

Cryptography and Network Security Chapter 16

Fourth Edition
by William Stallings

Lecture slides by Lawrie Brown

The background of the slide features several sets of concentric circles in a lighter shade of purple, resembling ripples in water. These circles are positioned in the lower right and bottom center areas of the slide.

Chapter 16 – IP Security

If a secret piece of news is divulged by a spy before the time is ripe, he must be put to death, together with the man to whom the secret was told.

—*The Art of War*, Sun Tzu



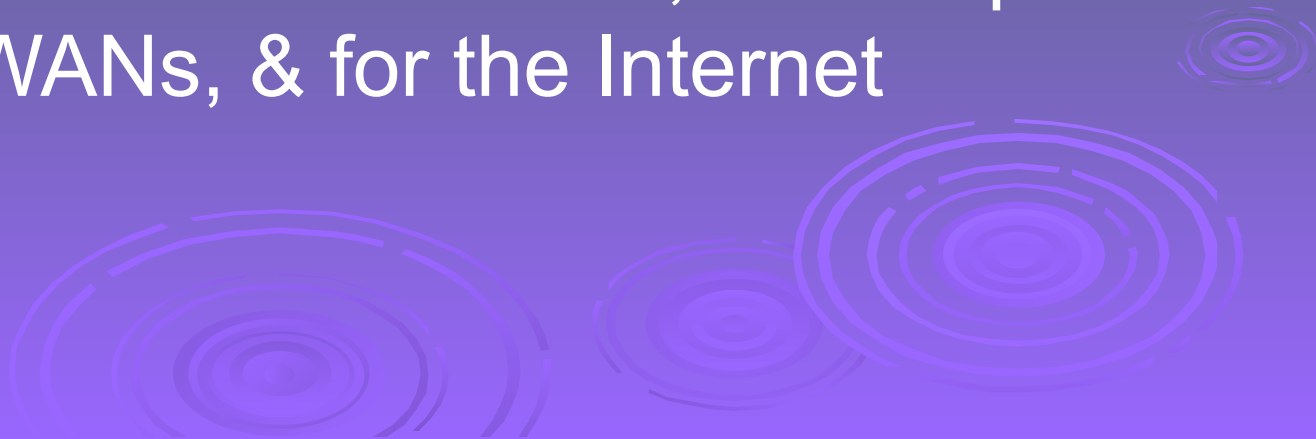
IP Security

- have a range of 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

