Lecture Introduction into Cyber Security

Internet Protocol Security (IPsec) (Part 1)

Asya Mitseva, M.Sc.
Prof. Dr.-Ing. Andriy Panchenko

Chair of IT Security
Brandenburg University of Technology Cottbus-Senftenberg

8 January 2019

Brandenburgische
Technische Universität
Cottbus - Senftenberg

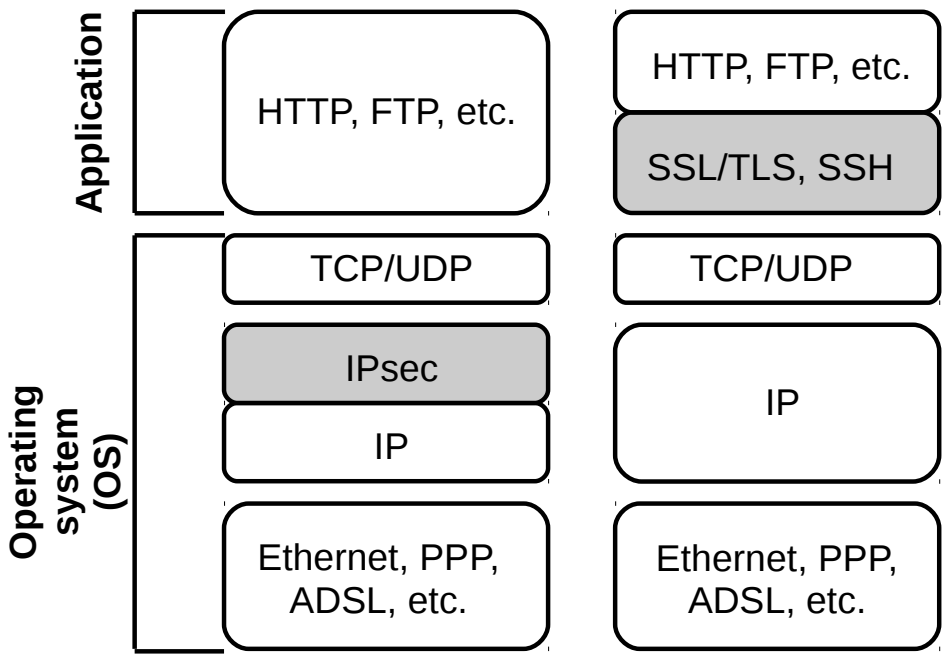
UNIVERSITÉ DU
LUXEMBOURG

Erasmus+

Introduction (1/2)

- **Real-time security protocol:** provides mutual *interactive* authentication between two communicating parties and establish a *session key* to cryptographically protect the subsequent conversation

- **Examples for real-time security protocols**
  - Internet Protocol security (IPsec)
  - Secure Socket Layer (SSL)/Transport Layer Security (TLS)
  - Secure Shell (SSH)



Introduction (2/2)

- **Real-time security protocols at layer 4**
  - *Advantages*
    - Easy to deploy, i.e., no changes to the OS needed
  - *Disadvantages*
    - Provide application-specific security only
    - Modification or insertion of (bogus) packets possible
    - Limited security benefits if the API is not sufficiently rich

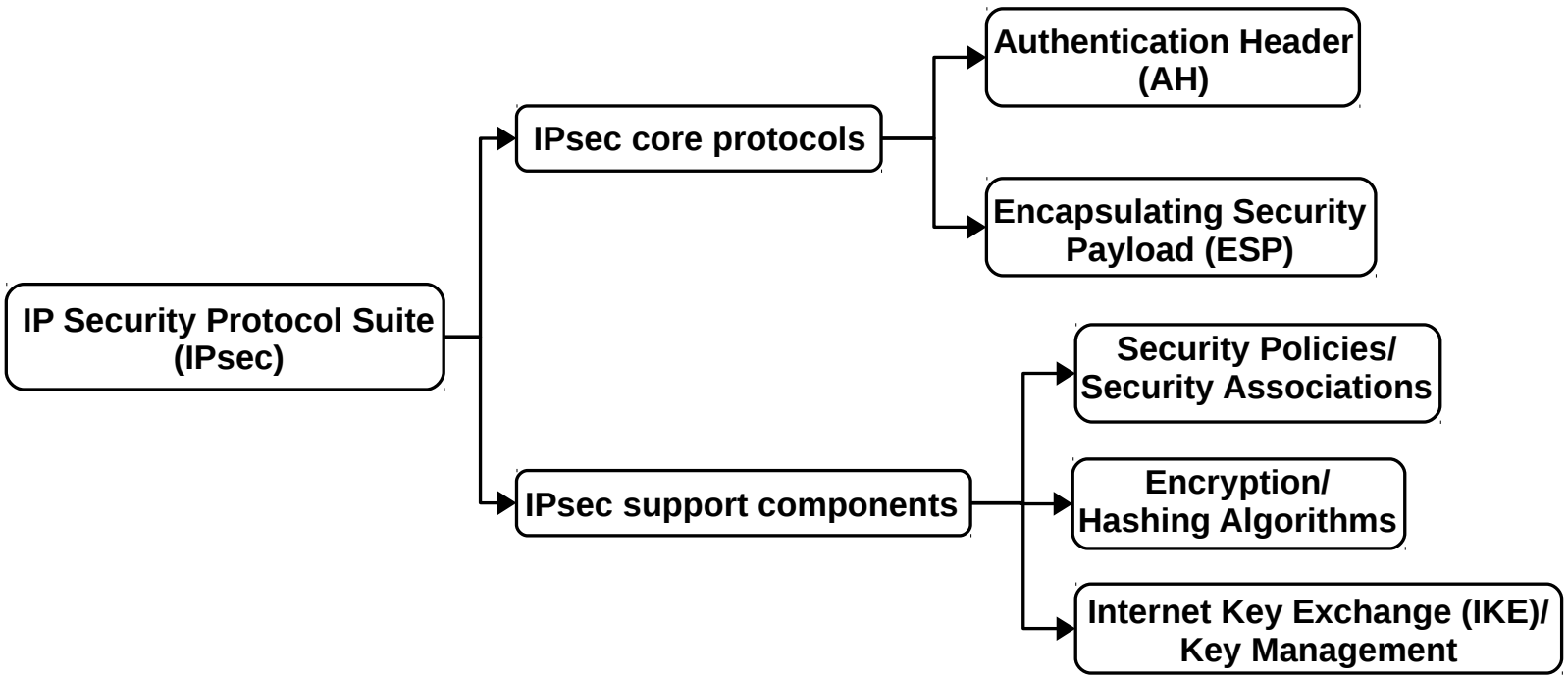
- **Real-time security protocols at layer 3**
  - *Advantages*
    - Cryptographic protection of each separate packet
    - Protect every protocol on top of IP, i.e., enable protection for security-ignorant applications
  - *Disadvantages*
    - Capable of authenticating distinct IP addresses but not individual users

Internet Protocol security (IPsec): Overview (1/3)

- Provide set of security services
  - Access control, confidentiality (encryption)
  - Limited traffic flow confidentiality
  - Data origin authentication, data integrity
  - Rejection of replayed packets
- Provide security features by adding additional headers to IPv4 & IPv6
- Execute packet-by-packet processing
- Often implemented in firewall or router and, thus, avoid overhead of security-related processing for end users
- Transparent to applications, i.e., no need to change software on user systems
- Transparent to end users, i.e., no need to train users on security mechanisms, issuing key material, etc.

