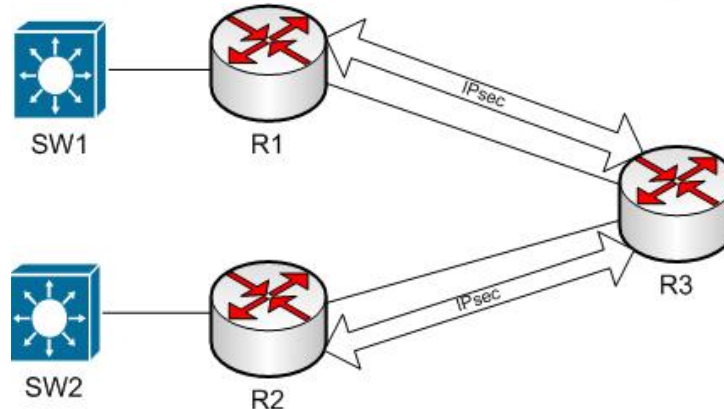


IP Security



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/cse571-17/>



1. IPSec
2. Authentication Header (AH)
3. Encapsulating Security Payload (ESP)
4. Internet Key Exchange (IKE)

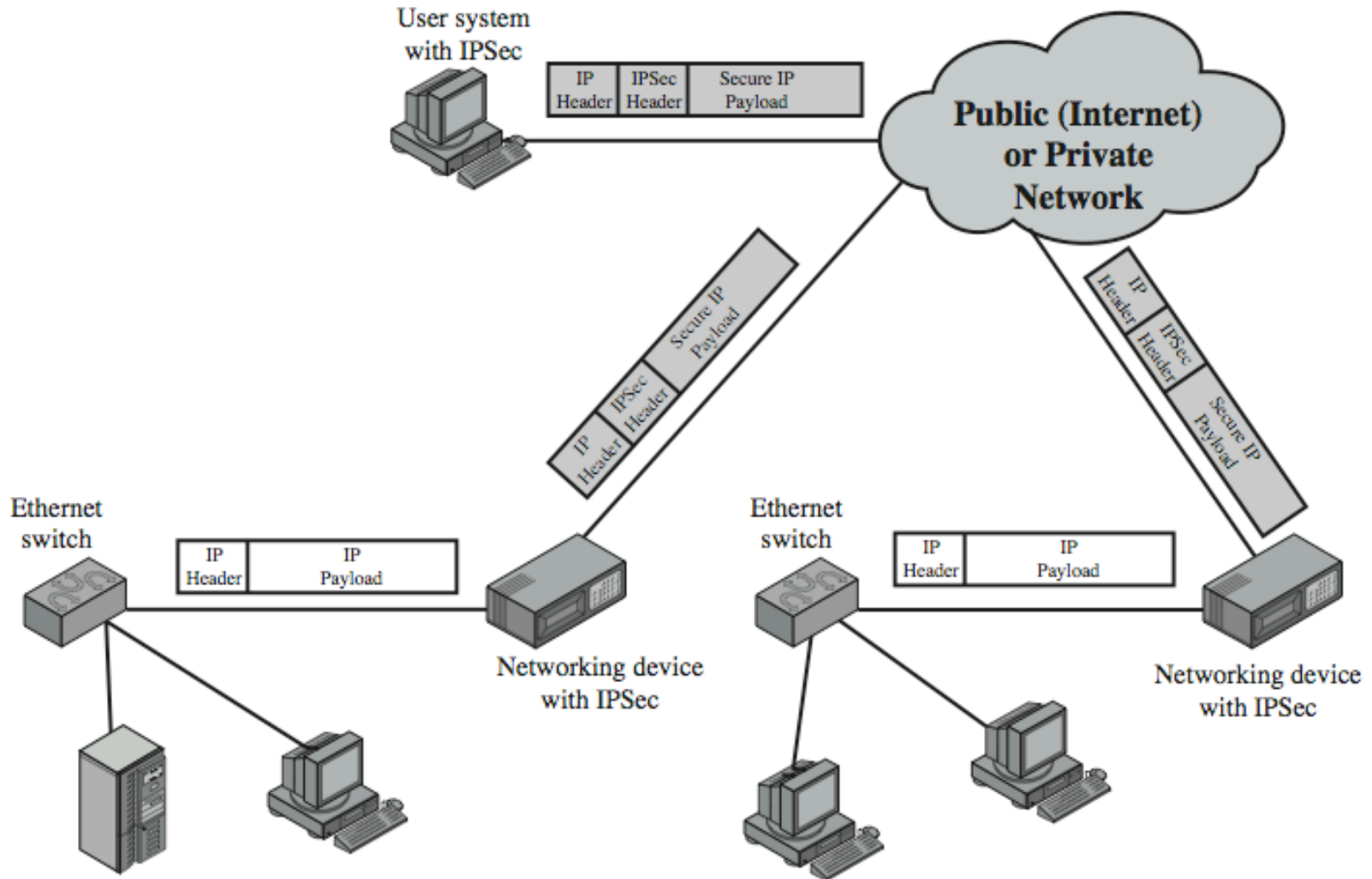
These slides are based partly on Lawrie Brown's slides supplied with William Stallings's book "Cryptography and Network Security: Principles and Practice," 7th Ed, 2017.

