IP SECURITY

PRESENTED BY:

KESHAB NATH

OUTLINE

- IP SECURITY OVERVIEW
- IP SECURITY ARCHITECTURE
- AUTHENTICATION HEADER
- ENCAPSULATING SECURITY PAYLOAD
- COMBINING SECURITY ASSOCIATIONS
- KEY MANAGEMENT

IP Security Overview

The standard Internet communication protocol is completely unprotected, allowing hosts to inspect or modify data in transit. Adding IPSec to the system will resolve this limitation by providing strong encryption, integrity, authentication and replay protection.

What Security Problem?

Today's Internet is primarily comprised of :

- Public
- Un-trusted
- Unreliable IP networks

Because of this inherent lack of security, the Internet is subject to various types of threats…

Internet Threats

- Data integrity

  The contents of a packet can be accidentally or deliberately modified.
- Identity spoofing

  The origin of an IP packet can be forged.
- Anti-reply attacks

  Unauthorized data can be retransmitted.
- Loss of privacy

  The contents of a packet can be examined in transit.

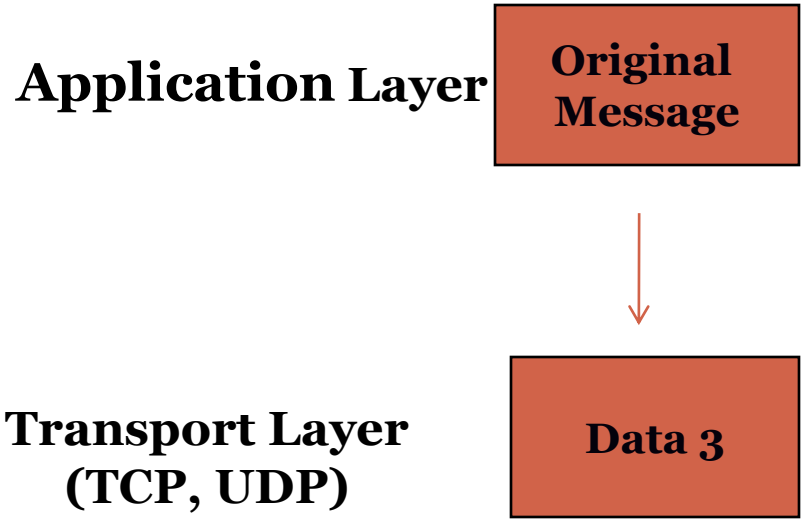
Security at What Level?

Application Layer	PGP, Kerberos, SSH, etc.
Transport Layer	Transport Layer Security (TLS)
Network Layer	IP Security
Data Link Layer	Hardware encryption

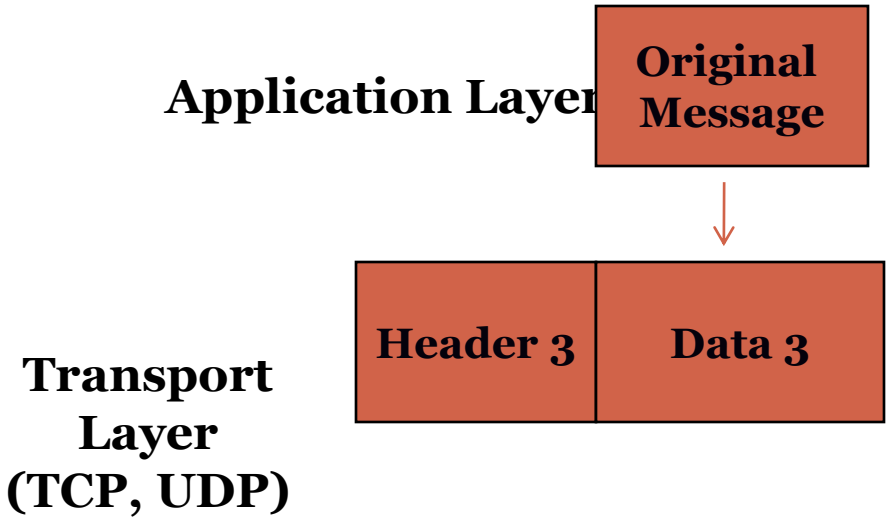
Encapsulation of Data for Network Delivery

Application Layer

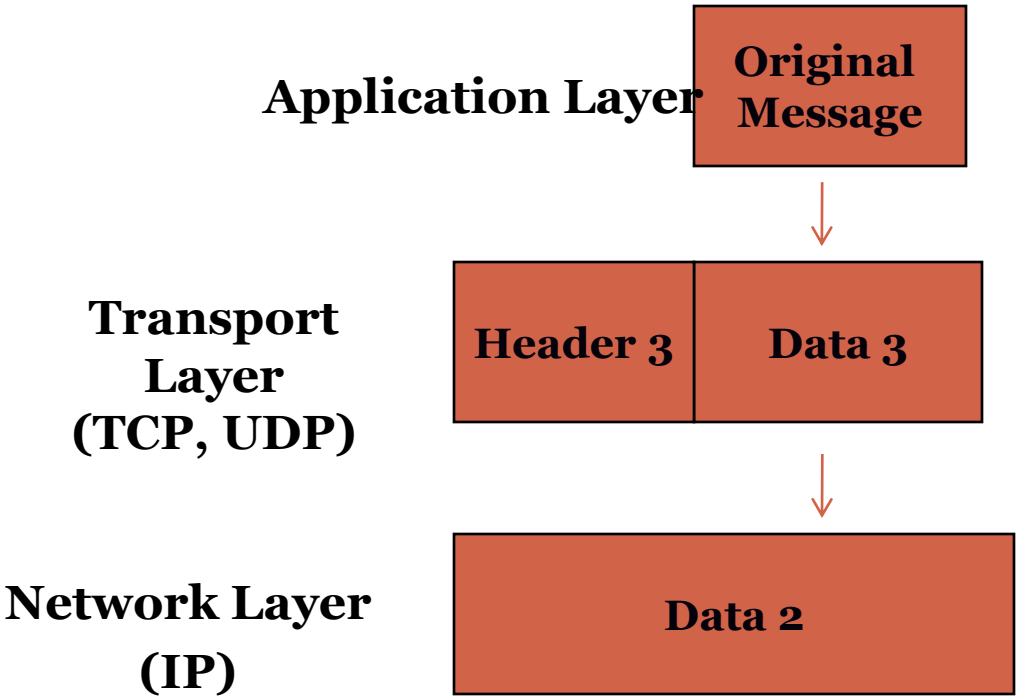
Encapsulation of Data for Network Delivery



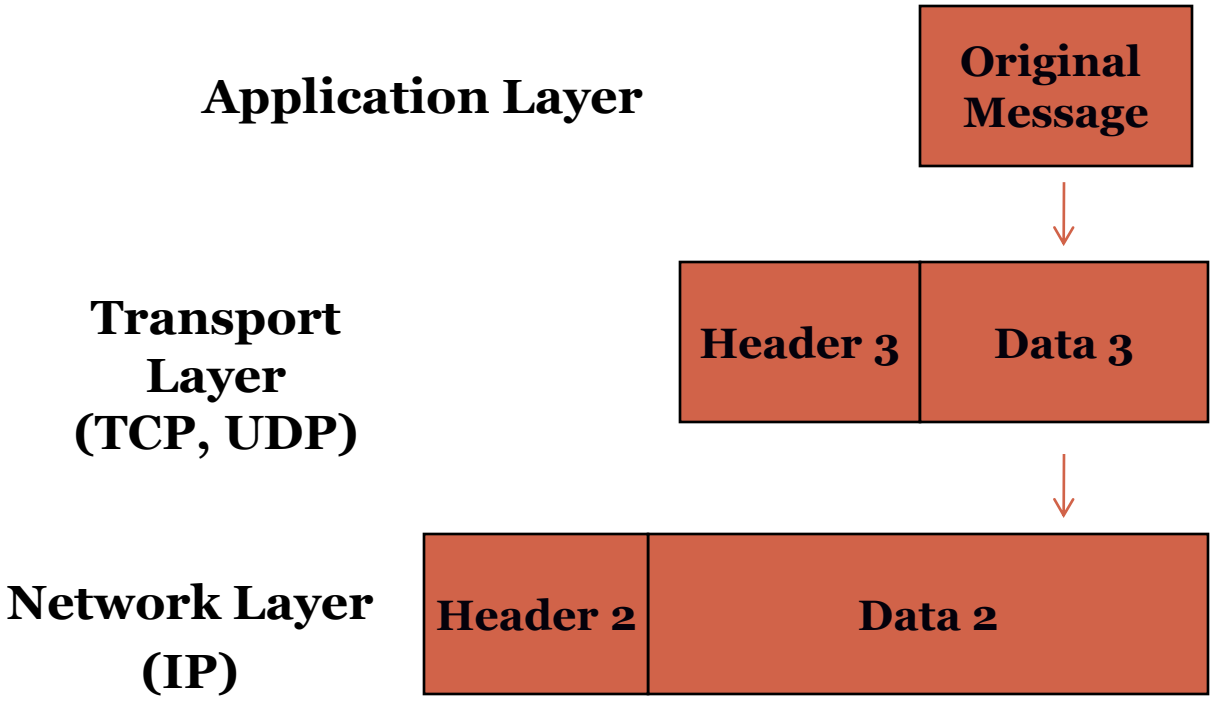
Encapsulation of Data for Network Delivery



