IPsec

Raj Jain
Washington University in Saint Louis
Saint Louis, MO 63130
Jain@cse.wustl.edu

Audio/Video recordings of this lecture are available at:

http://www.cse.wustl.edu/~jain/cse571-09/

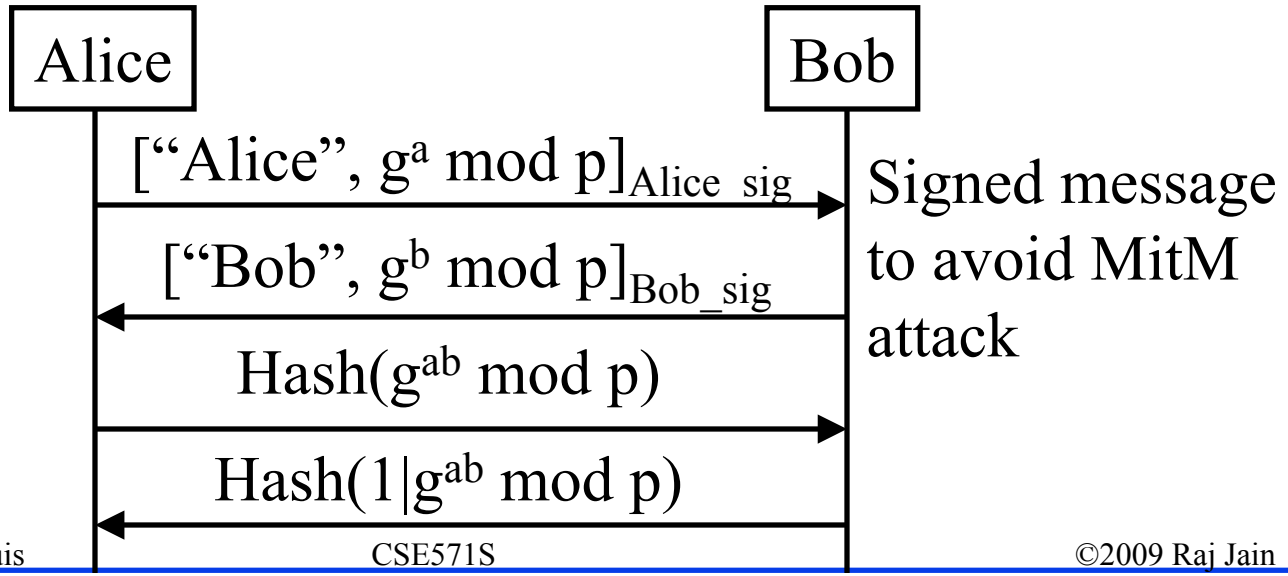
- Security Scheme Design Issues: Perfect Forward Secrecy
- IP Concepts: NAT, Tunnel, Firewall, Proxy Servers
- IP Headers
- IPsec: Concepts, AH, ESP
- AH, ESP Version 3

Security Scheme Design Issues

- Perfect Forward Secrecy
- Denial of Service Protection
- End Point Identifier Hiding
- Live Partner Reassurance

