Cristina Nita-Rotaru

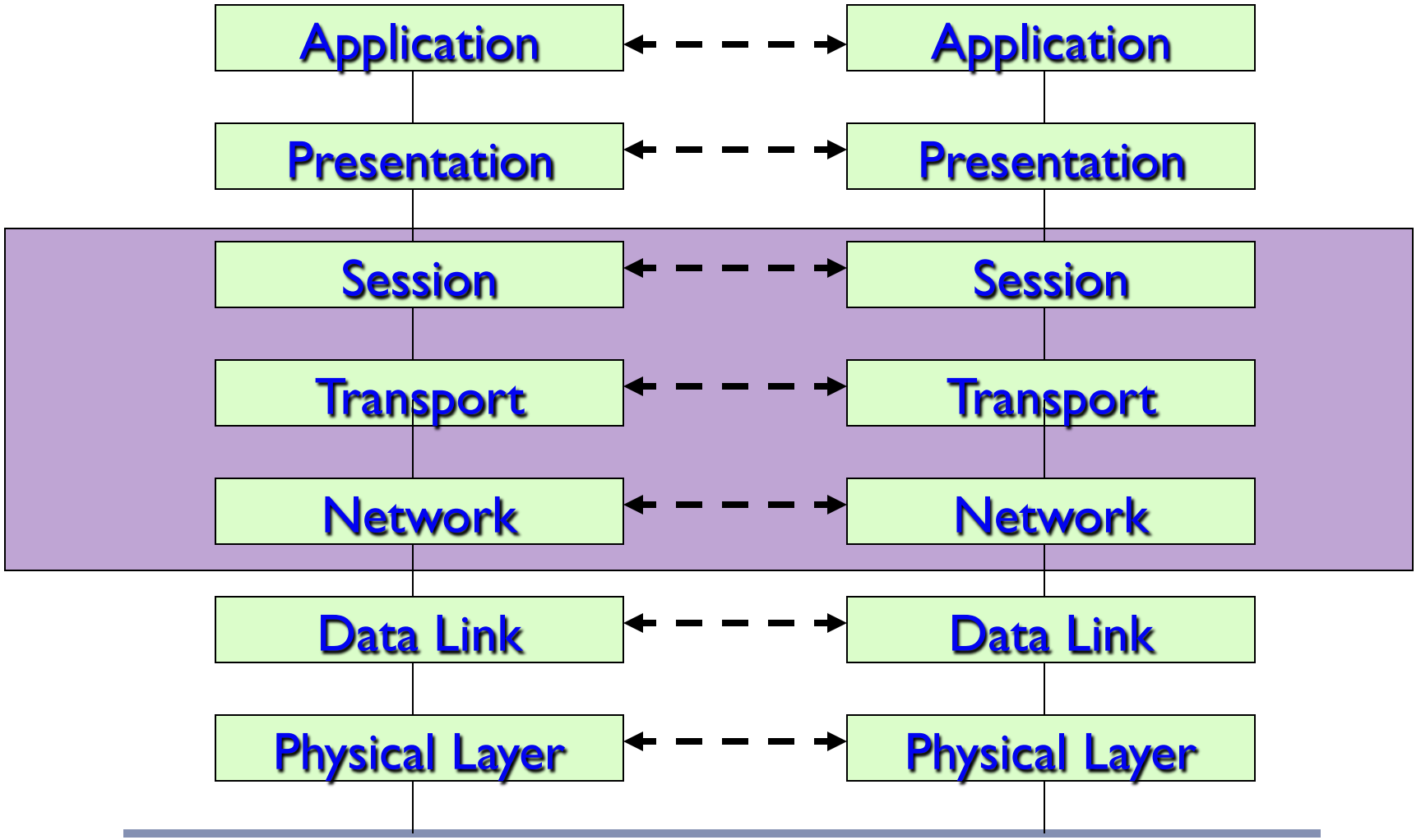
CS355: Cryptography

Lecture 20: IPSEC.

