# Information Security

CS3002

Lecture 20

7th November 2023

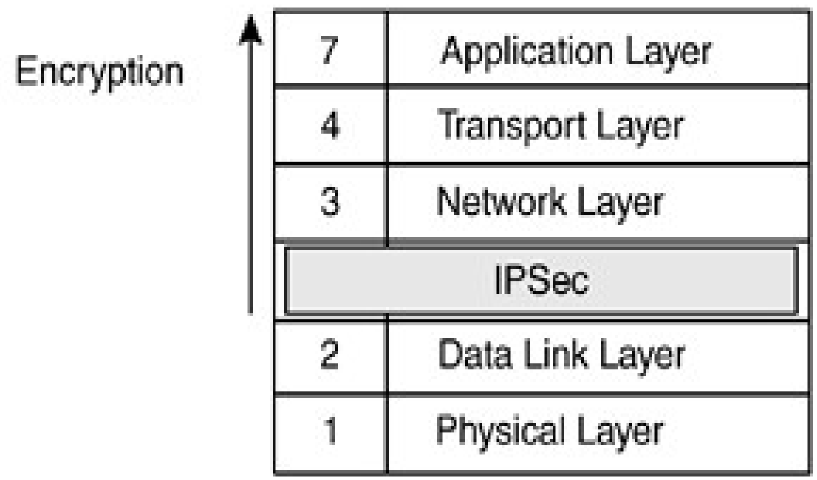
Dr. Rana Asif Rehman

Email: r.asif@lhr.nu.edu.pk

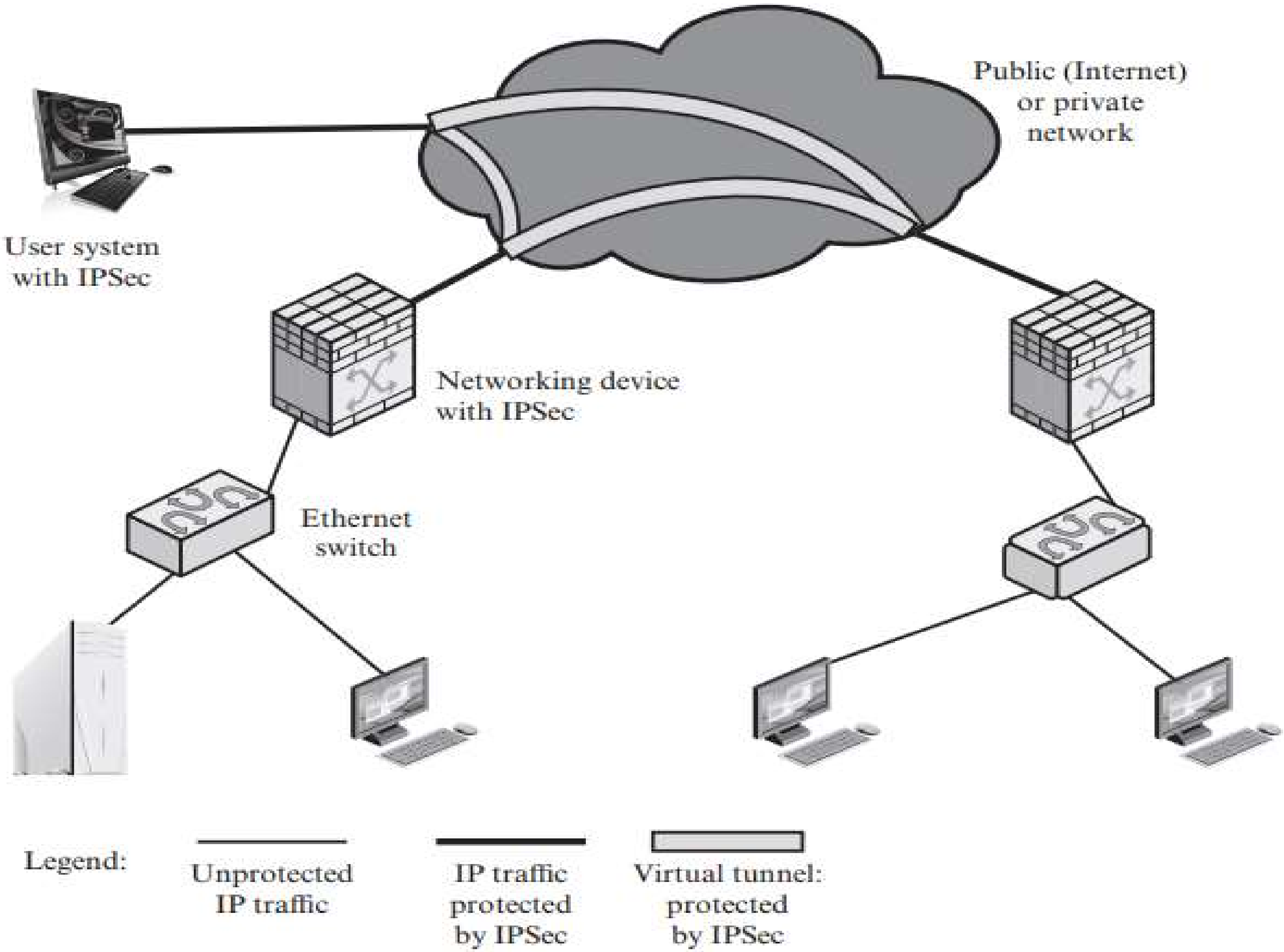
# IP Security (IPsec)

# IPsec

- Philosophy of IPsec: implementing security within the operating systems automatically causes applications to be protected without changing applications
- IPsec is within the OS. OS changes, applications and API to TCP don't.