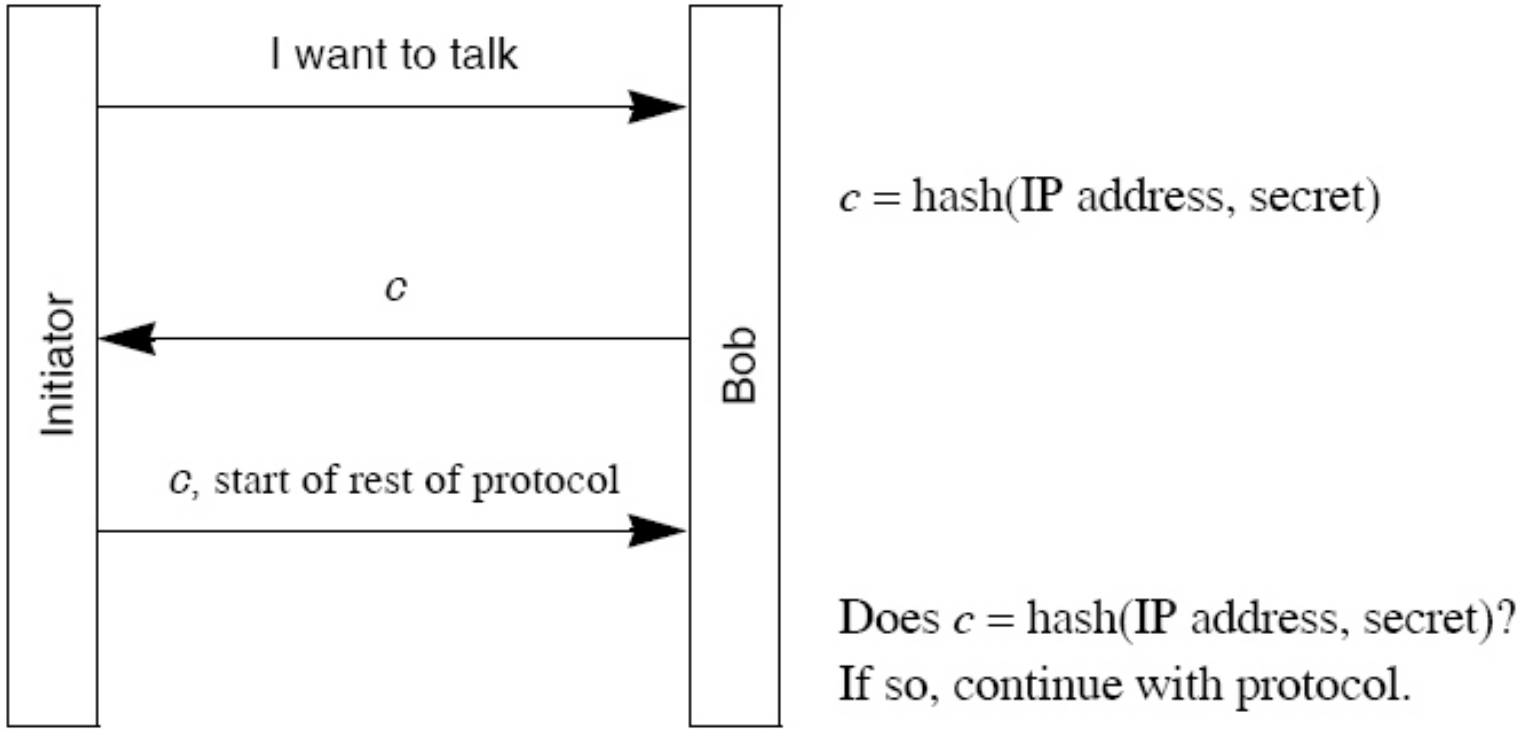
Perfect Forward Secrecy

- Attacker cannot decrypt a conversation even if he records the entire session and subsequently steals their long term secrets
- Use session keys not derivable from information stored at the node after session concludes
- **Escrow-Foilage**: Even if the long-term private keys have been escrowed, eavesdropper (passive) cannot decrypt



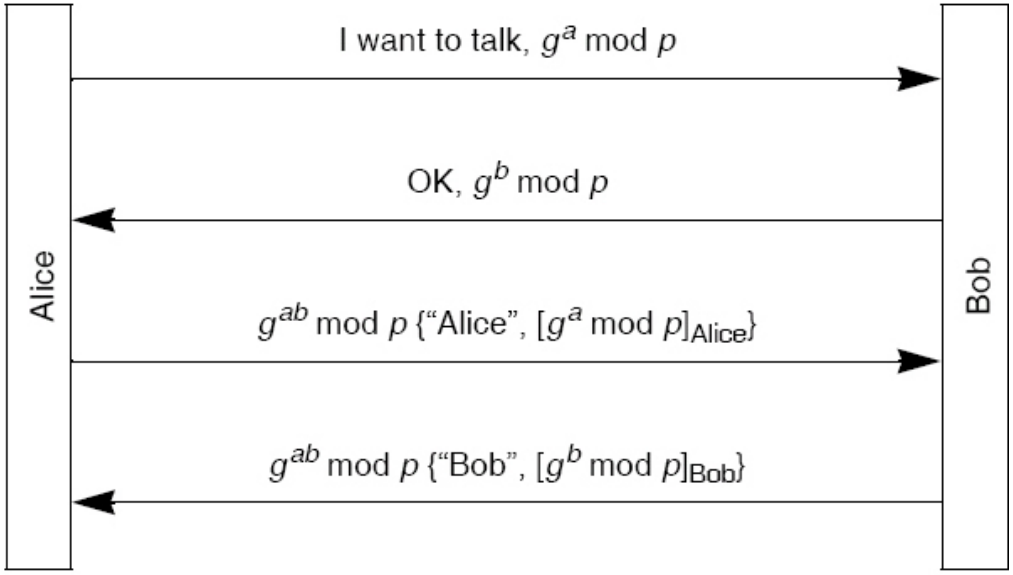
Denial of Service Protection

- **Rule**: Do not keep state until the response comes back
  $\Rightarrow$ All state in cookies sent back to the requester
- Adds a round-trip delay



