School of Electrical Engineering and Computing

SENG2250/6250
SYSTEM AND NETWORK SECURITY
(S2, 2020)

Internet Protocol Security (IPSec)

THE UNIVERSITY OF NEWCASTLE AUSTRALIA

Outline

- IPSec Overview
- Security Protocols and Modes
- IPSec Policy
- Internet Key Exchange (IKE) Protocol

IP Security Overview

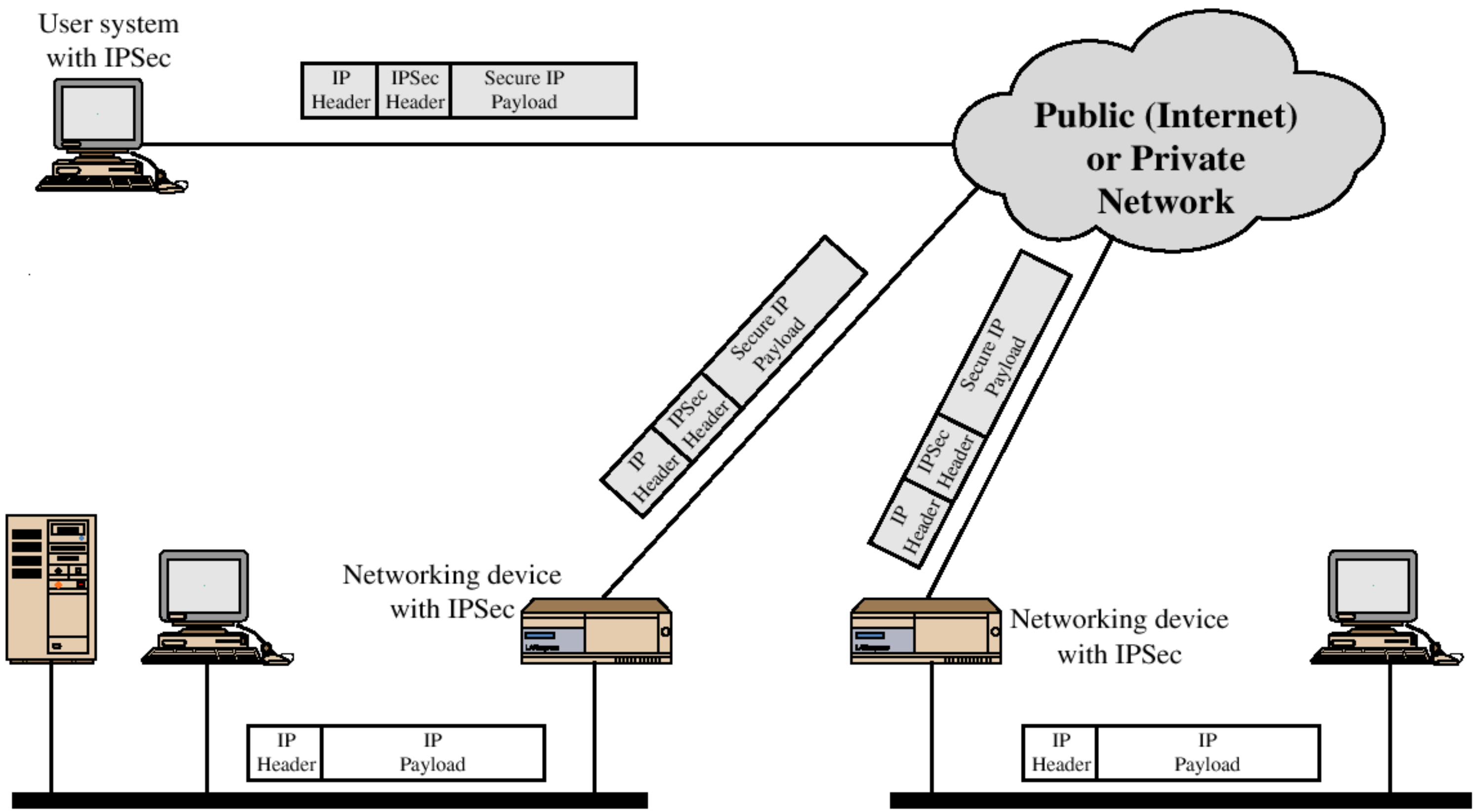
- IPSec (Internet Protocol Security) is a suite of standards for providing a rich set of security services at the network layer.
- Transparent to applications (below transport layer – TCP, UDP)
- IPSec Main Features:
  - *Source authentication*
  - *Message authentication and integrity check*
  - *Data confidentiality*
  - *Access control*

IPSec Applications

IPSec can provide security for varied application because it encrypts and/or authenticates all traffics at the IP level.