# An IPsec VPN Scenario



# IPsec

- Security at layer 3
- IPsec ensures:
  - Confidentiality, integrity, and authenticity
- Allows secure communication in the Internet
- Independent from the application or higher protocols
- Network-layer security instead of application-layer security
  - Compatible with schemes providing security at the application layer
    - Can be applied simultaneously

# IPsec

- Further advantages:
  - Can be applied to all network traffic
  - Routers/firewalls vendors can implement it (Can't implement SSL)
  - Transparent to the applications
  - Transparent to the users

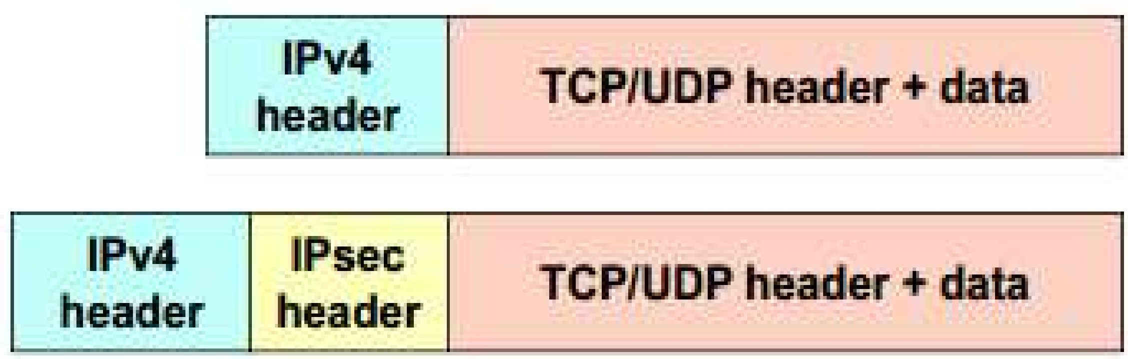
- Limitations:
  - Limited to IP Addresses
  - Has no concept of application users

# IPsec

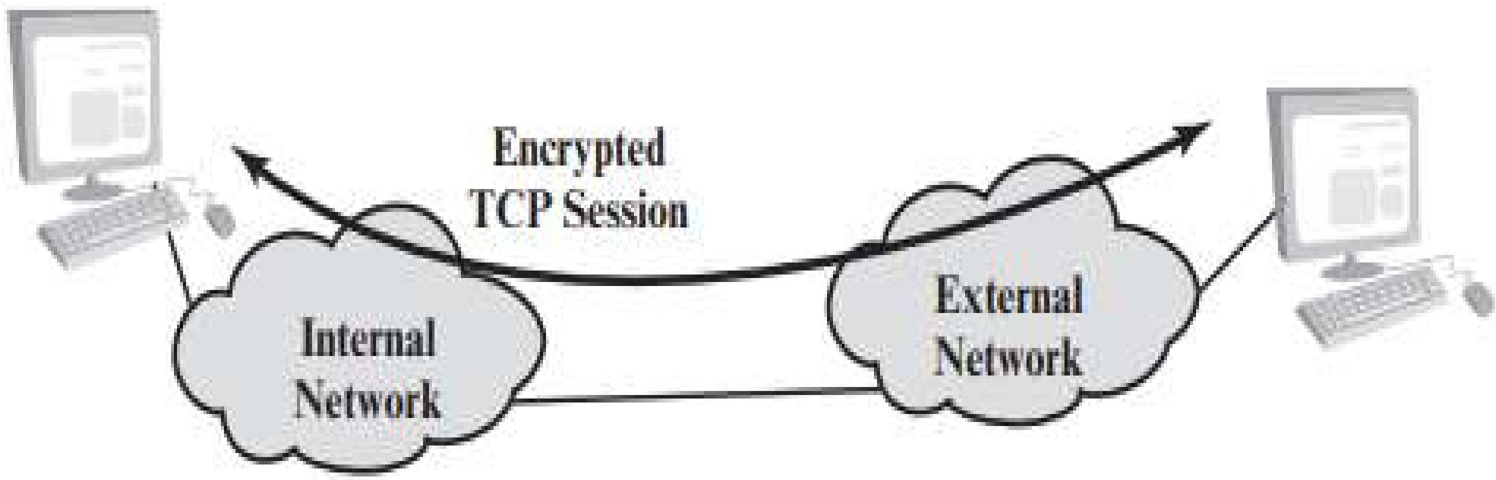
- Two Modes
  - Transport Mode
  - Tunnel Mode

# 1. Transport Mode

- Used for end-to-end security, that is used by hosts, not gateways (exception: traffic for the gateway itself e.g: SNMP, ICMP)
- Pro: computationally light
- Con: no protection of header variable fields



