

IPSEC

Notes derived from Stallings book

Interesting news

- BGP attack with no authentication
- BGP uses a persistent TCP connection
- Can send RST with few attempts when window size is large
 - As few as 4 guesses needed
- Current TCP spec. says to accept RST as long as in current window

More on the recent attack

- Send RST/SYN to BGP peer through spoofed address
 - Results in resetting the TCP connection
 - BGP peer thinks link is down
 - Could result in route flapping when the real peer sends a “link up” message
 - BGP is designed to dampen “route flaps”
 - when links could come up and down in a short period
 - Dampening leads to longer outages

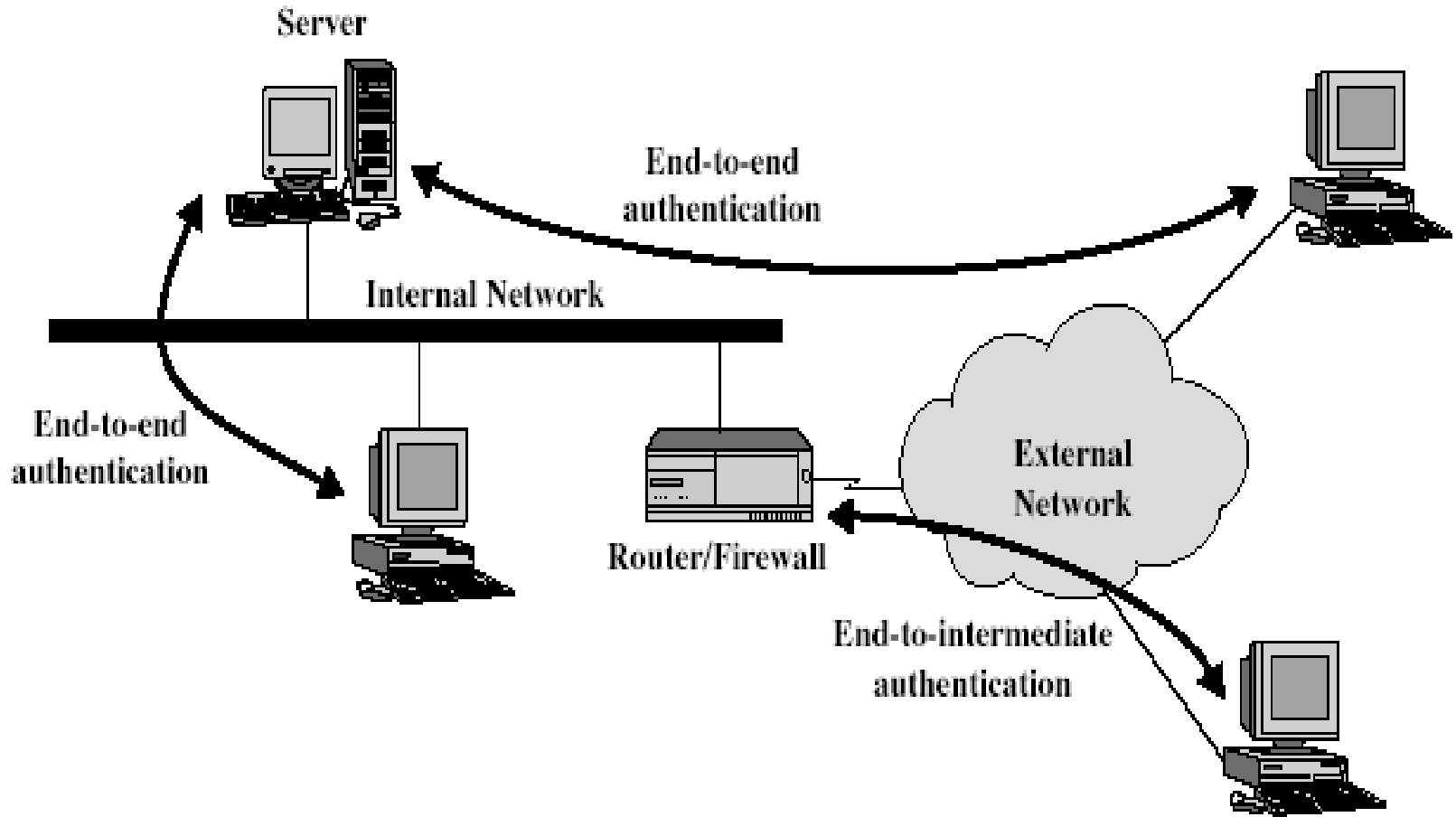
IPSEC

- Provides authentication, integrity, confidentiality at IP/network layer
 - Transparent to Transport layer & application
- SSL - at Transport layer (TCP)
- PGP -email --at application level