IP Security

- ❑ IPsec provides
 - Access control: User authentication
 - Data integrity
 - Data origin authentication
 - Rejection of replayed packets
 - Confidentiality (encryption)
 - Limited traffic flow confidentiality
- ❑ Benefits:
 - Security at Layer 3 ⇒ Applies to all transports/applications
 - Can be implemented in Firewall/router
 - ⇒ Security to all traffic crossing the perimeter
 - Transparent to applications and can be transparent to end users
 - Can provide security for individual users
- ❑ Applications: VPNs, Branch Offices, Remote Users, Extranets

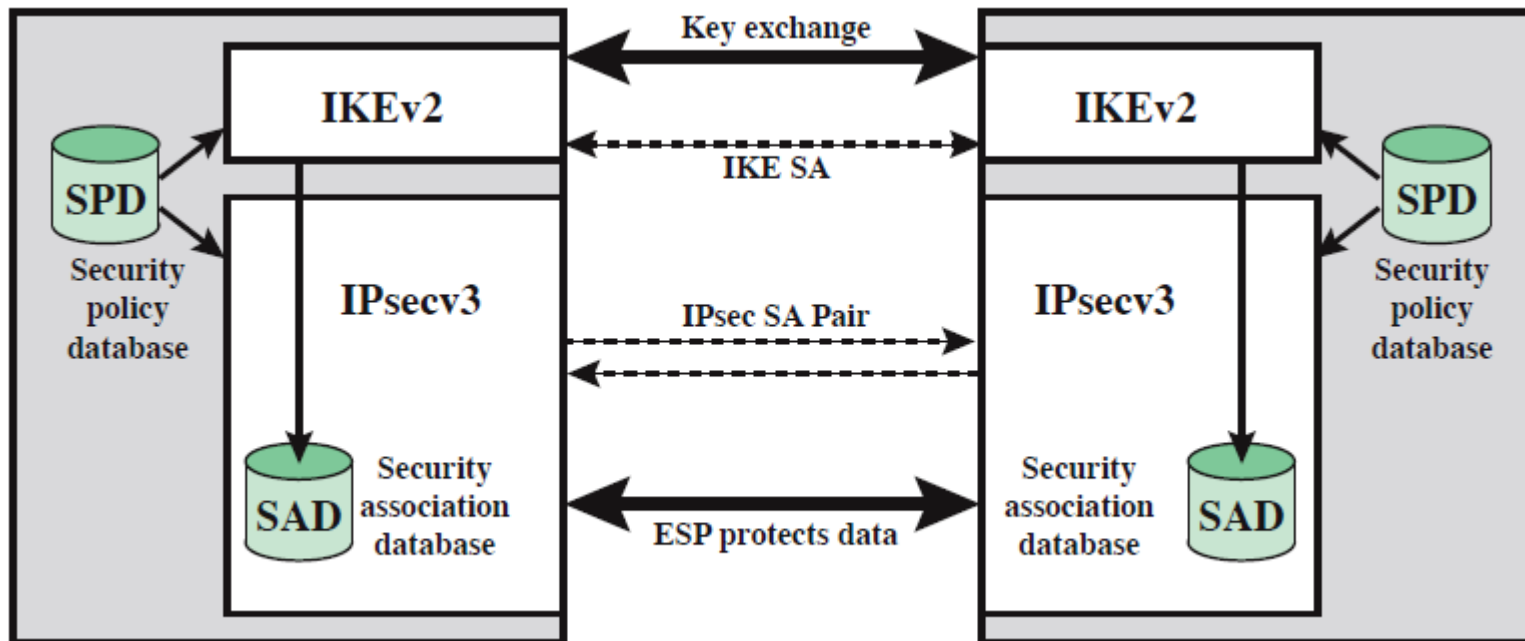
Ref: <http://en.wikipedia.org/wiki/IPsec>