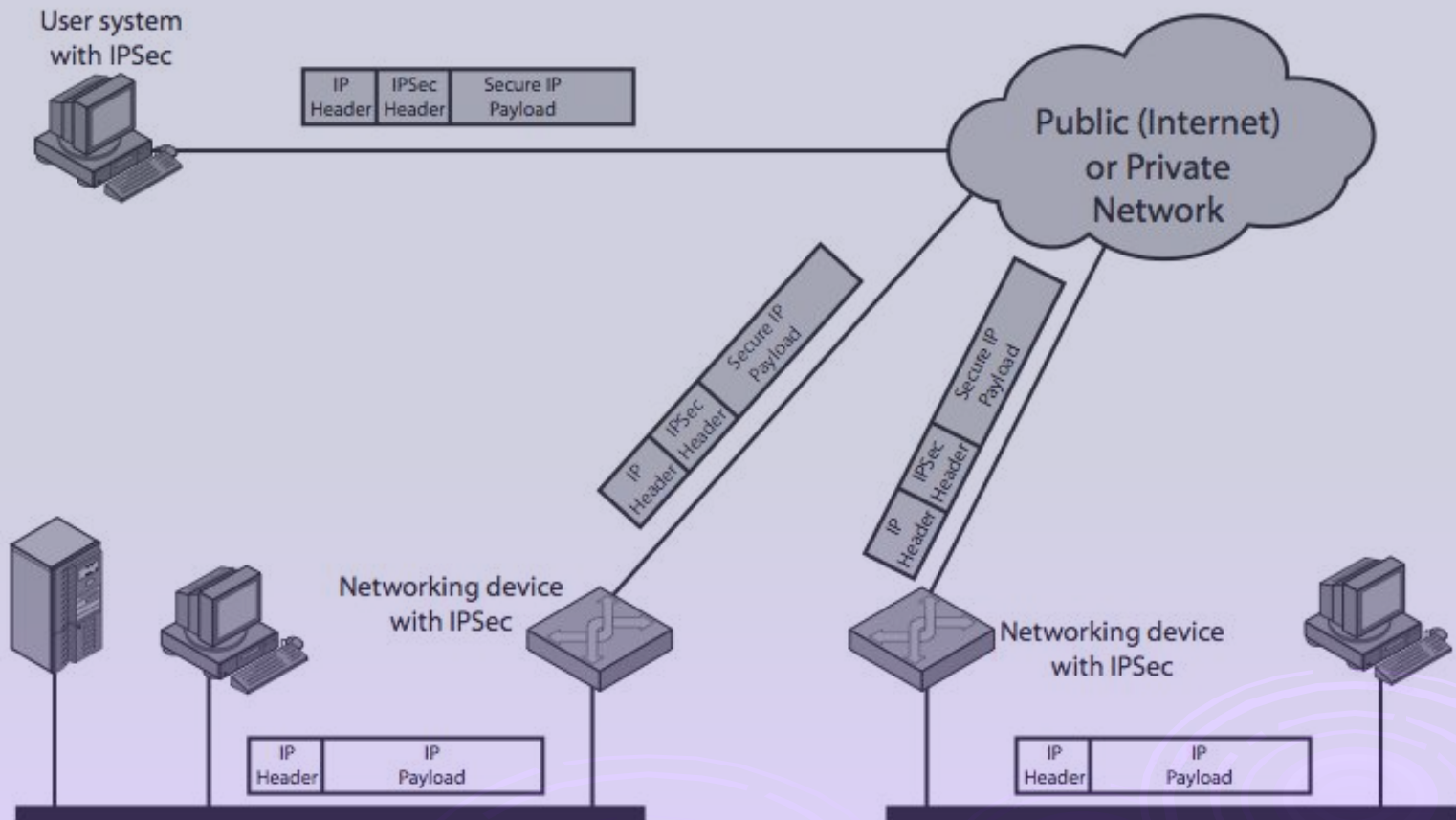


IPSec

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



IPSec Uses



Benefits of IPSec

- ❑ in a firewall/router provides strong security to all traffic crossing the perimeter
- ❑ in a firewall/router is resistant to bypass
- ❑ is below transport layer, hence transparent to applications
- ❑ can be transparent to end users
- ❑ can provide security for individual users
- ❑ secures routing architecture



IP Security Architecture

- 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
- have two security header extensions:
 - Authentication Header (AH)
 - Encapsulating Security Payload (ESP)