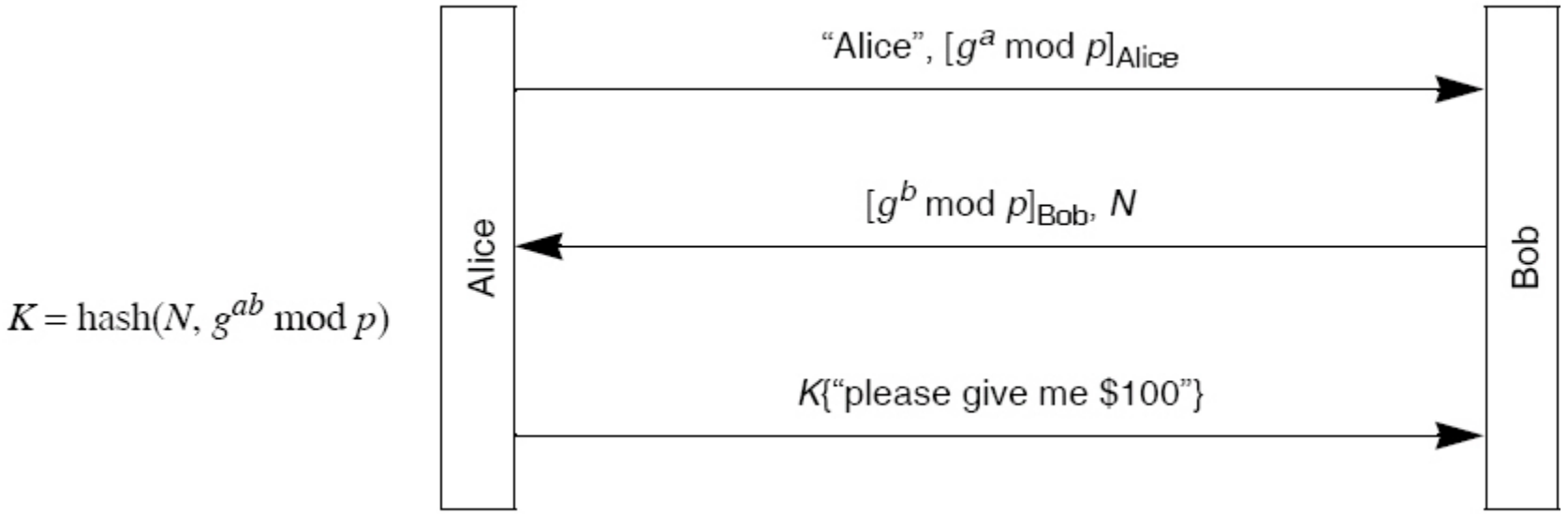
End Point Identifier Hiding

- Hide the identities from eavesdroppers
- Anonymous DH and use the key to divulge identities
  ⇒ Passive eavesdropper cannot learn identities
  but active Man-in-the-Middle can learn one or both identities
  ⇒ Authenticate
- Requester should divulge first



Live Partner Reassurance

- DH operations are expensive
  $\Rightarrow$ g, b, a are not changed often
- Keys should be based on a g^{ab} and an nonce
  $\Rightarrow$ Can't replay previous sessions



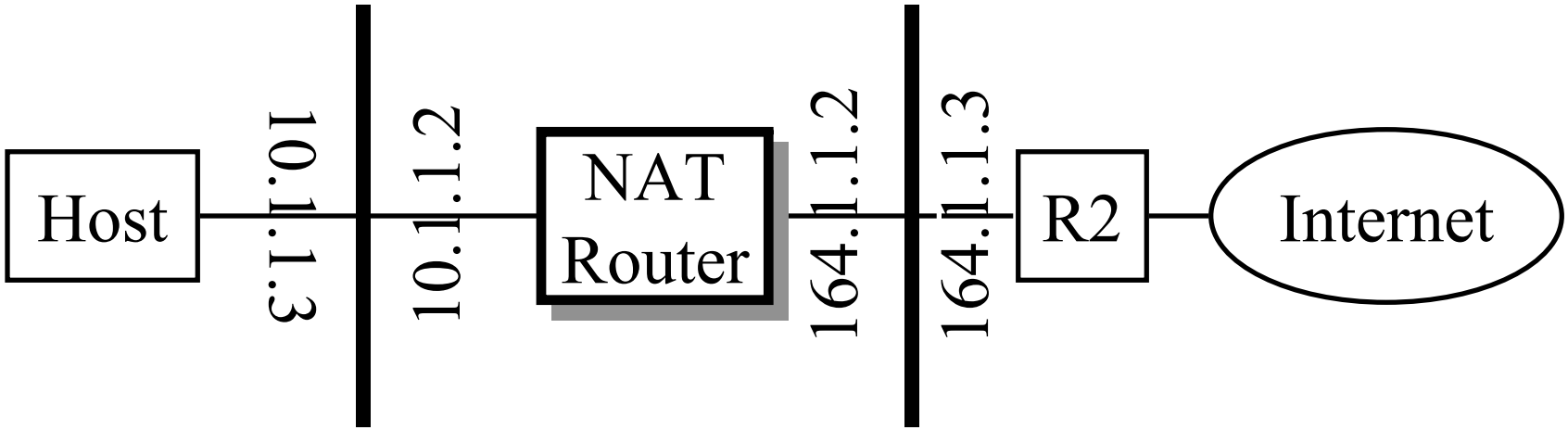
IP Concepts

- Private Addresses
- Network Address Translation
- Tunnel
- Firewalls
- Proxy Servers
- IPv4
- IPv6