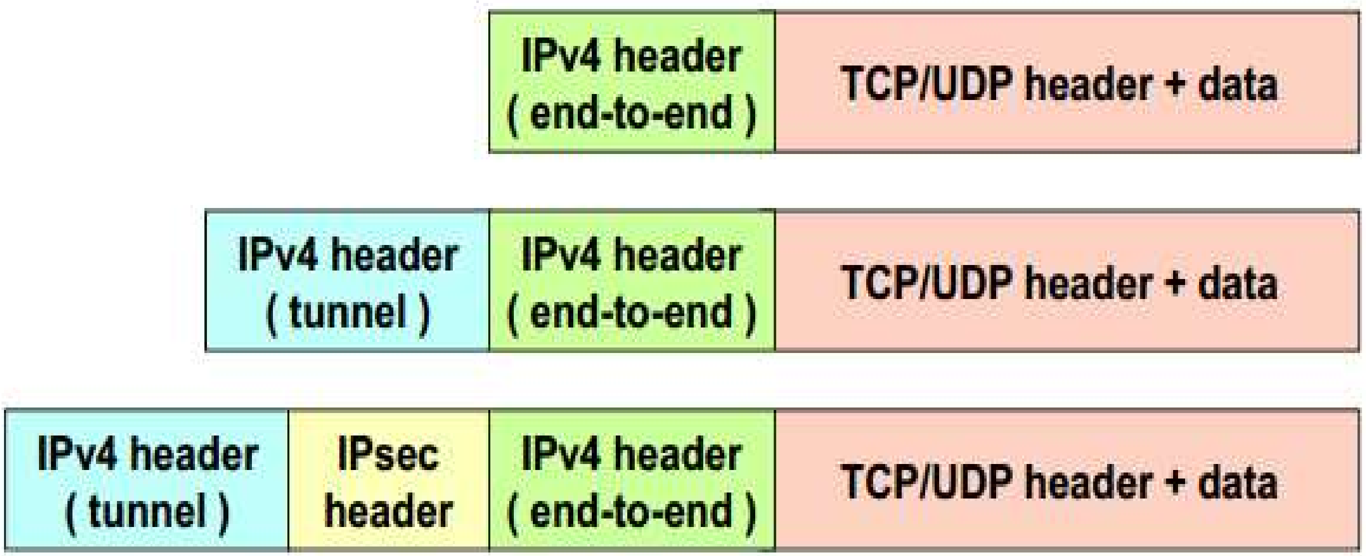
# Transport Mode



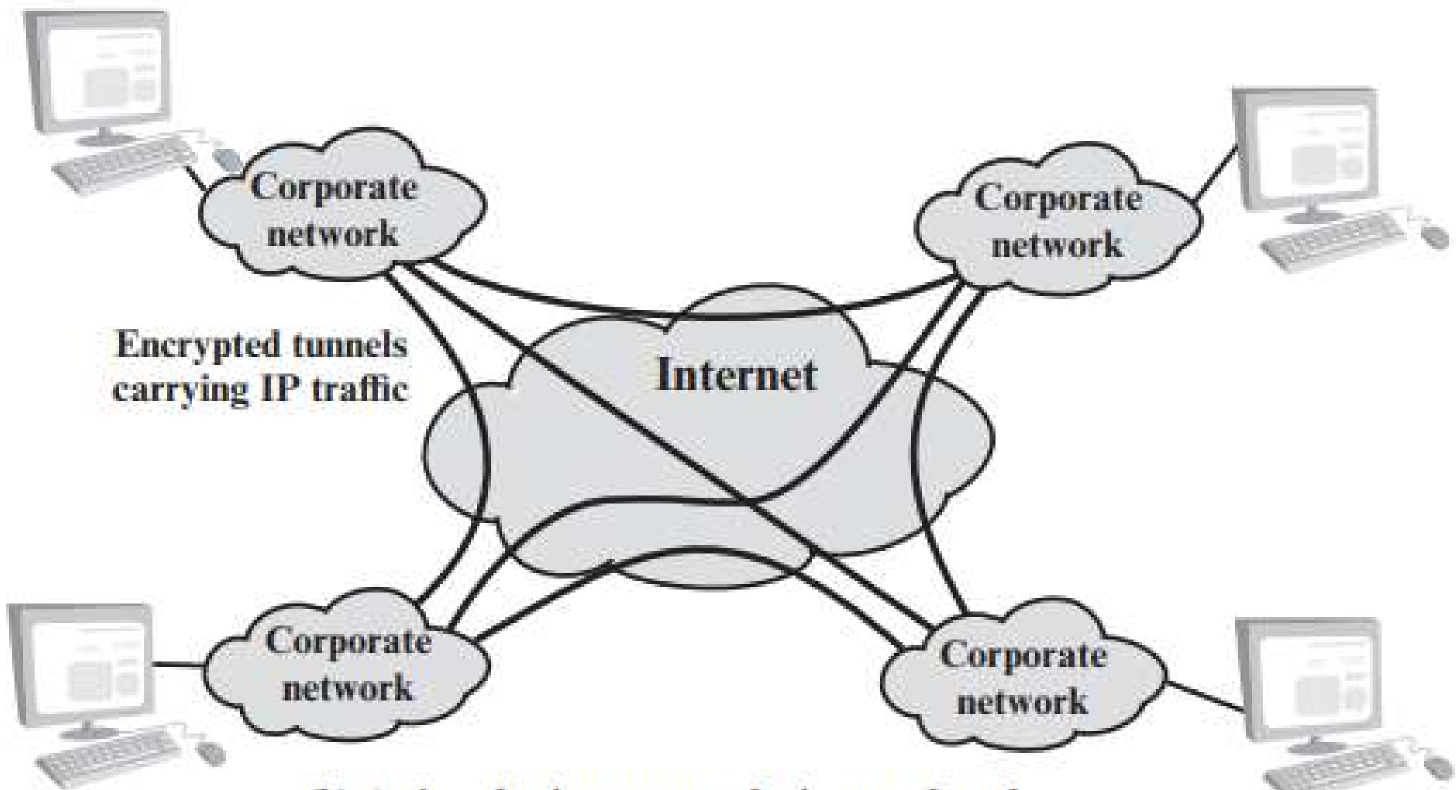

(a) Transport-level security

# 2. Tunnel Mode

- Used to create a VPN, usually by gateways
- Gateway-to-gateway mode
- Pro: protection of header variable fields
- Con: computationally heavy



# Tunnel Mode




(b) A virtual private network via tunnel mode

# Applications of IPsec

- Secure connection among different branches of the same company
  - Virtual Private Network (VPN)
- Secure remote access to an Intranet through the (insecure) Internet
  - Allows secure remote workers
- Secure communication between peers
- Adding security for electronic commerce applications

