Cryptography and Network Security

Third Edition

by William Stallings

Lecture slides by Lawrie Brown

The need...

- In CERTs 2001 annual report it listed 52,000 security incidents
- the most serious involving:
  - IP spoofing
    - intruders creating packets with false address then taking advantages of OS exploits
  - eavesdropping and sniffing
    - attackers listen for userids and passwords and then just walk into target systems
  - as a result the IAB included authentication and encryption in the next generation IP (IPv6)

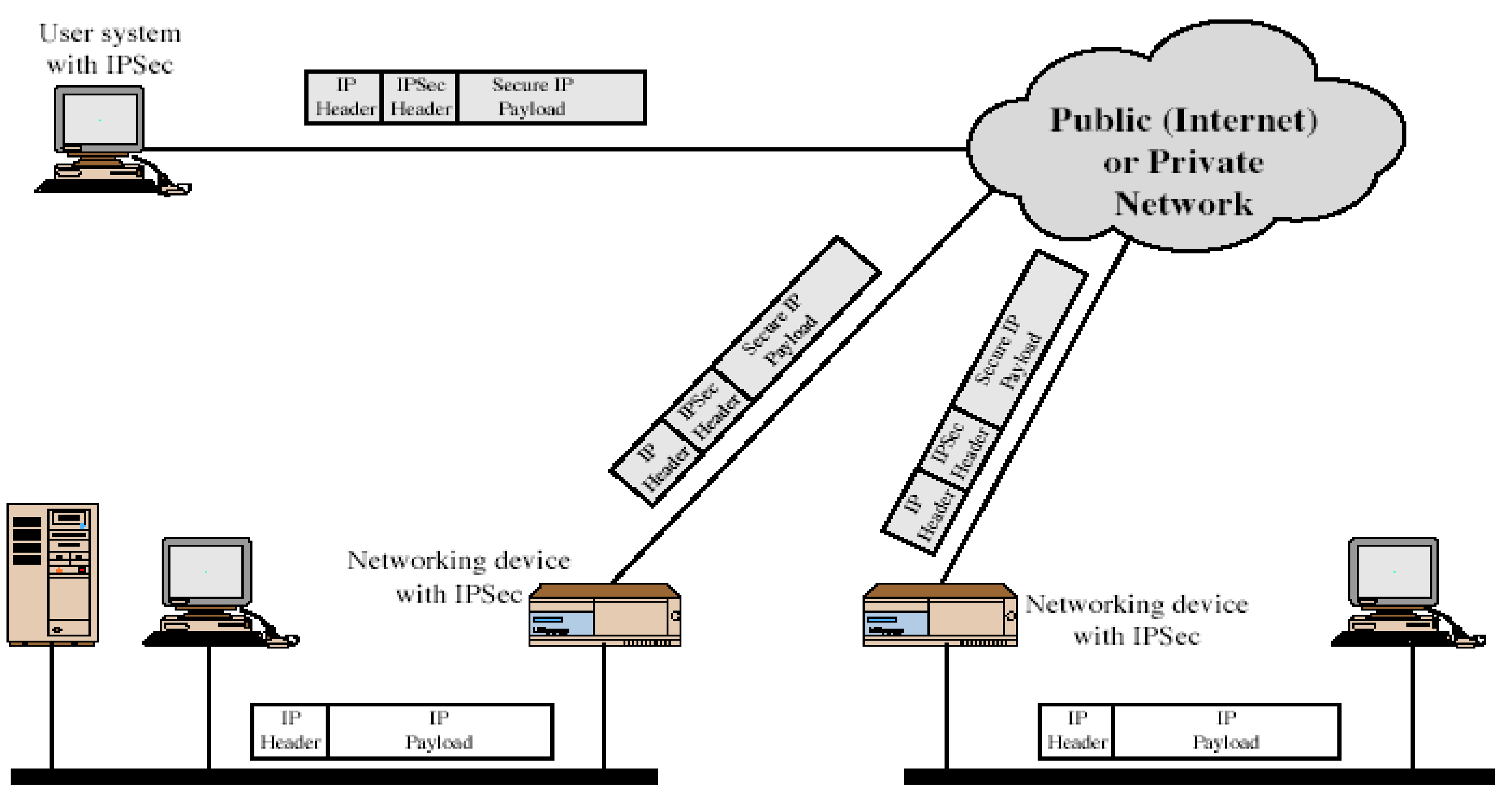
IP Security

- We’ve considered some application specific security mechanisms
  - eg. S/MIME, PGP, Kerberos, SSL/HTTPS
- however there are security concerns that cut across protocol layers
- would like security implemented by the network for all applications