Private Addresses

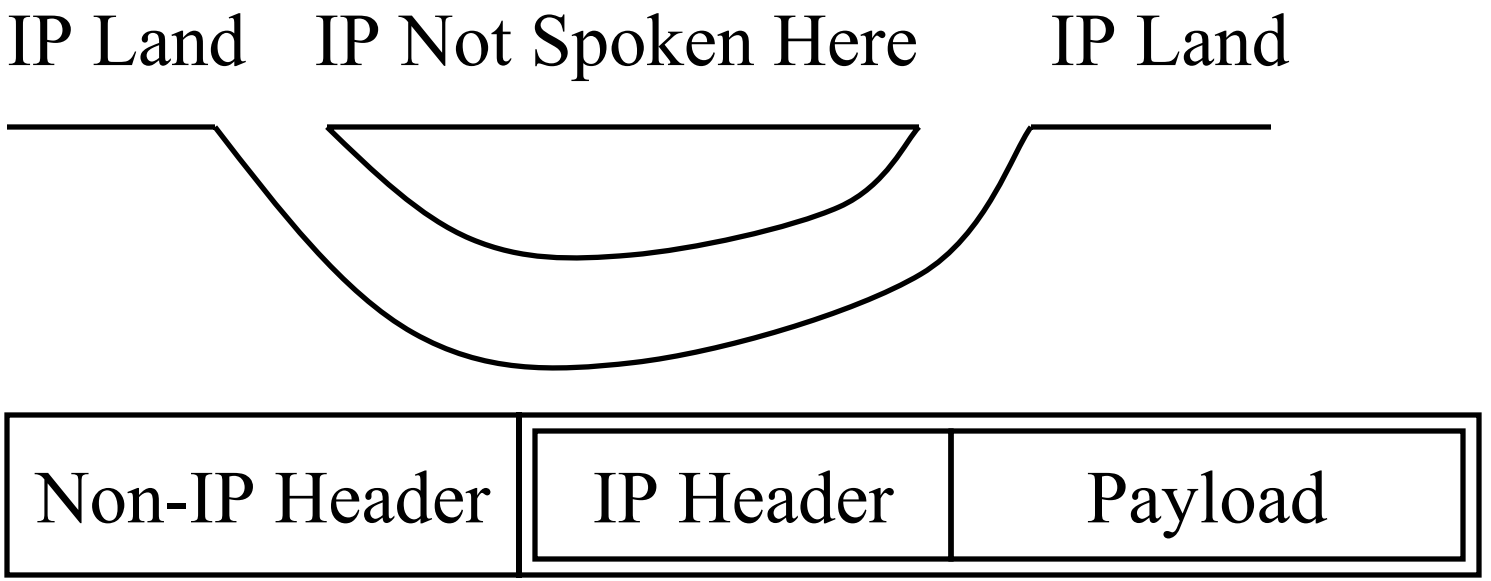
- 32-bit Address ⇒ 4 Billion addresses max
- Subnetting ⇒ Limit is much lower
- Shortage of IP address ⇒ Private addresses
- Frequent ISP changes ⇒ Private address
- Private ⇒ Not usable on public Internet
- RFC 1918 lists such addresses for private use
- Prefix = 10/8, 172.16/12, 192.168/16
- Example: 10.207.37.234

Network Address Translation (NAT)



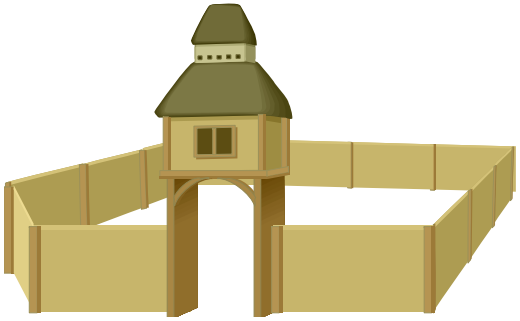
- NAT = Network Address Translation
  Like Dynamic Host Configuration Protocol (DHCP)
- Outgoing Packets: Change <Private source address, Source Port> to <public address, new Port>
- Incoming Packets: Change <Public Destination Address, Dest Port> to <Private IP address, original Port #>

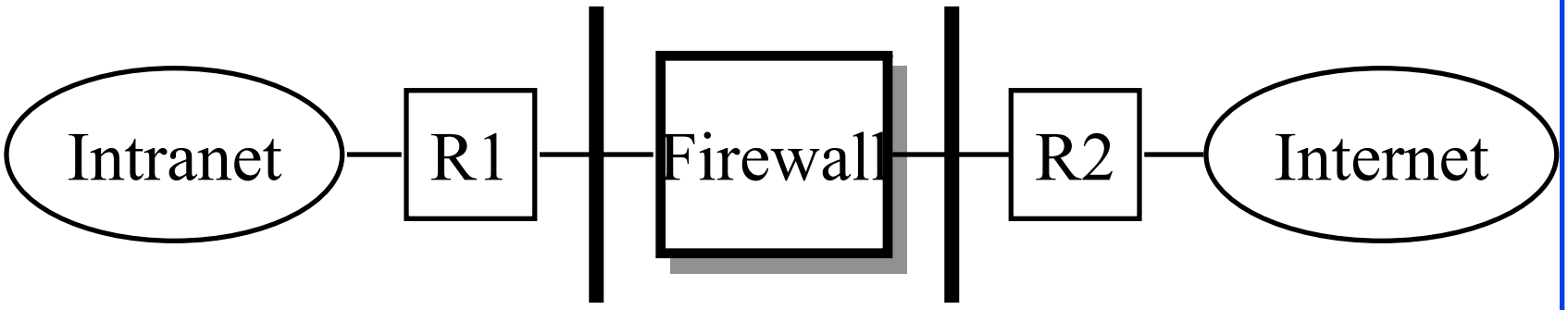
Tunnel



- Tunnel = Encaptulation
- Used whenever some feature is not supported in some part of the network, e.g., multicasting, mobile IP