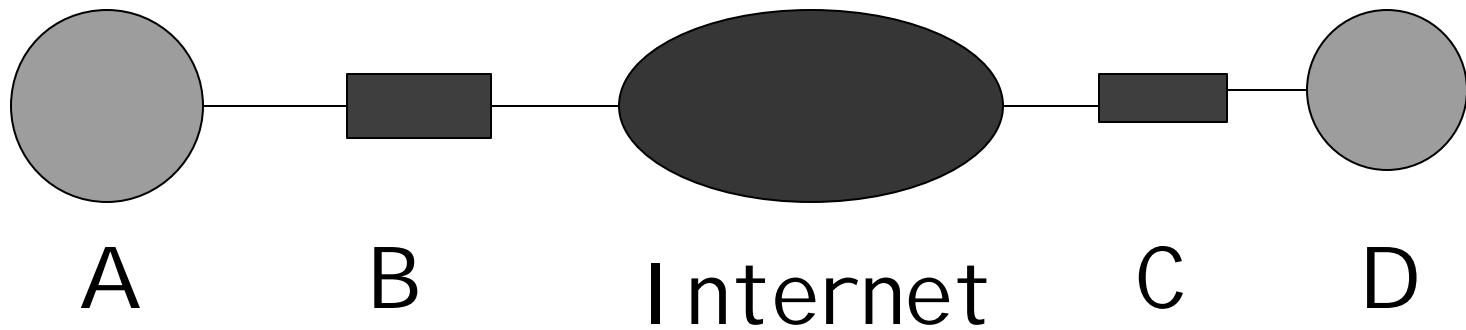
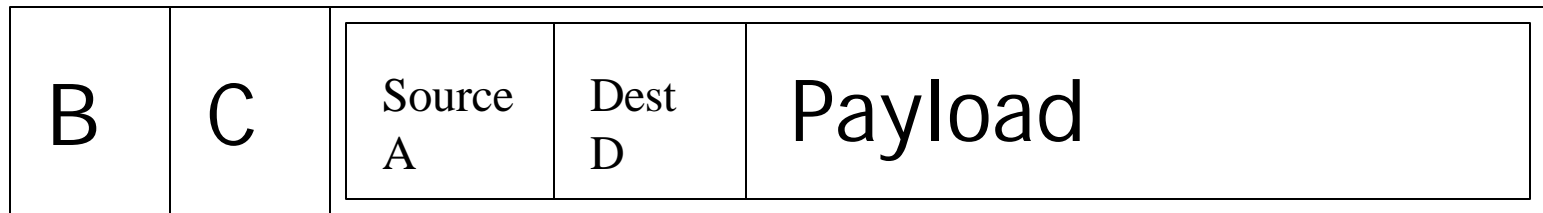
IPSEC

- Operates in two modes
 - Transport mode
 - End-to-end
 - Tunnel mode
 - Involves security gateways

IPSEC modes



IP tunneling



IPSEC protocols

- AH -Authentication Header
 - Authentication and integrity of payload and header
- ESP -Encapsulating Sec. Protocol
 - Confidentiality of payload
- ESP with ICV (Integrity Check Value)
 - Authentication, integrity and confidentiality of payload

IPSEC modes, protocols

- Can be combined
- AH transport mode
- AH tunneling mode
- ESP transport mode
- ESP tunneling mode

IPSEC Security Associations

- SA is a one-way relation between sender and receiver established by key exchange mechanisms
- Maintains security characteristics of data transfer from Tx to Rx
- Two-way secure exchange requires two SAs back and forth

What's an SA?

- IPSEC protocol mode:
 - transport, tunnel
- AH information
 - Algorithm, key, key lifetime, parameters
- ESP information
 - Algorithms, keys, key lifetimes etc.
- A sequence number 32-bits
- Anti-Replay window
- Lifetime of SA