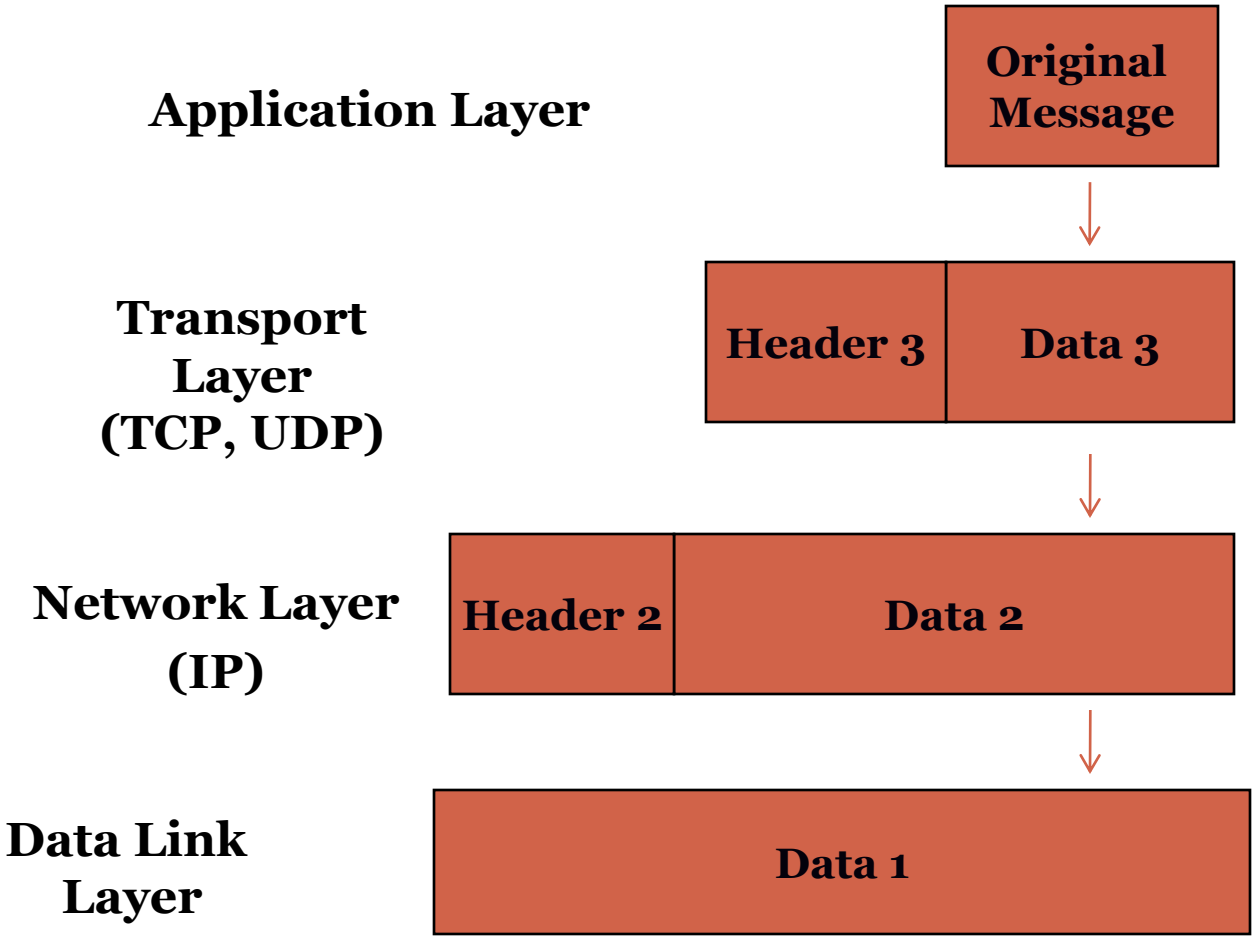
Encapsulation of Data for Network Delivery



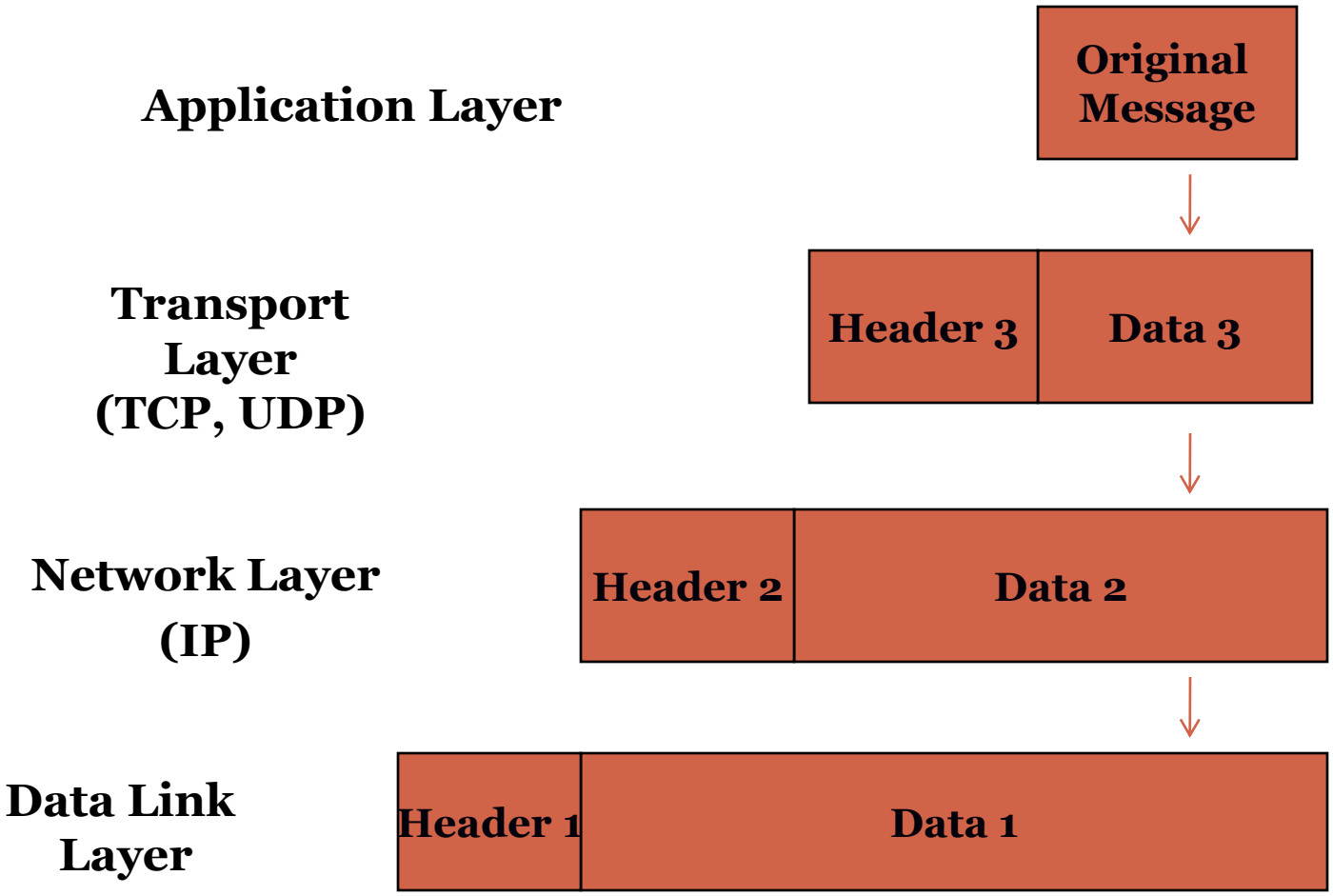
Encapsulation of Data for Network Delivery



