Aqsa Khalid
Lecturer
School of Computing

CS3002 Information Security

Security in TCP/IP

Source: Stallings chap 22

IPsec
Internet Protocol Security

IPsec

- Security at layer 3
- IPsec ensures:
  - confidentiality, integrity, and authenticity
- Allows secure communication on 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

- Philosophy: 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.

7	Application Layer
4	Transport Layer
3	Network Layer
IPSec	
2	Data Link Layer
1	Physical Layer

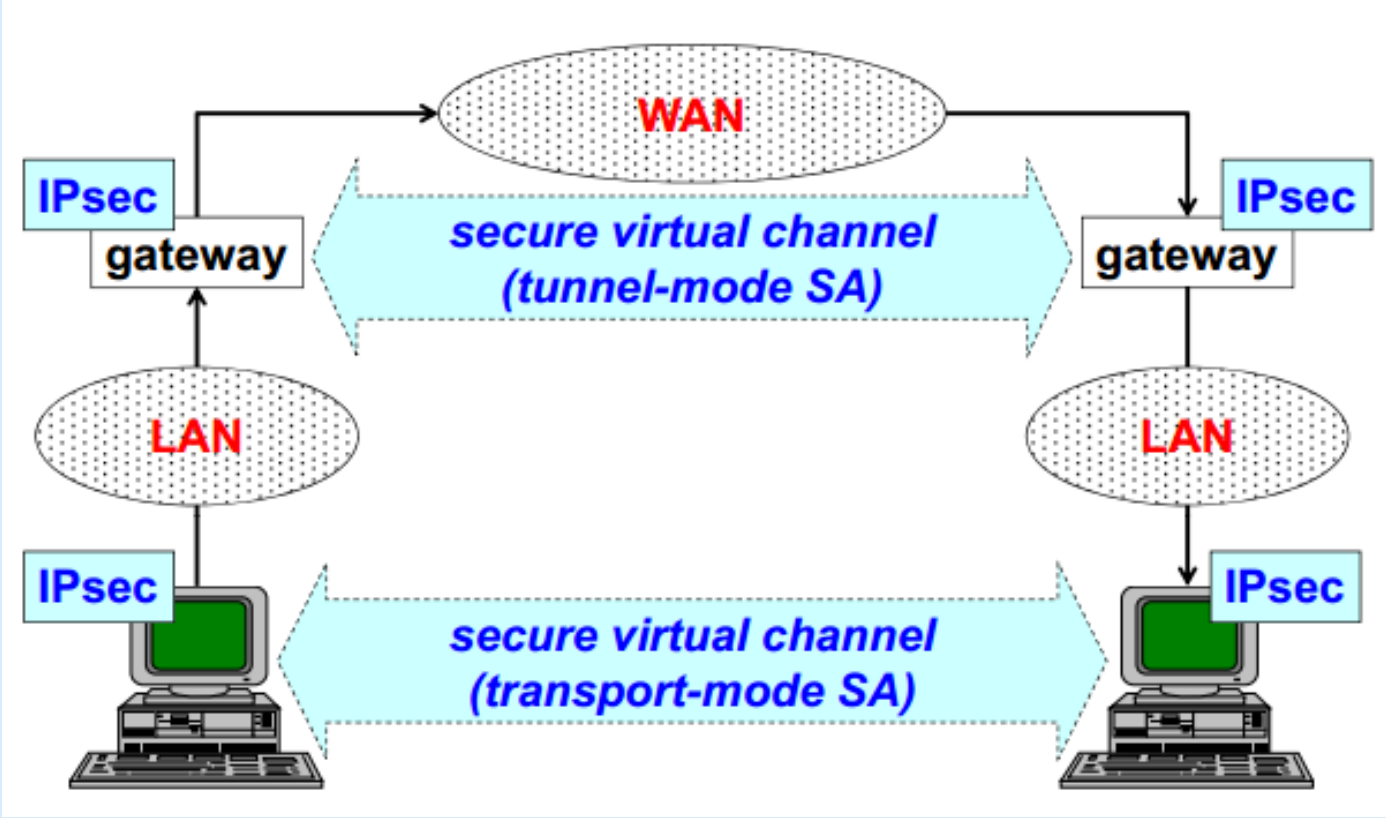
IPsec

- 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

Applications of IPsec

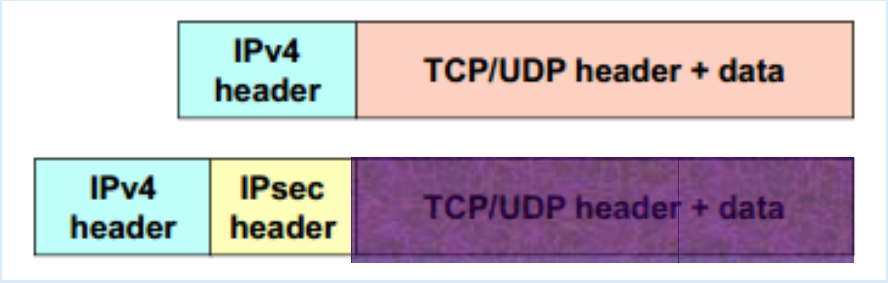
- Secure connection among different branches of the same company
  - Virtual Private Network (VPN)
- Secure remote access to an Intranet through the (insecure) Internet
  - Allows secure remote workers
- Secure communication between peers
- Adding security for electronic commerce applications

IPsec operating modes



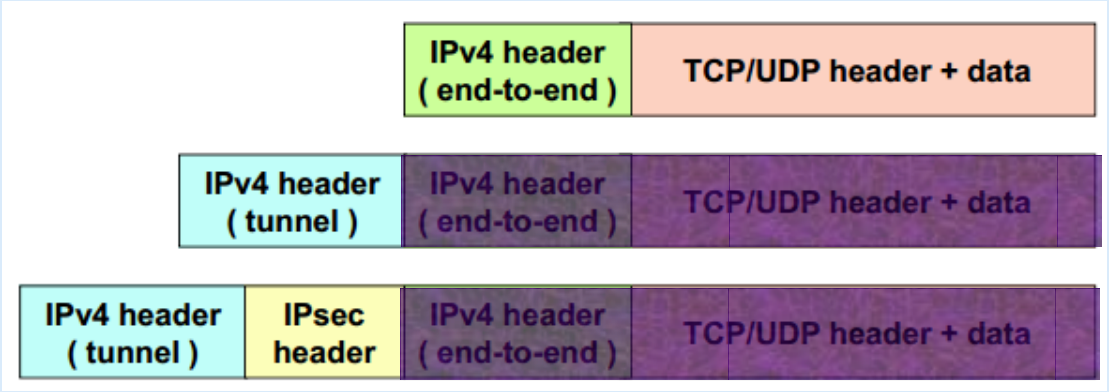
Transport mode