IP Security Applications



IP Security Architecture

- ❑ Internet Key Exchange (IKE)
- ❑ IPsec
- ❑ Security Association Database
- ❑ Security Policy database



Security Association Database

- ❑ Each host has a database of Security Associations (SAs)
- ❑ SA = One-way security relationship between sender & receiver
Two-way may use different security \Rightarrow Two SA's required
- ❑ Defined by 3 parameters:
 - Security Parameters Index (SPI)
 - IP Destination Address
 - Security Protocol Identifier: AH or ESP
- ❑ For each SA, the database contains:
 - SPI
 - Sequence number counter and counter overflow flag
 - Anti-replay window
 - AH Information and ESP information
 - Lifetime of the SA
 - Mode: Transport or tunnel or wildcard
 - Path MTU

Ref: http://en.wikipedia.org/wiki/Security_association

Washington University in St. Louis

<http://www.cse.wustl.edu/~jain/cse571-17/>

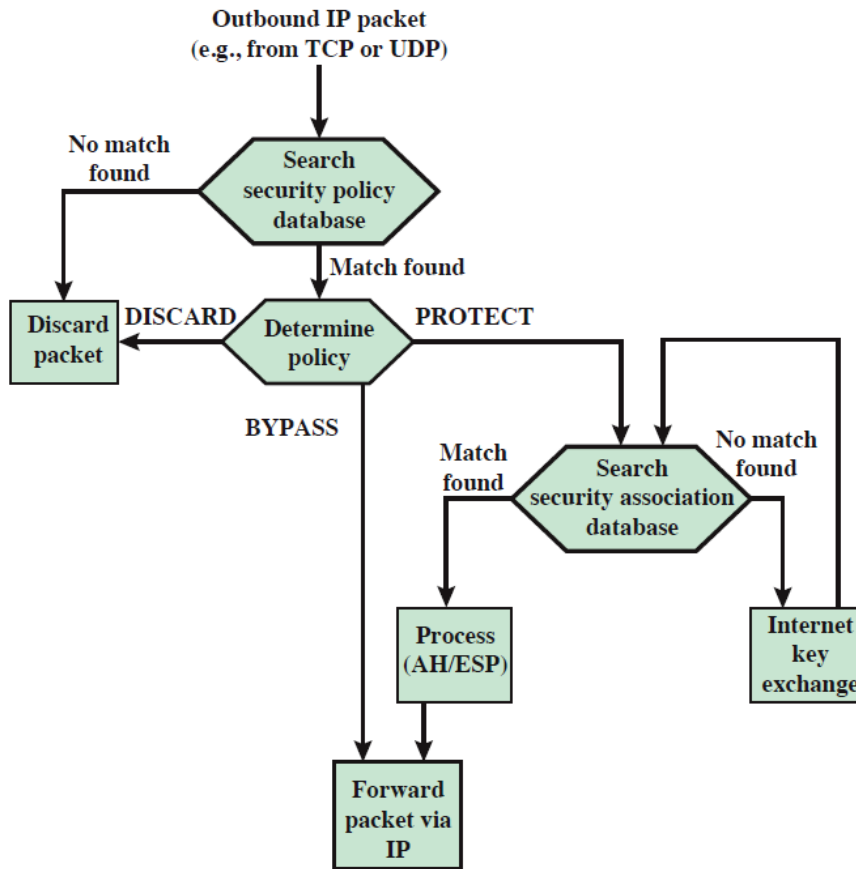
©2017 Raj Jain

Security Policy Database