Before Securing a Protocol…

- Understand what is does
- Define what are the security goals
- Define what is the attacker model
- Understand/examine the environment in which the protocol will be used

OSI/ISO Model



Internet Protocol - IP

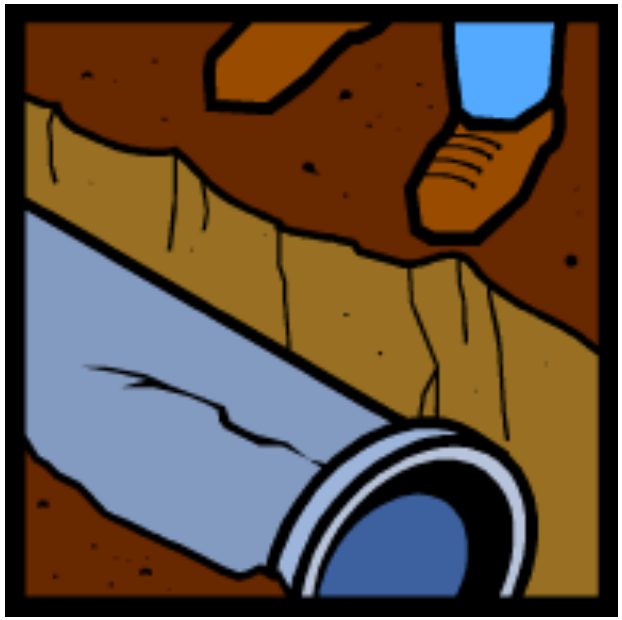
- IP is the current **delivery** protocol on the Internet, between **hosts**.
- IP provides ‘best effort’, unreliable delivery of packets.
- There are two versions:
  - IPv4 is the current routing protocol on the Internet
  - IPv6, a newer version, still not totally embraced by the community

Transport Protocols

- Provides communication between **processes** running on hosts.
- The most common transport protocols are **UDP and TCP.**
- OS provides support for developing applications on top of UDP and TCP.

Establishing a ``Secure Channel''

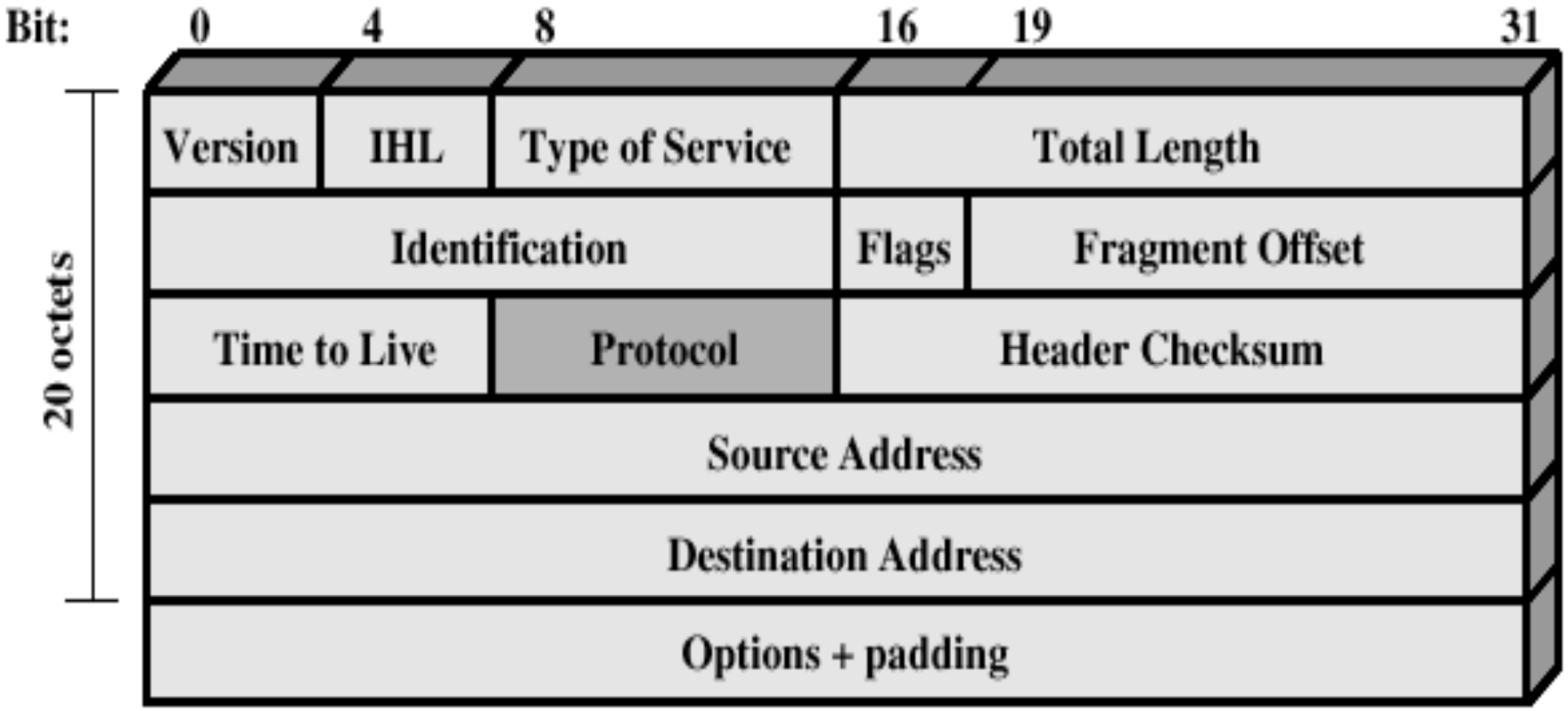
- Services provides: confidentiality, integrity and authentication
- At what level in the stack?
- What are advantages disadvantages based on the level
- Two protocols: SSL (TLS) and IPSec