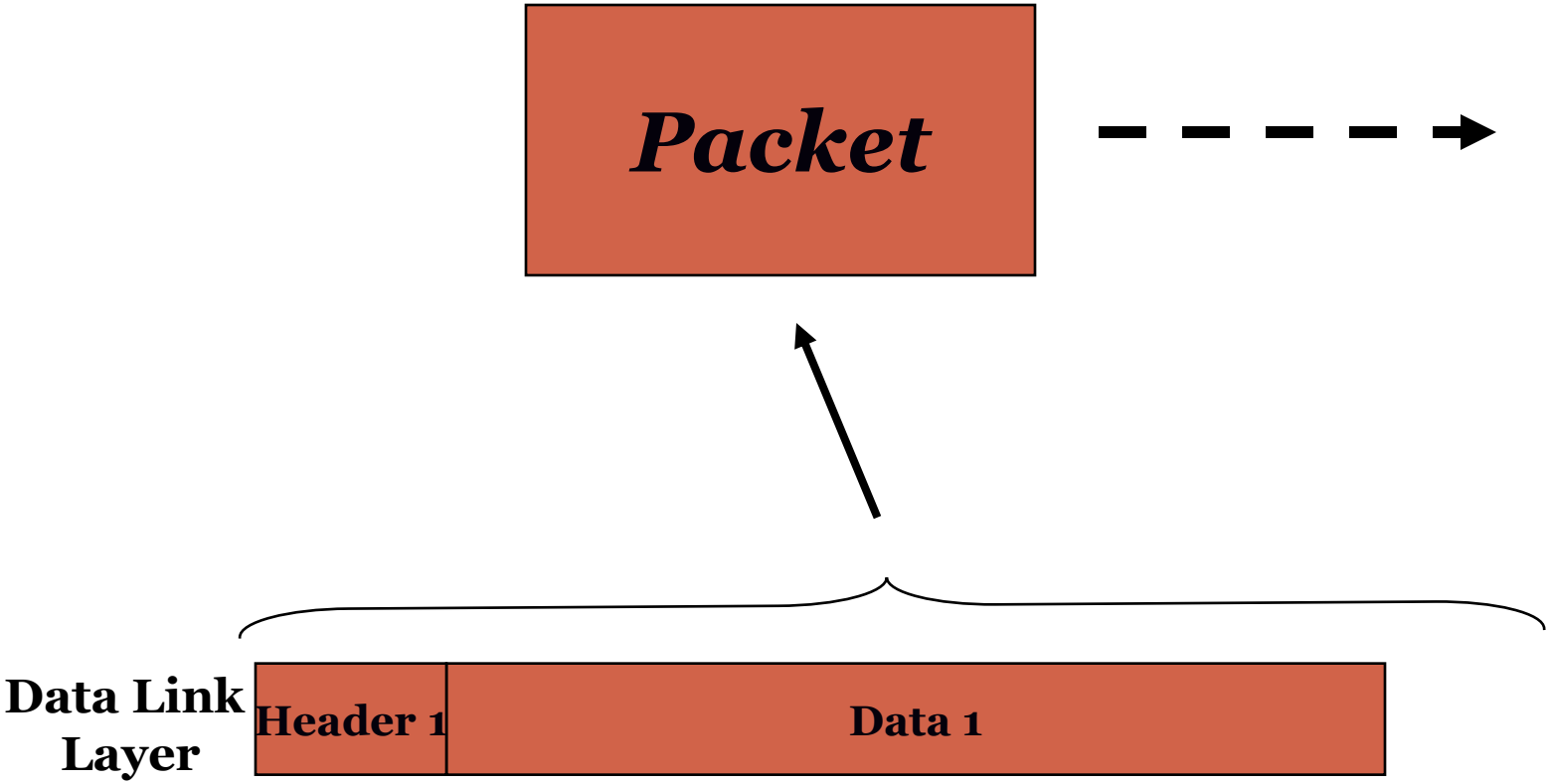
Encapsulation of Data for Network Delivery



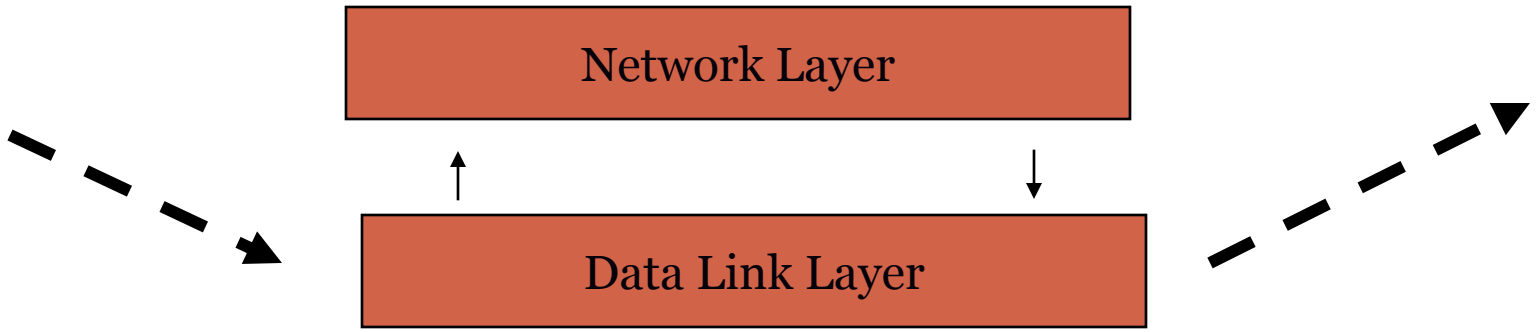
Encapsulation of Data for Network Delivery



Packet Sent by Host A



Packet Received by intermediary Router



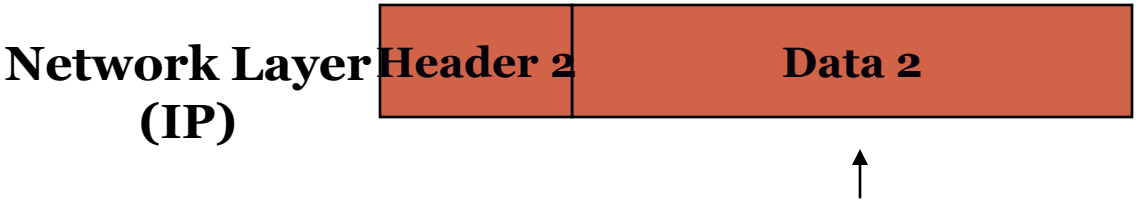
De-capsulation of Data from Network Delivery

De-capsulation of Data from Network Delivery

Data Link Layer

Data 1

De-capsulation of Data from Network Delivery

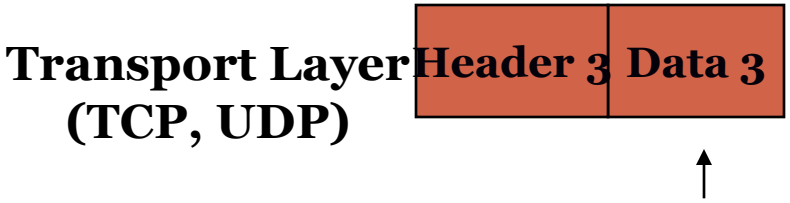


De-capsulation of Data from Network Delivery

Network Layer (IP)