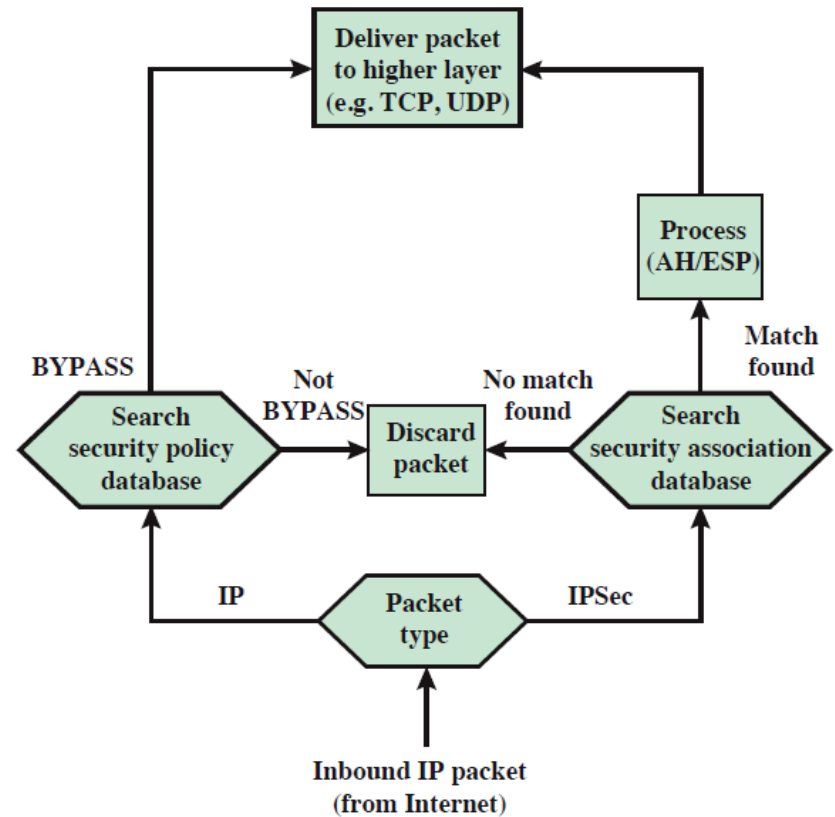
- ❑ Relates IP traffic to specific SAs
 - Match subset of IP traffic to relevant SA
 - Use selectors to filter outgoing traffic to map
 - Based on: local & remote IP addresses, next layer protocol, name, local & remote ports

| Protocol | Local IP | Port | Remote IP | Port | Action | Comment |
|----------|-----------|------|------------|------|-------------------------------|------------------------------|
| UDP | 1.2.3.101 | 500 | * | 500 | BYPASS | IKE |
| ICMP | 1.2.3.101 | * | * | * | BYPASS | Error messages |
| * | 1.2.3.101 | * | 1.2.3.0/24 | * | PROTECT: ESP intransport-mode | Encrypt intranet traffic |
| TCP | 1.2.3.101 | * | 1.2.4.10 | 80 | PROTECT: ESP intransport-mode | Encrypt to server |
| TCP | 1.2.3.101 | * | 1.2.4.10 | 443 | BYPASS | TLS: avoid double encryption |
| * | 1.2.3.101 | * | 1.2.4.0/24 | * | DISCARD | Others in DMZ |
| * | 1.2.3.101 | * | * | * | BYPASS | Internet |