What is IPSec ?

- Set of security mechanisms to protect the IP protocol
- Flexible: supports combinations of authentication, integrity, access control, and confidentiality
- Documented in RFCs and Internet drafts

IPv4 Header


Bit:
0
4
8
16
19
31
Version
IHL
Type of Service
Total Length
Identification
Flags
Fragment Offset
Time to Live
Protocol
Header Checksum
Source Address
Destination Address
Options + padding
20 octets

IPSec Overview

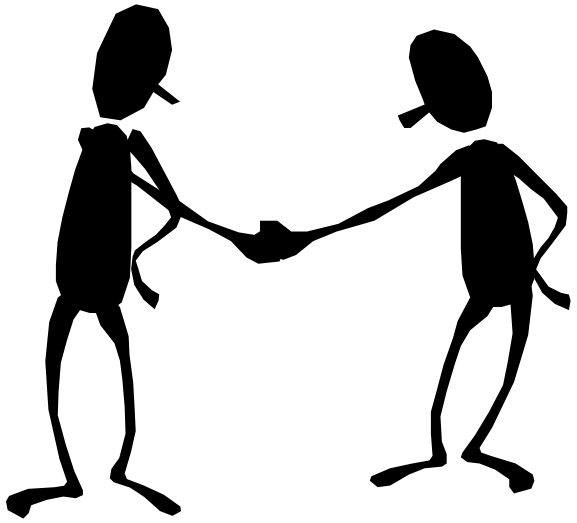
- Transparent to applications (below transport layer (TCP, UDP)
- Facilitate direct IP connectivity between sensitive hosts through untrusted networks
- Provides:
  - access control
  - integrity
  - data origin authentication
  - rejection of replayed packets
  - confidentiality
- Provide application-independent security
- No substitute for application layer security !!!
- **No protection against traffic analysis attacks !!!**

Security Mechanisms

- **Authentication Header (AH):** provides integrity and authentication without confidentiality
- **Encapsulating Security Payload (ESP)**: provides confidentiality and can also provide integrity and authentication
- Operates based on security associations
- **Tunnel-mode**: encapsulates an entire IP datagram
- **Transport-mode**: encapsulates an upper-layer protocol (e.g. TCP or UDP) and prepends an IP header in clear

	Transport Mode	Tunnel Mode
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.

Security Associations (SA)