# IPsec Overview

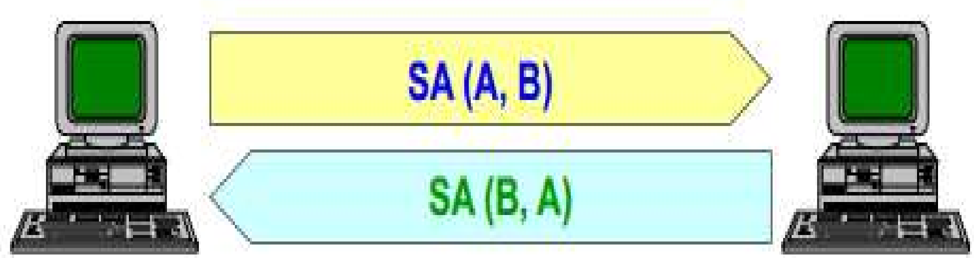
- IETF architecture for L3 security in IPv4 / IPv6:

- Definition of two specific packet types:
  - AH (Authentication Header)
    - for integrity, authentication, no replay
  - ESP (Encapsulating Security Payload)
    - for confidentiality, integrity, authentication, no replay

- Protocol for key exchange:
  - IKE (Internet Key Exchange)

# Security Association (SA)

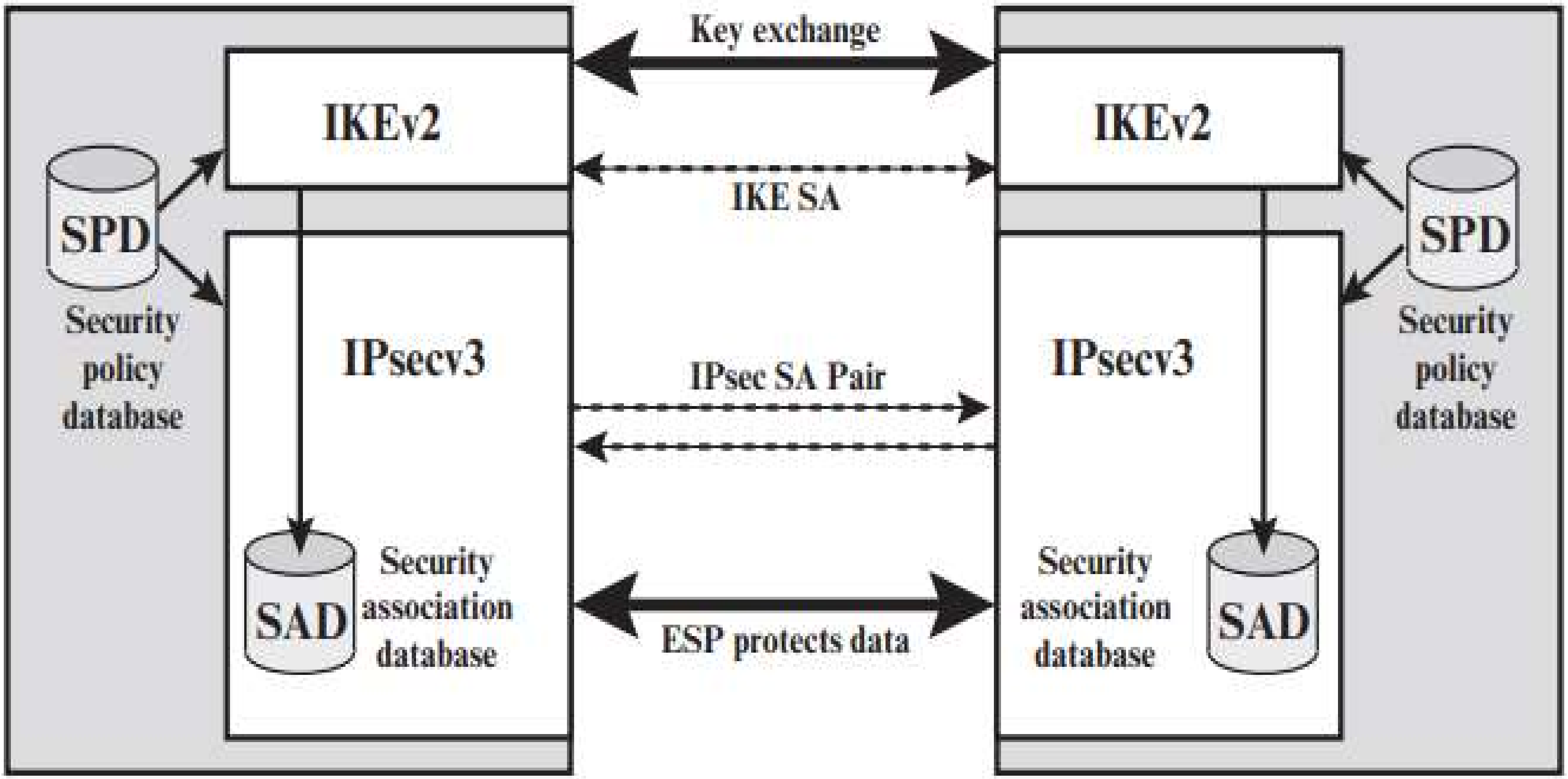
- Establishment of shared security attributes between sender and receiver to support secure communication
- Usually considered unidirectional
- Contain all the information required for execution of various network security services
- Three SA identification parameters
  - Security parameter index (SPI)
  - IP destination address
  - Security protocol identifier
- Two SA are needed to get complete protection of a bidirectional packet flow in IPsec