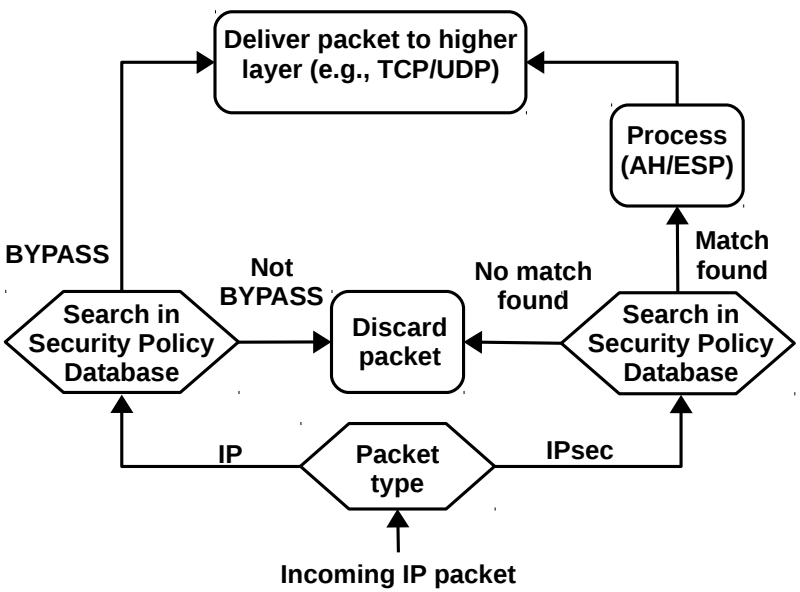
Internet Protocol security (IPsec): Overview (2/3)

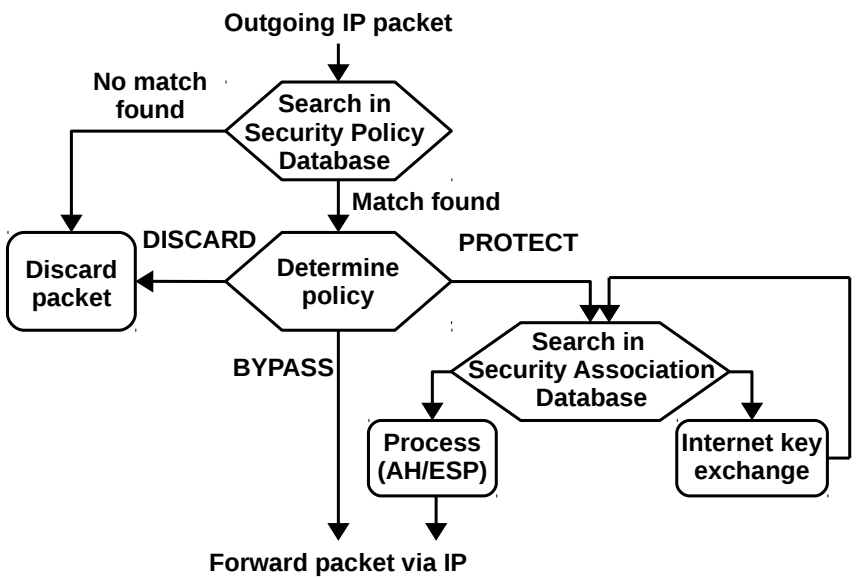
- Consist of two core protocols and set of supporting components
  - *Authentication Header (AH):* provides integrity & origin authentication
  - *Encapsulating Security Payload (ESP):* provides integrity, origin authentication, and encryption services
  - AH/ESP rely on pre-shared session keys & predefined crypto algorithms
  - *Supporting components:* specify mechanisms used for encryption and set up session keys for AH and ESP



Internet Protocol security (IPsec): Overview (3/3)

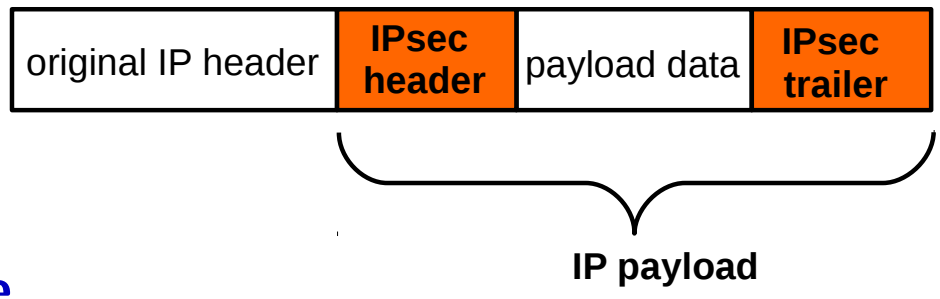
- *Secure Policy Database* contains rules identifying if a packet should be
  - PROTECTed using IPsec security services
  - Allowed to BYPASS IPsec protection or
  - DISCARDed
- *Security Association Database* determines how packets are processed
  - E.g., is AH/ESP used, which crypto algorithms and keys should be used



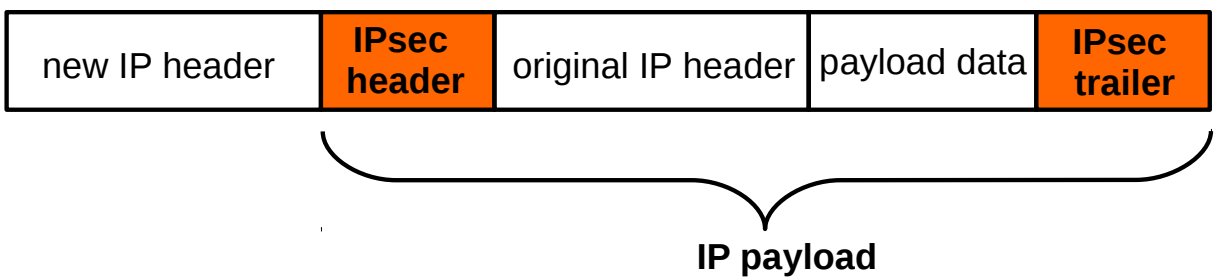


IPsec: Transport vs. Tunnel Mode

- IPsec can operate in two modes: *transport* and *tunnel* mode
- **Transport mode**
  - New header (and new trailer) are added between the original IP header and the payload of the packet
  - Provide protection primarily for upper-layer protocols