IPSec

- general IP Security mechanisms
- provides
  - authentication
  - confidentiality
  - key management
- applicable to use over LANs, across public & private WANs, & for the Internet

IPSec Uses


User system with IPSec
IP Header
IPSec Header
Secure IP Payload
Public (Internet) or Private Network
IP Header
IPSec Header
Secure IP Payload
IP Header
IPSec Header
Secure IP Payload
Networking device with IPSec
Networking device with IPSec
IP Header
IP Payload
IP Header
IP Payload

Benefits of IPSec

- in a firewall/router provides strong security to all traffic crossing the perimeter
- is resistant to bypass
- is below transport layer, hence transparent to applications
- can be transparent to end users
- can provide security for individual users if desired
- additionally in routing applications:
  - assure that router advertisments come from authorized routers
  - neighbor advertisments come from authorized routers
  - insure redirect messages come from the router to which initial packet was sent
  - insure no forging of router updates

IP Security Architecture

- RFC 2401 (Primary RFC)
- specification is quite complex
- defined in numerous RFC’s
  - incl. RFC 2401/2402/2406/2408
  - many others, grouped by category
- mandatory in IPv6, optional in IPv4

IPSec Services

- Two protocols are used to provide security:
  - Authentication Header Protocol (AH)
  - Encapsulation Security Payload (ESP)
- Services provided are:
  - Access control
  - Connectionless integrity
  - Data origin authentication
  - Rejection of replayed packets
    - a form of partial sequence integrity
  - Confidentiality (encryption)
  - Limited traffic flow confidentiality