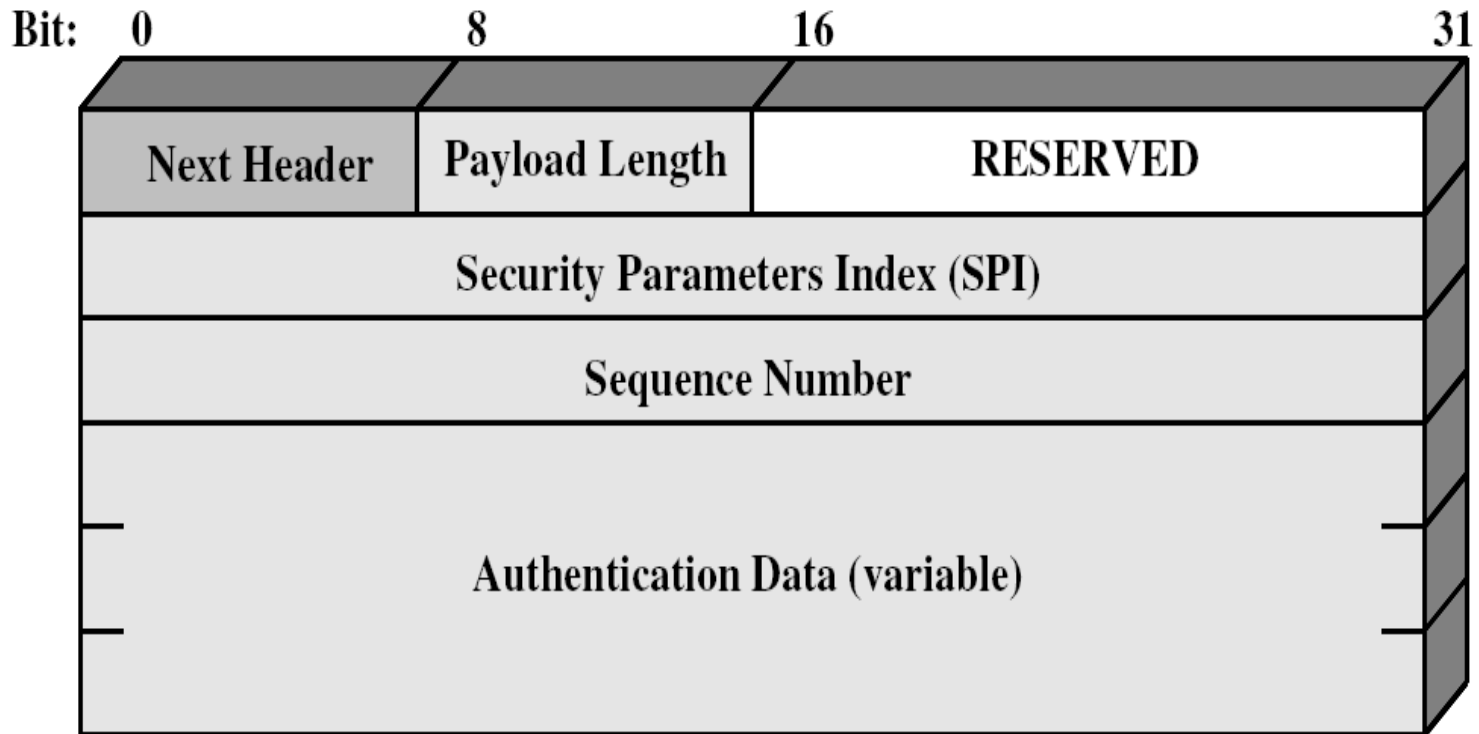
More on SA

- SA can be established at different granularities
 - On a host-to-host basis
 - On a user-to-user basis
 - On a session-by-session basis