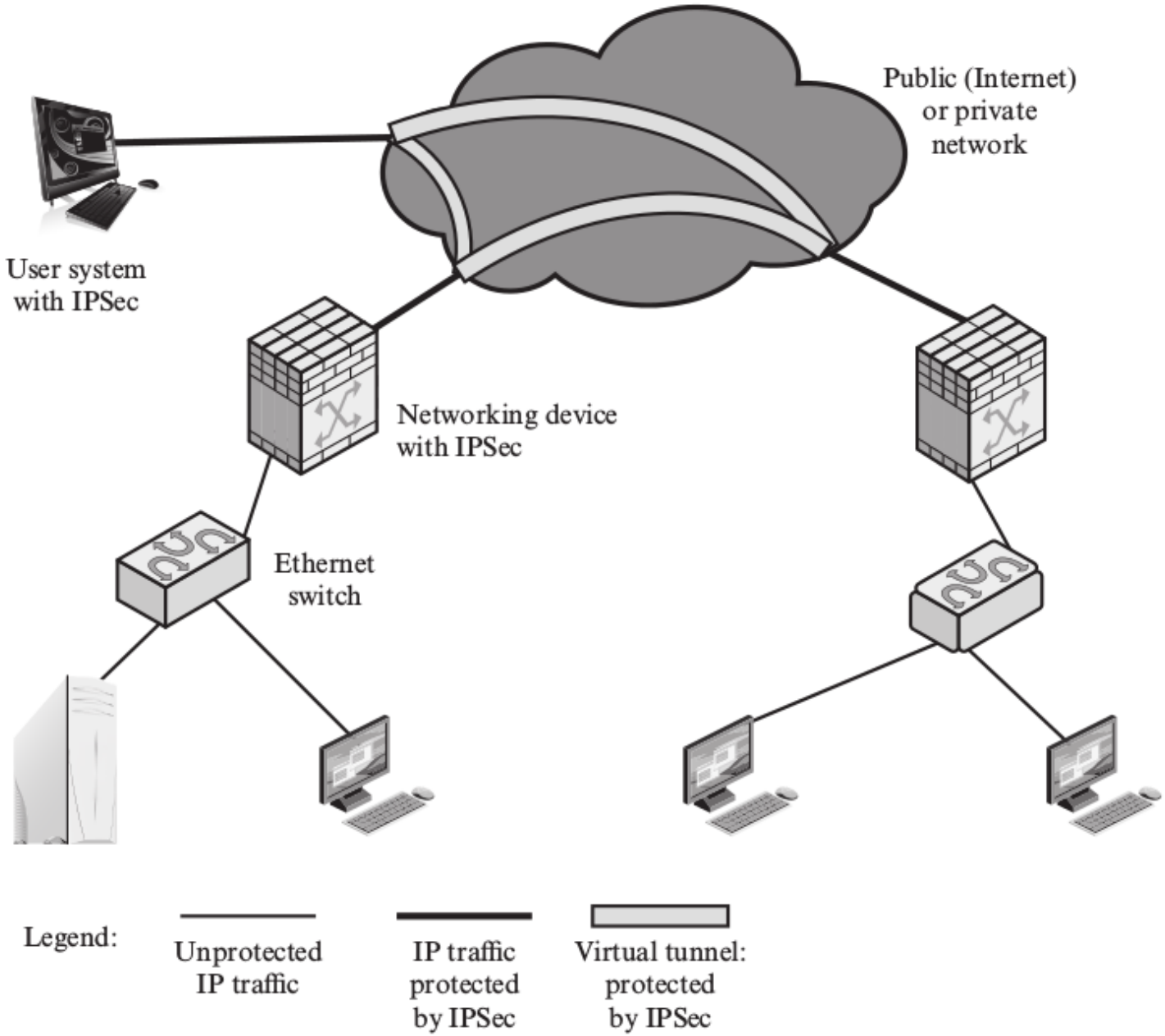
- **Tunnel mode**
  - IPsec header (and IPsec trailer) are added to the original IP packet and new IP header is inserted to the protected packet
  - Provide protection of the entire IP packet



Applications of IPsec (1/2)

- **Secure connectivity between branch offices over the Internet**
  - Branch offices of company located in different geographic areas
  - Deploy IPsec in access points/firewalls at the edge of each branch office's network
- **Secure remote access over the Internet**
  - A user connects to the Intranet of company from outside
  - Deploy IPsec on the remote host and in access points/firewalls at the edge of the company's network
- **Secure communication between different organizations**
- **Secure connectivity between individual hosts**
- **Secure exchange of routing information between border gateways of different autonomous systems**

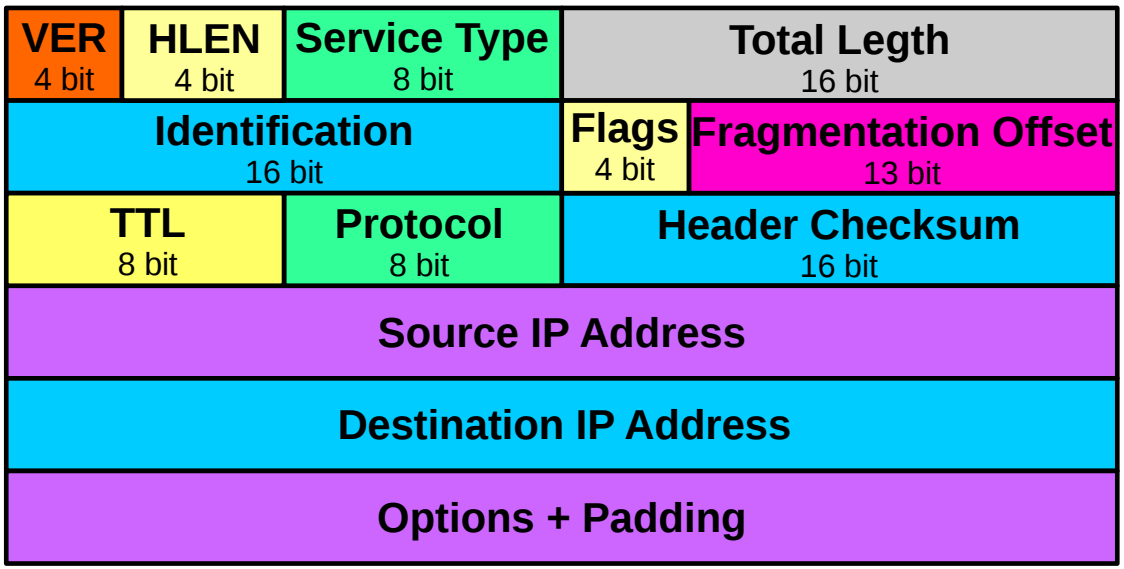
Applications of IPsec (2/2)