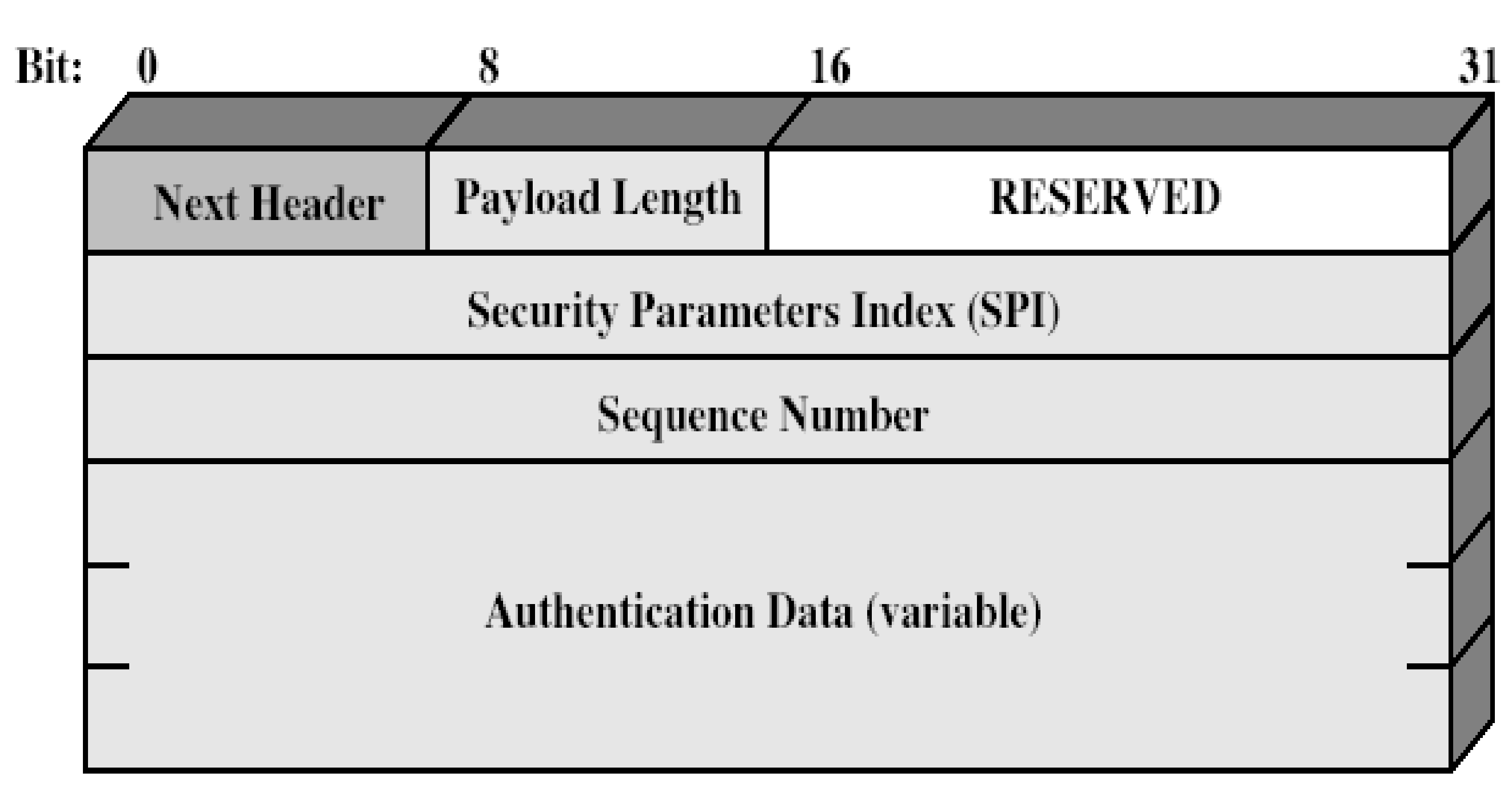
Security Associations

- a one-way relationship between sender & receiver that affords security for traffic flow
- identified by 3 parameters:
  - Security Parameters Index (SPI)
    - a bit string
  - IP Destination Address
    - only unicast allowed
    - could be end user, firewall, router
  - Security Protocol Identifier
    - indicates if SA is AH or ESP
- has a number of other parameters
  - seq no, AH & EH info, lifetime etc
- have a database of Security Associations

Authentication Header (AH)

- RFC 2402
- provides support for data integrity & authentication of IP packets
  - end system/router can authenticate user/app
  - prevents address spoofing attacks by tracking sequence numbers
- based on use of a MAC (message authentication code)
  - HMAC-MD5-96 or HMAC-SHA-1-96
  - MAC is calculated:
    - immutable IP header fields
    - AH header (except for Authentication Data field)
    - the entire upper-level protocol data (immutable)
- parties must share a secret key