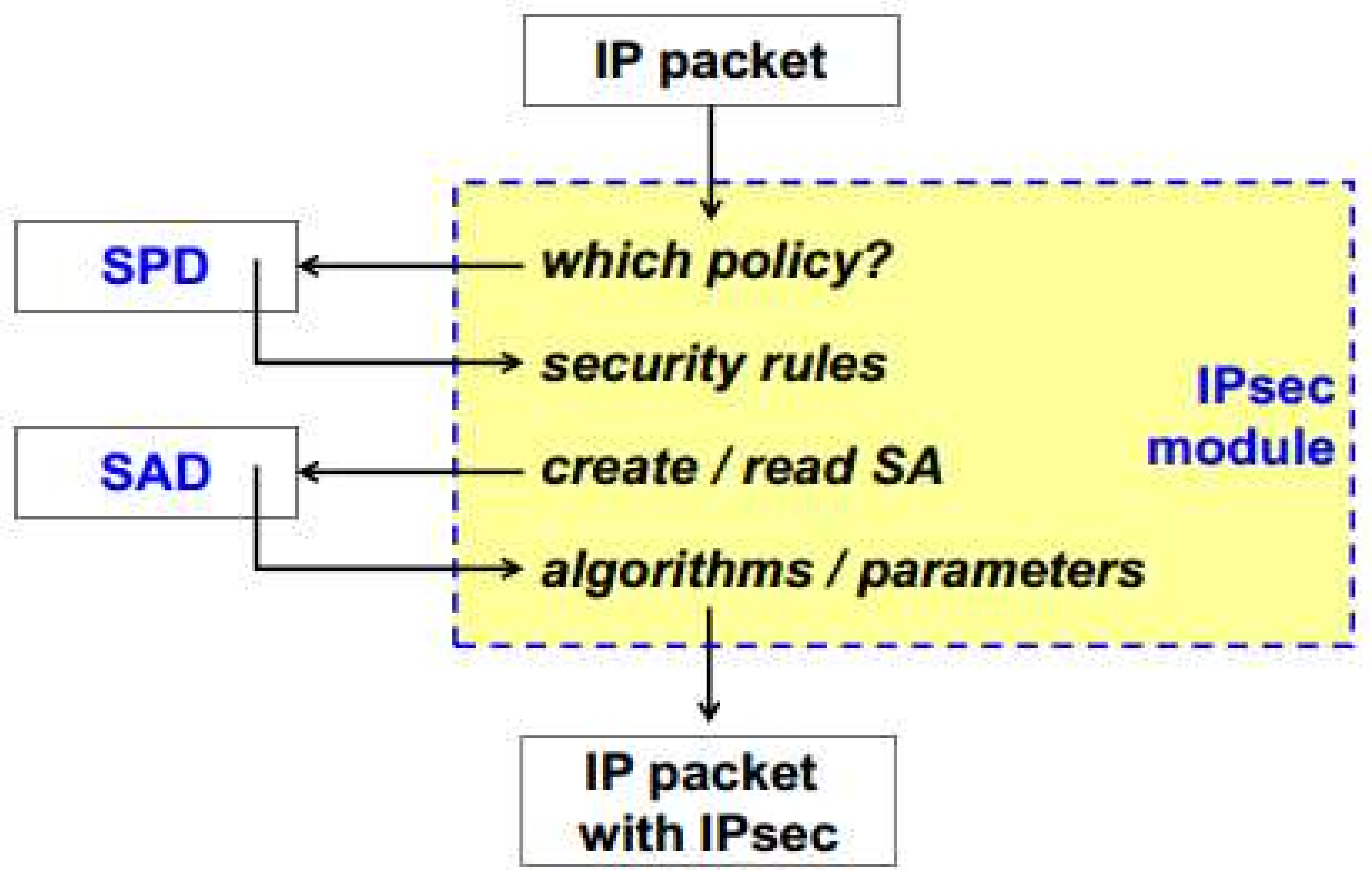
# IPsec Local Databases

- SAD (SA Database)
  - list of active SA and their characteristics (algorithms, keys, parameters)
  - maintained by user-processes
- SPD (Security Policy Database)
  - list of security policies to apply to the different packet flows
  - a-priori configured (e.g. manually) or connected to an automatic system (e.g. ISPS, Internet Security Policy System)