Authentication Header (AH): Overview

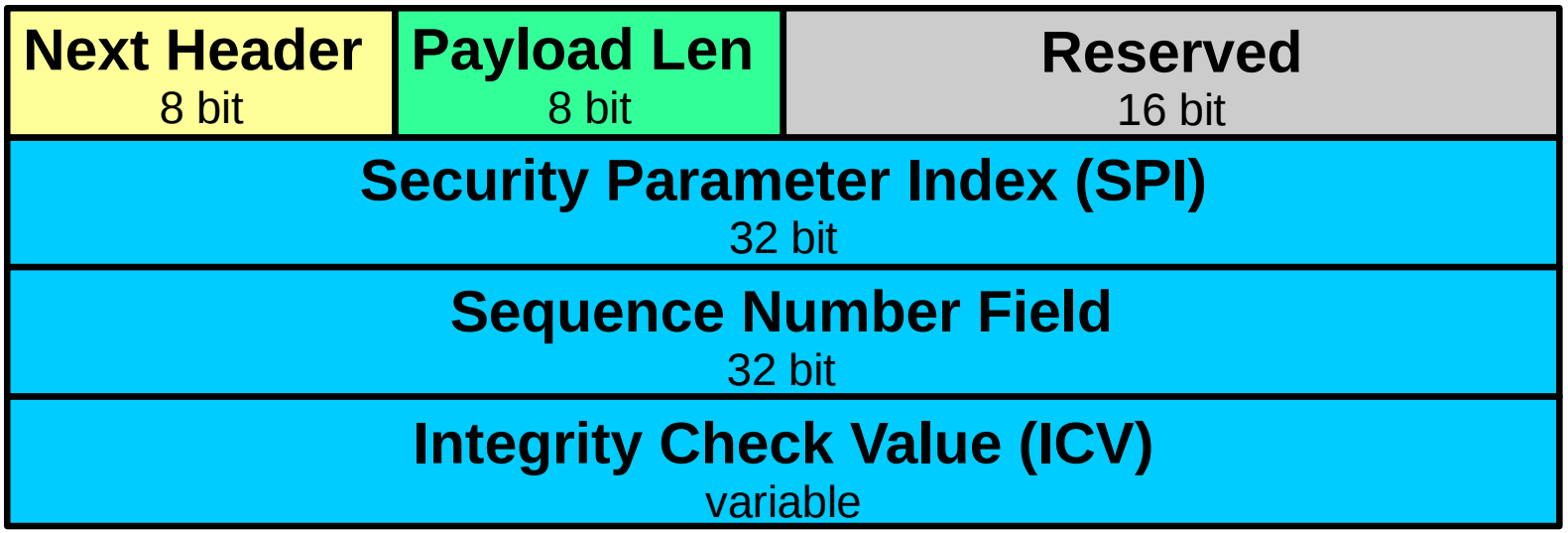
- Designed to provide integrity protection of the payload of an IP packet and its *immutable* and *predictable* IP headers
- Enable sender authentication of an IP packet
- Protect against packet replay attacks
- AH can be applied in both modes: transport and tunnel
- Mandatory-to-implement encryption algorithms used with AH
  - MUST implement HMAC-SHA1-96
  - SHOULD implement AES-XCBC-MAC-96
  - MAY implement HMAC-MD5-96
- To compute HMAC, sender and receiver share predefined secret key
  - IKE key establishment protocol is used to set up the key
  - The key is stored in *security association* by both sender and receiver

Mutable, Predictable, and Immutable Fields in IP Header



- **Mutable fields**: Modified during transit
  - E.g., Time to live (TTL), header checksum, service type, flags, etc.
  - Set to zero for the calculation of the integrity check value in AH
- **Predictable fields**: May change during transit but in predicted way
  - E.g., destination IP address
- **Immutable fields**: Remain unchanged during transmit