Authentication Header

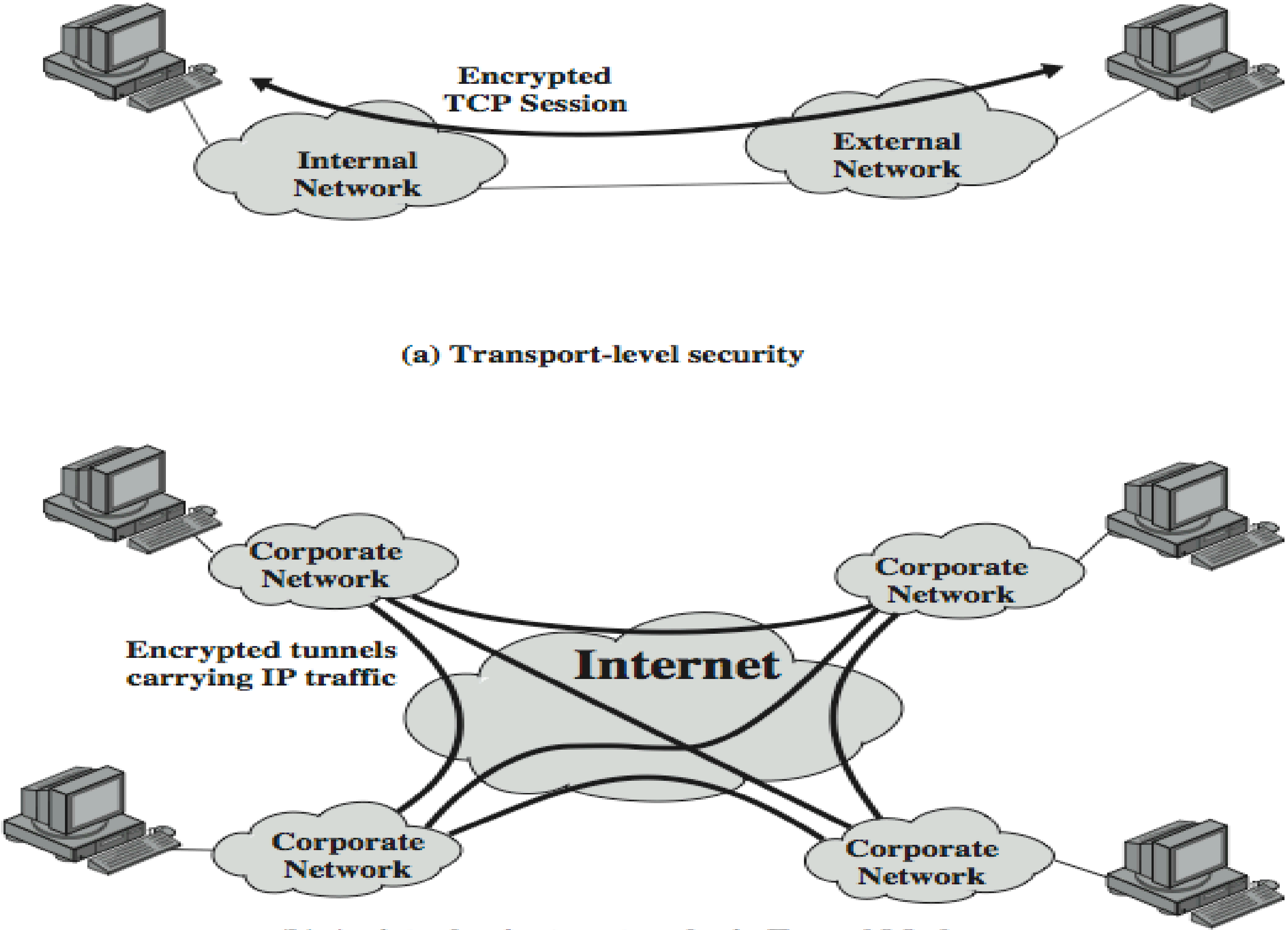


Bit: 0	8	16	31
Next Header	Payload Length	RESERVED	
Security Parameters Index (SPI)			
Sequence Number			
Authentication Data (variable)			

Transport and Tunnel Modes

- Both AH and ESP have two modes
  - transport mode is used to encrypt & optionally authenticate IP data
    - data protected but header left in clear
    - can do traffic analysis but is efficient
    - good for ESP host to host traffic
  - tunnel mode encrypts entire IP packet
    - add new header for next hop
    - good for VPNs, gateway to gateway security