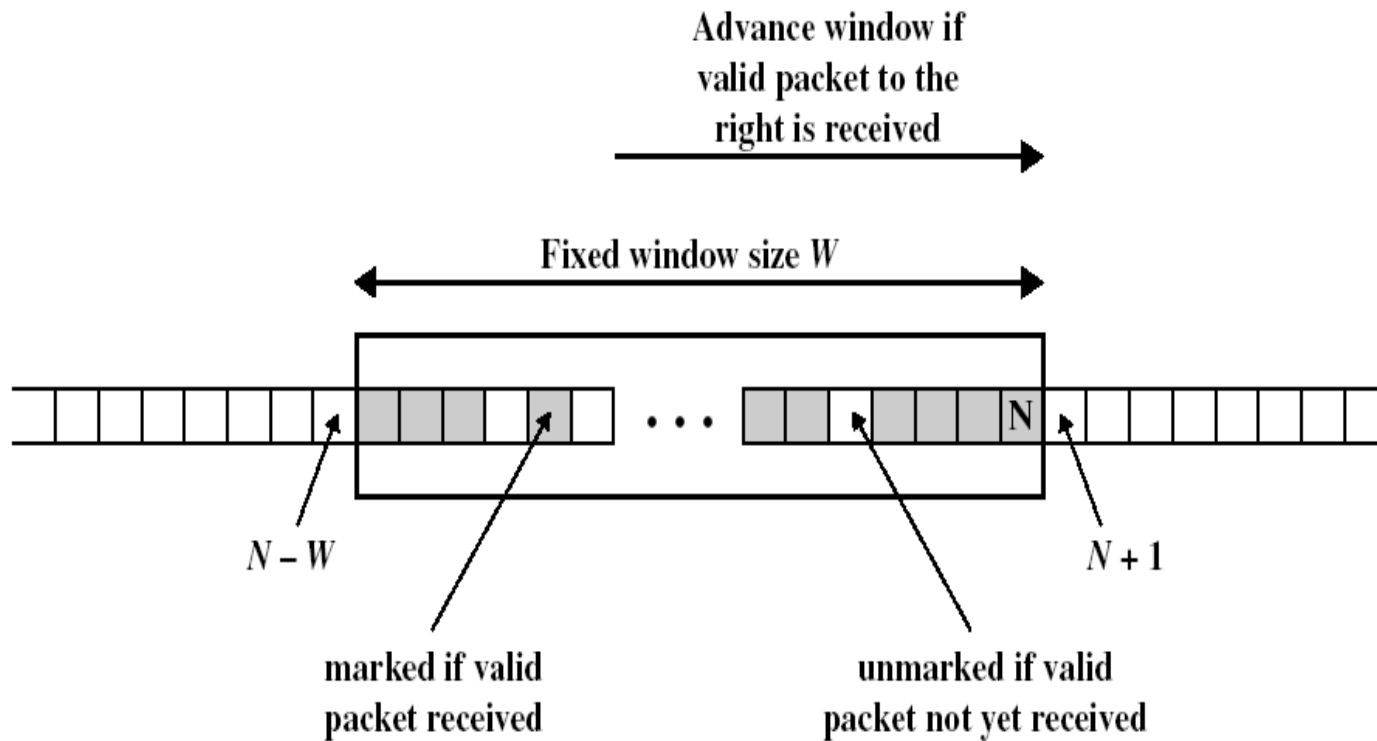
Authentication

- Provided through MAC on IP packet header data and payload
 - Header fields that change are set to 0
- Provides origin authentication
 - Prevents source address spoofing
- Provides data integrity –through MAC
- Provides optional replay prevention