- Virtual private network
- Secure remote access
- Enhancing electronic commerce security
- …

A Typical Scenario



A Typical Scenario

- A company maintains LANs at dispersed locations, where non-secure traffic is conducted in each LAN.
- IPSec protocols operate in networking devices (routers and firewalls) to secure offsite traffic.
- These devices encrypt & compress all outbound traffic, and decrypt & decompress all inbound traffic.
- These security operations are transparent to workstations and servers on each LAN.
- Security service is also possible for individual users who dial into the public network.

History and Standards

- IPSec is specified by numerous documents
  - *RFC 2401: An overview of the security architecture.*
  - *RFC 2402: Description of a packet authentication extension to IPv4 and IPv6.*
  - *RFC 2046: Description of a packet encryption extension to IPv4 and IPv6.*
  - *RFC 2048: Specification of key management capabilities.*
- Support for the features is mandatory for IPv6 but optional for IPv4.
- IPSec is implemented as extension headers in IP Packet.

IPSec Security Protocols

- There are two major component
  - *Security protocols*
    - Authentication Header (AH) protocols
    - Encapsulating Security Payload (ESP) protocols
  - *Modes*
    - Transport mode
    - Tunnel mode

IPSec Security Protocols

	AH	ESP (enc.)	ESP (enc.+auth.)
Access Control	√	√	√
Connectionless Integrity	√		√
Data origin auth.	√		√
Anti-replay	√	√	√
Confidentiality		√	√
Limited traffic flow conf.		√	√

IPSec Protocols

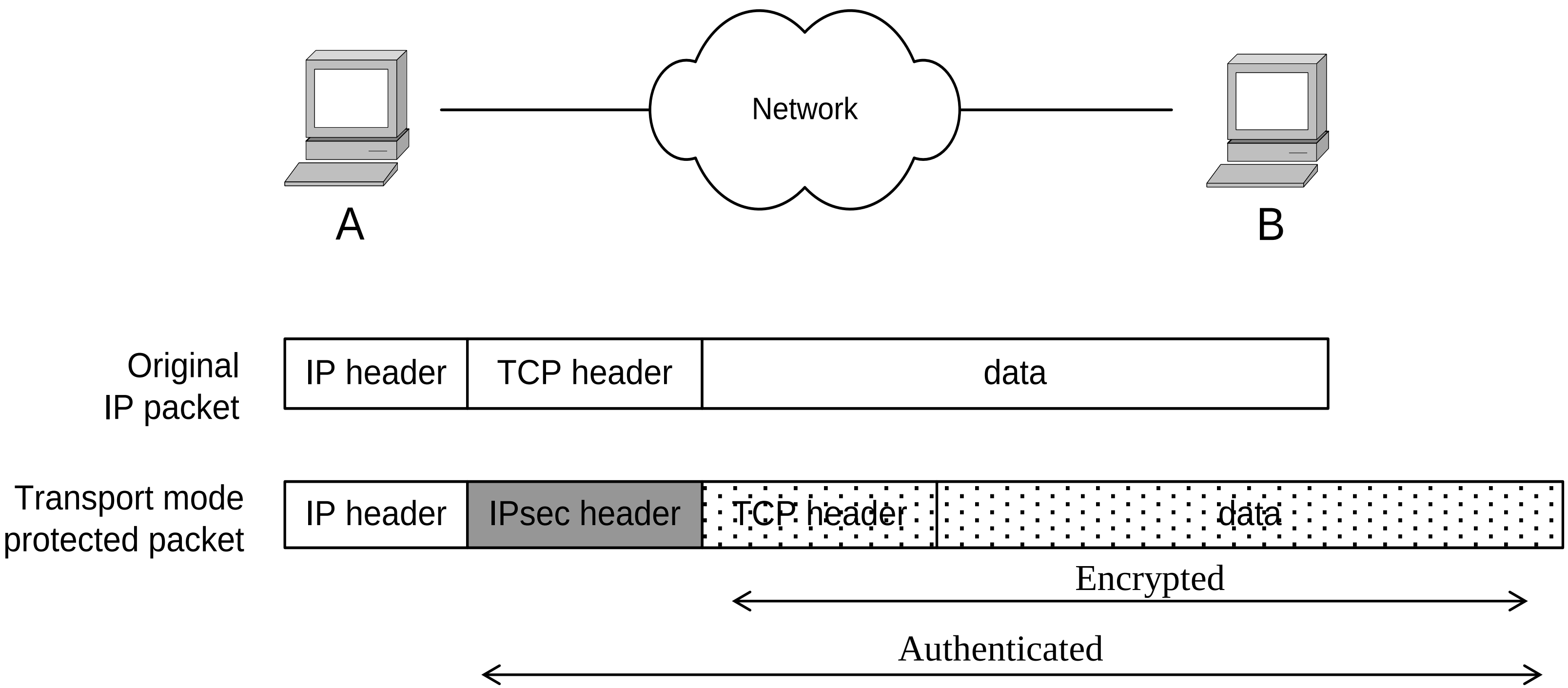
- AH and ESP protocols are largely independent of the cryptographic algorithms and key management protocols used to secure the IP traffic.
- These protocols can use any underlying cryptographic algorithm to implement the authentication and confidentiality services, such as DES for encrypting the outbound traffic, MD5 or SHA-1 to create hashed MAC.