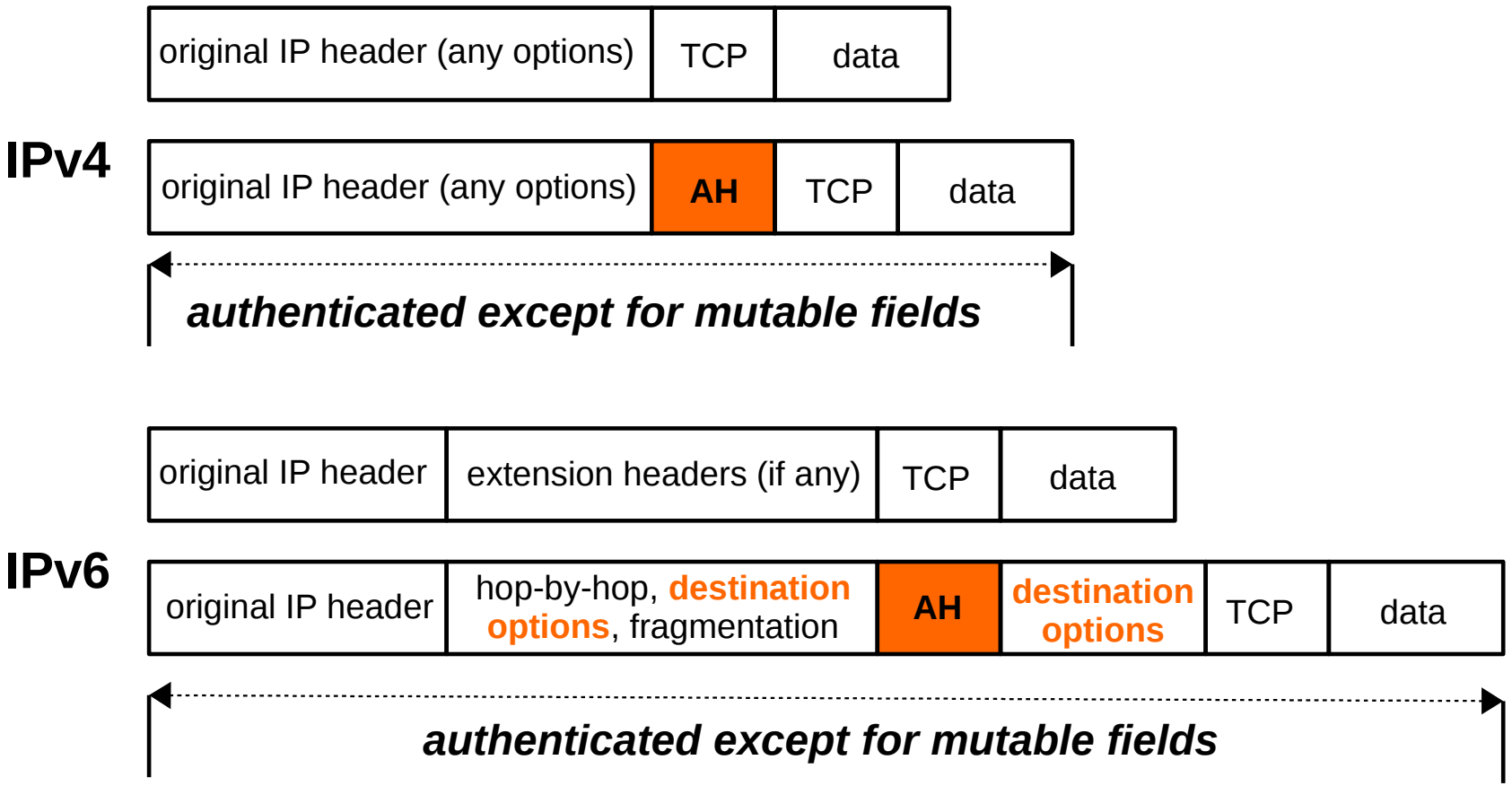
Authentication Header Format



- *Next Header*: Show the type of the payload carried by the IP packet
- *Payload Len*: Determine the length of the authentication header
- *Reserved*: Field reserved for future use
- *SPI*: Define encryption algorithms and keys used to compute the ICV
- *Sequence Number*: Counter value incremented by one for each packet sent; provide packet replay protection
- *ICV*: Contain integrity check value computed for this packet

Authentication Header Location: Transport Mode

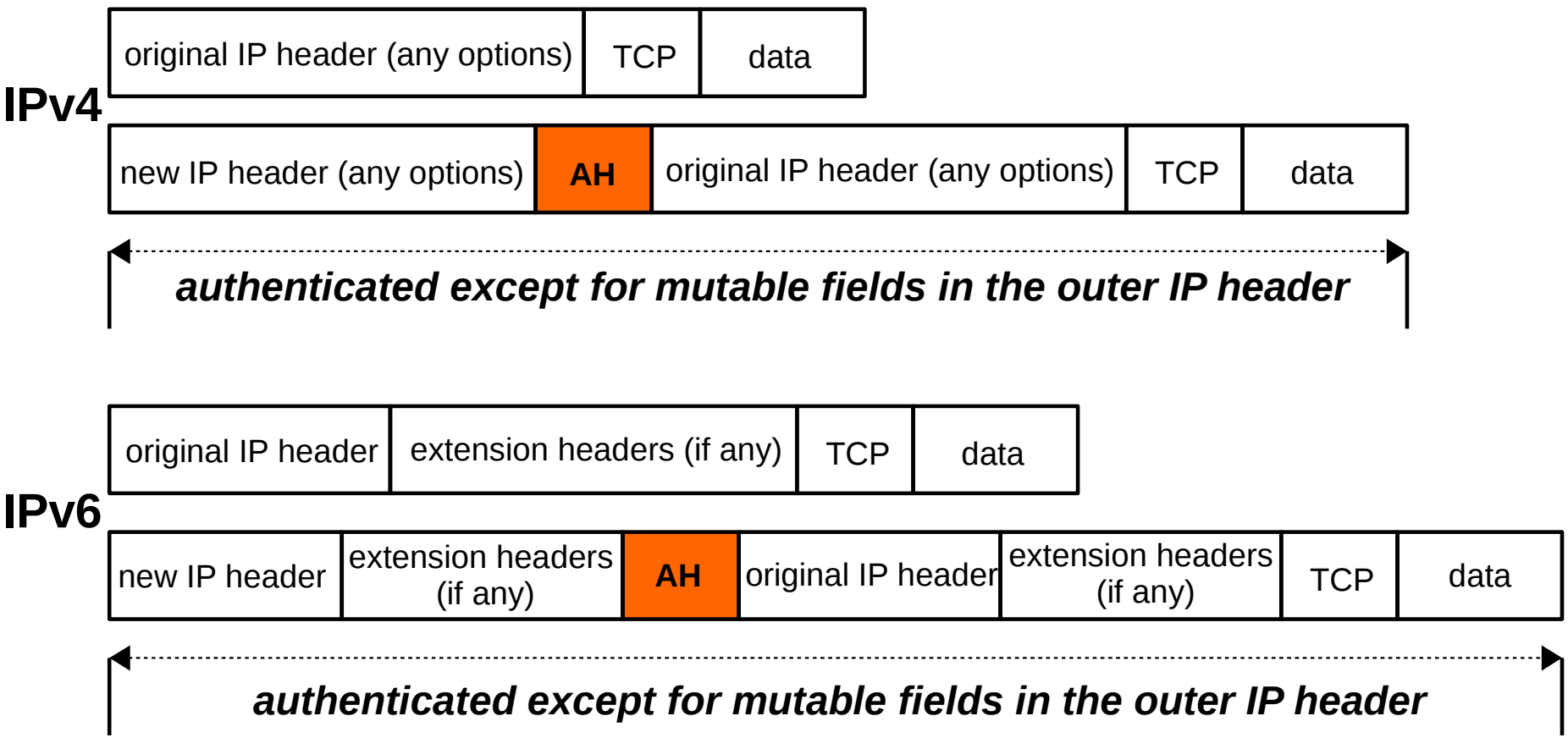
- AH is added after the IP header and before the next layer protocol



- *Destination options* extension in IPv6 can appear before or after AH or both depending on the semantics desired