Authentication Header



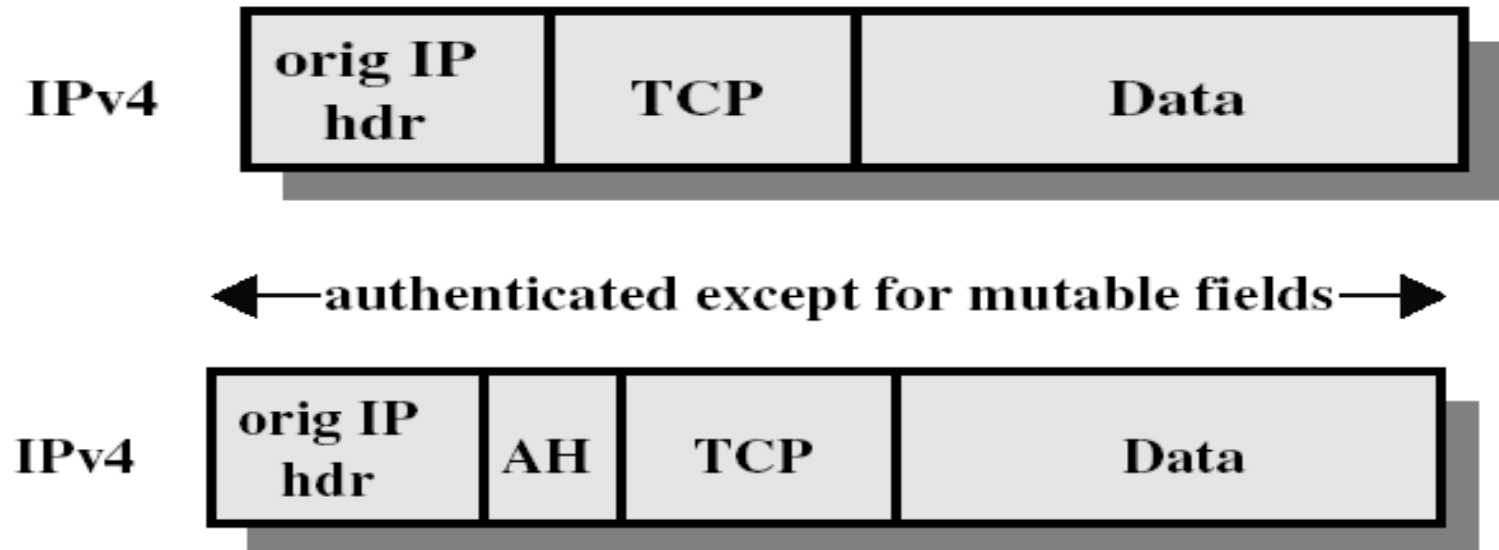
Anti-Replay mechanism



AH transport mode

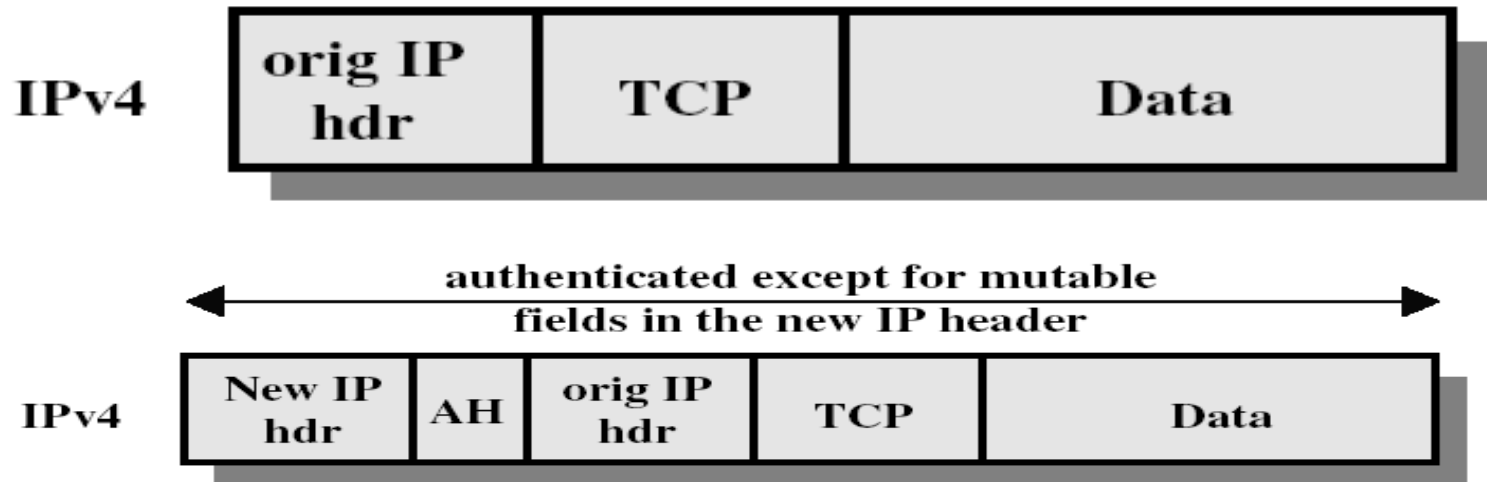
AH protocol number = 51

AH in turn points to the original protocol number



AH Tunnel mode

- Transport/tunnel mode is determined by Security Association (SA)