Modes

- The AH and ESP protocols operate in one of two possible modes: **tunnel** mode or **transport** mode.
- Tunnel mode contains two IP headers
  - *Outer IP header: specifies the IPSec processing destination.*
  - *Inner IP header: contains the source and the ultimate destination of packet.*
- Transport mode
  - *Contains only one IP header which specifies the apparent source address and the ultimate destination address of the packet.*

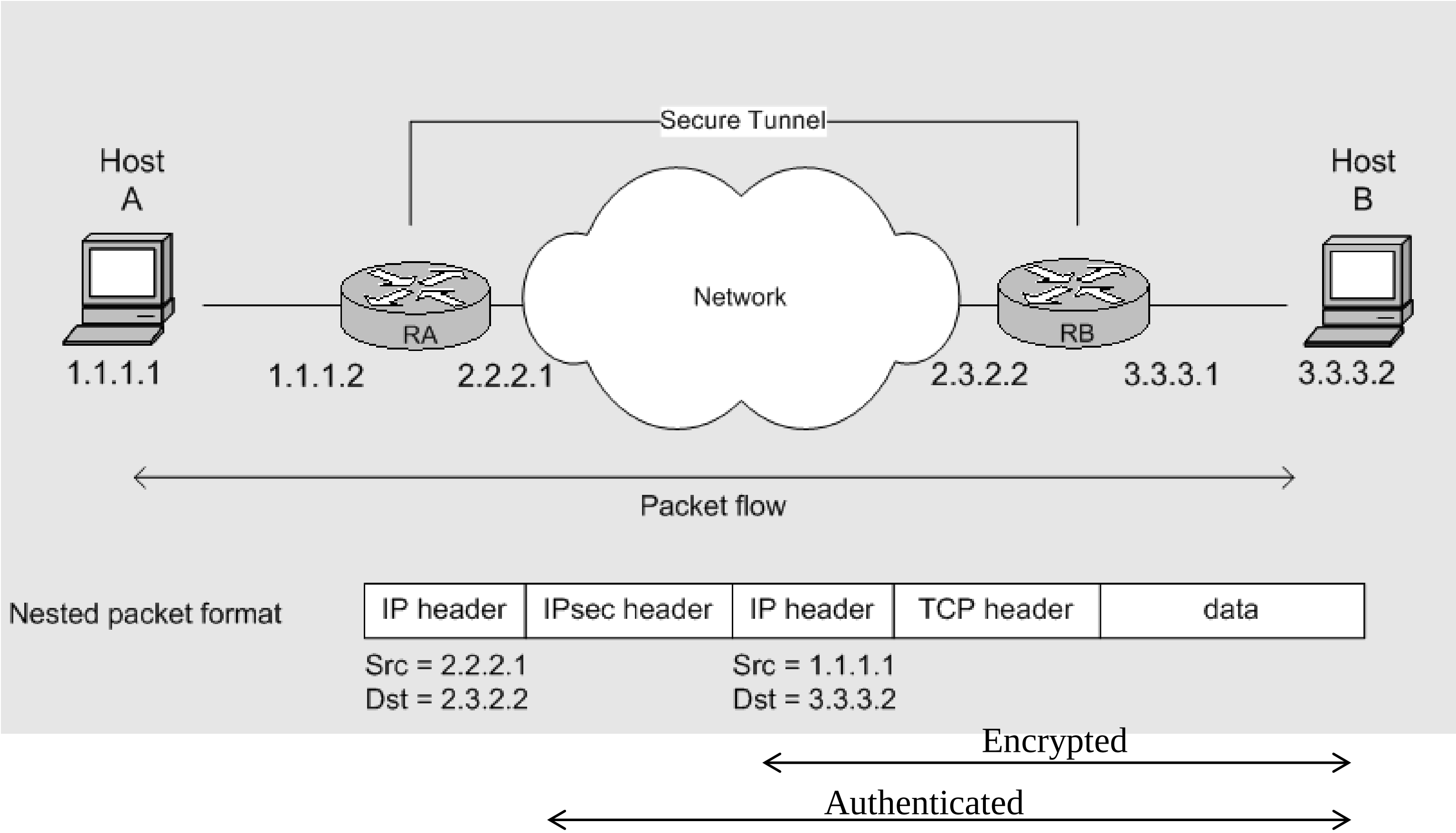
Transport Mode with IPSec

Encrypt / Authenticate an IP packet preserving **most** of the original IP packet.



Tunnel Mode with IPSec

Encrypt / Authenticate an IP packet, while encapsulating the original IP packet entirely.



AH Header Fields

AH Header Field	Description