IPSec Services

- ❑ 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

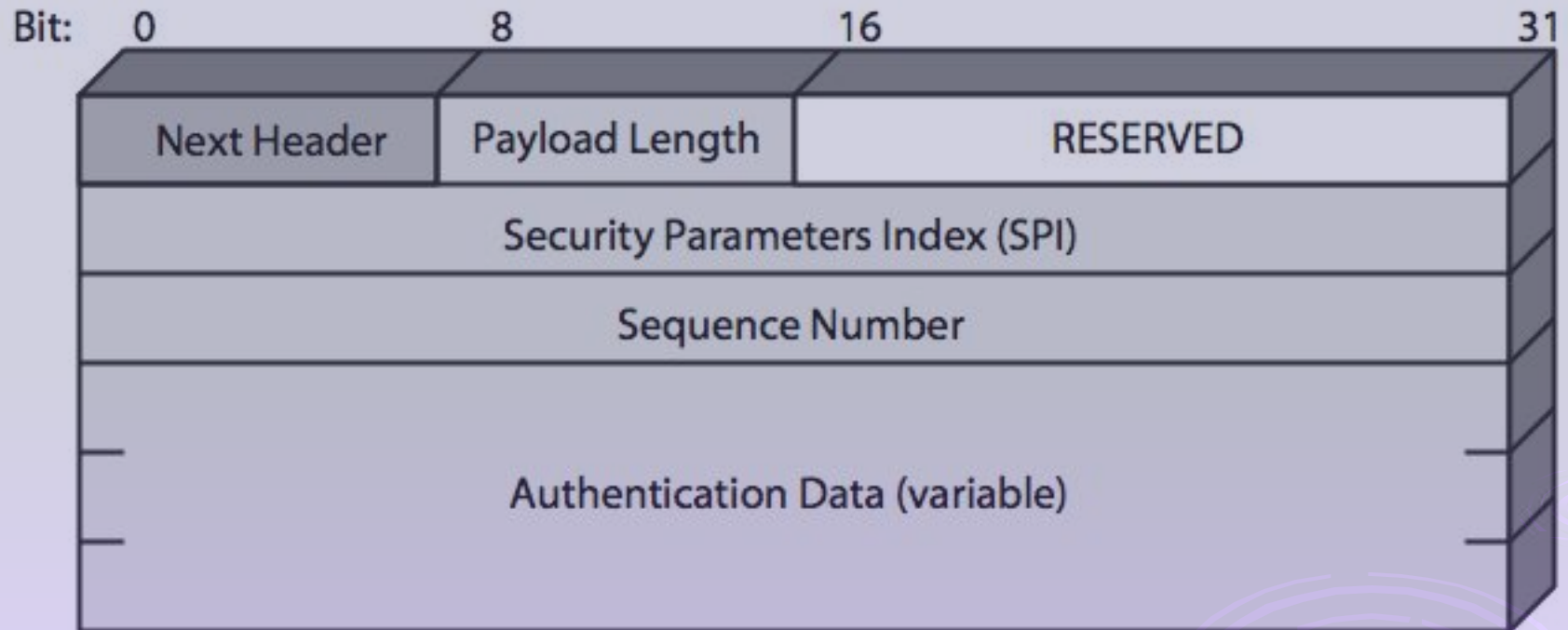
- a one-way relationship between sender & receiver that affords security for traffic flow
- defined by 3 parameters:
 - Security Parameters Index (SPI)
 - IP Destination Address
 - Security Protocol Identifier
- has a number of other parameters
 - seq no, AH & EH info, lifetime etc
- have a database of Security Associations

Authentication Header (AH)