- 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 fields



Tunnel Mode

- used to create a VPN, usually by gateways
- Gateway-to-gateway mode
- pro: protection of header variable fields
- con: computationally heavy



IPsec Architecture

- IETF architecture for L3 security in IPv4 / IPv6:
- definition of two specific packet types:
  - AH (Authentication Header)
    - for integrity, authentication and anti-replay
  - ESP (Encapsulating Security Payload)
    - for confidentiality, integrity, authentication & anti-replay
- protocol for key exchange:
  - IKE (Internet Key Exchange)

Security Policies

Security Policies

- Rules to decide if an IP packet needs to be processed and how

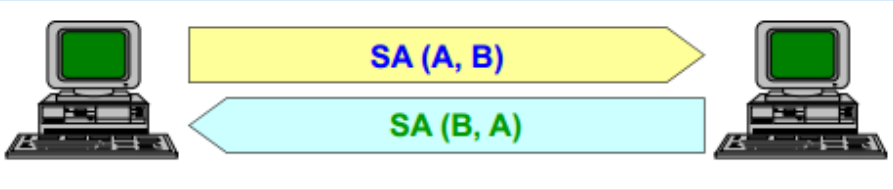
A policy defines

a) packet selection rules like source, destination, port

b) action to take (encrypt, authenticate, block)
   - e.g. authenticate all outbound TCP packets from database server (say 192.168.5.1) going to port 5500
   - encrypt all traffic going to remote gateway (say 170.34.12.6)