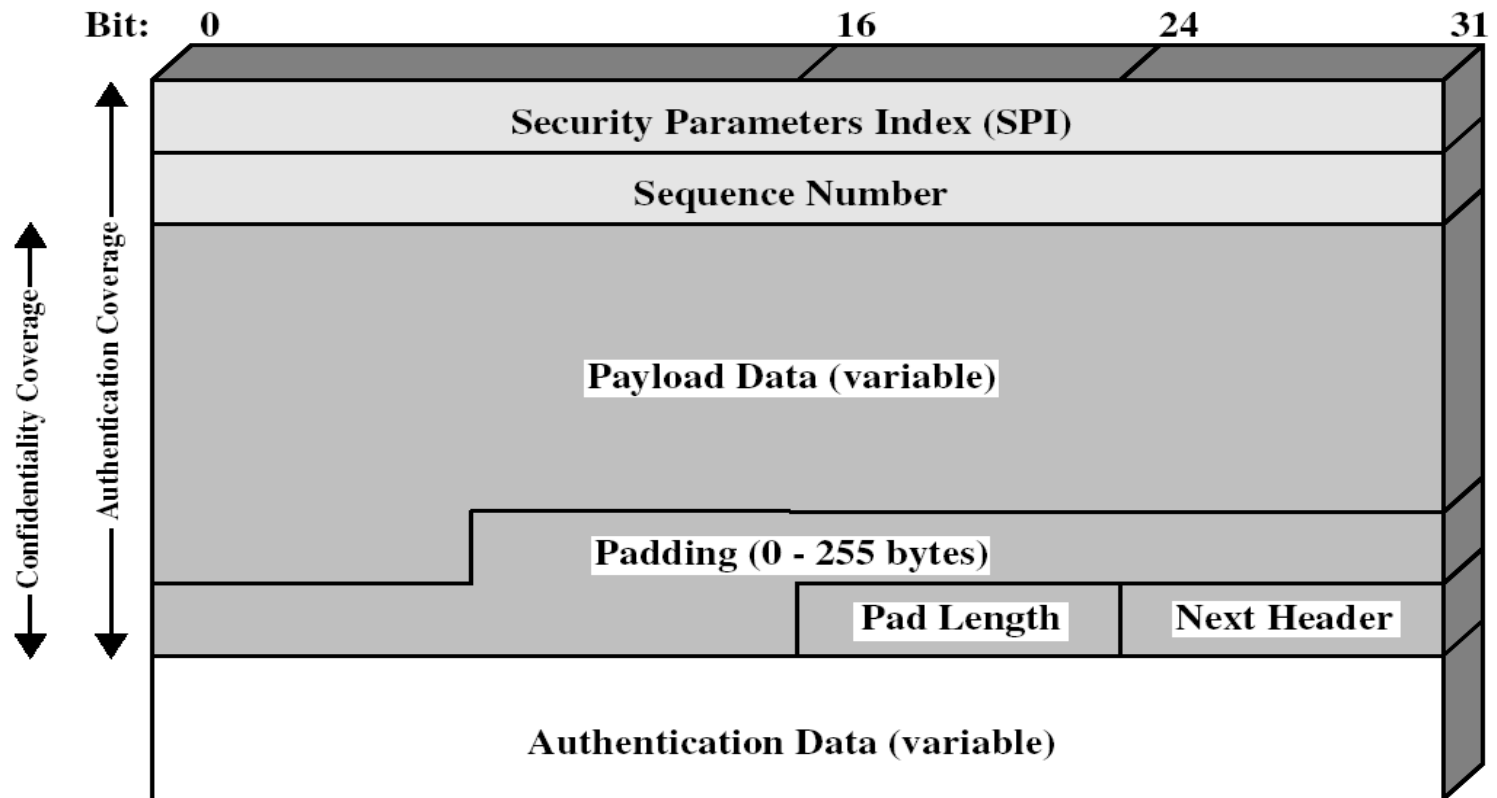
Authentication algorithms

- Employs SHA-1 and MD5 hashes
- Compute the entire hash and truncate to (default) 96 bits to produce I CV
- Mutable fields ignored (set to 0)
 - TTL, IP checksum, authentication data

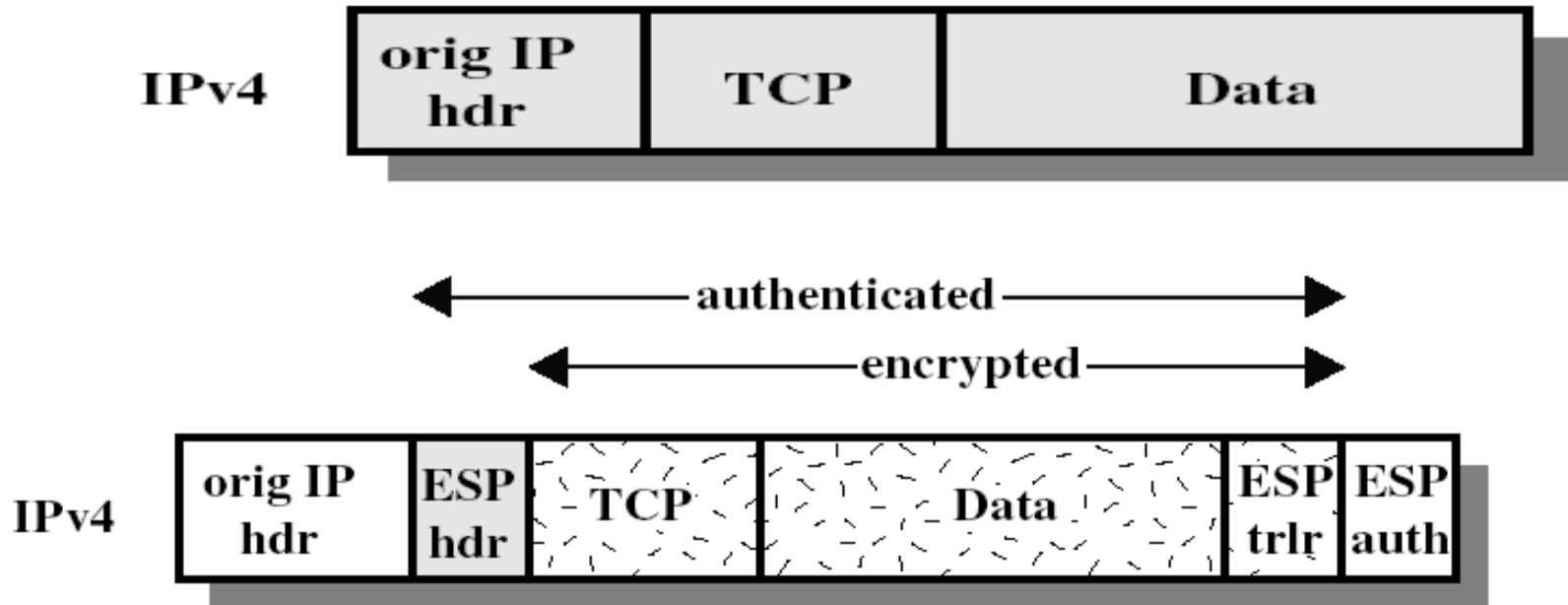
IPSEC encryption

- Must support DES in CBC mode
- Other algorithms that are supported:
 - 3-key triple DES
 - RC5, IDEA, 3-key triple IDEA, CAST, Blowfish
- Employs MD5 and SHA-1 for authentication (optional)