Next header	Identifies the type of the next payload after the authentication header.
Payload length	Specifies the length of the authentication header in 32-bit words.
Reserved	Reserved for future use.
Security parameters index (SPI)	In conjunction with the destination IP address and the IPSec protocol (AH or ESP), uniquely identifies the security association for a packet.
Sequence number	Contains a monotonically increasing counter value against replay attacks.
Authentication data	Contains the integrity check value (ICV) for the packet for data origin authentication and connectionless integrity.

AH in Transport Mode (IPv4)

Before AH

IP header	TCP/UDP header	Payload

After AH

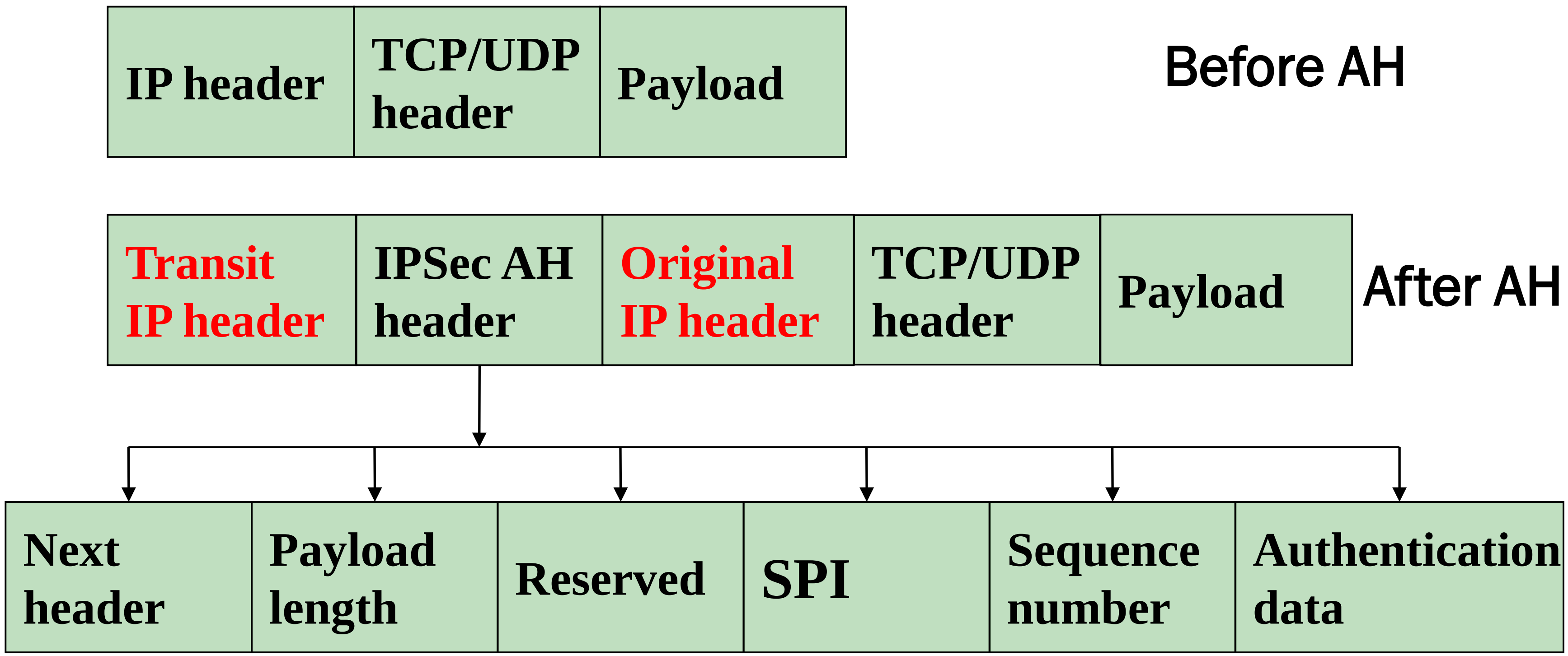
IP header	IPSec AH header	TCP/UDP header	Payload