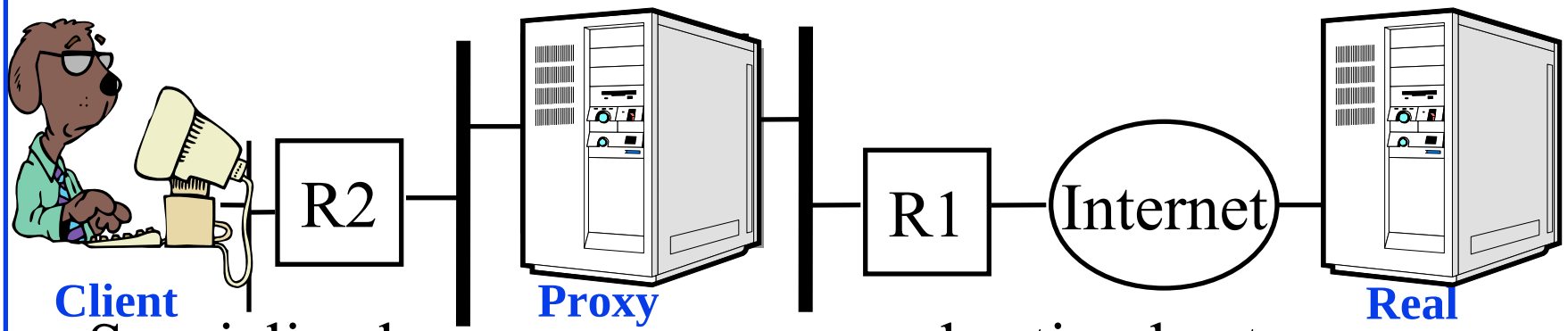
Firewall





- Enforce rules on what internal hosts/applications can be accessed from outside and vice versa
- One point of entry. Easier to manage security.
- Discard based on IP+TCP header. Mainly port #.
- Firewall-Friendly applications: Use port 80.

Proxy Servers



- Specialized server programs on bastion host
- Take user's request and forward them to real servers
- Take server's responses and forward them to users
- Enforce site security policy ⇒ Refuse some requests.
- Also known as application-level gateways
- With special "Proxy client" programs, proxy servers are almost transparent

IP Headers

- IPv6:

Ver	Traffic Class	Flow Label	
Payload Length		**Next Header**	Hop Limit
Source Address			
Destination Address			

- IPv4:

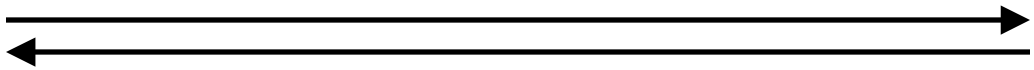
Version	IHL	Type of Service	Total Length
Identification		Flags	Fragment Offset
Time to Live	Protocol	Header Checksum	
Source Address			
Destination Address			
Options			Padding

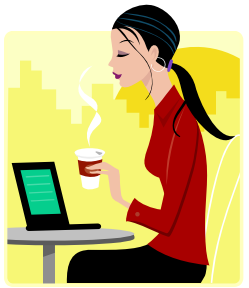
IPsec

- Security at layer 3
- Competition: Layer 2 VPN, Layer 4 SSL, etc
- Advantages:
  - Applies to all applications
  - Routers/firewalls vendors can implement it (Can't implement SSL)
- Limitations:
  - Limited to IP Addresses
  - Has no concept of application users

Security Association

- One way relationship between sender and receiver
- For two way, two associations are required
- Three SA identification parameters
  - Security parameter index
  - IP destination address
  - Security protocol identifier