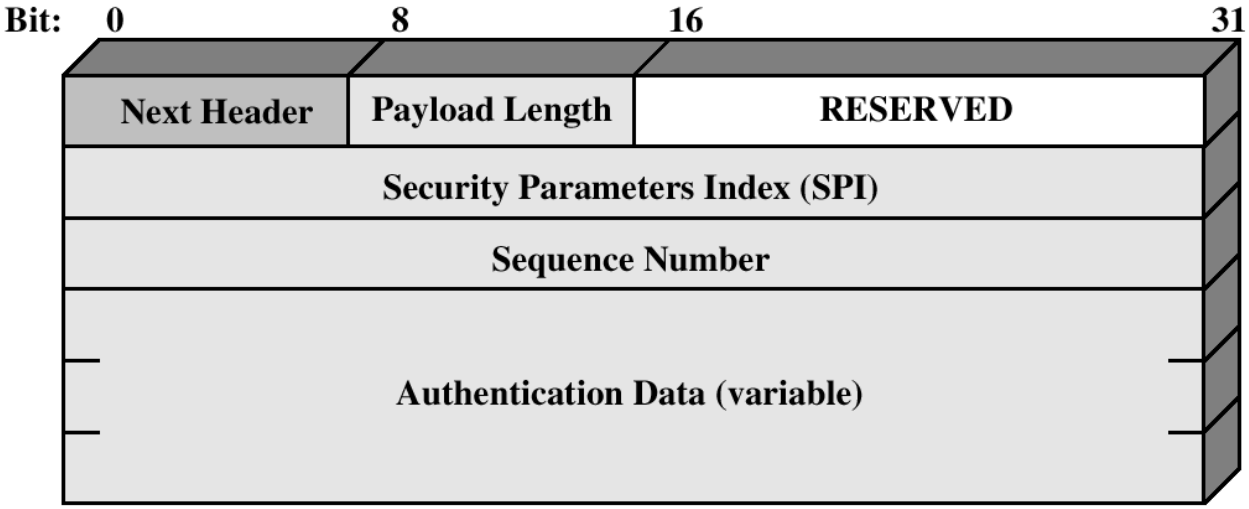
- A relationship between a sender and a receiver.
- Identified by two parameters:
  - Security Parameter Index (SPI)
  - IP Destination address
- Being established through the key management protocol outside the IP security protocol
- SPI + IP destination address uniquely identifies a particular Security Association
- SAs are unidirectional, sender supplies SPI to receiver

Parameters of a Security Association

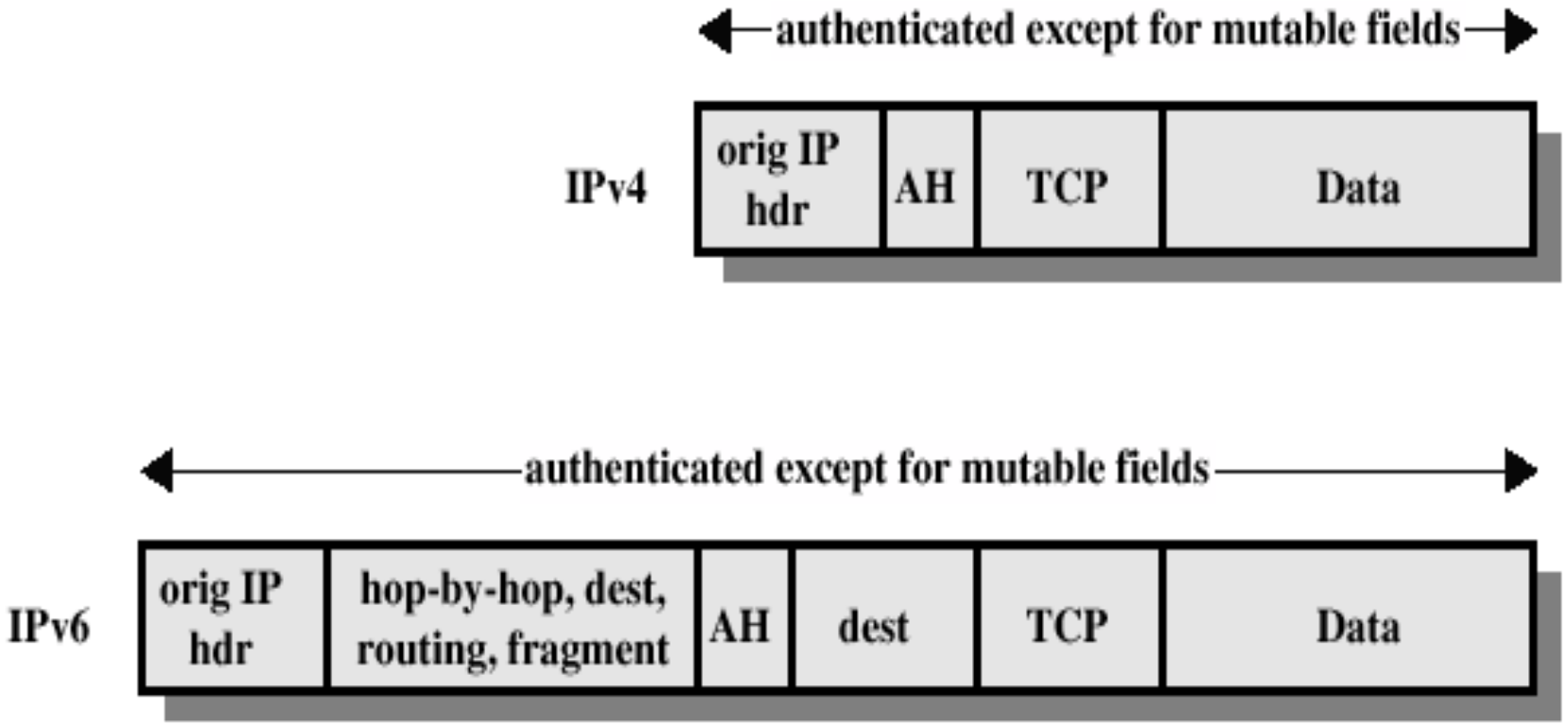
- Authentication algorithm and mode for AH
- Encryption algorithm, algorithm mode, initialisation vector, and transform for ESP
- Key(s) and key lifetimes used with ESP and AH
- Lifetime of the Security Association
- Authentication algorithm with ESP (if used)
- Sensitivity level of protected data