Authentication Header Location: Tunnel Mode

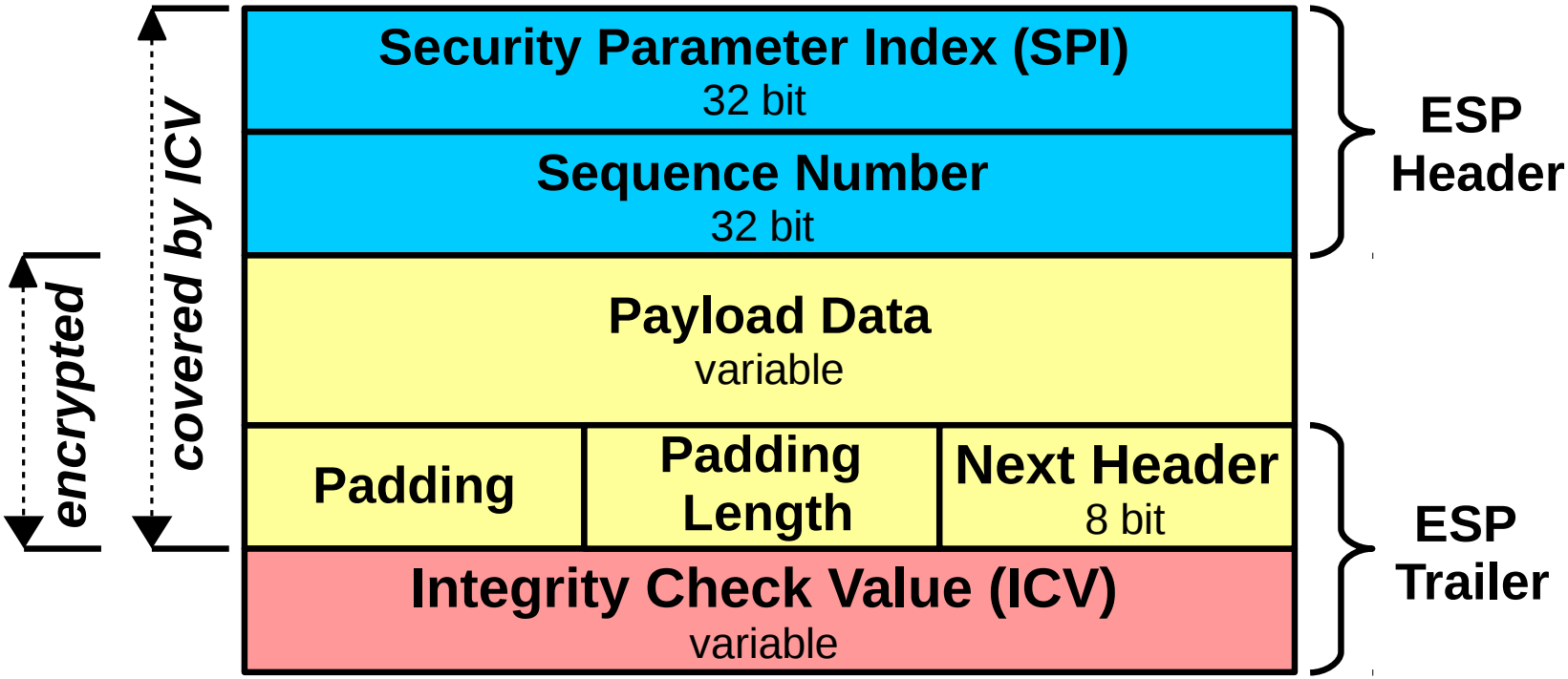
- AH is added after the outer IP header
- AH protects the entire inner IP packet (incl. all inner IP headers)
- Mixed inner and outer IP versions are allowed



Encapsulating Security Payload (ESP): Overview

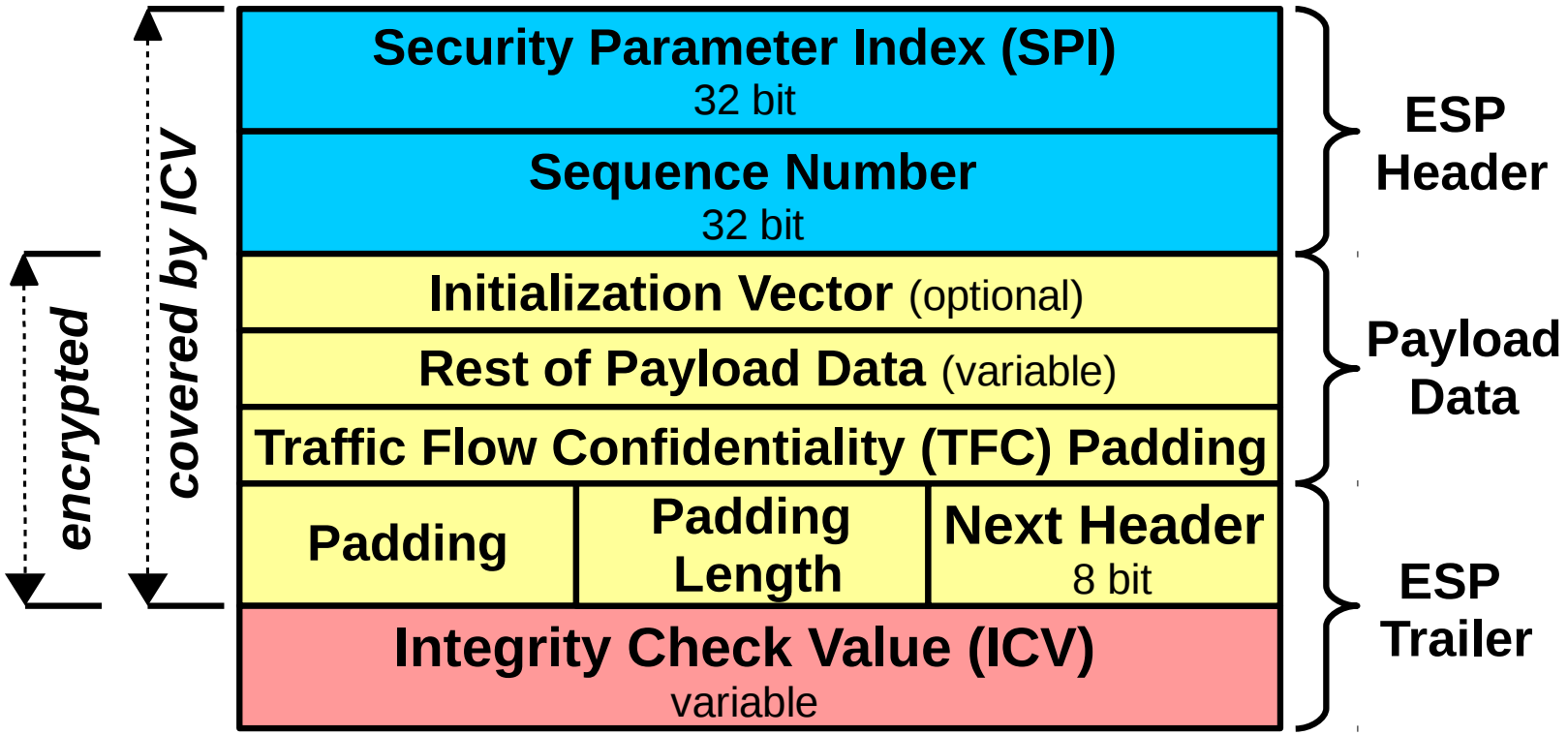
- Designed to provide confidentiality and integrity protection of the payload of an IP packet
  - Confidentiality and integrity are optional
  - *But*, at least one of them should be selected
- Encrypt the payload of an IP packet if the confidentiality is enabled
- May add dummy packets to provide traffic flow confidentiality
- Enable sender authentication & protect against packet replay attacks
- Packet replay protection is selected only if the integrity is enabled
- ESP packet consists of ESP header, ESP trailer, and payload data
- ESP can be applied in both modes: transport and tunnel