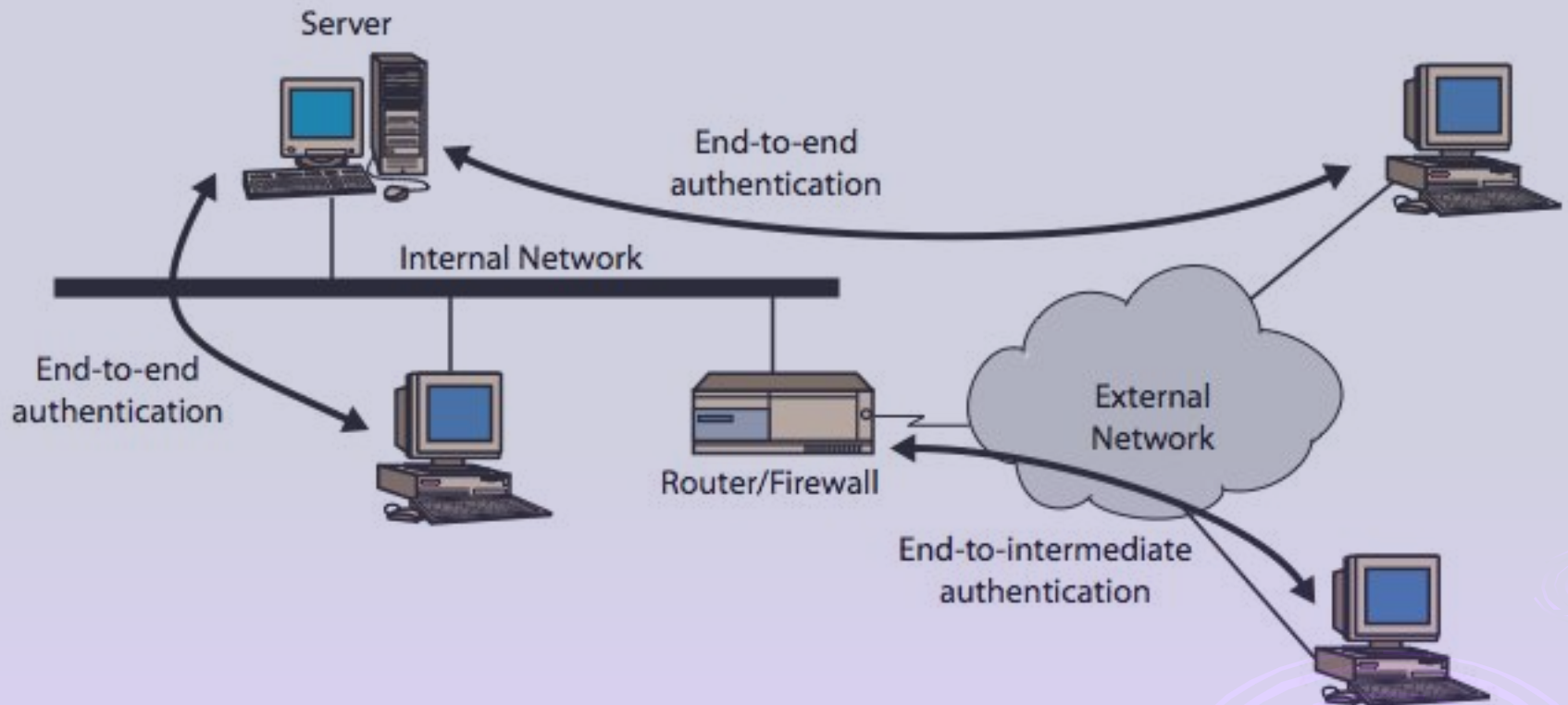
- provides support for data integrity & authentication of IP packets
 - end system/router can authenticate user/app
 - prevents address spoofing attacks by tracking sequence numbers
- based on use of a MAC
 - HMAC-MD5-96 or HMAC-SHA-1-96
- parties must share a secret key