# IPsec Architecture



# How IPsec Works (sending)

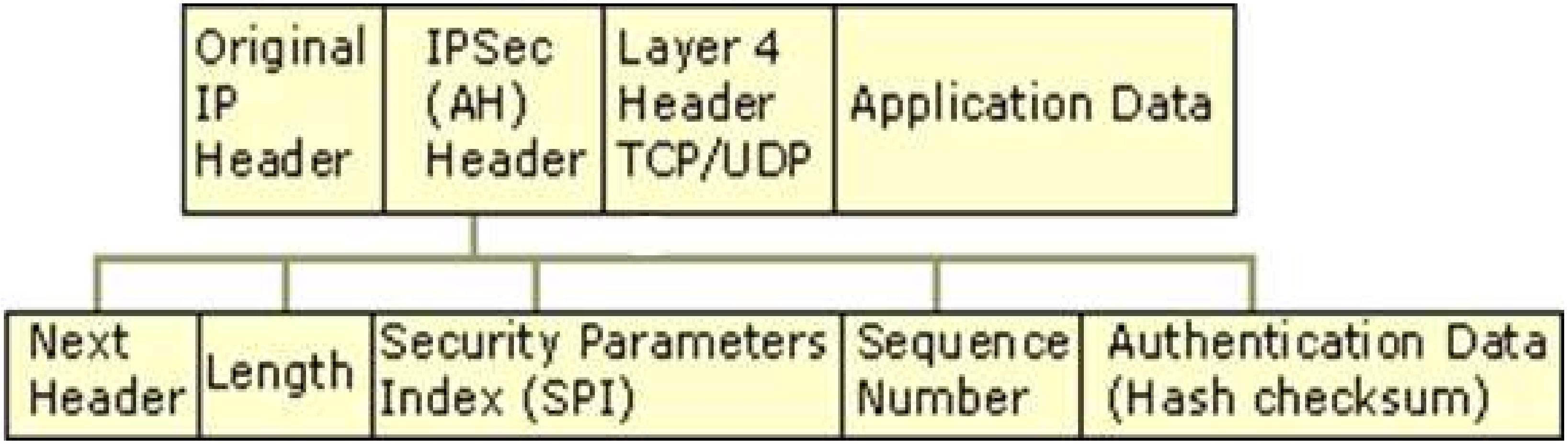


# AH

- Authentication Header
- Mechanism (first version, RFC-1826):
  - data integrity and sender authentication
  - compulsory support of keyed-MD5 (RFC-1828)
  - optional support of keyed-SHA-1 (RFC-1852)

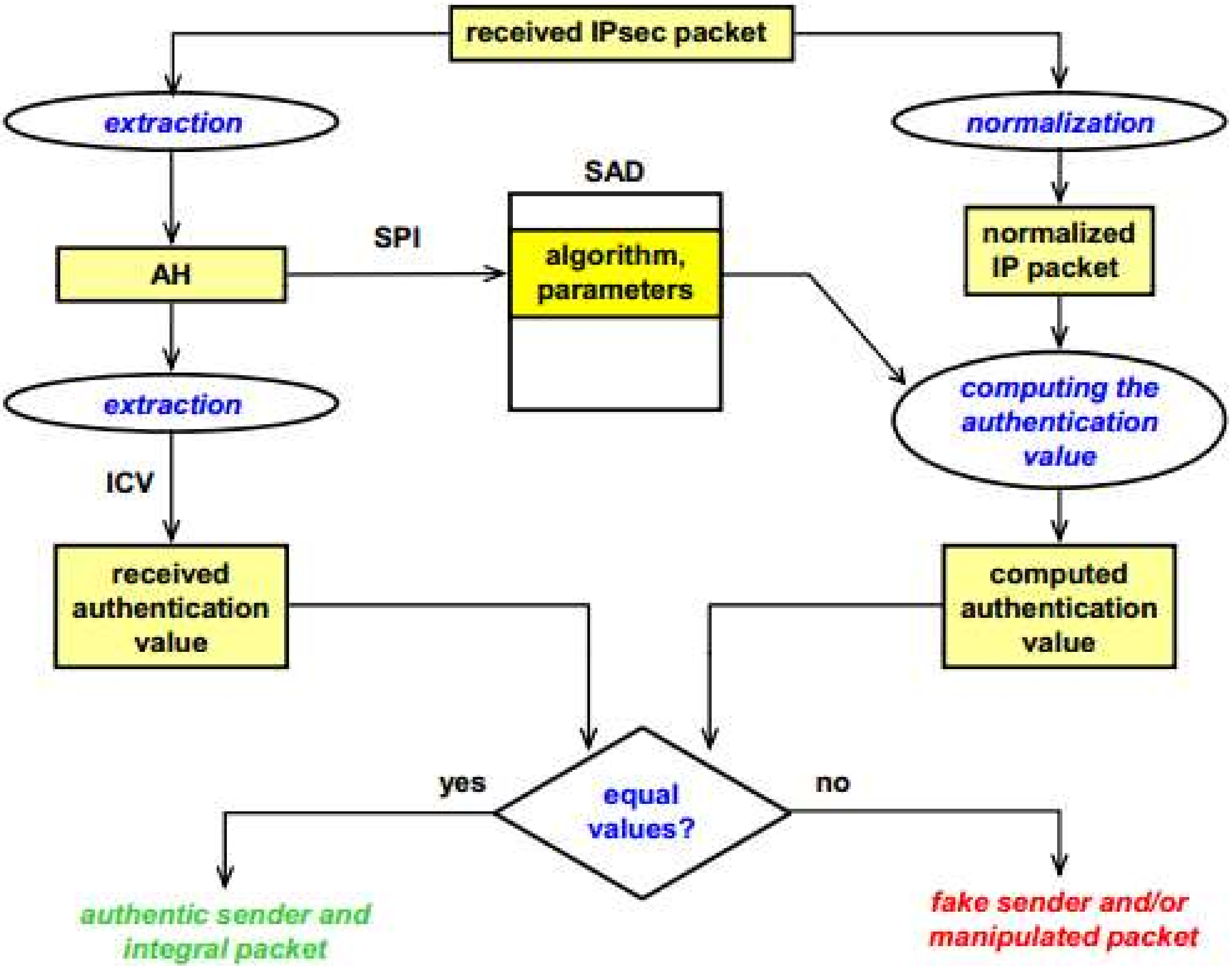
- Mechanism (second version, RFC-2402):
  - data integrity, sender authentication and protection from replay attack
  - HMAC-MD5
  - HMAC-SHA-1