Security Associations

- A contract between two peers on security parameters (like keys, cipher algorithms, key expiry)
- Separate associations in each direction
  - two SA are needed to get complete protection of a bidirectional packet flow in IPsec

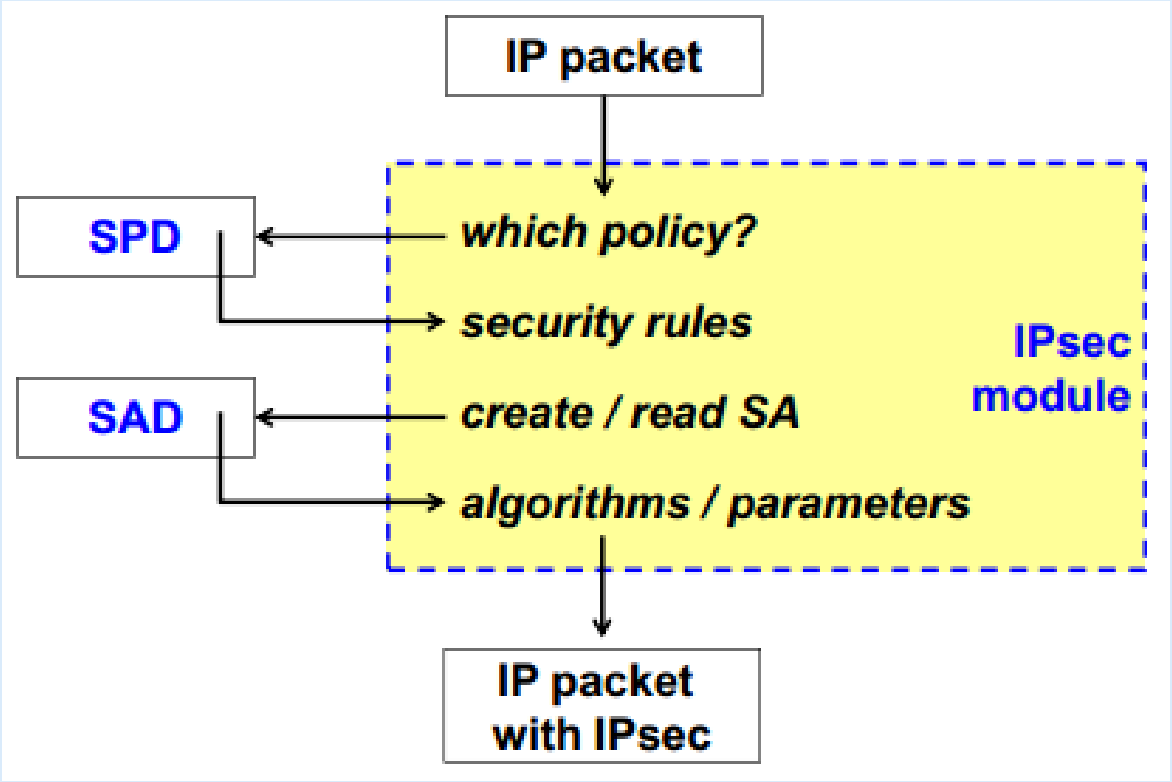


- Three SA identification parameters
  - Security parameter index (SPI)
  - IP destination address
  - IPsec protocol (AH or ESP)

IPsec local databases

- SAD (SA Database)
  - list of active SA and their characteristics
  - 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)