Next header	Payload length	Reserved	SPI	Sequence number	Authentication data

SPI: Security parameters index

Authentication is across all immutable fields

AH in Tunnel Mode (IPv4)



Authentication is across all immutable fields

Integrity Check Value (ICV)

- AH protocol excludes any unpredictable mutable fields when calculating ICV.
- AH protocol includes only the immutable fields and mutable but predictable fields when calculating an ICV for a packet.

AH Protocol – ICV

- AH security protocol can use keyed message authentication codes (MACs) based on symmetric encryption algorithms or hashed MACs based on hash functions for calculations of ICV authentication data.
- Standards-compliant AH implementation must support HMAC with MD5 and HMAC with SHA-1.

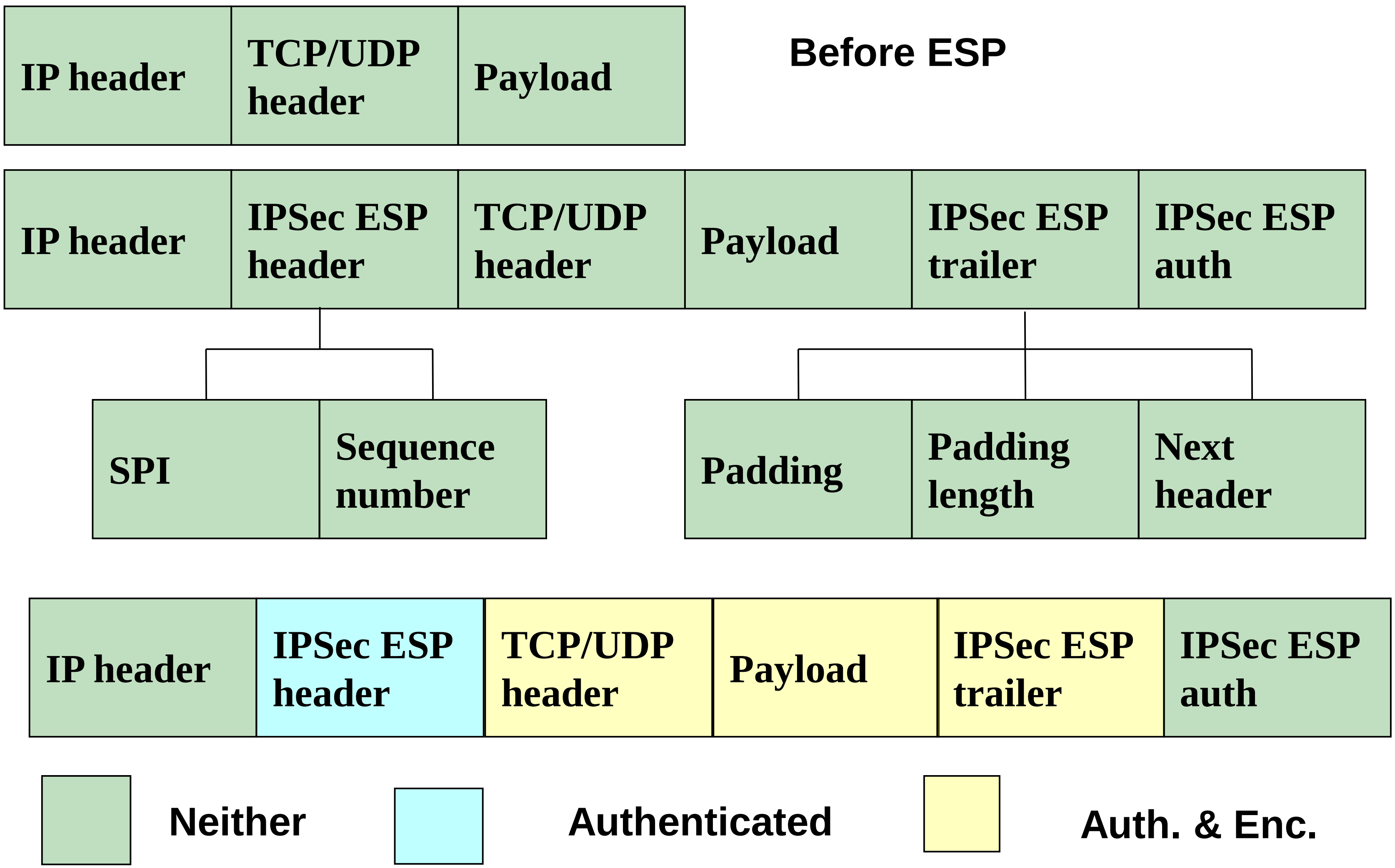
Mutable vs. Immutable Header fields (IPv4)