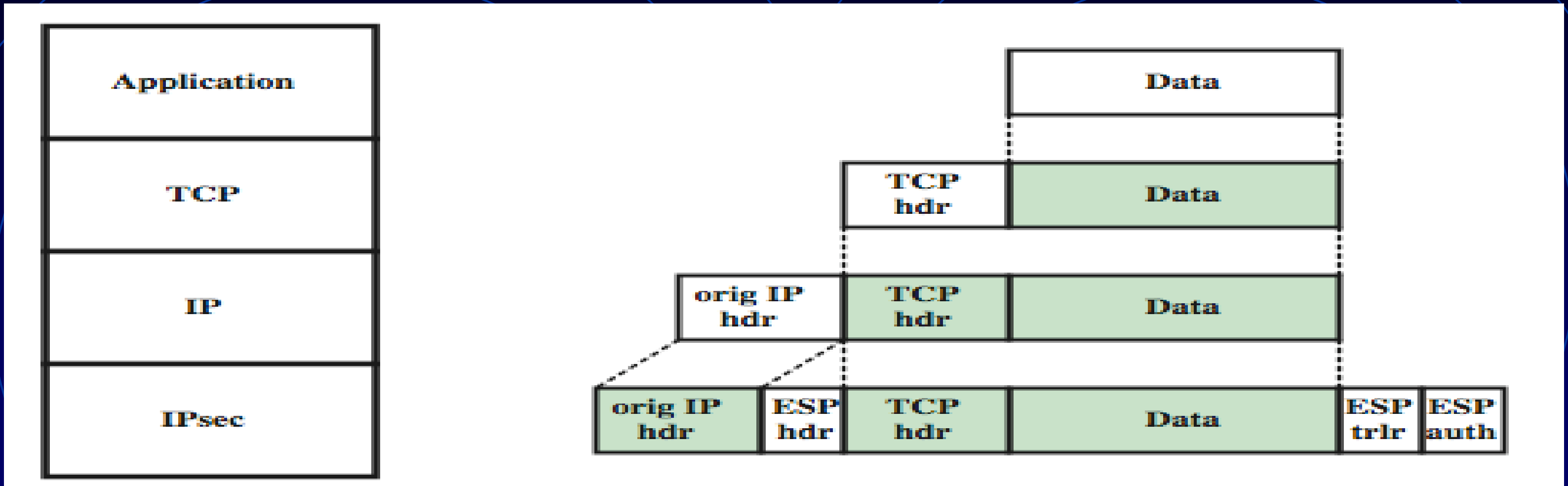
Transport & Tunnel Modes



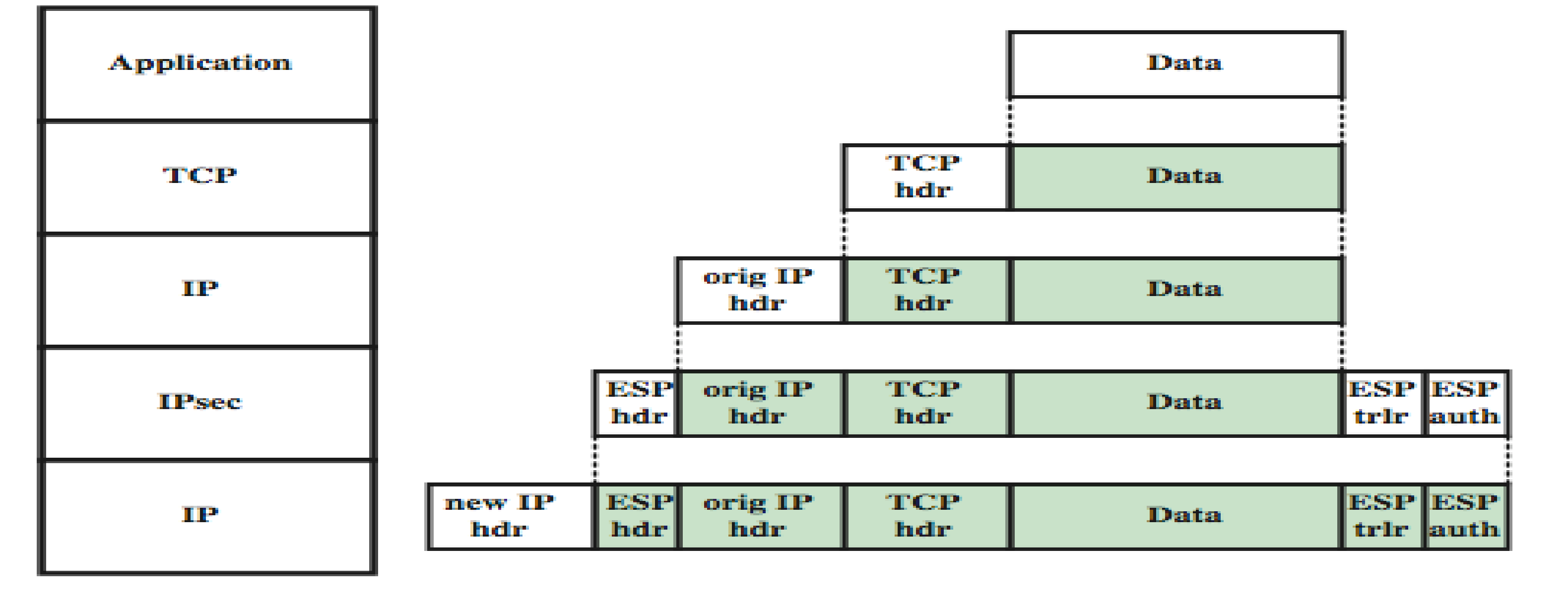
(a) Transport-level security

(b) A virtual private network via Tunnel Mode

Transport & Tunnel Modes



(a) Transport mode

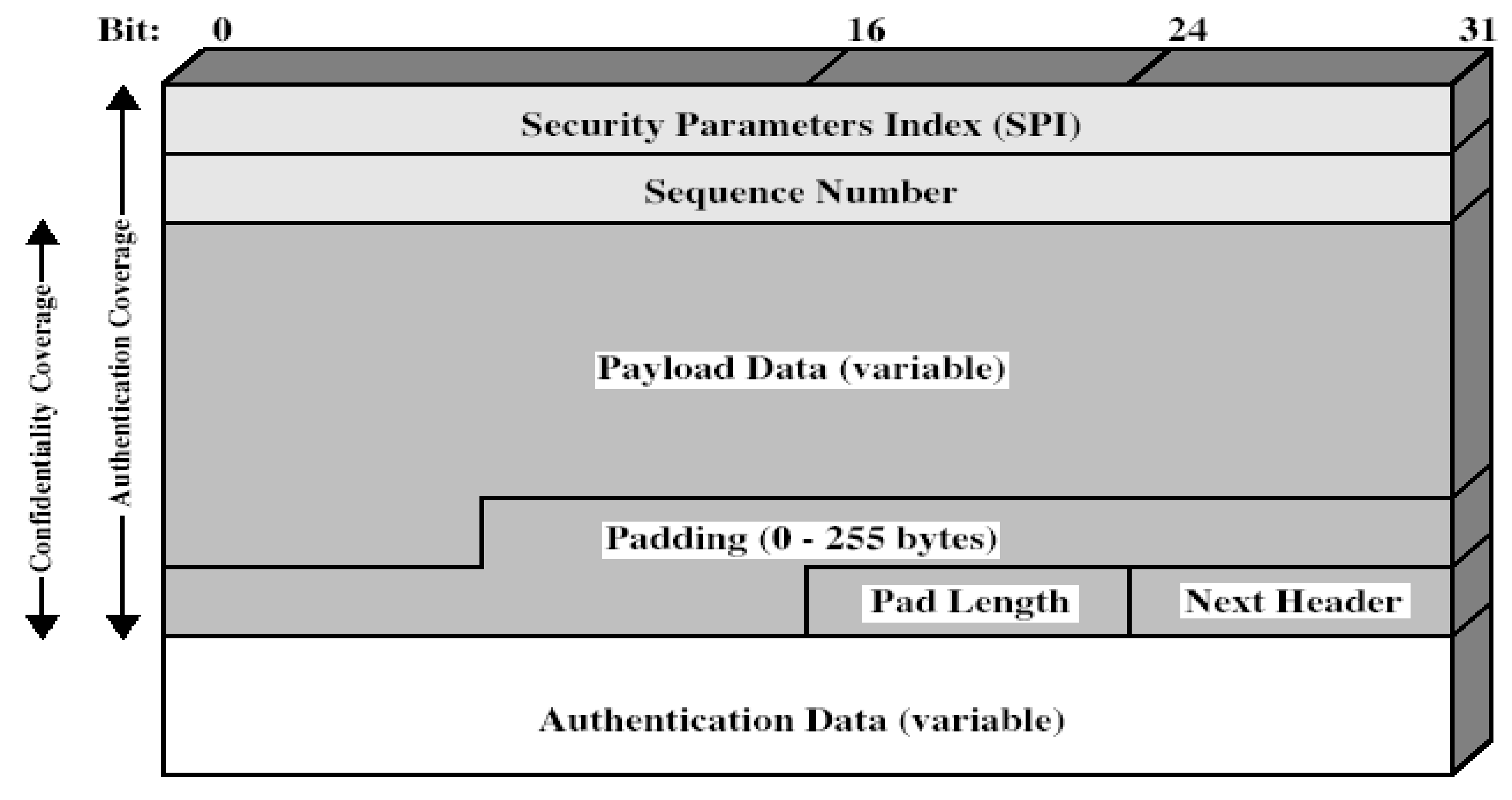


(b) Tunnel mode

Encapsulating Security Payload (ESP)

- RFC 2406
- provides message content confidentiality & limited traffic flow confidentiality
- can optionally provide the same authentication services as AH
- supports range of ciphers, modes, padding
  - incl. DES, Triple-DES, RC5, IDEA, CAST etc
  - CBC most common
  - pad to meet blocksize, for traffic flow

Encapsulating Security Payload



Bit: 0 16 24 31

Security Parameters Index (SPI)

Sequence Number

Payload Data (variable)

Padding (0 - 255 bytes)