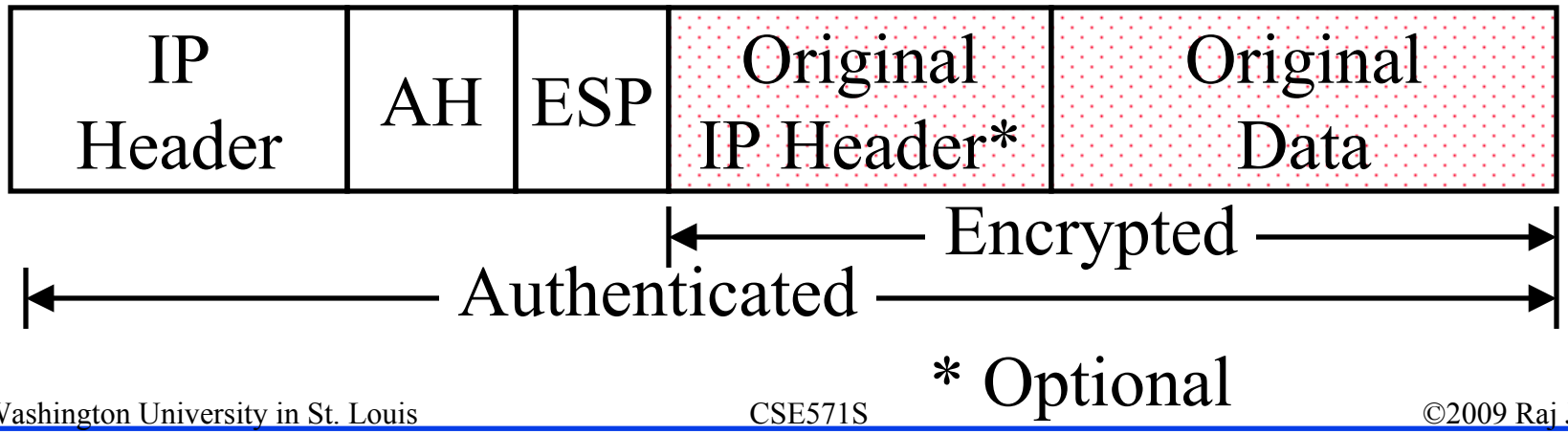


IPsec Concepts

- IPsec Security Association: One-way
- Security Parameter Index: Allows receiver to retrieve info from security association database.
  - Chosen by receiver
  - SPI+[DA]+[SA]

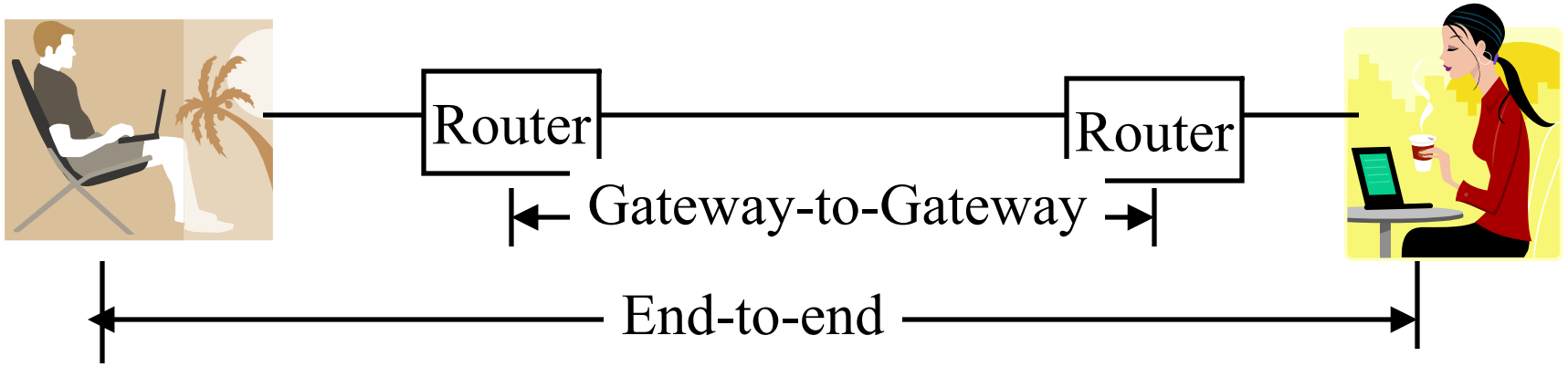
IPSec

- Secure IP: A series of proposals from IETF
- Separate Authentication and privacy
- Authentication Header (AH) ensures data *integrity* and *data origin authentication*
- Encapsulating Security Protocol (ESP) ensures *confidentiality, data origin authentication, connectionless integrity, and anti-replay service*