ESP Packet Format (1/2)



- *SPI*: Define encryption algorithms and keys used to encrypt the payload data and compute the ICV
- *Sequence Number*: Counter value incremented by one for each packet sent; provide packet replay protection
- *ICV*: Contain integrity check value computed for this packet

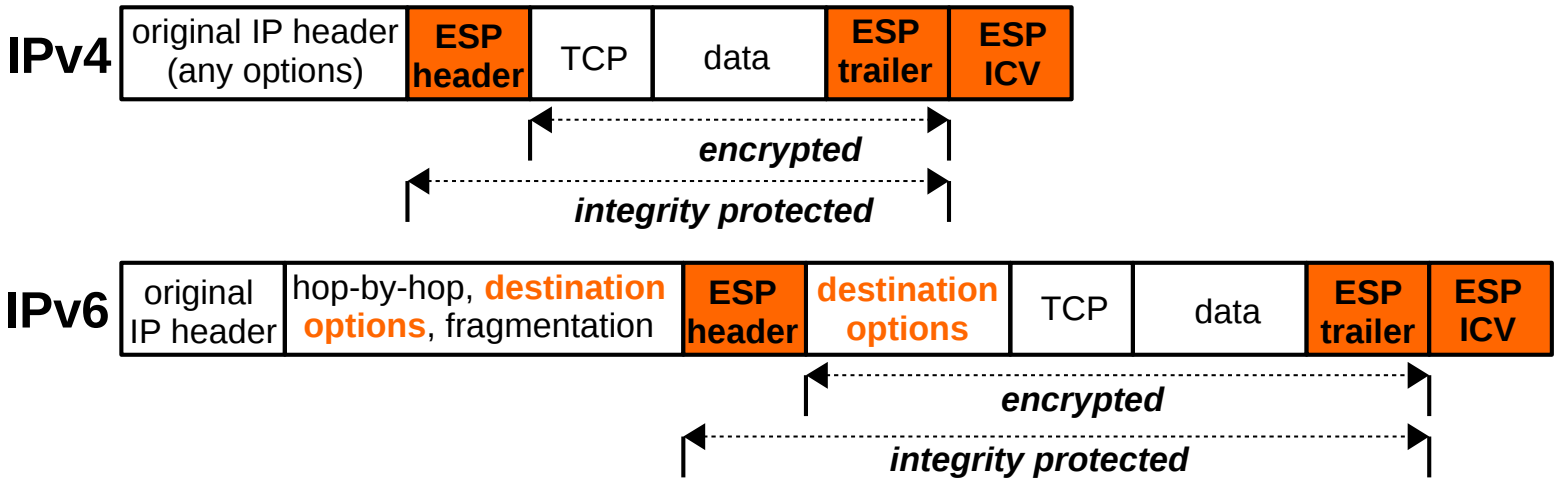
ESP Packet Format (2/2)



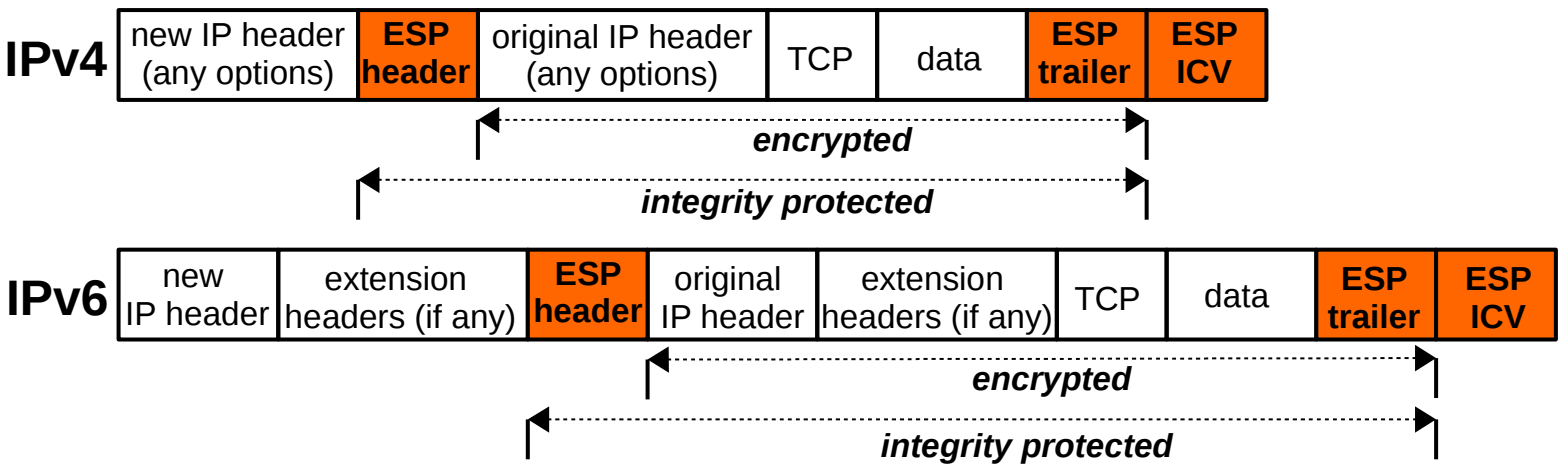
- *TFC Padding*: Add pad bytes to the payload data; aim to provide confidentiality
- *Padding*: Pad bytes required for the crypto algorithm or alignment
- *Padding Length*: Define the number of pad bytes in the Padding field
- *Next Header*: Show the type of the payload carried by the IP packet

ESP Location

- **Transport mode**



- **Tunnel mode**
  - Provide privacy for the sender and the receiver
  - If the traffic is transmitted through IPsec gateways



Encryption Algorithms Applied for ESP

- **Algorithms used to encrypt the payload data**
  - MUST support NULL encryption, AES-CBC, TripleDES-CBC
  - SHOULD support AES-CTR, but not DES-CBC
- **Algorithms used for integrity and sender authentication**
  - MUST implement HMAC-SHA1-96
  - SHOULD implement AES-XCBC-MAC-96
  - MAY implement NULL integrity, HMAC-MD5-96
- **NULL encryption**
  - Does nothing to alter plaintext data
  - Mathematically defined by the use of the Identity function: $\mathrm{NULL}(b) = I(b) = b$
  - Does not include the IP header in computing the authentication data