Pad Length

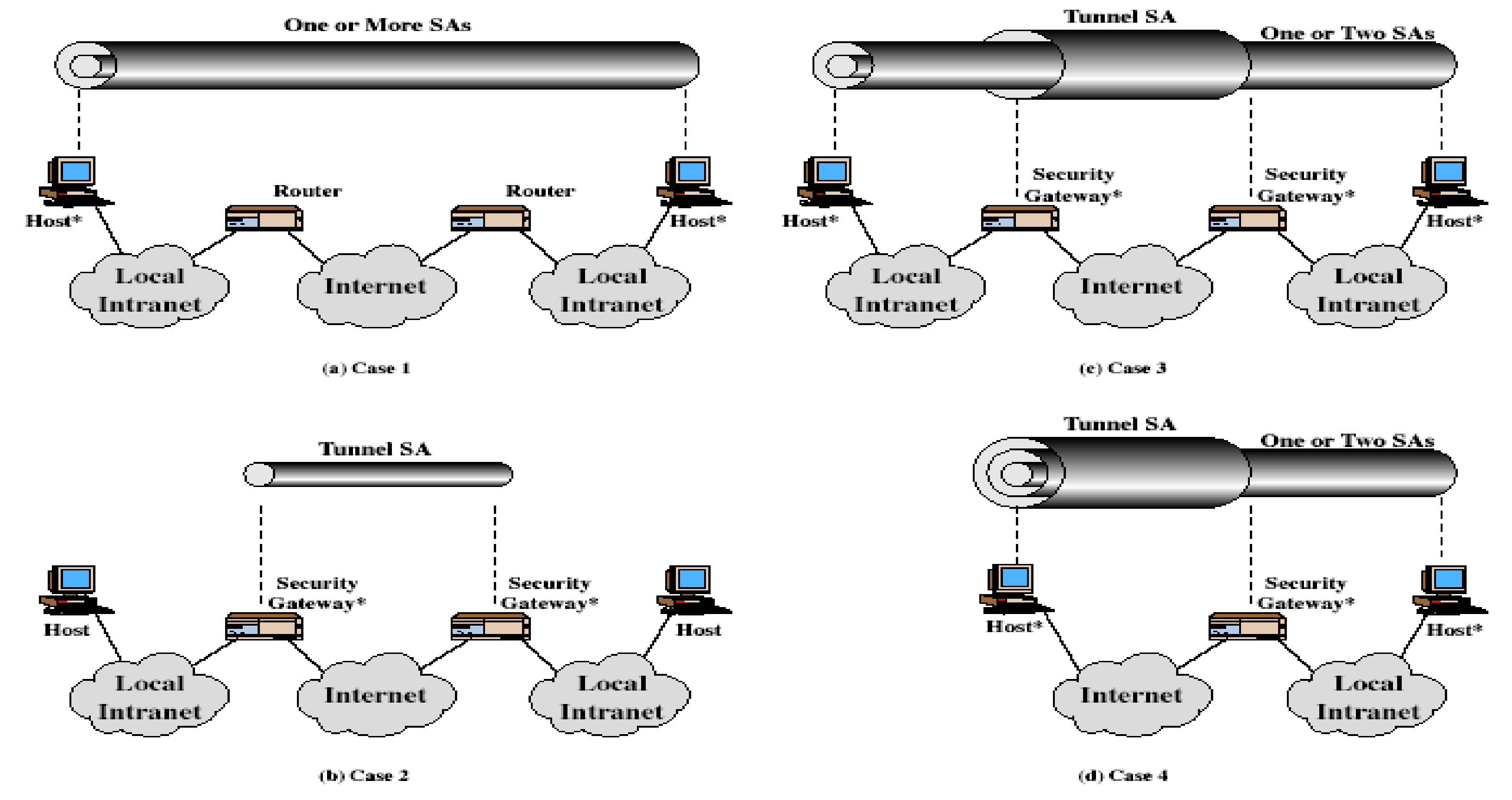
Next Header

Authentication Data (variable)

Combining Security Associations

- SA’s can implement either AH or ESP
- to implement both need to combine SA’s
  - form a security bundle
- have 4 cases (see next)

Combining Security Associations



(a) Case 1

(c) Case 3

(b) Case 2

(d) Case 4

a. AH in transport mode

b.ESP in transport mode

c. AH followed by ESP in transport mode(ESP SA inside an AH SA

d. any one a, b, c inside an AH or ESP in tunnel mode

Key Management

- handles key generation & distribution
- typically need 2 pairs of keys
  - 2 per direction for AH & ESP
- manual key management
  - sysadmin manually configures every system
- automated key management
  - automated system for on demand creation of keys for SA’s in large systems
  - has Oakley & ISAKMP elements