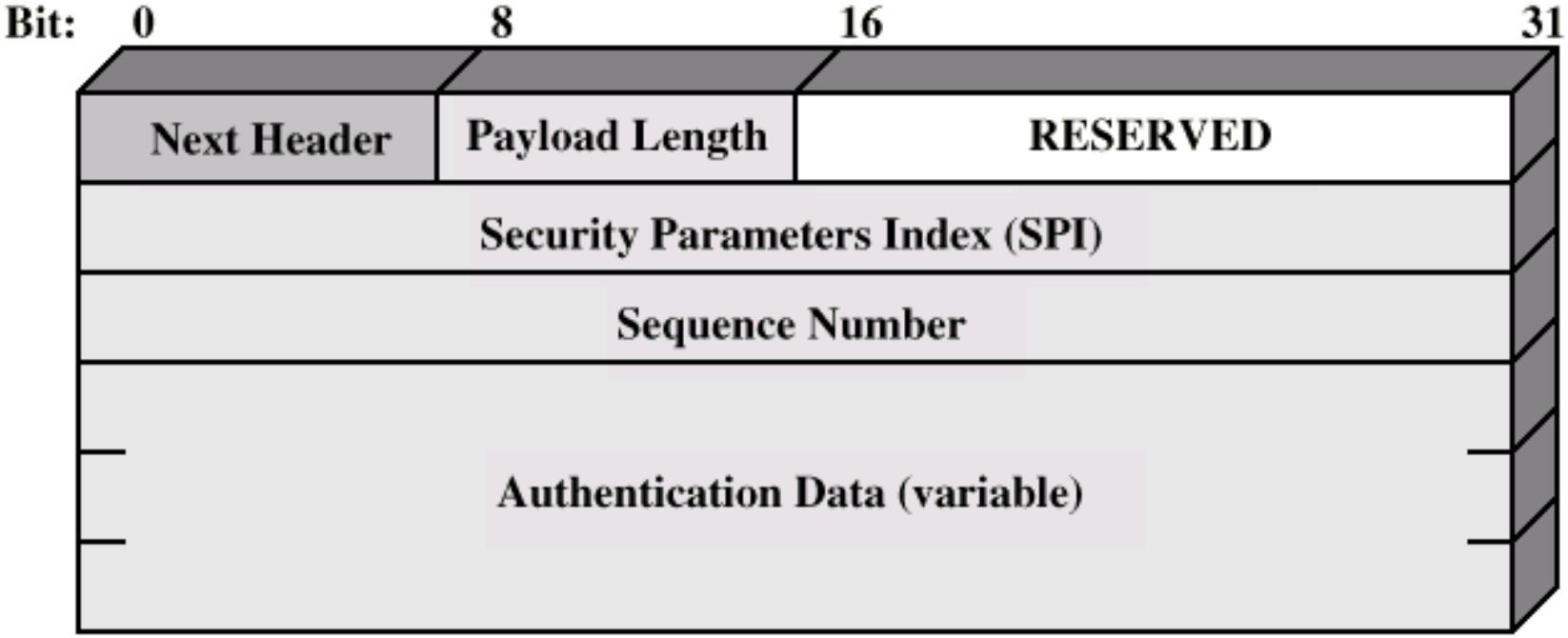


Tunnel vs. Transport Mode

- Gateway-to-gateway vs. end-to-end

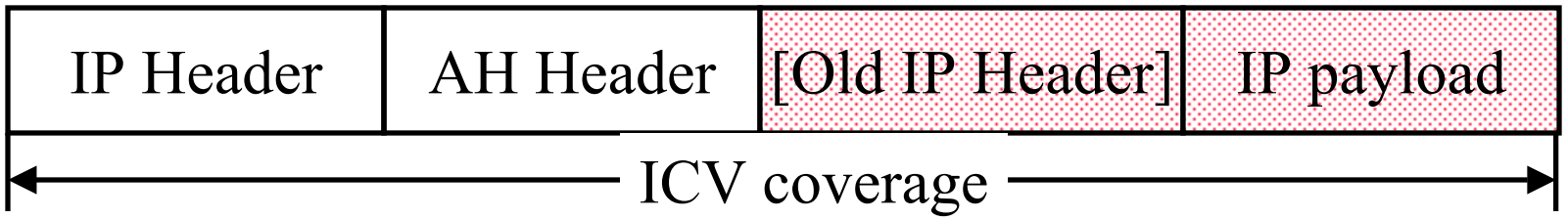


Authentication Header



- Next Header = TCP=6, UDP=17, IP=4, AH=51
  ⇒ Designed by IPv6 fans
- Payload Length = Length of ***AH*** in 32-bit words − 2 (for IPv4)
  =Length of AH in 64-bit words -1 (for IPv6)
- SPI = Identifies Security association (0=Local use, 1-255 reserved)
- Authentication data = Integrity Check Value