Processing Models



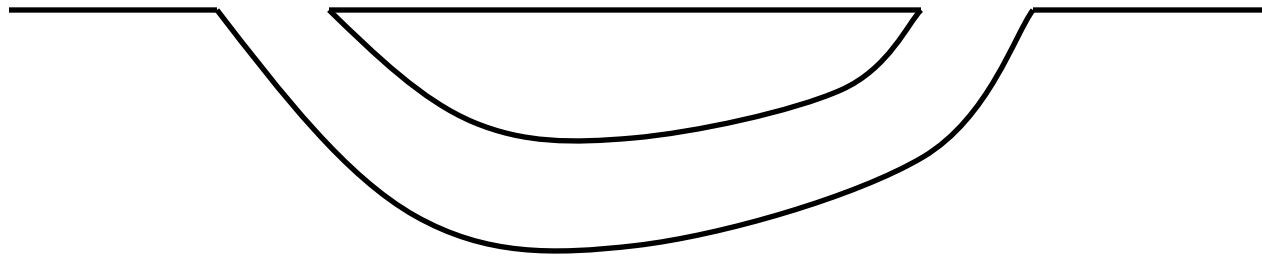
a. Outbound Packets



b. Inbound Packets

Tunnel

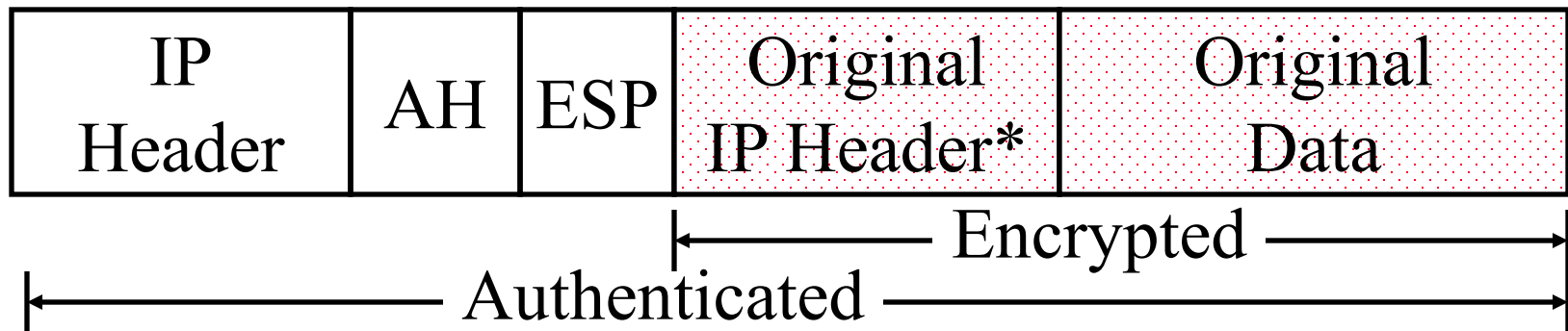
IP Land IP Not Spoken Here IP Land



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

IPSec

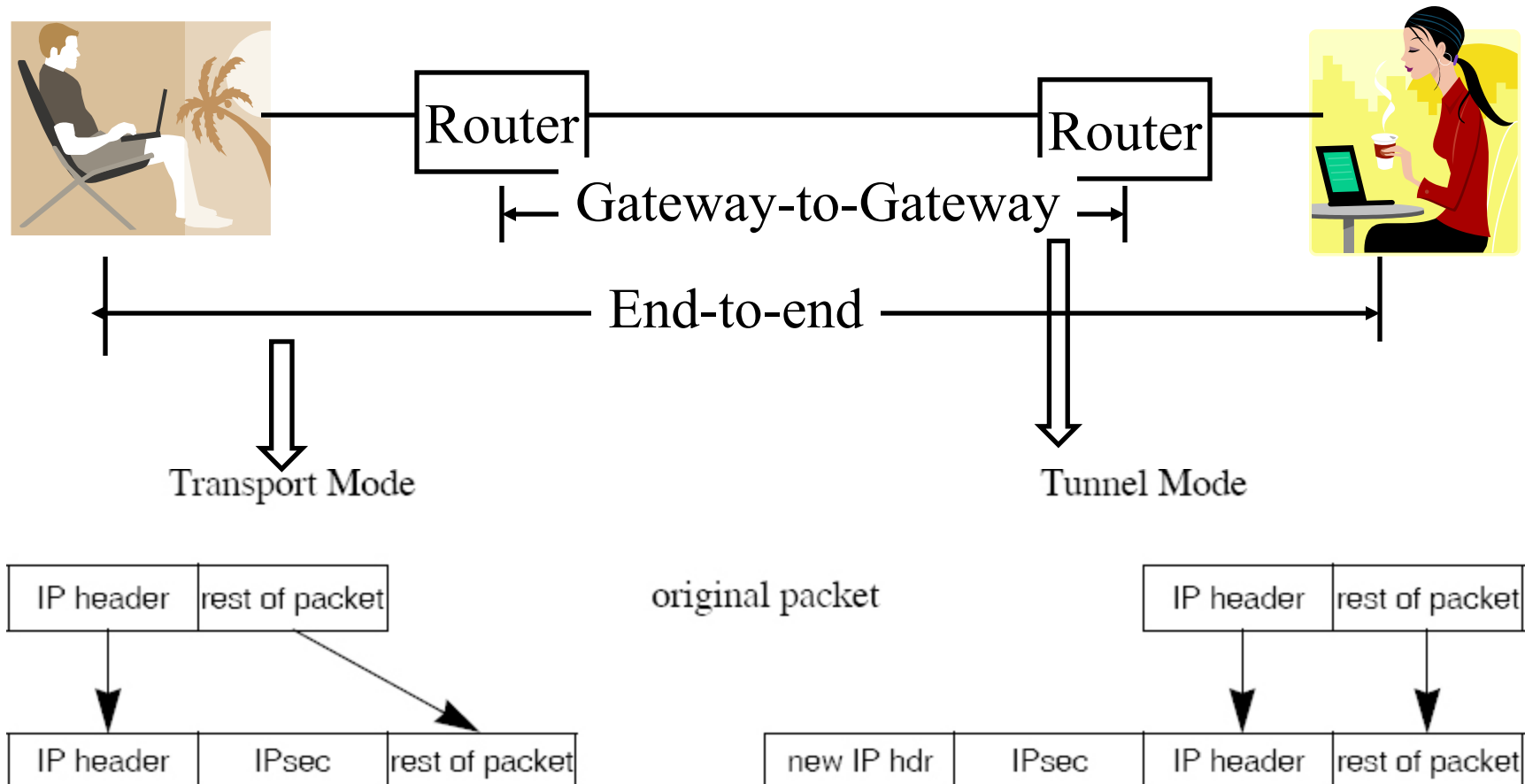
- ❑ Secure IP: A series of proposals from IETF
- ❑ Separate Authentication and privacy
- ❑ Authentication Header (AH) ensures data *integrity* and *data origin authentication*
- ❑ Encapsulating Security Protocol (ESP) ensures *confidentiality*, *data origin authentication*, *connectionless integrity*,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