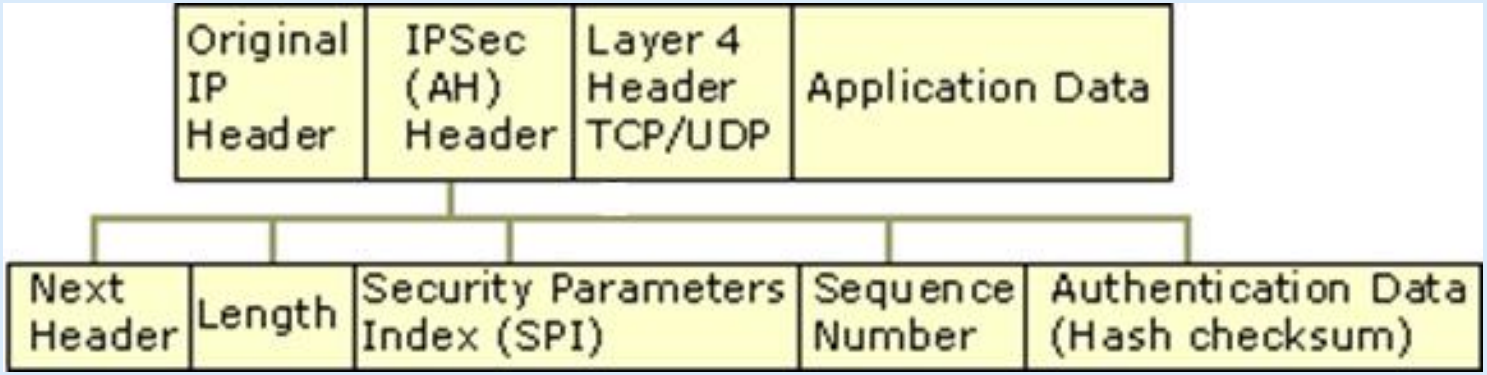
How IPsec works (sending)



Authentication Header (AH)

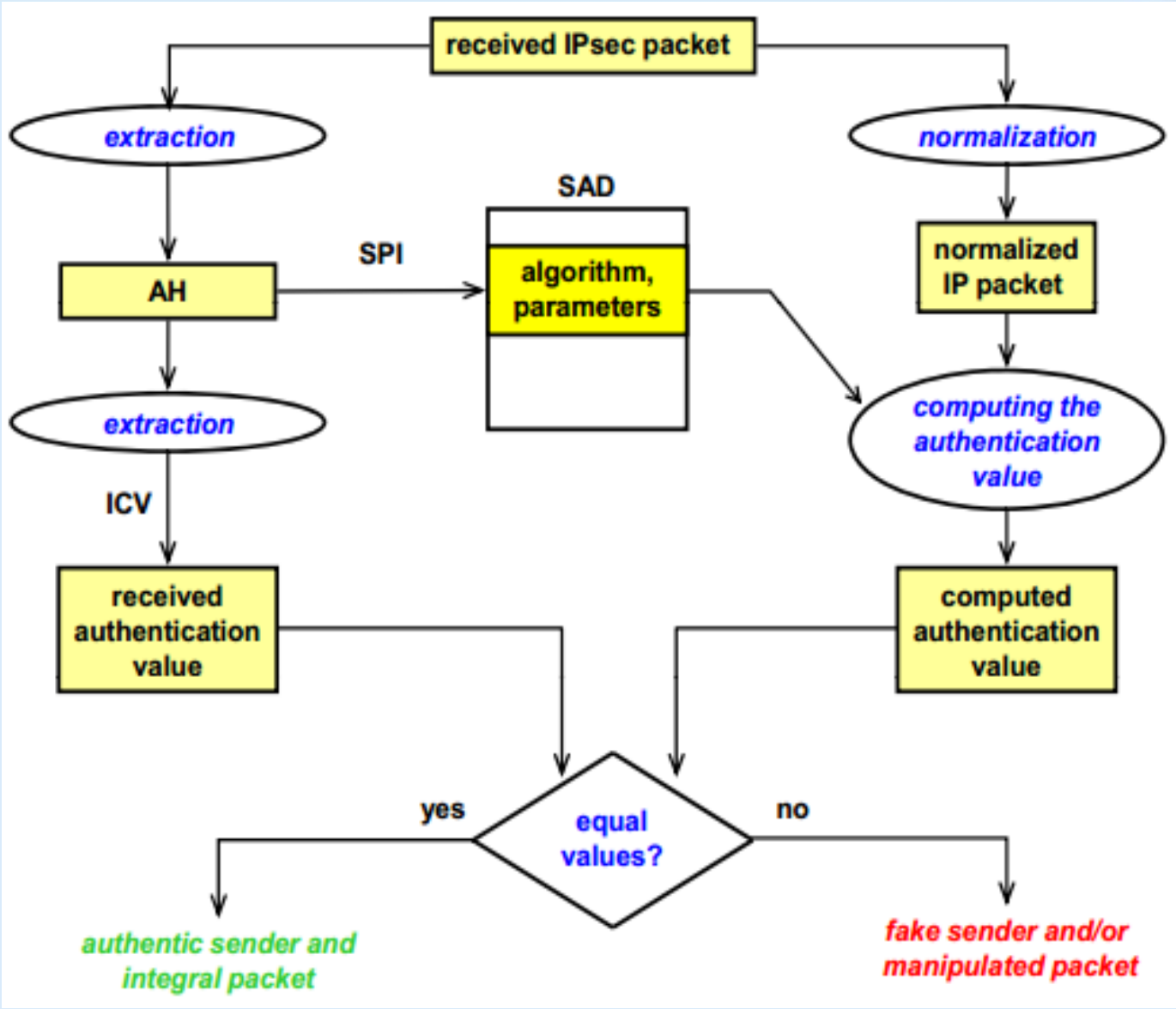
- first version mechanism (RFC-1826):
  - data integrity and sender authentication
  - compulsory support of keyed-MD5 (RFC-1828)
  - optional support of keyed-SHA1 (RFC-1852)
- second version mechanism (RFC-2402):
  - data integrity, sender authentication and protection from replay attack
  - HMAC-MD5
  - 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 (receiving)