Authentication Header

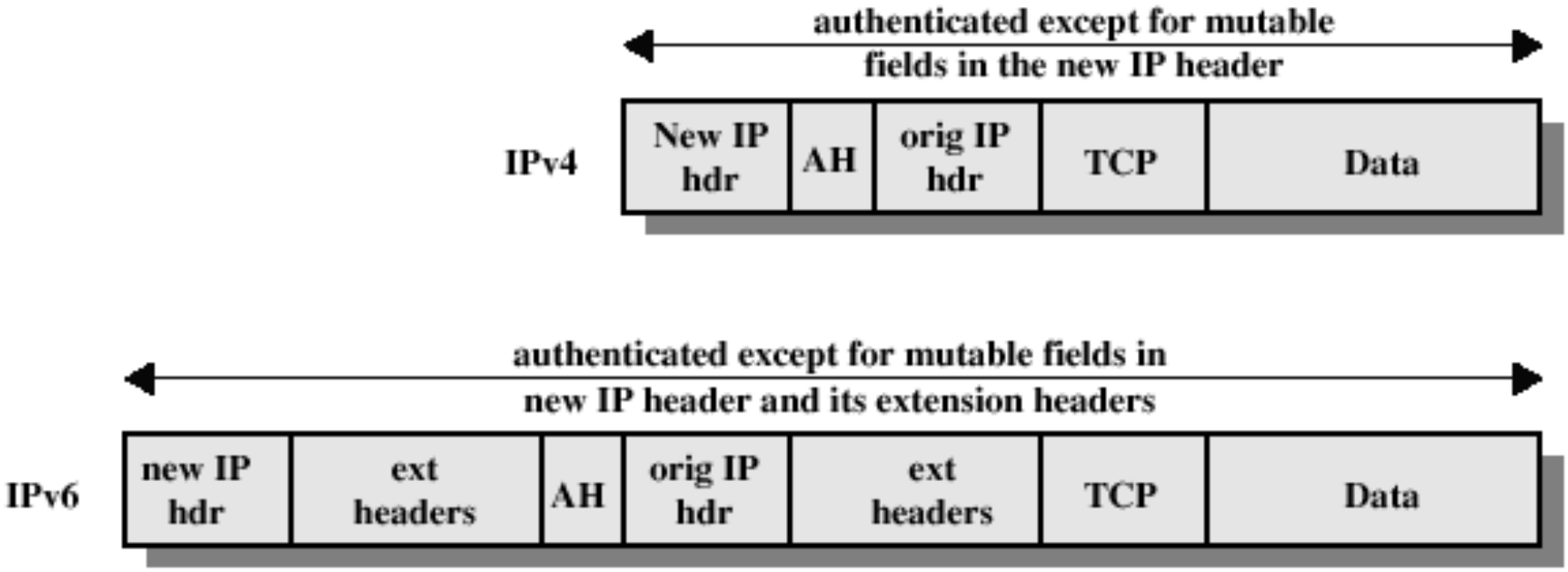
- Provides support for data integrity and authentication (MAC code) of IP packets.
- Guards against replay attacks.
- Integrity and data source authentication provided using HMAC (requires a secret key shared between source and destination)
- Non-repudation can be provided if using digital signatures