Data 2

De-capsulation of Data from Network Delivery



De-capsulation of Data from Network Delivery

Transport Layer
(TCP, UDP)

Data 3

De-capsulation of Data from Network Delivery

IP SECURITY

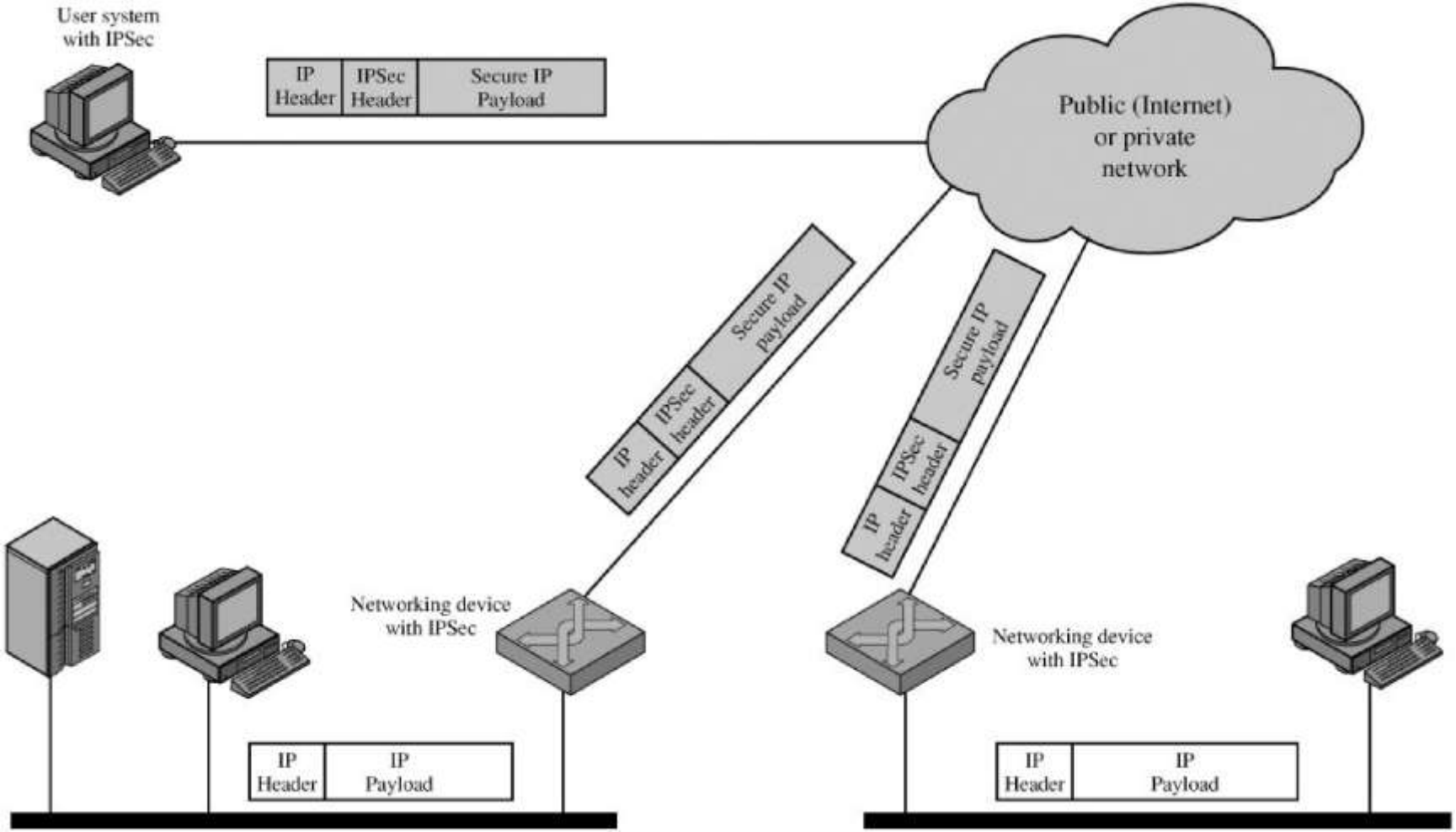
IP-level security encompasses three functional areas:

- Authentication
- Confidentiality
- Key management

IP SECURITY

- Authentication- The authentication mechanism ensures that the received packet was sent by the identified source. It also assures that the packet has not been altered in transit.
- Confidentiality- The confidentiality facility enables communicating nodes to encrypt messages to prevent eavesdopping by third parties.
- Key management- It is concerned with secure exchange of keys

IP Security Scenario



Applications of IP Security

- Secure branch office connectivity over the Internet.
- Secure remote access over the Internet.
- Establishing extranet and intranet connectivity with partners.
- Enhancing electronic commerce security.

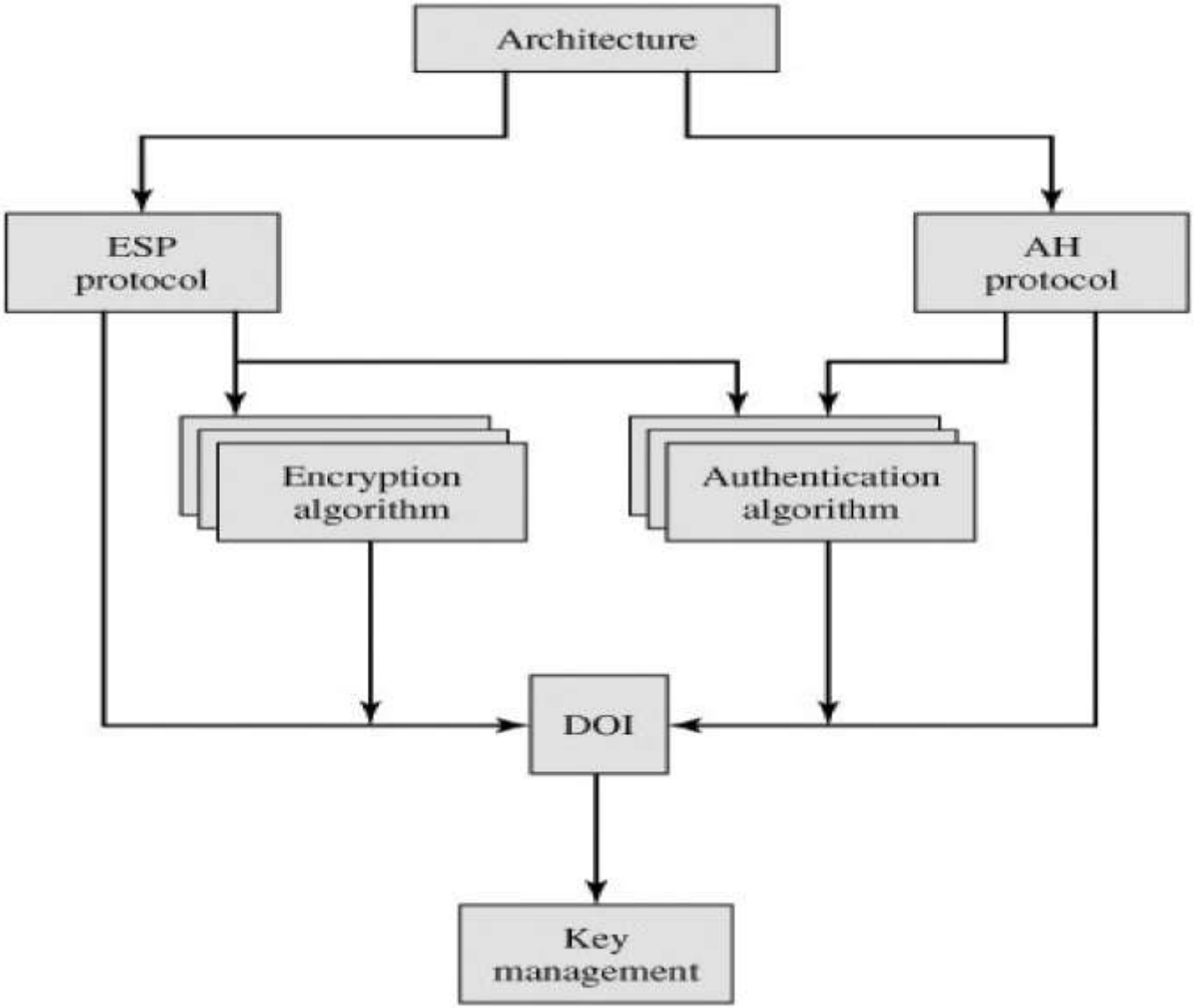
Benefits of IPsec

- Provides strong security when implemented in a firewall or router that can be applied to all traffic crossing the perimeter.
- IPsec is resistant to bypass if all traffic from the outside must use IP and the firewall is the only way of entrance from the Internet into the organization.
- Is below transport layer, hence transparent to applications.
- Can be transparent to end users.
- Can provide security for individual users if needed.