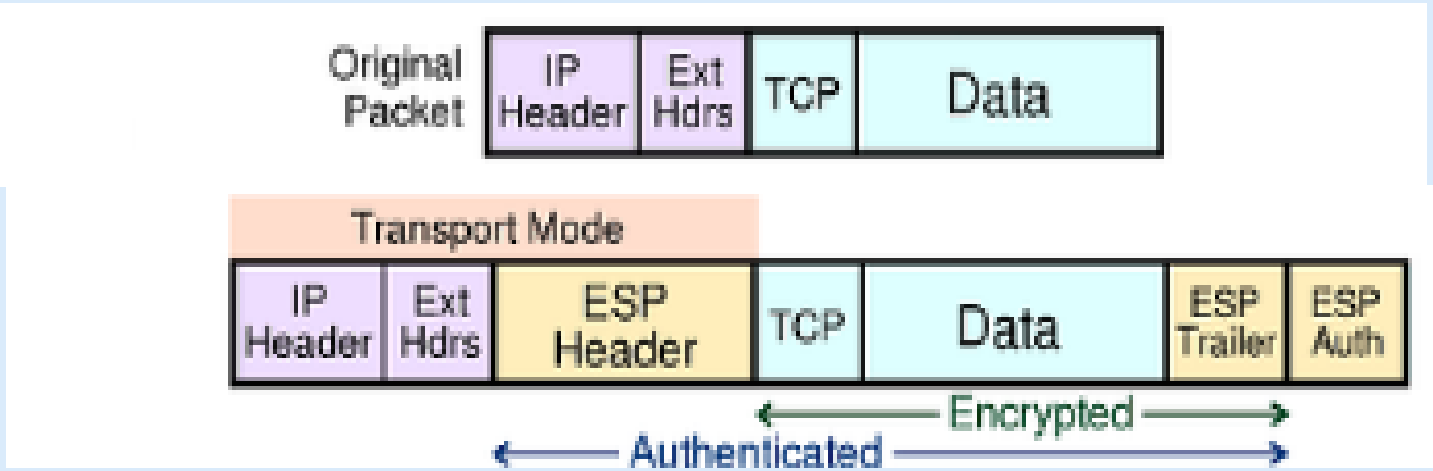


Encapsulating Security Payload (ESP)