Authentication Header

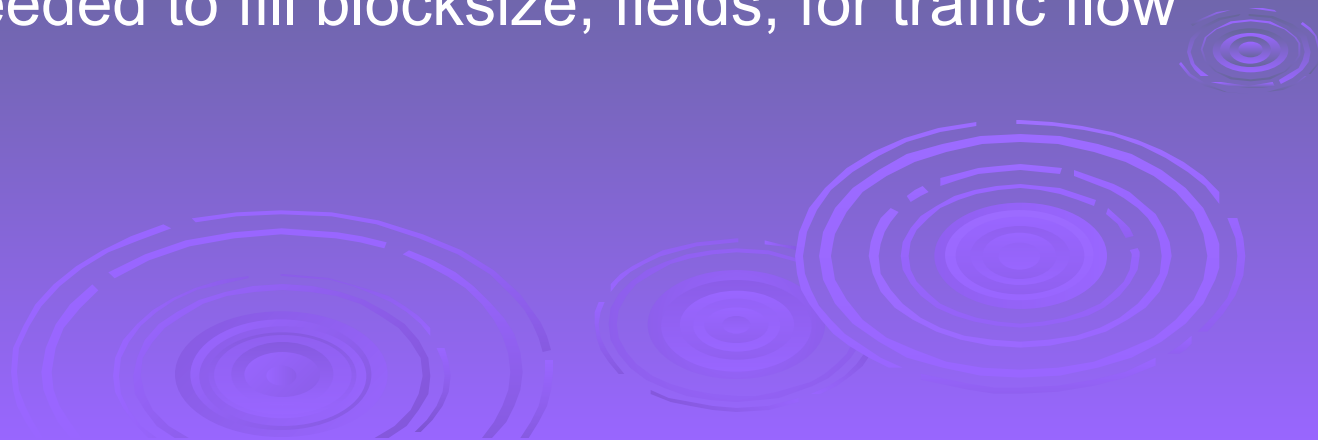


Transport & Tunnel Modes

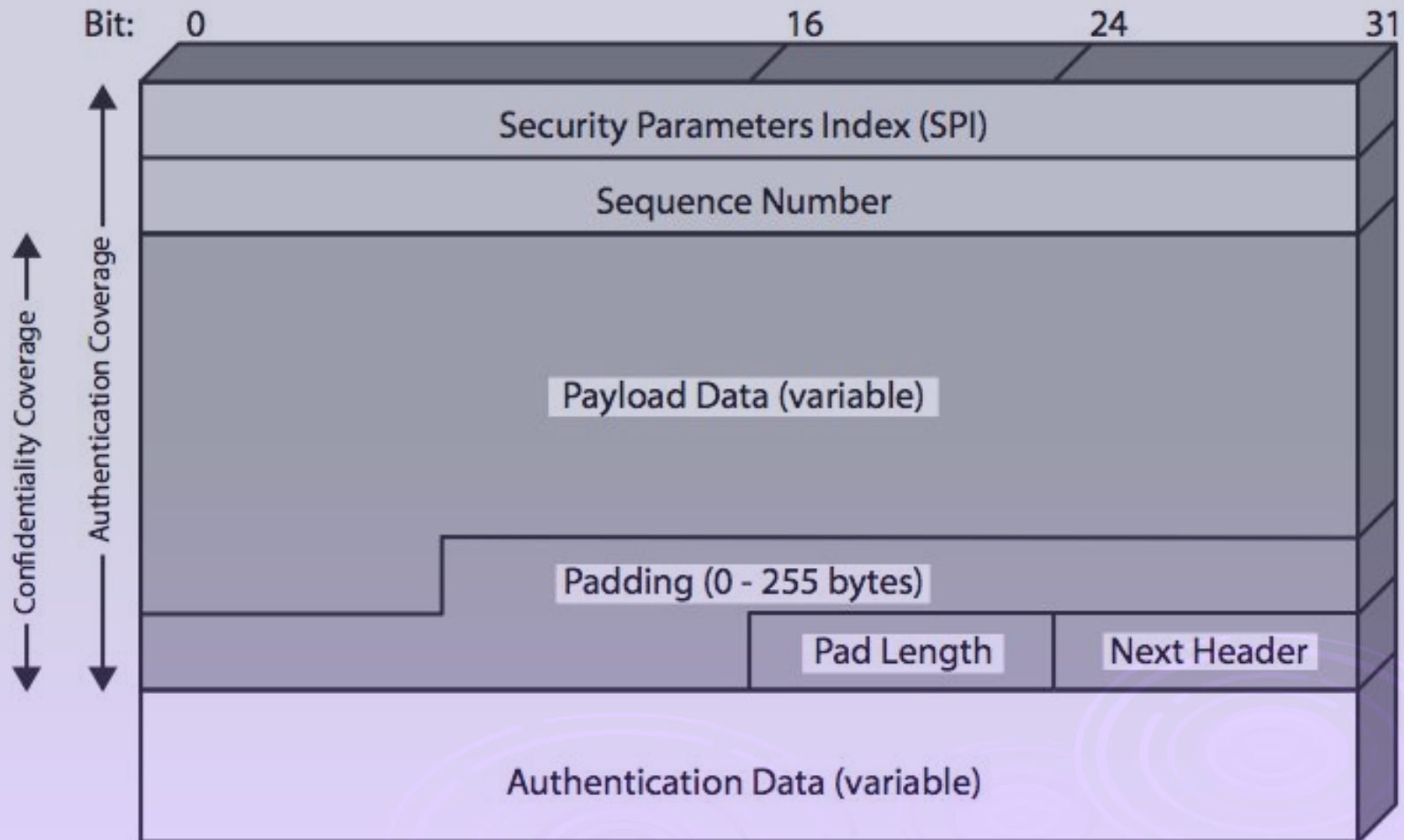


Encapsulating Security Payload (ESP)

- 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 & other modes
 - padding needed to fill blocksize, fields, for traffic flow