IPsec Documents

- Architecture – Covers the general concept security requirements, definitions, and mechanisms defining IPsec technology.
- Authentication Header(AH)- An extension header to provide message authentication. Current specification is RFC 4302.
- Encapsulating Security Payload- Consists of an encapsulating header and trailer used to provide encryption or combined encryption/authentication. Current specification is RFC 4303.
- Internet Key Exchange(IKE)- A collection of documents describing the key management schemes for use with IPsec.
- Cryptographic algorithms- Includes a large set of documents that define and describe cryptographic algorithms for encryption, message authentication, pseudo random functions, and cryptographic key exchange.
- Domain of Interpretation- Contains values needed for the other documents to relate to each other. These include identifiers for approved encryption and authentication algorithms, as well as operational parameters such as key lifetime

IPSec Document Overview



IPSec Security Services

- Connectionless integrity

  Assurance that received traffic has not been modified. Integrity includes anti-reply defenses.

- Data origin authentication

  Assurance that traffic is sent by legitimate party or parties.

- Confidentiality (encryption)

  Assurance that user's traffic is not examined by non-authorized parties.

- Access control

  Prevention of unauthorized use of a resource.

- Limited traffic flow confidentiality

Security Associations

- A one-way relationship between a sender and a receiver that affords security services to the traffic carried on it.

A security association is uniquely identified by three parameters:

- **Security Parameters Index (SPI):** A bit string assigned to this SA and having local significance only. The SPI is carried in AH and ESP headers to enable the receiving system to select the SA under which a received packet will be processed.
- **IP Destination Address:** Currently, only unicast addresses are allowed; 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 indicates whether the association is an AH or ESP security association

Security Association Parameters

Security Association Database defines the parameters associated with each SA. A security association is normally defined by the following parameters:

- **Sequence Number Counter:** A 32-bit value used to generate the Sequence Number field in AH or ESP headers.
- **Sequence Counter Overflow**: A flag indicating whether overflow of the Sequence Number Counter should generate an auditable event and prevent further transmission of packets on this SA (required for all implementations).
- **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 (required for AH implementations).

Security Association Parameters

- **ESP Information**: Encryption and authentication algorithm, keys, initialization values, key lifetimes, and related parameters being used with ESP (required for ESP implementations).

- **Lifetime of This Security Association:** 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 (required for all implementations).
- **IPSec Protocol Mode:** Tunnel, transport, or wildcard (required for all implementations).
- **Path MTU:** Any observed path maximum transmission unit (maximum size of a packet that can be transmitted without fragmentation) and aging variables (required for all implementations).

Security Association Selectors

The means by which IP traffic is related to specific SAs (or no SA in the case of traffic allowed to bypass IPSec) is the nominal Security Policy Database (SPD).

The following selectors determine an SPD entry:

- **Destination 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).
- **Source 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).
- **UserID**: 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.

Security Association Selectors

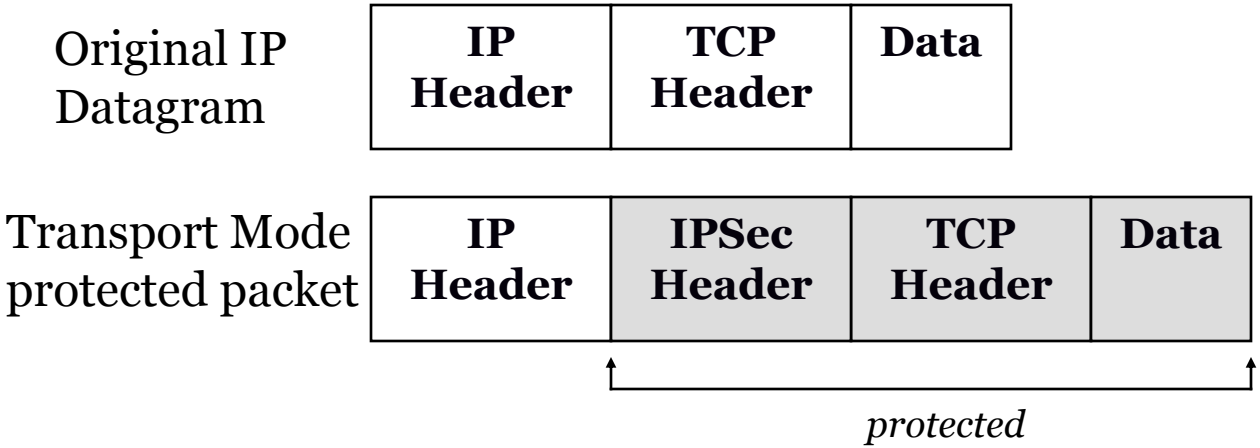
- **Data Sensitivity Level:** Used for systems providing information flow security (e.g., Secret or Unclassified).
- **Transport Layer Protocol:** Obtained from the IPv4 Protocol or IPv6 Next Header field. This may be an individual protocol number, a list of protocol numbers, or a range of protocol numbers.
- **Source and Destination Ports**: These may be individual TCP or UDP port values, an enumerated list of ports, or a wildcard port.

IPSec Modes of Operation

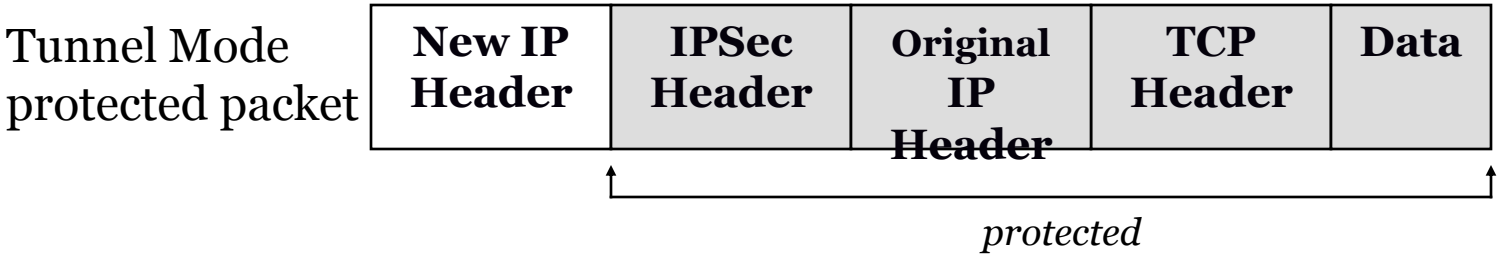
- Both AH and ESP supports two modes of use:
- Transport mode –Provides protection primarily for upper layer protocols.ESP in transport mode encrypts and optionally authenticates the IP payload but not the IP header. AH authenticates the IP payload and selected portions of the IP header.
- Tunnel mode - Provides protection to the entire IP packet. After the AH or ESP fields are added to the IP packet, the entire packet plus security fields is treated as payload of new outer packet with a new outer IP header.

IPSec Modes of Operation

- Transport Mode: protect the upper layer protocols



- Tunnel Mode: protect the entire IP payload



Transport mode vs. Tunnel mode functionalities

	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 plus selected portions of outer IP header
ESP	Encrypts IP payload and any IPv6 extesion header	Encrypts inner IP packet
ESP with authentication	Encrypts IP payload and any IPv6 extesion header. Authenticates IP payload but no IP header	Encrypts inner IP packet. Authenticates inner IP packet.