AH Authentication: Transport Mode



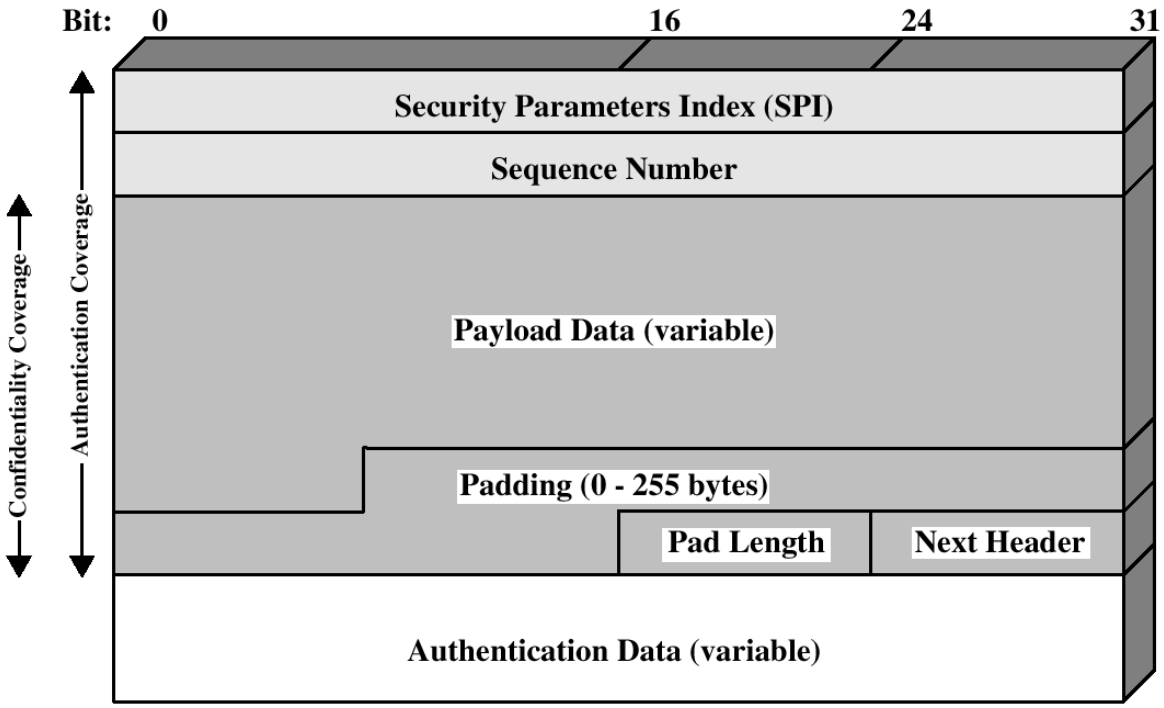
AH Authentication: Tunnel Mode



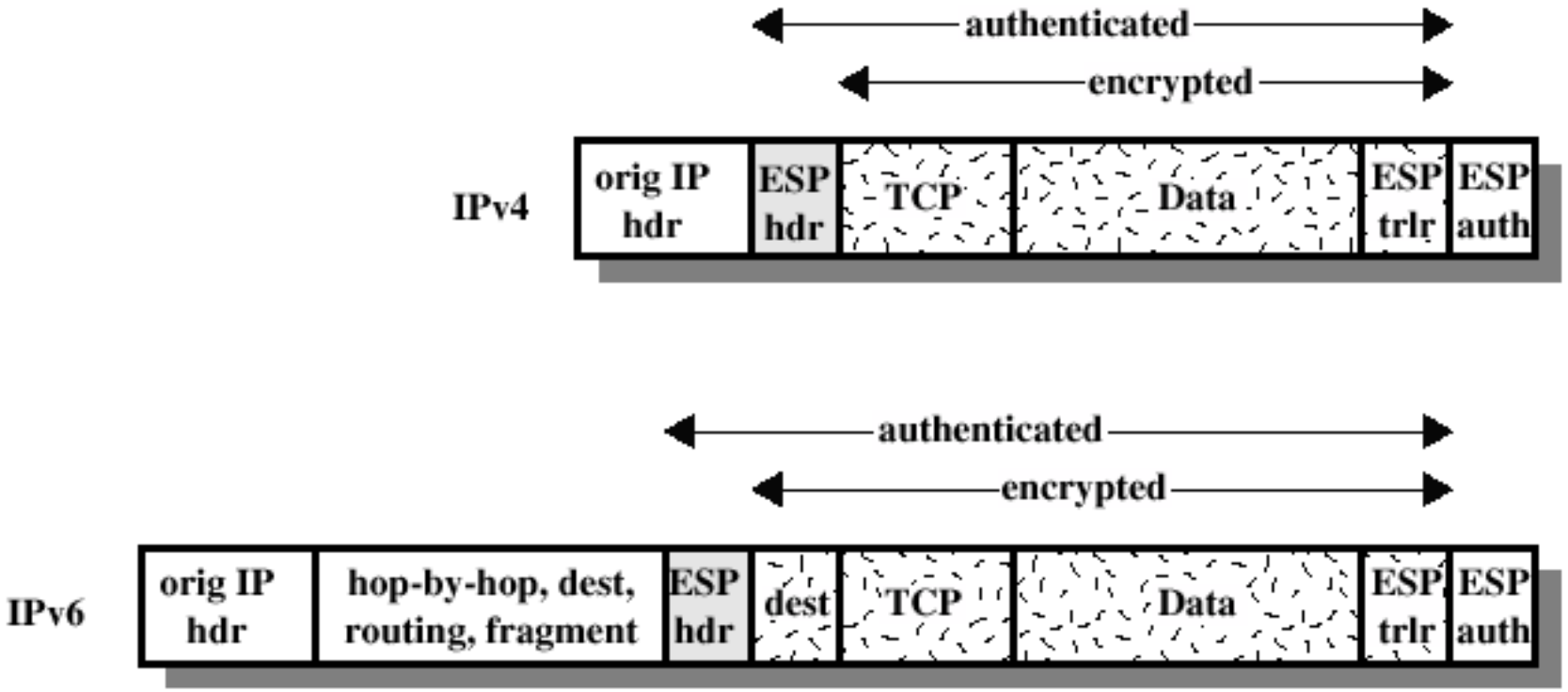
The new IP header contains different IP addresses than the ultimate destination and source