Encapsulating Security Payload



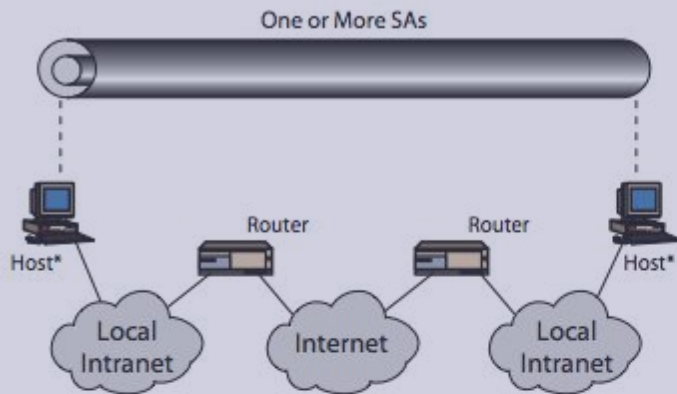
Transport vs Tunnel Mode ESP

- 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

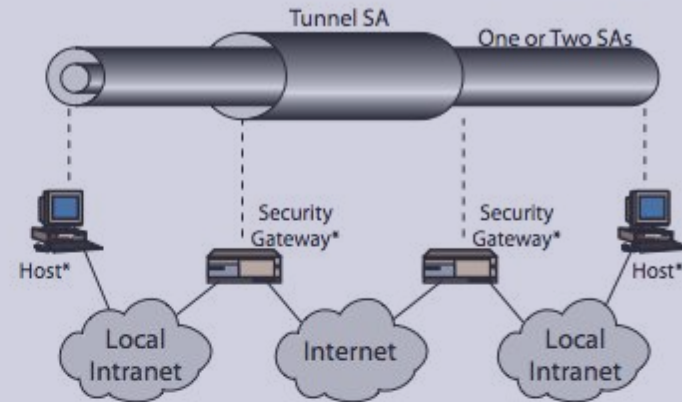
Combining Security Associations

- SA's can implement either AH or ESP
- to implement both need to combine SA's
 - form a security association bundle
 - may terminate at different or same endpoints
 - combined by
 - transport adjacency
 - iterated tunneling
- issue of authentication & encryption order

