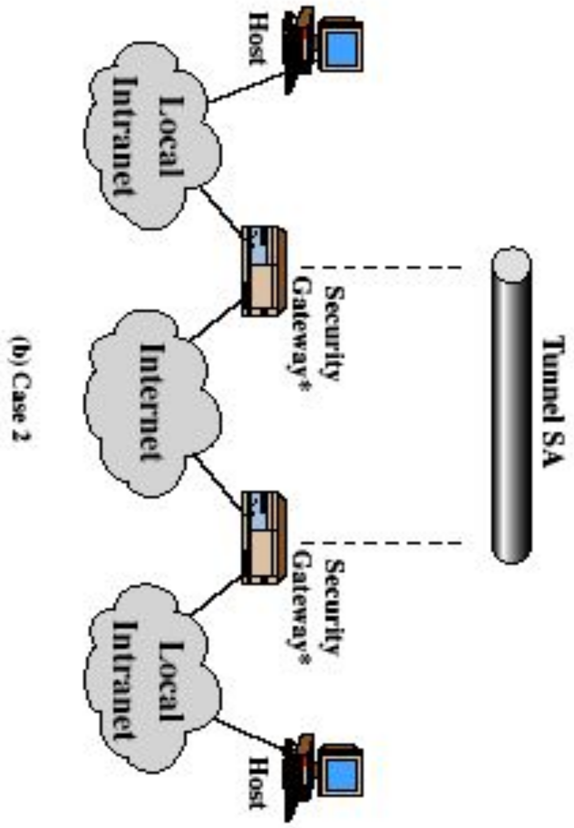
- All security is provided between end systems that implement IPSec.
- For any two end systems to communicate via an SA, they must share the appropriate secret keys.
- Among the possible combinations:
  - AH in transport mode
  - ESP in transport mode
  - ESP followed by AH in transport mode (an ESP SA inside an AH SA)
  - Any one of the preceding, inside an AH or ESP in tunnel mode
- Support for
  - authentication
  - encryption
  - authentication before encryption
  - authentication after encryption



# Case #2

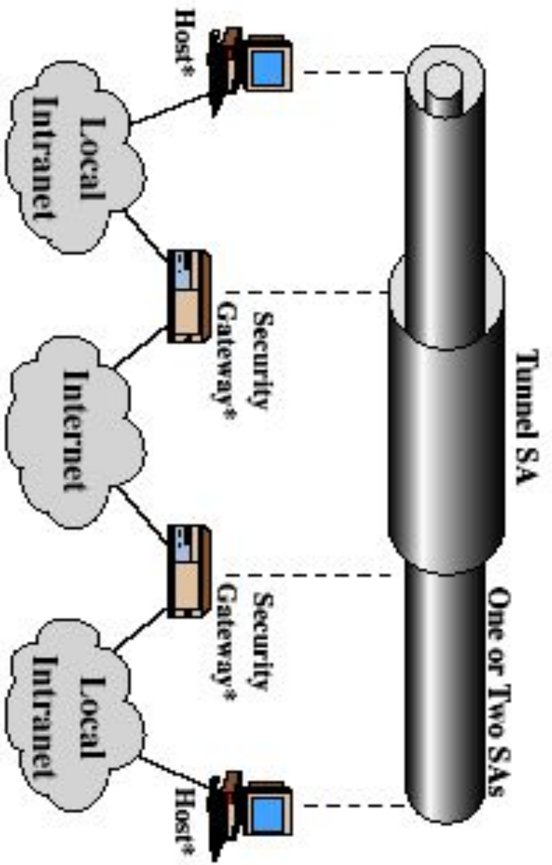
- Security is provided only between gateways (routers, firewalls, etc.) and no hosts implement IPSec (simple virtual private network support)