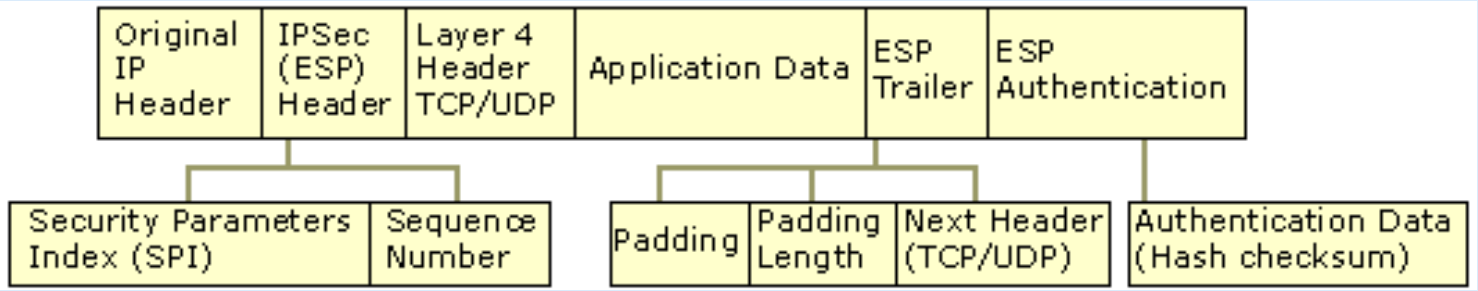
- first version (RFC-1827) gave only confidentiality
  - base mechanism: DES-CBC (RFC-1829)
- Second version (RFC-2406):
  - provides confidentiality & authentication (but not the IP header, so the coverage is not equivalent to that of AH)