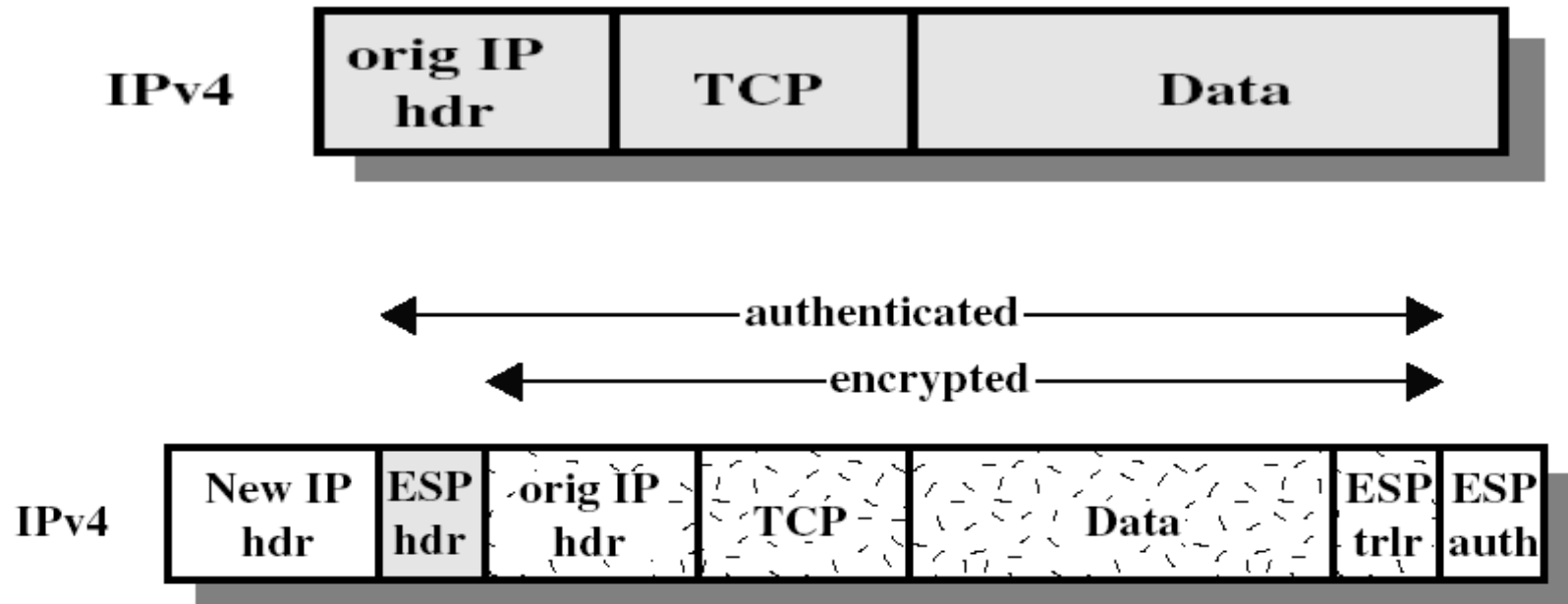
IPSEC ESP format



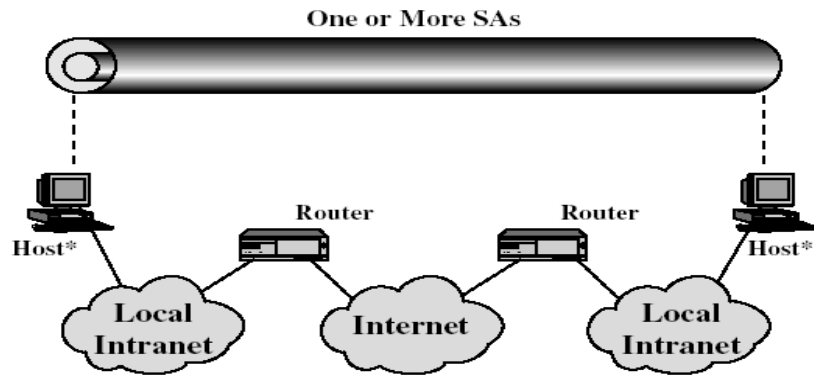
ESP Transport mode



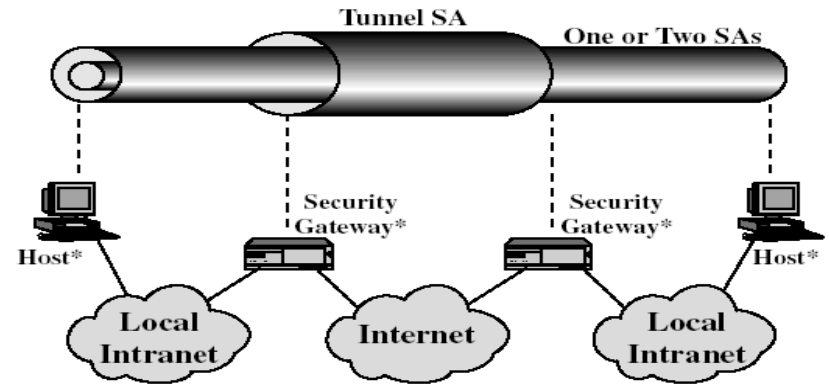
ESP Tunnel mode



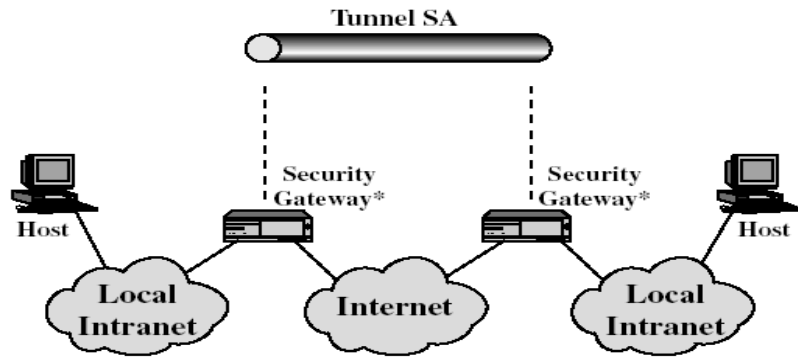
Combinations of SAs



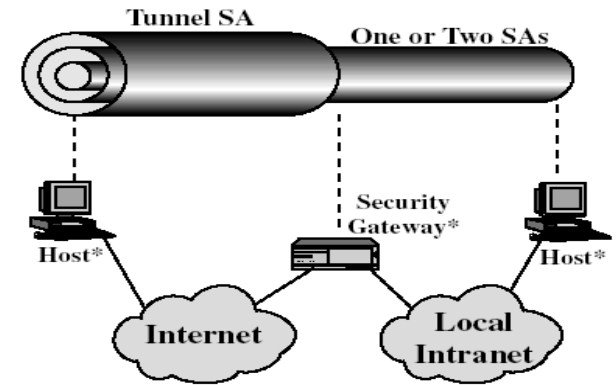
(a) Case 1



(c) Case 3



(b) Case 2



(d) Case 4

* = implements IPSec

Protocols -- Services

	AH	ESP (encryption only)	ESP (encryption plus authentication)
Access control	✓	✓	✓
Connectionless integrity	✓		✓
Data origin authentication	✓		✓
Rejection of replayed packets	✓	✓	✓
Confidentiality		✓	✓
Limited traffic flow confidentiality		✓	✓

Key Management

- Can be done manually or automated
- Default automated: I SAKMP/Oakley
- Oakley key determination protocol
 - Enhanced Diffie-Hellman algorithm
- I SAKMP – Internet Security Association and Key Management Prot
 - Specifies the specific message formats

Oakley key determination

- Remember Diffie-Hellman?
- Employs a large prime number q and a , a primitive root of q
- A selects random integer X_A , as its private key
- A computes its public key $Y_A = a^{X_A} \text{ mod } q$
- Session key = $(Y_B)^{X_A} \text{ mod } q = (Y_A)^{X_B} \text{ mod } q = a^{X_A X_B} \text{ mod } q$

Attacks on Diffie-Hellman

- Man-in-the-middle attack
- C can pretend to be B to A and pretend to be A to B
 - A establishes key with C (thinking B)
 - B establishes key with C (thinking A)
- C can relay messages from A to B, and B to A –can play havoc

Other Attacks on D-H

- No authentication of IDs of parties
- Clogging/DOS attack
 - Send a lot of requests for session establishment
 - The victim will be busy generating keys

Oakley

- Employs cookies to prevent clogging attacks
- A cookie has to be returned before key generation begins
- If the attacker pretends to be someone else, cannot return the cookie
- Key generation aborted quickly

More on Oakley

- Employs D-H (768, 1024, 1536 bits) and elliptic curve analog of D-H (155, 185 bits) -called groups
- Employs nonces (pseudorandom num) to protect against replay attacks
- Different authentication mechanisms used to thwart man-in-the-middle attacks

Authentication

- Three different methods
- Digital signatures
 - Sign mutually obtainable hash with a private key
- Public-key encryption
- Symmetric key encryption
 - Keys exchanged out of band

Want to learn more?

- Look up RFCs 2401, 2402, 2406,2408

Summary of today's class

- IPSEC provides a network layer level security architecture
- Employs AH, ESP protocols and transport, tunnel modes
 - Provides authentication, confidentiality and data integrity
- Employs MAC (MD5/SHA-1) and DES