Authentication Header

- Provides support for data integrity and authentication of IP packets.
- Authentication is based on the use of a message authentication code (MAC), hence the two parties must share a secret key.

Authentication Header

The Authentication Header consists of the following fields :

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

  Sequence Number (32 bits): A monotonically increasing counter value
- **Authentication Data (variable):** A variable-length field (must be an integral number of 32-bit words) that **contains** the Integrity Check Value (ICV), or MAC

Authentication Header

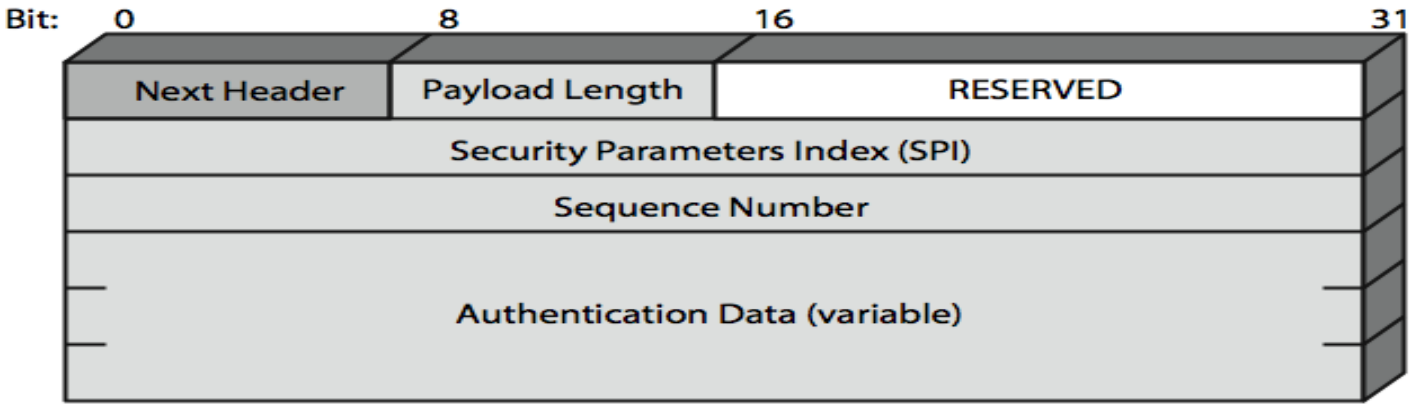


Figure 16.3 IPSec Authentication Header

Encapsulating Security Payload (ESP)

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

Encapsulating Security Payload

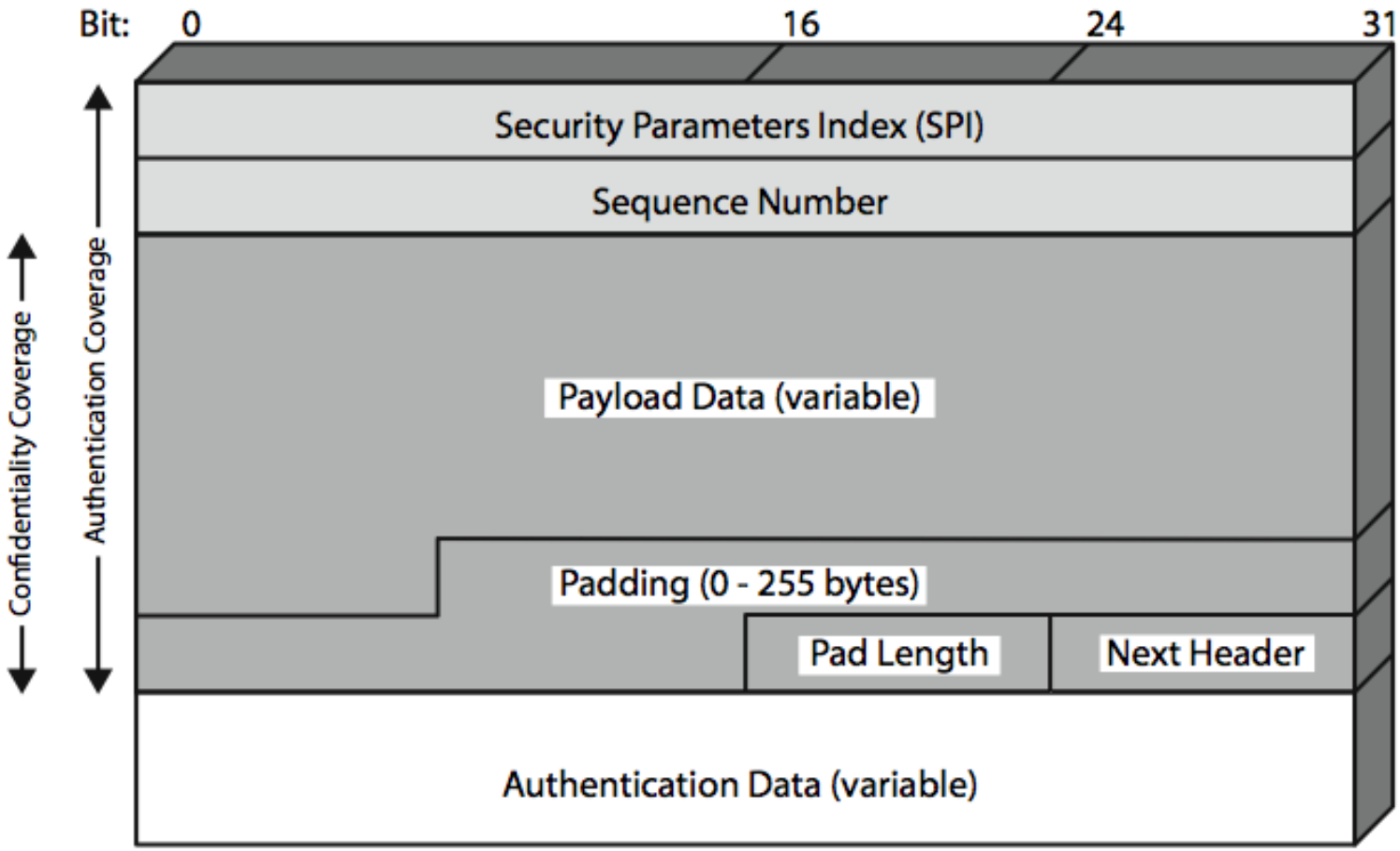


Fig-1. ESP Format

Encapsulating Security Payload

- **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):** for various reasons
- **Pad Length (8 bits):** Indicates the number of pad bytes immediately preceding this field
- **Next Header (8 bits):** Identifies the type of data contained in the payload data field by identifying the first header in that payload
- **Integrity Check Value (variable):** A variable-length field that contains the Integrity Check Value computed over the ESP packet minus the Authentication Data field

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 0.**
- 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