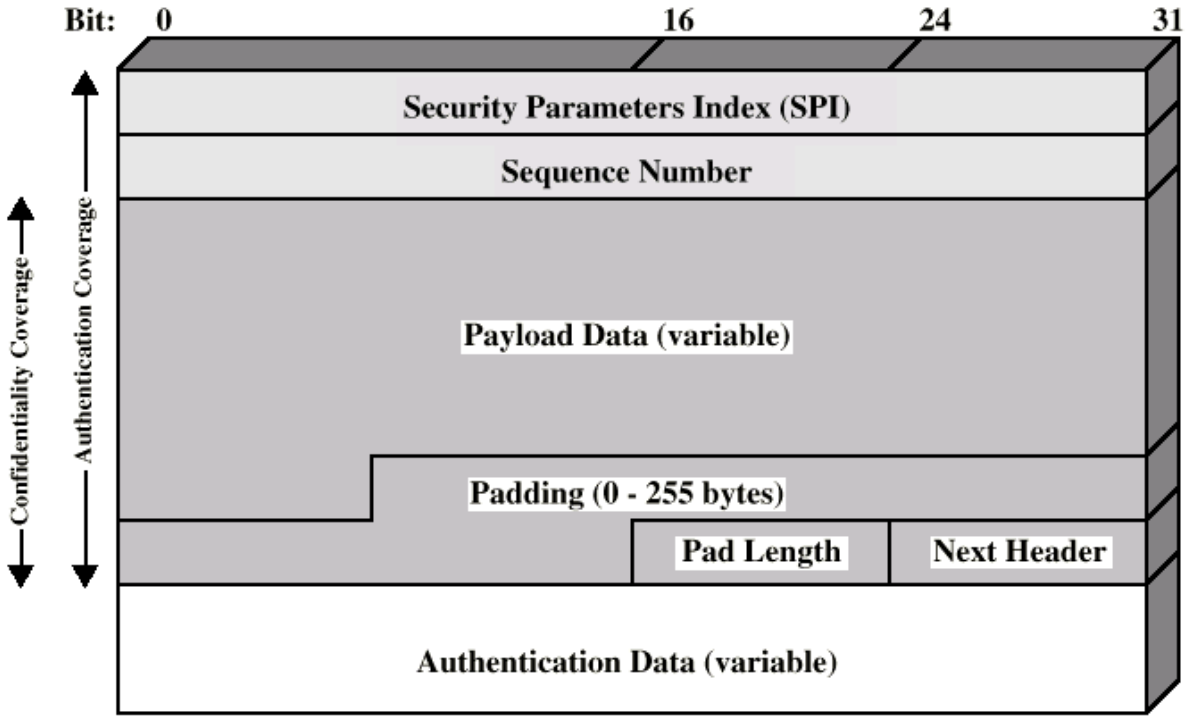
AH ICV Computation



The AH ICV is computed over:

- IP header fields that are either *immutable* in transit or that are *predictable* in value upon arrival at the endpoint for the AH SA, e.g., source address (immutable), destination address with source routing (mutable but predictable)
- The AH header (Next Header, Payload Len, Reserved, SPI, Sequence Number, and the Authentication Data (which is set to zero for this computation), and explicit padding bytes (if any))
- The upper level protocol data, which is assumed to be immutable in transit

ESP Packet



- Payload data: IP, TCP, UDP packet
- Pad Length in bytes
- Next Header: Type of payload (TCP, UDP, …)
- Authentication Data: Integrity Check Value over ESP packet

Encapsulating Security Payload (ESP)

- Provides encryption and/or integrity
  $\Rightarrow$ Confidentiality=ESP, Integrity=AH or ESP, Confidentiality+Integrity=ESP, ESP+AH
- Null encryption algorithm $\Rightarrow$ No confidentiality
- IV and authentication data sizes available from SA database

Current State of IPsec

- Best currently existing VPN standard
  - For example, used in Cisco PIX firewall, many remote access gateways
- IPsec has been out for a few years, but wide deployment has been hindered by complexity

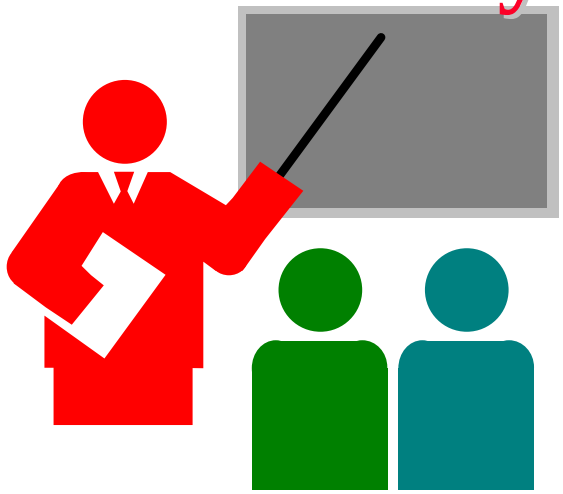
AH Version 3

- RFC4302, December 2005 (V2 in RFC2402, November 1998, V1 in RFC1826, August 1995)
- Uniform algorithm for Security Parameter Index (SPI) for unicast and multicast
- Unicast: SPI alone, or SPI+protocol may be used to select SA
- Multicast: SPI+DA or SPI+DA+SA
- Extended 64-bit sequence numbers for high-speed communications
- Separate RFC for mandatory algorithms

ESP Version 3

- RFC4303, December 2005 (V2 in RFC2406, November 1998, V1 in RFC1827, August 1995)
- Uniform algorithm for SPI for unicast and multicast
- Extended 64-bit sequence numbers
- Separate RFC for mandatory algorithms
- Combined Mode algorithms: Combined Confidentiality+Integrity algorithms in addition to separate confidentiality and integrity algorithms
- Can add extra bytes before padding for traffic flow confidentiality
- Can generate and discard dummy padding packets (Next header=59)
- Issue: No version number in the header. But older versions will reject new algorithms and options

Summary



1. Design Issues: Perfect forward secrecy, Denial of Service Protection, End Point Identifier hiding, Live partner assurance
2. NAT, Firewall, Proxy Servers, Tunnel (Encapsulation)
3. Security Association and Security parameter index
4. AH is for integrity
5. ESP can be used for Confidentiality and/or integrity

Homework 13

- Read chapters 16 and 17 of the textbook.
- Submit answer to the following:

For each of the fields in IPv4 header, indicate whether the field is immutable, mutable but predictable, or mutable (zeroed prior to ICV calculation).