- 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

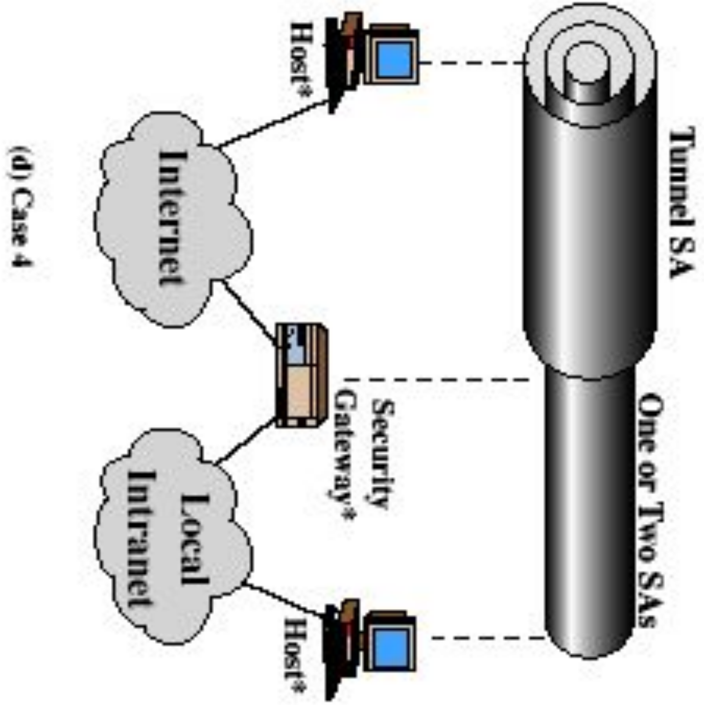
- Builds on Case 2 by adding end-to-end security. Same combinations discussed for cases 1 and 2 are allowed
- Gateway-to-gateway tunnel provides either authentication or confidentiality or both for all traffic between end systems
- When the gateway-to-gateway tunnel is ESP, it also provides a limited 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




(c) Case 3

# Case #4

- 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



# Key Management

- IPSEC handles key generation & distribution
- typically needs 2 pairs of keys
  - transmit and receive pair for both AH & ESP
- manual key management (mandatory)
  - system administrator manually configures every system
- automated key management (mandatory)
  - 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
- ISAKMP and Oakley

# ISAKMP

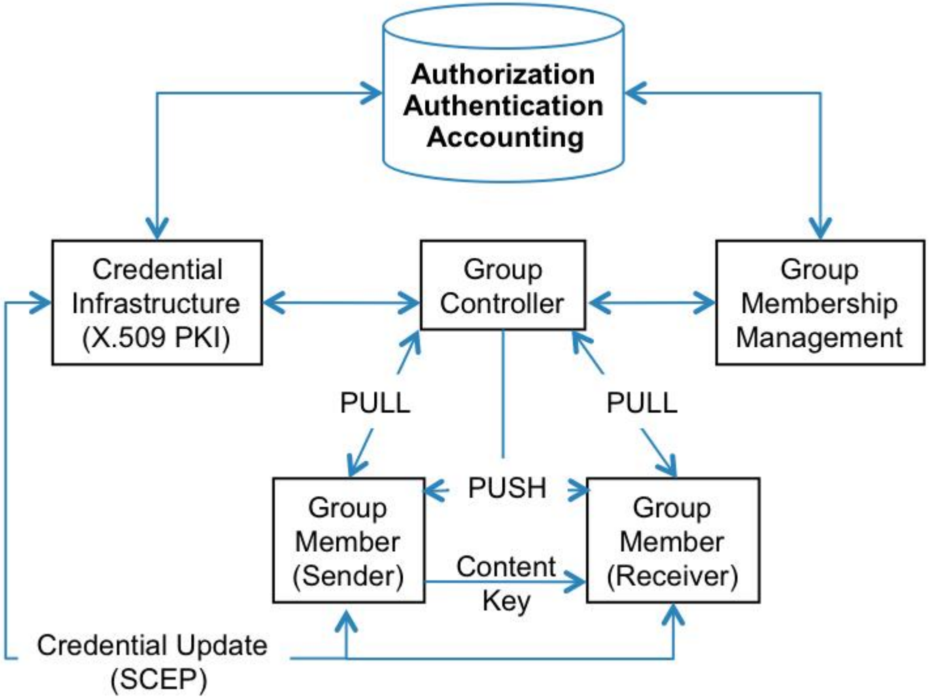
- Internet Security Association and Key Management Protocol. Designed by NSA. Work on top of UDP.
- provides framework for key management
- defines procedures and packet formats to establish, negotiate, modify & delete SAs
- independent of key exchange protocol, encryption alg & authentication method

# Oakley

- a key exchange protocol
- based on Diffie-Hellman key exchange
- adds features to address weaknesses
  - cookies, groups (global params), nonces, DH key exchange with authentication
- can use arithmetic in prime fields or elliptic curve fields

# Group Domain of Interpretation (GDOI)

- it is a protocol for group key management
- it is run between a group member and a "group controller" (key server) and establishes a security association among two or more group members



# Credits

These slides are based on material from:

- Slides of Prof. D'Amore from CNS 2019-2020
- Christof Paar and Jan Pelzl. Understanding Cryptography: A Textbook for Students and Practitioners. Springer. http://www.crypto-textbook.com/
- William Stallings. Cryptography and Network Security.
- Wikipedia (english version)