with a default of $W = 64$

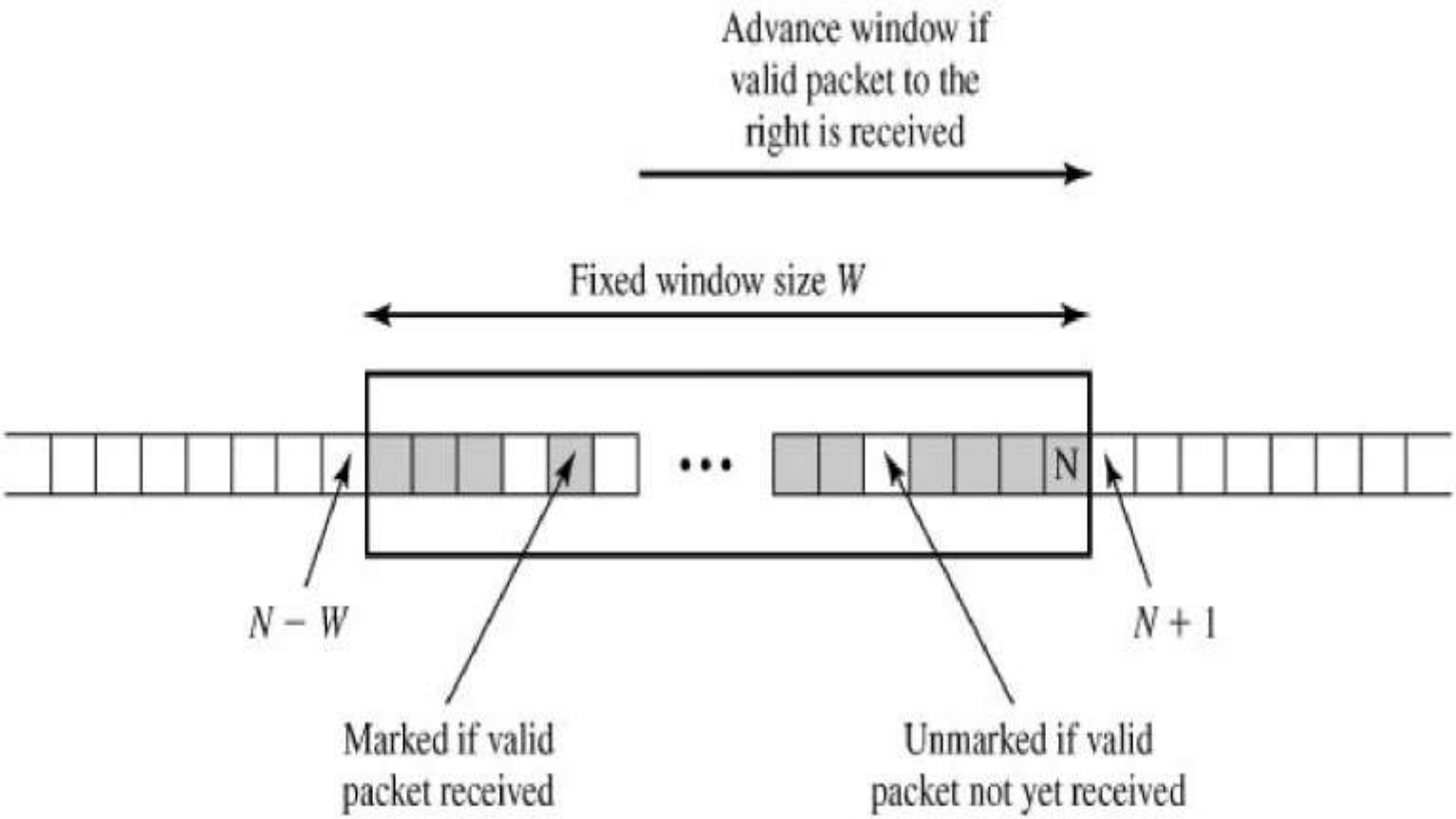


Fig-2. Antireplay Mechanism

Transport vs Tunnel Mode ESP

- transport mode is used to encrypt & optionally authenticate IP data
  - data protected but header left in clear
  - can do traffic analysis but is efficient
  - good for ESP host to host traffic
- tunnel mode encrypts entire IP packet
  - add new header for next hop
  - good for VPNs, gateway to gateway security