ESP Packet Processing

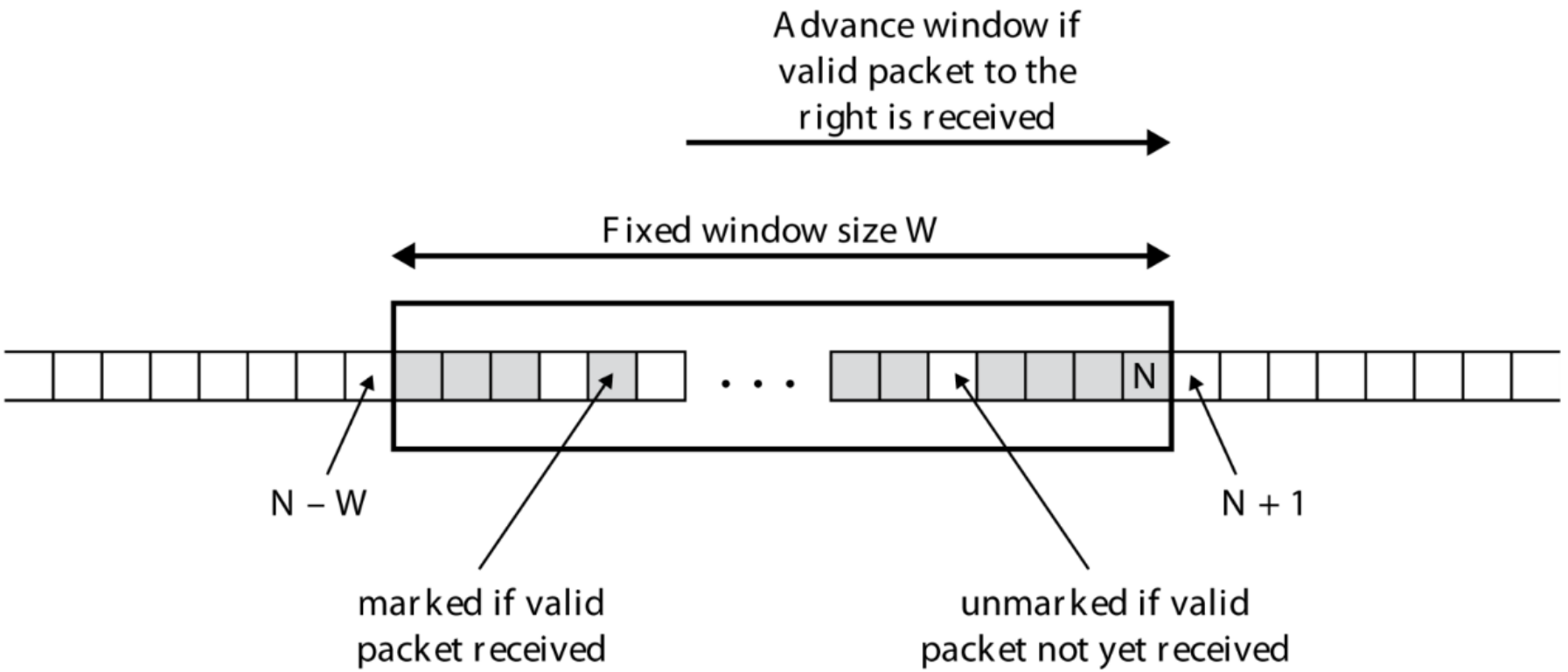
- **Outbound packet processing**
  1. Encapsulate data into the ESP Payload field
  2. Add TFC and encryption padding if necessary
  3. Encrypt the result using shared key and selected crypto algorithm
  4. Compute ICV over the ESP packet, incl. SPI, Sequence Number, Payload Data, Padding, Pad Length, Next header
- **Inbound packet processing**
  1. Preliminary sequence number check by using Sequence Number field in ESP header
  2. Compute ICV over the ESP packet minus the ICV field and verify if it is the same as the ICV carried in the packer
  3. Decrypt ESP Payload Data, Padding, Pad Length, Next header using shared key and selected crypto algorithm
  4. Remove any TFC and encryption padding if necessary
  5. Check if Next Header field is 59 (i.e., dummy packet) & discard packet
  6. Reconstruct the original IP datagram

AH vs. ESP

- AH **and** ESP provide
  - Payload data integrity
  - Protection against packet replay attacks
  - Sender authentication
- **ESP supports payload data confidentiality, but AH does not**
- **AH supports integrity protection of most of the fields in the outer IP header, but ESP does not**
- **In tunnel mode, ESP provides sender and receiver privacy and data flow confidentiality if traffic is exchanged between two IPsec gateways and TFC padding is enabled**

Packet Replay Protection in AH & ESP (1/2)

- **Replay attack:** Copy of authenticated, already transmitted packet is sent later to an intended receiver
- **IPsec provides defense against replay attacks by using**
  - *Sequence Number* counter added to AH and ESP headers
  - *Window* of acceptable sequence numbers of size *W*



Packet Replay Protection in AH & ESP (2/2)

- Right edge of the window indicates the highest sequence number N
- Left edge of the window indicates the lowest sequence number $N - W$
- If packet with sequence number higher than the rightmost one is received, the window moves to the right
- Inbound processing of packets with anti-replay service enabled
  - If received packet falls within the window and is new, the ICV is checked. If the packet is authenticated, the corresponding slot in the window is marked.
  - If received packet is on the right side of the window and is new, the ICV is checked. If the packet is authenticated, the window moves to the right and the corresponding slot is marked.
  - If received packet is on the left of the window or the ICV check fails, the packet is discarded.

Security Associations (SAs)

- One-way logical connection between the sender and the receiver
- Determine the security services to the traffic on that connection
- Manually configured or negotiated through Internet Key Exchange
- Two SAs are required for bi-directional communication
- Sender stores several SAs for different receivers, types of traffic, etc.
- SA is uniquely identified by
  - *Security Parameter Index (SPI)*: Carried in AH/ESP headers to enable receiver to select SA used to protect the packet
  - *IP Destination Address*: IP address of the receiver of the SA
  - *Security Protocol Identifier*: Shows if the association is AH or ESP SA

References

- William Stallings, *Cryptography and Network Security*, Chapter 20
- Charlie Kaufman et al., *Network Security: Private Communication in a Public World*, Chapter 16, 17
- RFC 4301, https://tools.ietf.org/html/rfc4301
- RFC 4302, https://tools.ietf.org/html/rfc4302
- RFC 4303, https://tools.ietf.org/html/rfc4303
- RFC 4835, https://tools.ietf.org/html/rfc4835
- RFC 2410, https://tools.ietf.org/html/rfc2410
- RFC 6071, https://tools.ietf.org/html/rfc6071