Field	Immutable	Mutable	Predictable	Comment
Version	✓			
Internet header length	✓			
Total length	✓			
Identification	✓			
Protocol	✓			
Source address	✓			
Destination address	✓			Without loose or strict source routing.
Type of service (TOS)		✓		
Flags		✓		
Time to Live(TTL)		✓		
Header checksum		✓		
Destination address			✓	With loose or strict source routing.
Fragment offset			✓	Excluded from ICV

Encapsulating Security Payload (ESP) Protocol

- ESP security protocol selectively affords the confidentiality service or authentication service to IP traffic.
- In transport mode, ESP secures upper-layer protocols.
- In tunnel model, ESP extends protection to the inner IP header.

ESP in Transport Mode (IPv4)



ESP in Transport Mode (IPv6)

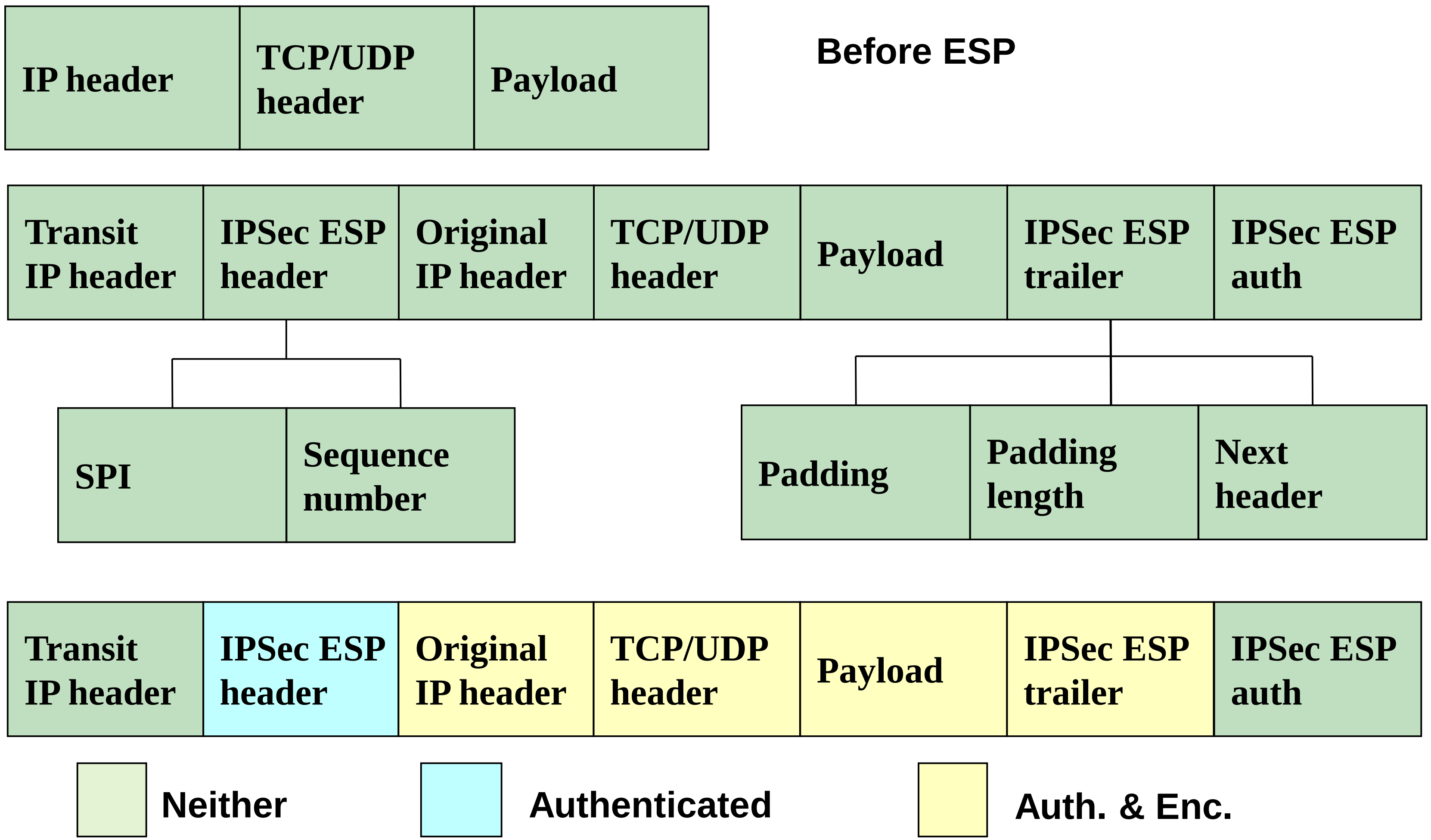
IP header	Extension Headers	TCP/UDP header	Payload	**Before ESP**