Transport vs Tunnel Mode ESP

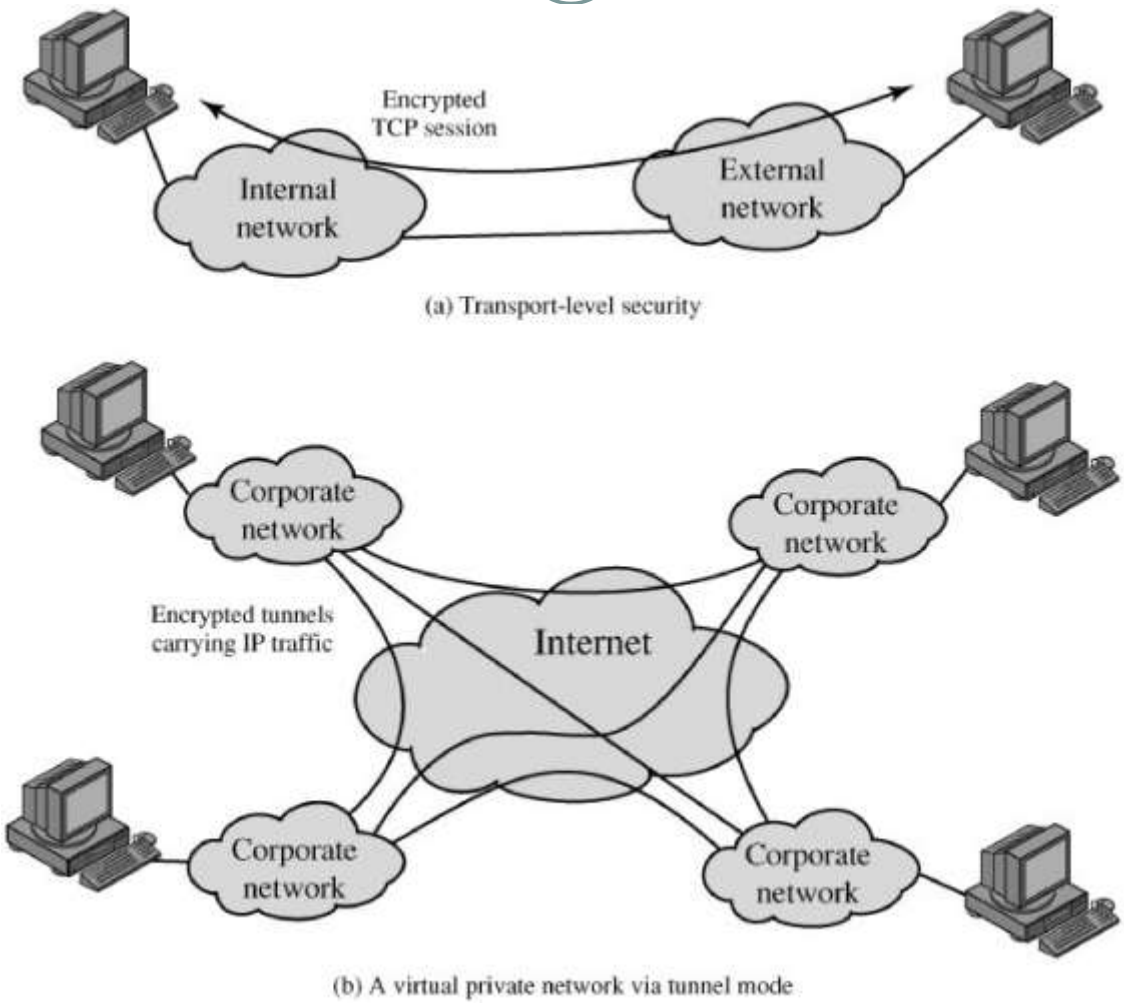


Fig-3. Transport-Mode vs. Tunnel-Mode Encryption

Transport vs Tunnel Mode ESP

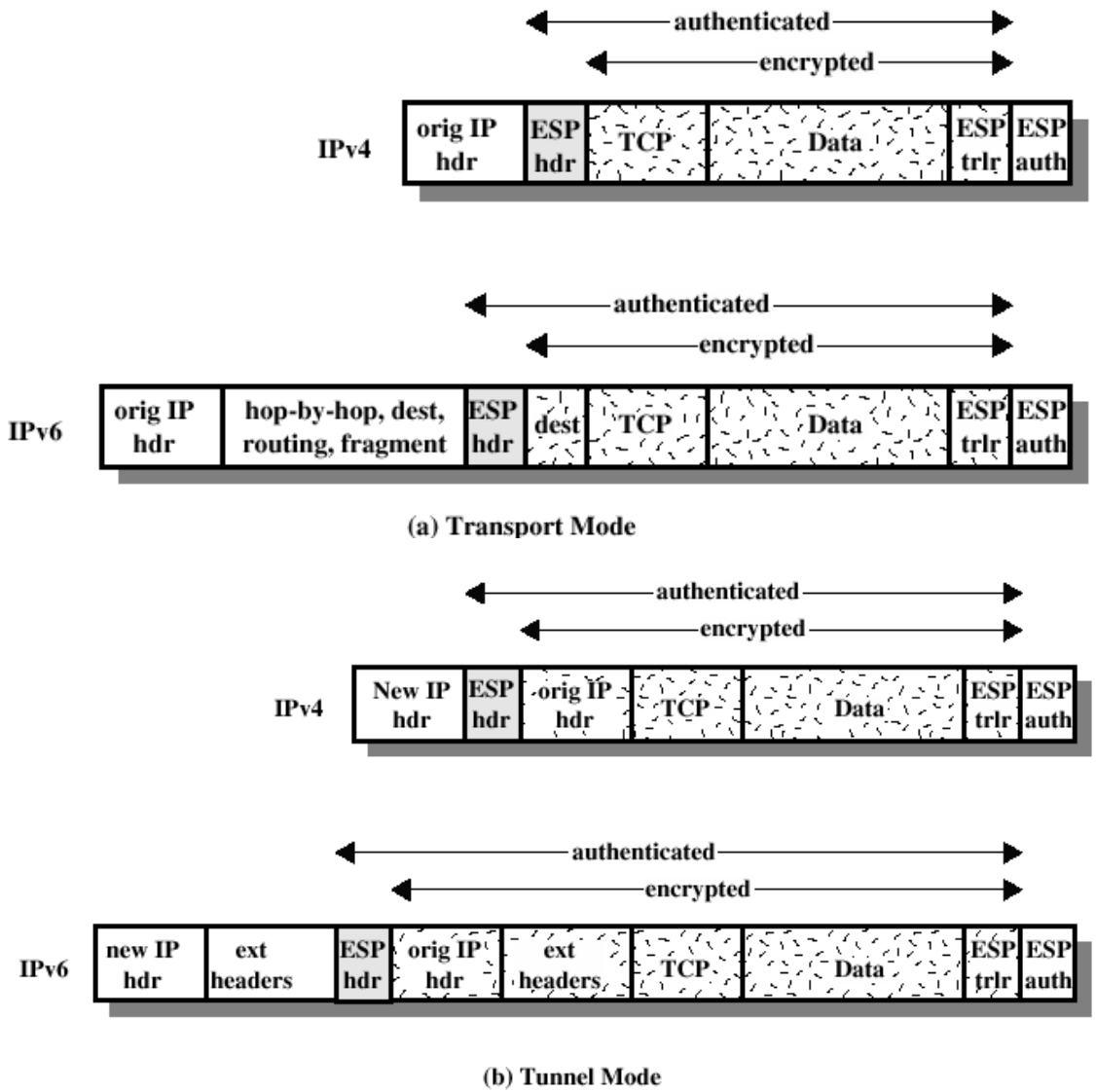


Fig-4. Scope of ESP Encryption and Authentication

Combining Security Associations

- SA's can implement either AH or ESP
- to implement both need to combine SA's
  - form a security association bundle
  - may terminate at different or same endpoints
  - combined by
    - transport adjacency
    - iterated tunneling
- issue of authentication & encryption order

Authentication Plus Confidentiality

Transmitting IP packet that has both confidentiality and authentication between hosts

1) **ESP with Authentication Option:** Authentication after encryption using Transport mode ESP or Tunnel mode ESP.
2) **Transport Adjacency:** Another way to apply Authentication after encryption

- Use two bundled transport SAs, with the inner being an ESP SA and the outer being an AH SA.
- Here ESP is used without authentication option.

Advantage: Authentication covers more fields, including the source and destination IP addresses.

Disadvantage: Overhead of two SAs vs one SA.

3) **Transport-Tunnel Bundle:** Authentication before encryption

- Use a bundle consisting of an inner AH transport SA and an outer ESP tunnel SA.

Advantages:

a) Impossible to intercept the message and alter the authentication data without detection.
b) Authentication information with the message may be stored at the destination for later references.

Basic Combinations of Security Associations

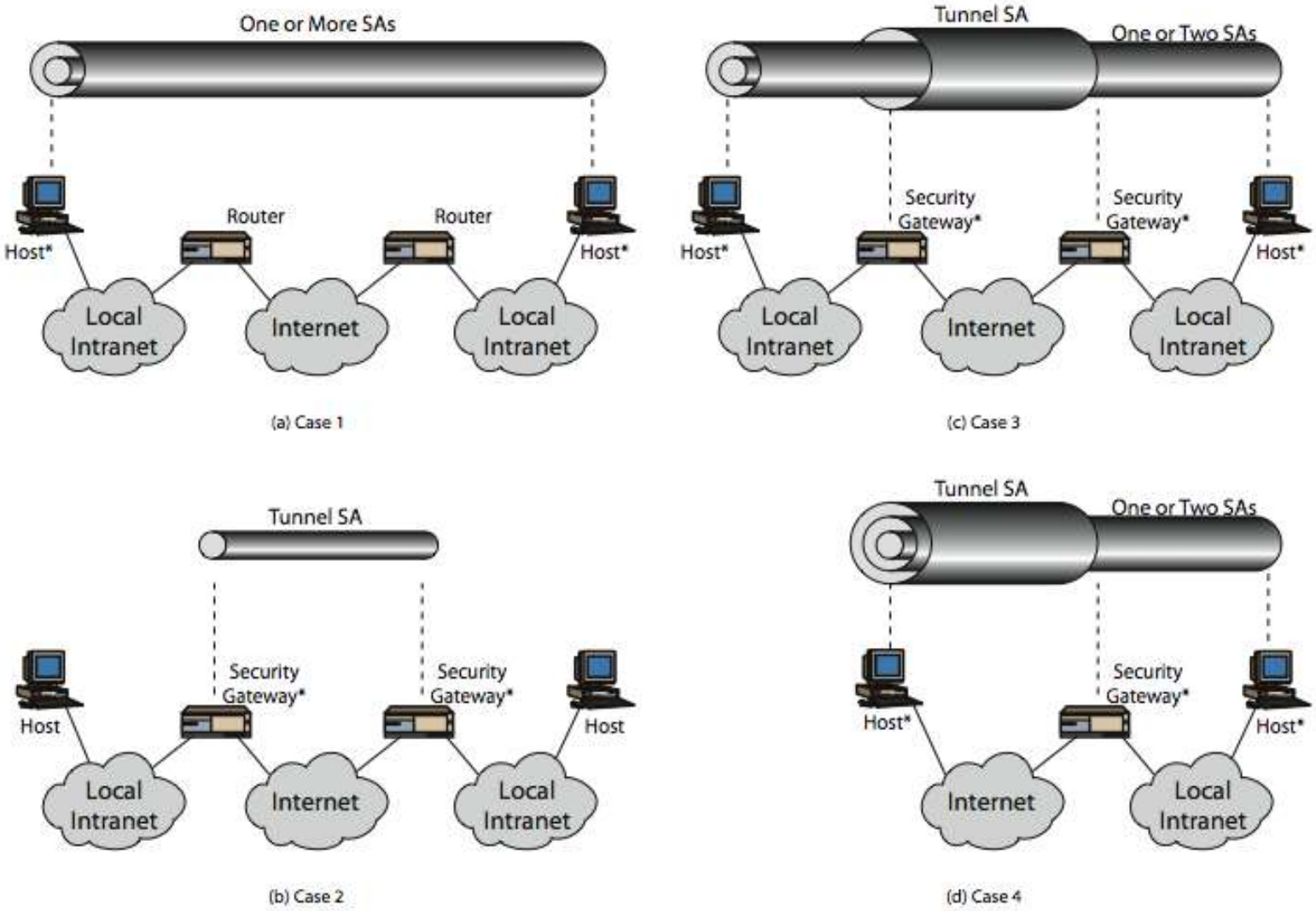


Fig-5. Basic Combinations of Security Associations

Key Management

- handles key generation & distribution
- typically need 2 pairs of keys
  - 2 per direction for AH & ESP
- manual key management
  - System administrator manually configures every system
- automated key management
  - automated system for on demand creation of keys for SA's in large systems
  - has Oakley & ISAKMP elements

References

Cryptography and Network Security Principles and Practices, 4th Ed - William Stallings

THANK YOU