Encapsulating Security Payload

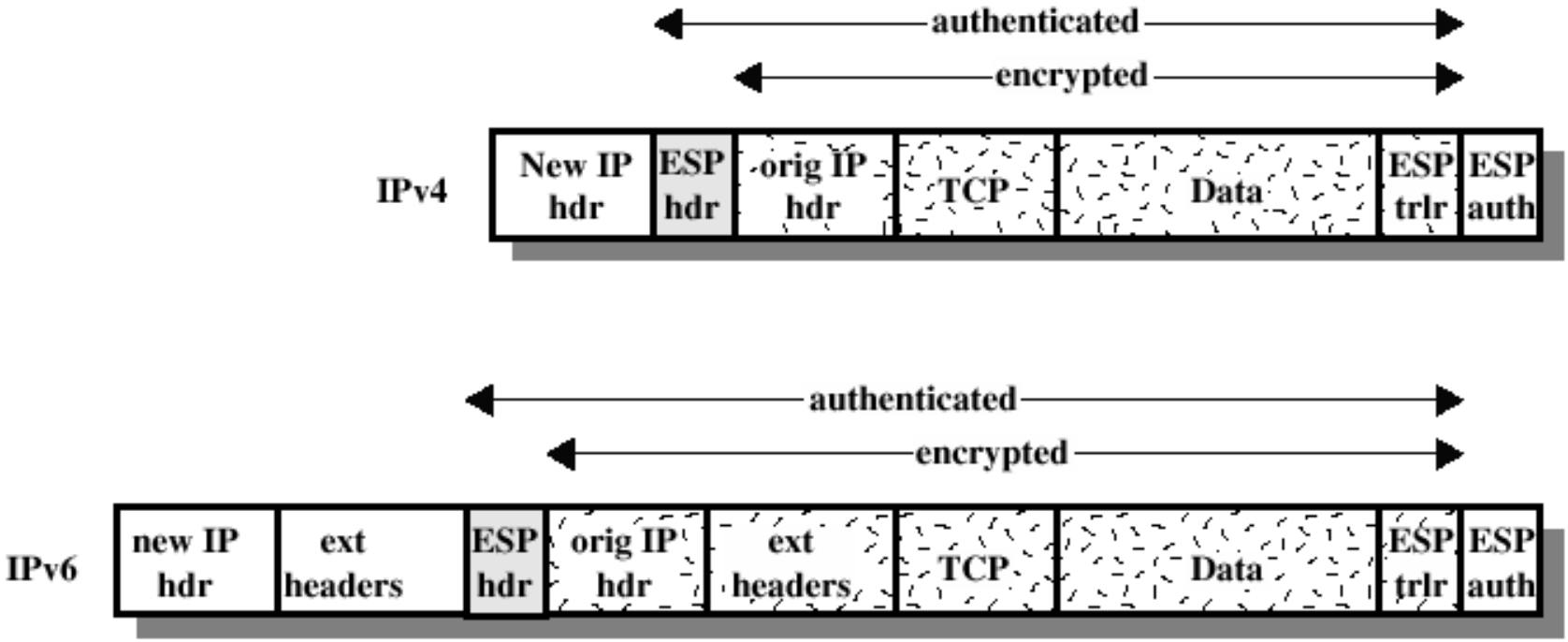
- ESP provides confidentiality services



ESP Encryption and Authentication: Transport Mode

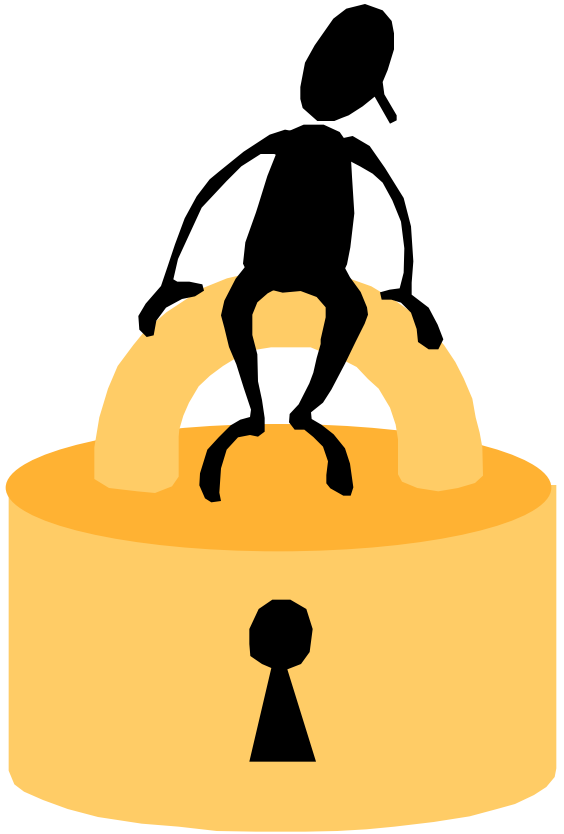


ESP Encryption and Authentication: Tunnel Mode



Cryptographic Algorithms

- Encryption:
  - Three-key triple DES
  - RC5
  - IDEA
  - Three-key triple IDEA
  - CAST
  - Blowfish
- Authentication:
  - HMAC-MD5
  - HMAC-SHA-1