# AH Packet



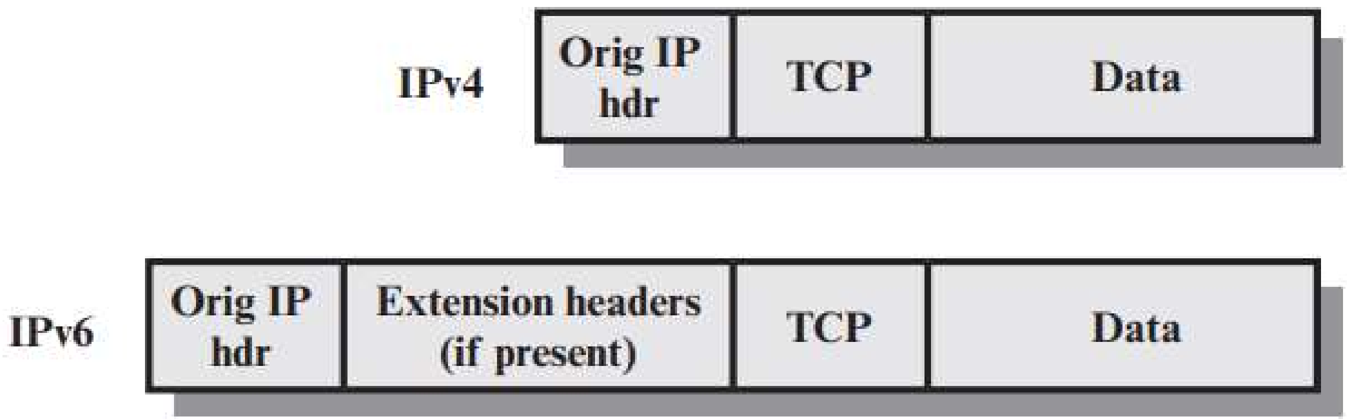

- Next header: identifies the nature of the payload (TCP/UDP)
- Length: Indicates the length of the AH header
- SPI: Identifies the correct security association for the communication
- Sequence Number: Provides anti-replay protection for the SA
- Auth. Data: contains the Integrity Check Value (ICV) that is used to verify the integrity of the message. The receiver calculates the hash value and checks it against this value (calculated by the sender) to verify integrity.

# AH Verification



# ESP

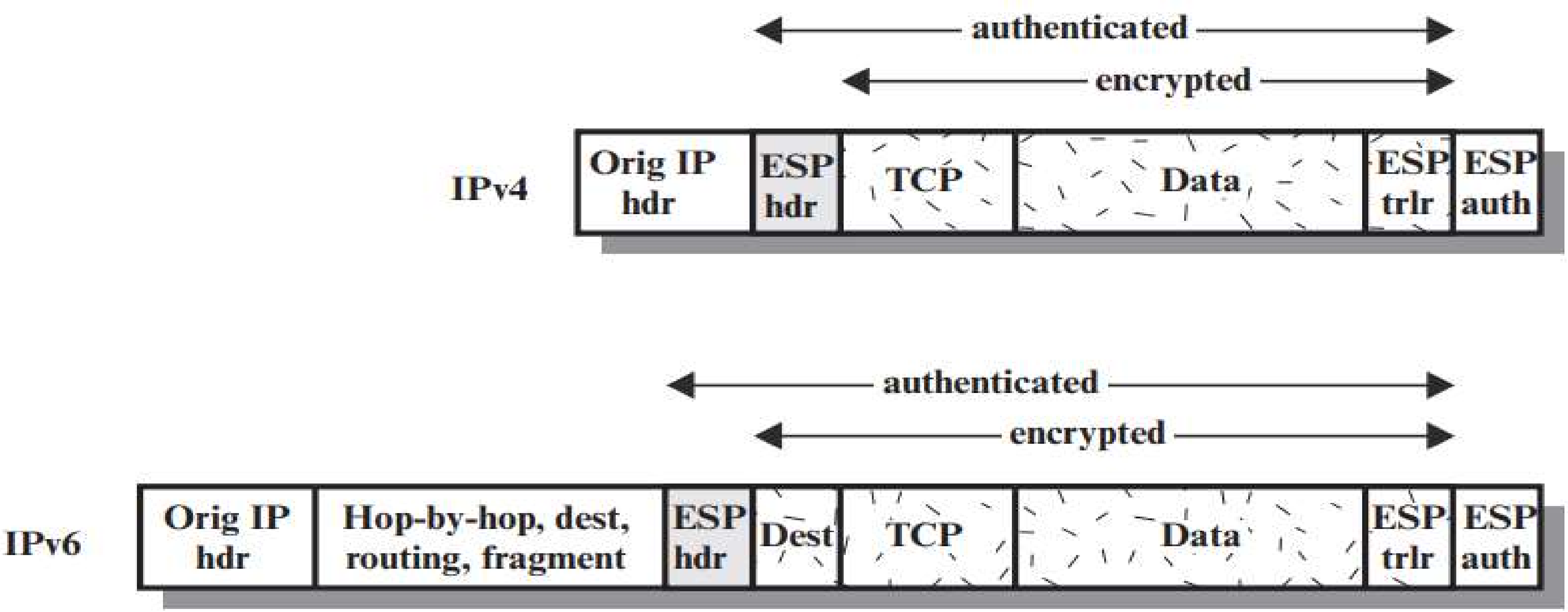
- Encapsulating Security Payload (ESP)
- First version (RFC-1827) gave only confidentiality
  - base mechanism: DES-CBC (RFC-1829)
- Second version (RFC-2406):
  - provides confidentiality & authentication (but not the IP header, so the coverage is not equivalent to that of AH)