IP header	Extension Headers	IPSec ESP header	TCP/UDP header	Payload	IPSec ESP trailer	IPSec ESP auth

IP header	Extension Headers	IPSec ESP header	TCP/UDP header	Payload	IPSec ESP trailer	IPSec ESP auth

Neither **Authenticated** **Auth. & Enc.**

ESP in Tunnel Mode (IPv4)



ESP in Tunnel Mode (IPv6)

IP header	Extension Headers	TCP/UDP header	Payload

Before ESP

Transit IP header	Ext. Headers	IPSec ESP header	Original IP header	Ext. Headers	TCP/UDP header	Payload	IPSec ESP trailer	IPSec ESP auth

Transit IP header	Ext. Headers	IPSec ESP header	Original IP header	Ext. Headers	TCP/UDP header	Payload	IPSec ESP trailer	IPSec ESP auth

Neither Authenticated Auth. & Enc.

IPSec Policy Based Approach

- IPSec follows a policy-based approach to enforce the local security decisions of a system.
- Policy-based security enables an administrator to specify the local security requirements of a system through a policy database.
- IPSec consults this database and provides security protection to traffic so as to satisfy the local system policy.

IPSec Policy

- IPSec policy file contains a list of entries, each having three attributes:
  - *IPSec policy option*
  - *Selector*
  - *Security Association*

IPSec Policy Options

- IPSec policy options specifies the security protections, if any, that IPSec should afford to the traffic.
- Three IPSec policy choices when processing an IP packet:
  - *Discard packet*
  - *Protecting the packet with the AH and the ESP security Protocols.*
  - *Letting the packet bypass the IPSec processing.*

IPSec Policy Options

- Discard Policy Option prevents the packet from exiting an IP host, being delivered to an upper-layer protocol in a host, or transiting through a security gateway.
- Protect policy option instructs IPSec to afford AH, ESP, or a combination of AH and ESP to the packet before the packet exits a host or transits via a security gateway.
- Bypass policy option informs IPSec that the packet should leave the IPSec environment without any processing.

Selectors

Selectors map IP traffic to IPSec policies based on information in an IP header and higher-layer protocols.

Parameter	Description
Destination IP address	It is a single address, a range of addresses or a wildcard address. For an address range or wildcards, they allow multiple destination hosts (behind a gateway, firewall etc) share the same security association.
Source IP address	It is a single address, a range of addresses or a wildcard address. For an address range or wildcards, they allow multiple source systems (behind a gateway, firewall etc) share the same security association.
Name	It is a user identifier or a system name.
Transport layer protocol	It specifies the protocol number for the upper-layer protocol, such TCP and UDP.
Source and destination ports	It is an individual TCP or UDP port value, an enumerated list of ports, or a wildcard port.

Example

Protocol	Source IP	Source Port	Destination IP	Destination Port	Action	Comments
UDP	10.1.2.156	500	*	500	Bypass	IKE

It allows UPD traffic from 10.1.2.156 via 500 to bypass the checking and reach the destination hosts. This traffic is for IKE packets.

Security Associations (SA)

- SA is a simplex (unidirectional), logical connection that provides security services to a traffic stream between two IP nodes.
- An SA serves as a contract between two or more entities and completely specifies how they use security services to communicate securely.

Security Association

- An SA specifies a number of parameters, such as the AH authentication algorithm, the ESP encryption algorithm, the ESP authentication algorithm, keys, IVs, IPSec protocol transport or tunnel mode and lifetime.