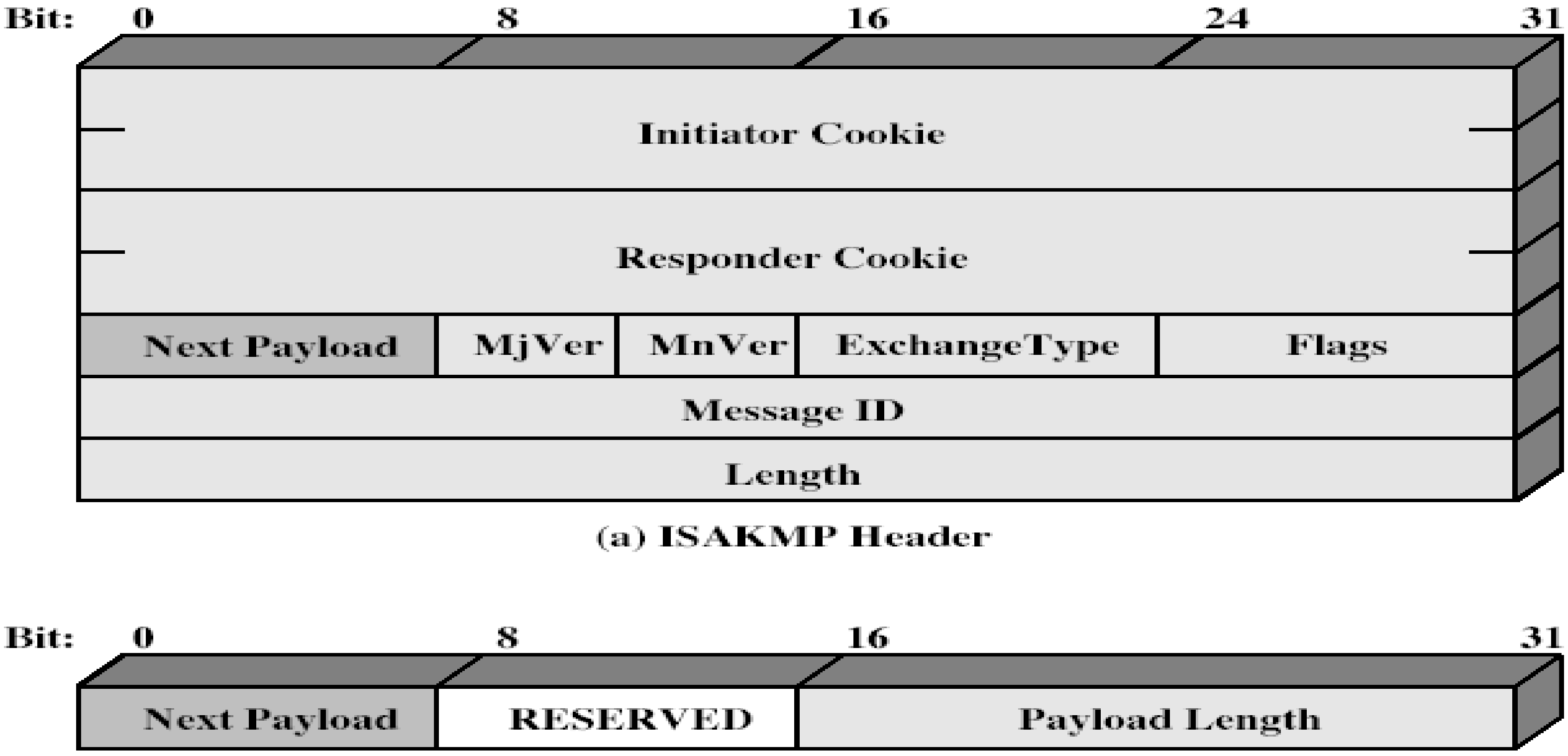
Oakley

- RFC 2412
- a key exchange protocol
- based on Diffie-Hellman key exchange
- adds features to address weaknesses
  - cookies, groups (global params), nonces, DH key exchange with authentication
- can use arithmetic in prime fields or elliptic curve fields

ISAKMP

- Internet Security Association and Key Management Protocol (RFC 2407)
- provides framework for key management
- defines procedures and packet formats to establish, negotiate, modify and delete SAs
- independent of key exchange protocol, encryption algorithm and authentication method

ISAKMP



Bit: 0	8	16	24	31
Initiator Cookie				
Responder Cookie				
Next Payload	MjVer	MnVer	ExchangeType	Flags
Message ID				
Length				

(a) ISAKMP Header

Bit: 0	8	16	31
Next Payload	RESERVED	Payload Length	

(b) Generic Payload Header

Summary

- have considered:
  - IPSec security framework
  - AH Protocol
  - ESP Protocol
  - key management & Oakley/ISAKMP