(a) Before Applying ESP

# ESP in Transport Mode

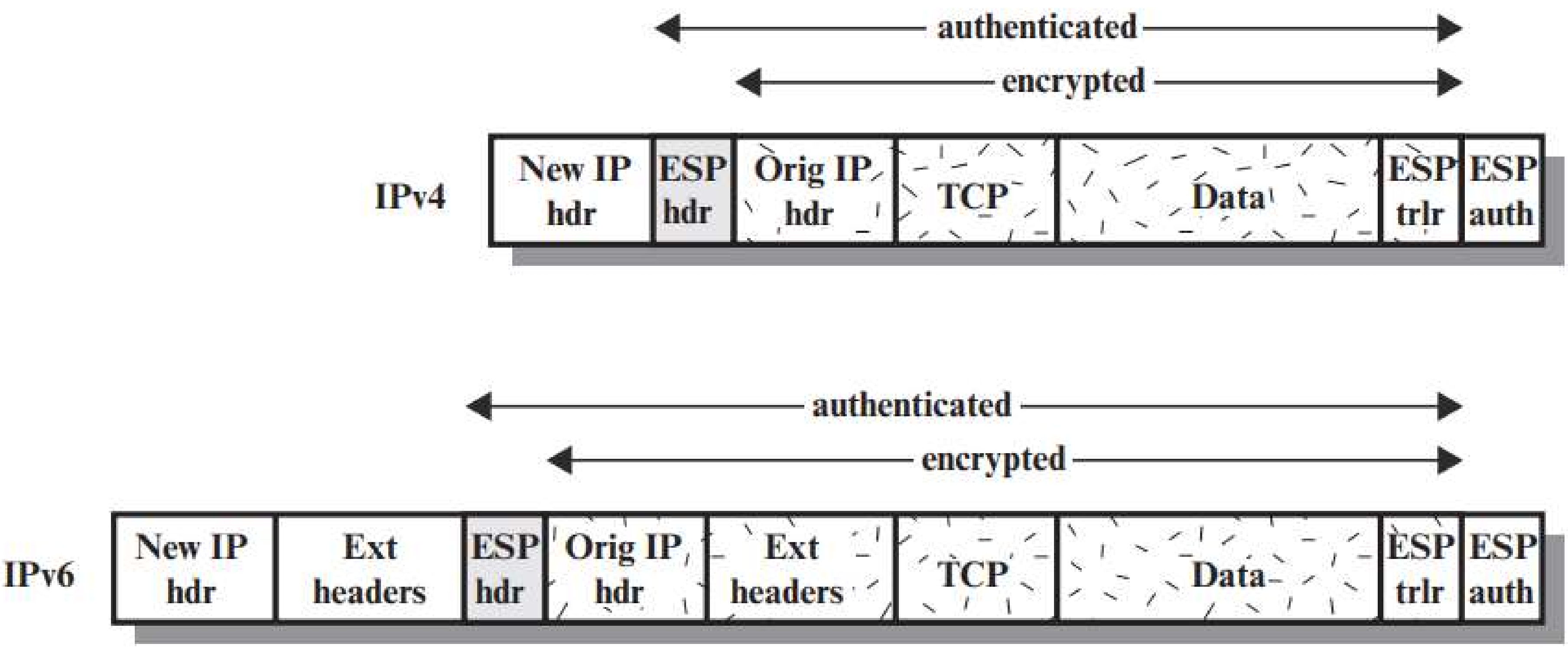
- Pro: the payload is hidden (including info needed for QoS or intrusion detection)
- Con: the header remains in clear




(b) Transport Mode

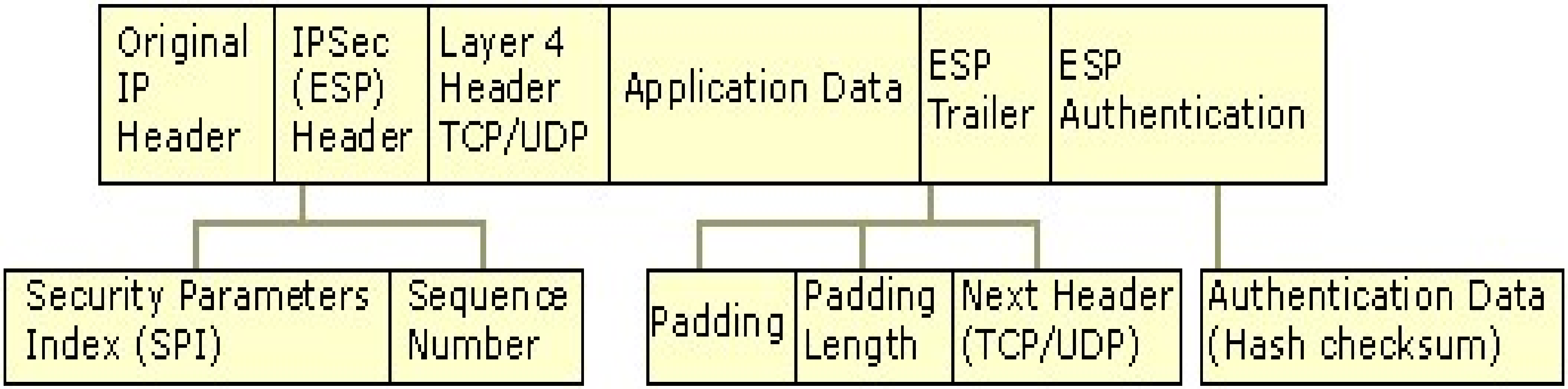
# ESP Tunnel Mode

- Pro: hides both the payload and (original) header
- Con: larger packet size




(c) Tunnel Mode

# ESP Packet




- SPI: Identifies the correct security association for the communication
- Sequence number: Provides anti-replay protection for the SA
- Next header: Identifies the nature of the payload (TCP/UDP)
- Auth. Data: Contains the Integrity Check Value (ICV), and a message authentication code that is used to verify the sender's identity and message integrity. The ICV is calculated over the ESP header, the payload data and the ESP trailer
- Initialization Vector (IV): optional. Is after the Sequence number

# ESP Packet: Encryption & Authentication