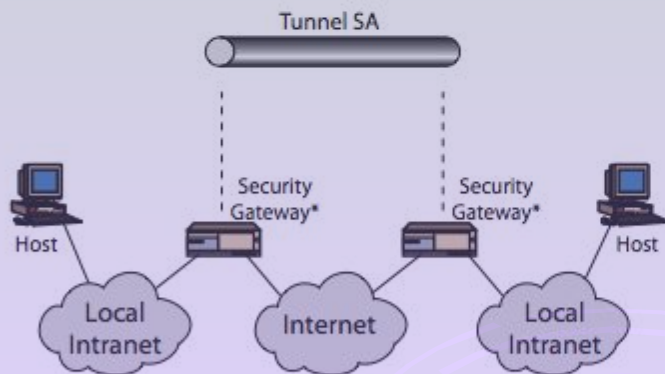
Combining Security Associations



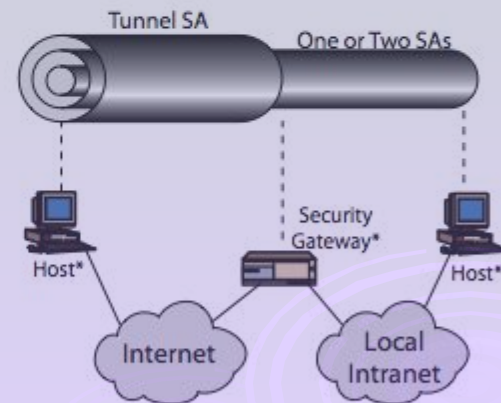
(a) Case 1



(c) Case 3



(b) Case 2



(d) Case 4

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

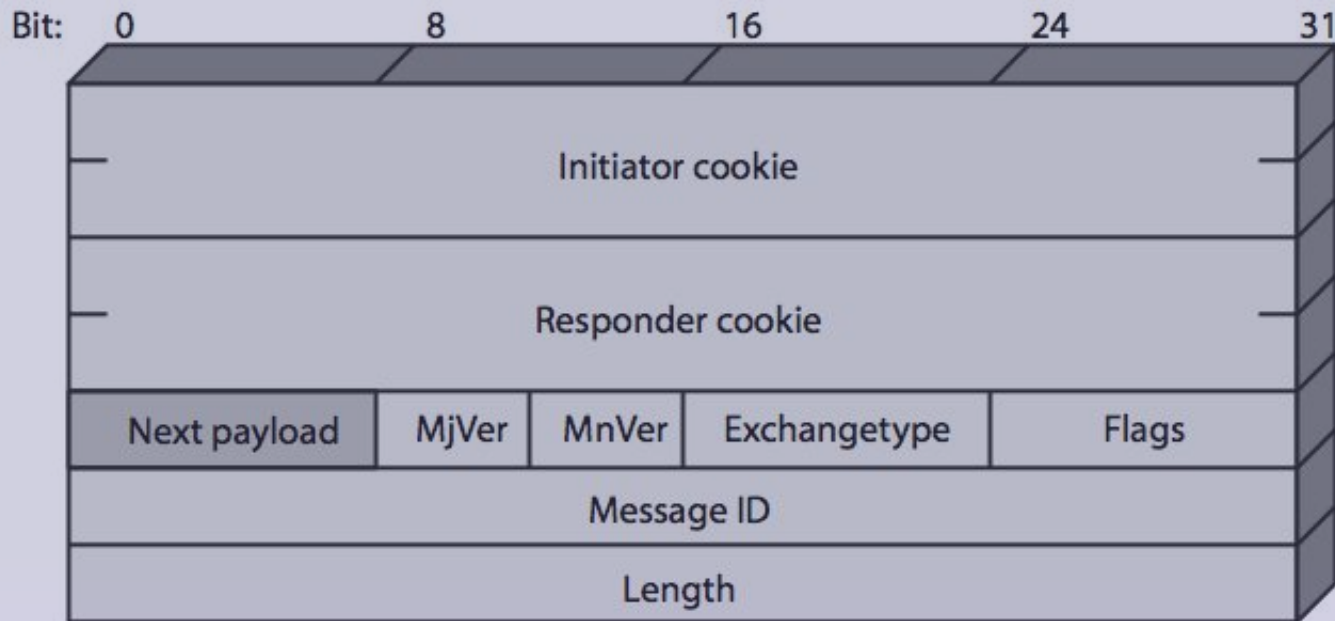
- a key exchange protocol
- based on Diffie-Hellman key exchange
- adds features to address weaknesses
 - cookies, groups (global params), nonces, DH key exchange with authentication
- can use arithmetic in prime fields or elliptic curve fields



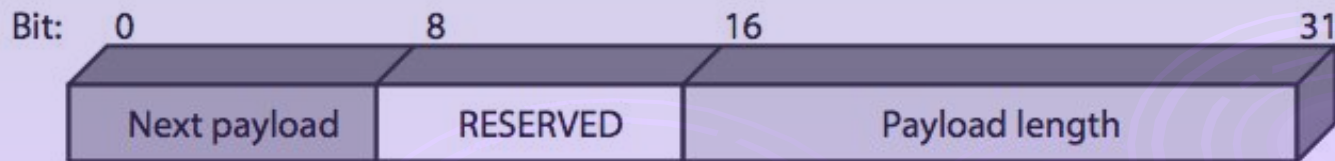
ISAKMP

- ❑ Internet Security Association and Key Management Protocol
- ❑ provides framework for key management
- ❑ defines procedures and packet formats to establish, negotiate, modify, & delete SAs
- ❑ independent of key exchange protocol, encryption alg, & authentication method

ISAKMP



(a) ISAKMP Header



(b) Generic Payload Header

ISAKMP Payloads & Exchanges

- have a number of ISAKMP payload types:
 - Security, Proposal, Transform, Key, Identification, Certificate, Certificate, Hash, Signature, Nonce, Notification, Delete
- ISAKMP has framework for 5 types of message exchanges:
 - base, identity protection, authentication only, aggressive, informational



Summary

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