SA Lifetime

- The lifetime of an SA is the interval after which the SA is no longer valid and must be terminated.
- If the key-management scheme uses PKI certificate for the identification of a peer node, the lifetime of the established SA must not exceed the valid period of the certificate.

IPSec Internet Key Exchange (IKE) Protocols

The IKE protocol operates in two phases

- IKE establishes an SA to secure its own traffic.
- It establishes another SA to provide security to application data.

IKE Phases

- Phase 1
  - *Mutual authentication and key establishment.*
  - *It's known as the ISAKMP SA, or sometimes it is referred to as the IKE SA.*
- Phase 2
  - *Establishment of ESP or AH SA.*

IKE Phase 1

- There are two types of Phase 1 exchanges, called modes:
  - *Aggressive mode*
    - Mutual authentication and session key establishment in three messages.
  - *Main mode*
    - Use six messages
    - Has additional functionality such as the ability to hide endpoint identifiers from eavesdroppers and additional flexibility in negotiating cryptographic algorithms.

IKE Phase 1 – Main Mode

Initiator (Alice) **Responder (Bob)**

CKY-A, <list> →

← **CKY-A, CKY-B, <algo>**

negotiation

CKY-A, CKY-B, g^x, N_A →

← **CKY-A, CKY-B, g^y, N_B**

key exchange

CKY-A, CKY-B, $\{A, Sig_A(M_{AB})\}_{Ke}$ →

← **CKY-A, CKY-B, $\{B, Sig_B(M_{BA})\}_{Ke}$**

authentication

- CKY: cookie
- KM: derived from (N_A | N_B, g^{xy})
- K_e: derived from KM
- M_{AB}: MAC_{KM}(g^x | g^y | CKY-A | CKY-B | <list> | A)
- M_{BA}: MAC_{KM}(g^y | g^x | CKY-B | CKY-A | <list> | B)

IKE Phase 1 – Aggressive Mode

Initiator (Alice) **Responder (Bob)**

CKY-A, <list>, g^x, N_A, A

CKY-A, CKY-B, <algo>, g^y, N_B, B, $Sig_B(M_{BA})$

CKY-A, CKY-B, $Sig_A(M_{AB})$

- Only three message flows
- No identity protection

Features of IKE

- Cookies are used to avoid denial of service attacks which exploit the computational expense of calculating keys.
  - *The idea is to force legitimate parties to carry out a cookie exchange before significant computations are carried out.*
- Parameters for the Diffie-Hellman key exchange can be negotiated.
  - *Including the group, with the option of some Elliptic curve based DH exchanges possible.*
  - *Public keys for DH can be exchanged, with authenticity to avoid man-in-the-middle attacks.*
- Nonces are used to protect against replay attacks.

IKE Phase 2

- Once an IKE SA is setup between **A** and **B**, either A or B can initiate an IPSec SA through the ”quick mode” exchange.
- The **quick mode** exchange establishes an ESP and/or AH/SA, which involves negotiating crypto parameters, optionally doing a Diffie-Hellman exchange.

IKE Phase 2

1. A $\leftarrow\rightarrow$ B: phase-1 SA
2. A $\rightarrow$ B: X, Y, CP, SPI_A, N_A, [g^a mod p]
3. B $\rightarrow$ A: X, Y, CPA, SPI_B, N_B, [g^b mod p]
4. A $\rightarrow$ B: X, Y, ack

- X: contains cookies from Phase 1.
- Y: distinguishes Phase 2 session from others.
- CP: is crypto proposal, CPA is crypto proposal accepted.
- ack: means ready to accept now.

All messages are protected with encryption and integrity keys from Phase 1.

Comparing IPSec, SSL/TLS, SSH

- All three have initial (authenticated) key establishment then key derivation.
  - *IKE in IPSec*
  - *Handshake Protocol in SSL/TLS (can be unauthenticated!)*
  - *Authentication Protocol in SSH*
- All protect cipher suite negotiation.
- All three use keys established to build a “secure channel”.

Comparing IPSec, SSL/TLS, SSH

- Operate at different network layers.
  - *This brings pros and cons for each protocol suite.*
  - *Recall "Where shall we put security?"*
  - *Naturally support different application types, can all be used to build VPNs.*
- All practical, but not simple.
  - *Complexity leads to vulnerabilities.*
  - *Complexity makes configuration and management harder.*
  - *Complexity can create computational bottlenecks.*
  - *Complexity necessary to give both flexibility and security.*