ESP in transport mode

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

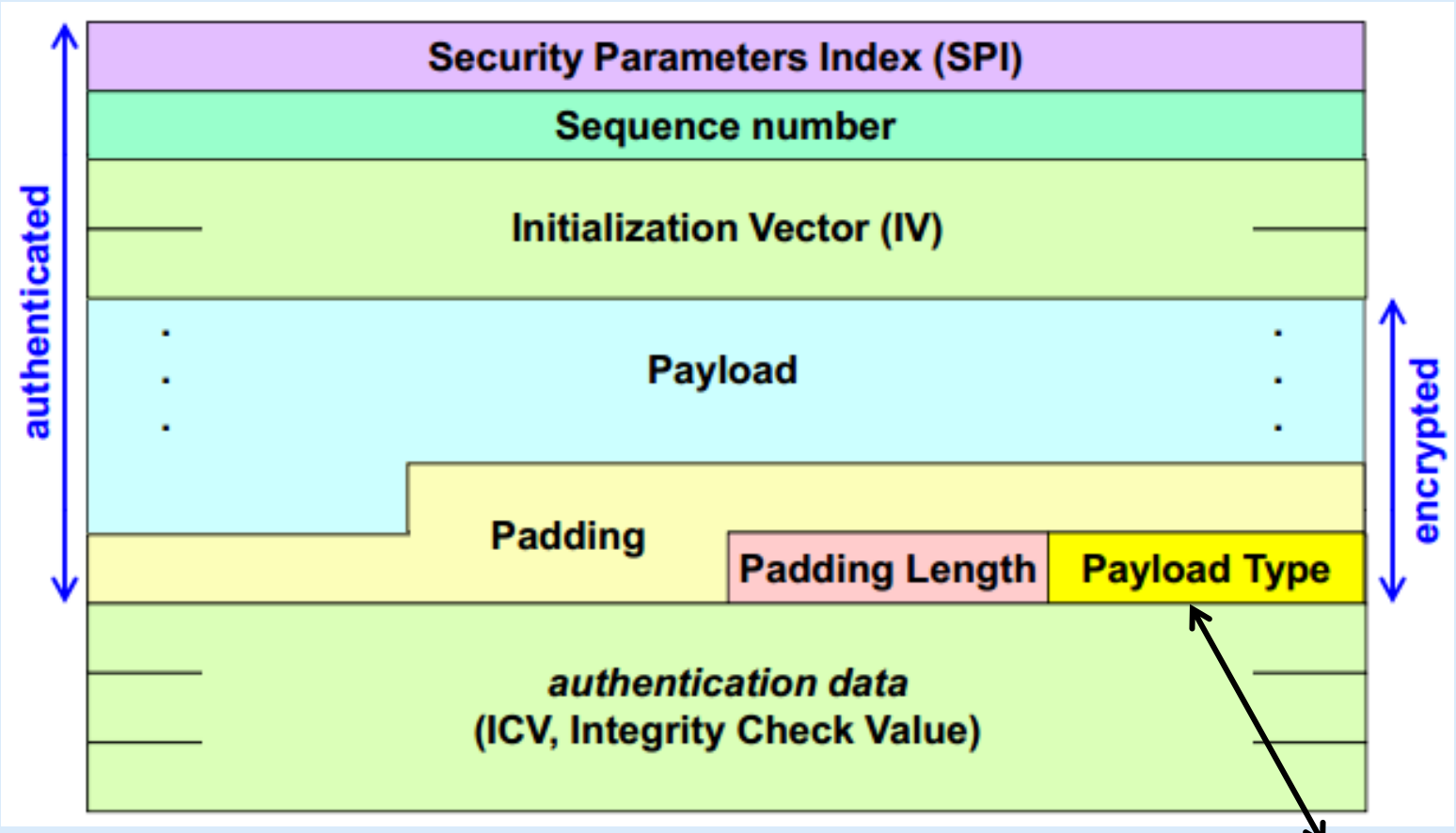


ESP Packet



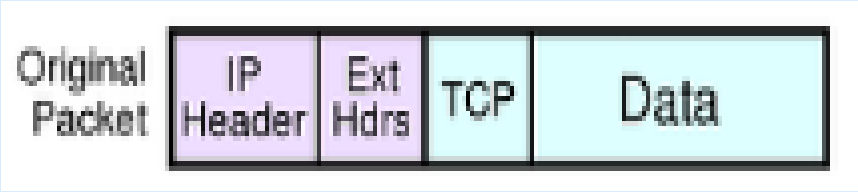
- SPI: Identifies the correct security association for the communication
- Sequence number: Provides anti-replay protection for the SA
- Next header: Identifies the nature of the payload (TCP/UDP)
- Auth. Data: Contains the Integrity Check Value (ICV), which is a message authentication code used to verify 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. After the sequence number

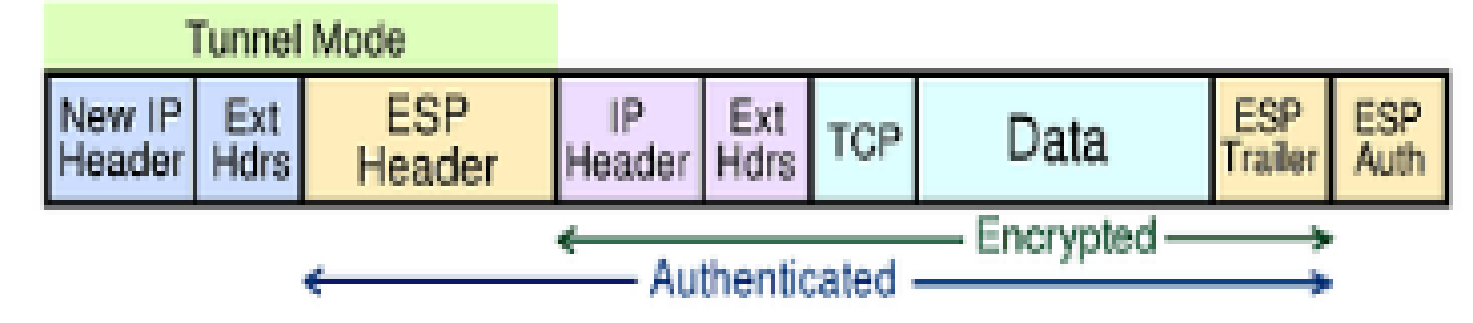
ESP Packet: Encryption & Authentication



ESP tunnel mode

- pro: hides both the payload and (original) header
- con: larger packet size





IPSec: AH & ESP packet format