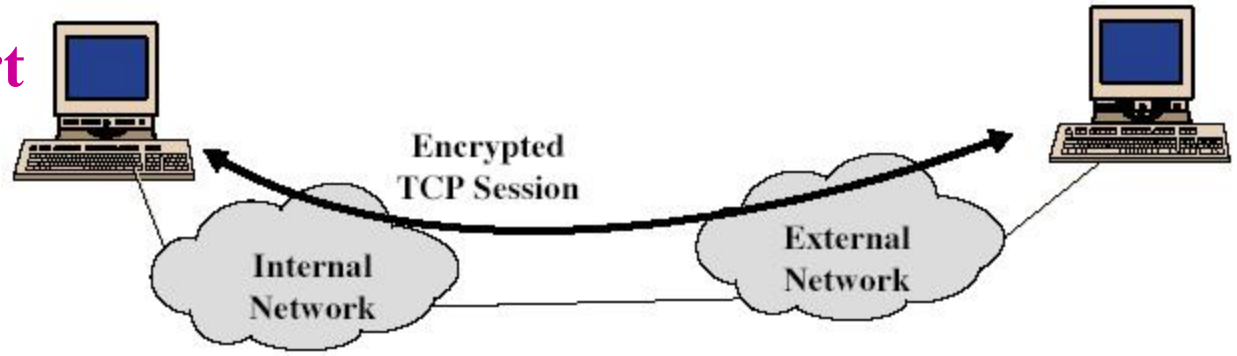


Defending Against Replay Attacks

- Based on the sequence number (32 bits) carried in every packet
- For every packet the sequence number is incremented
- The receiver maintains a window (32 or more), window is moved only when received packets verified: “packets are authenticated and sequence number is in the window”
- Duplicates are rejected!

Transport vs. Tunnel Mode

Transport



Tunnel