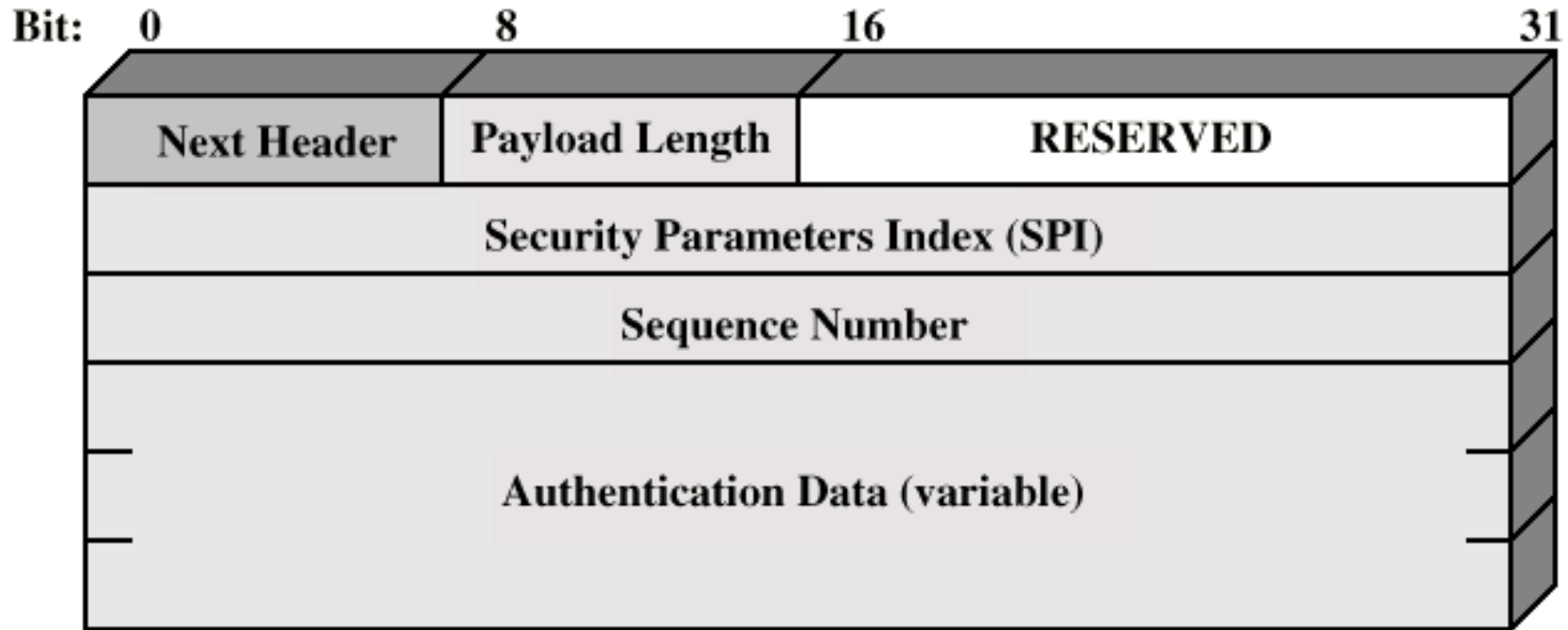
* Optional

Tunnel vs. Transport Mode

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

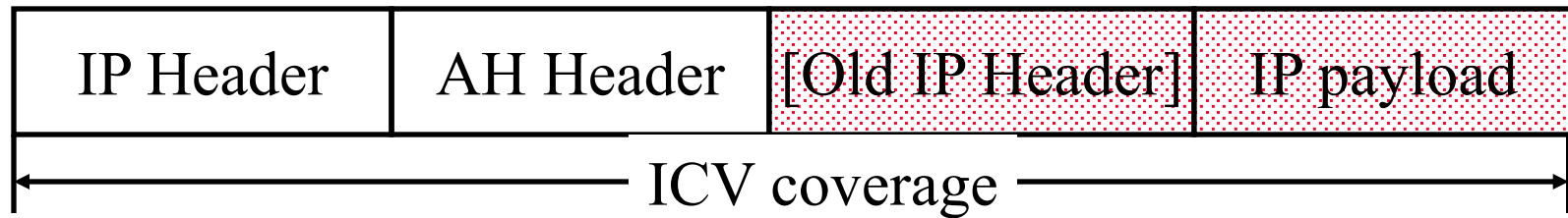


Authentication Header



- ❑ 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

AH Version 3

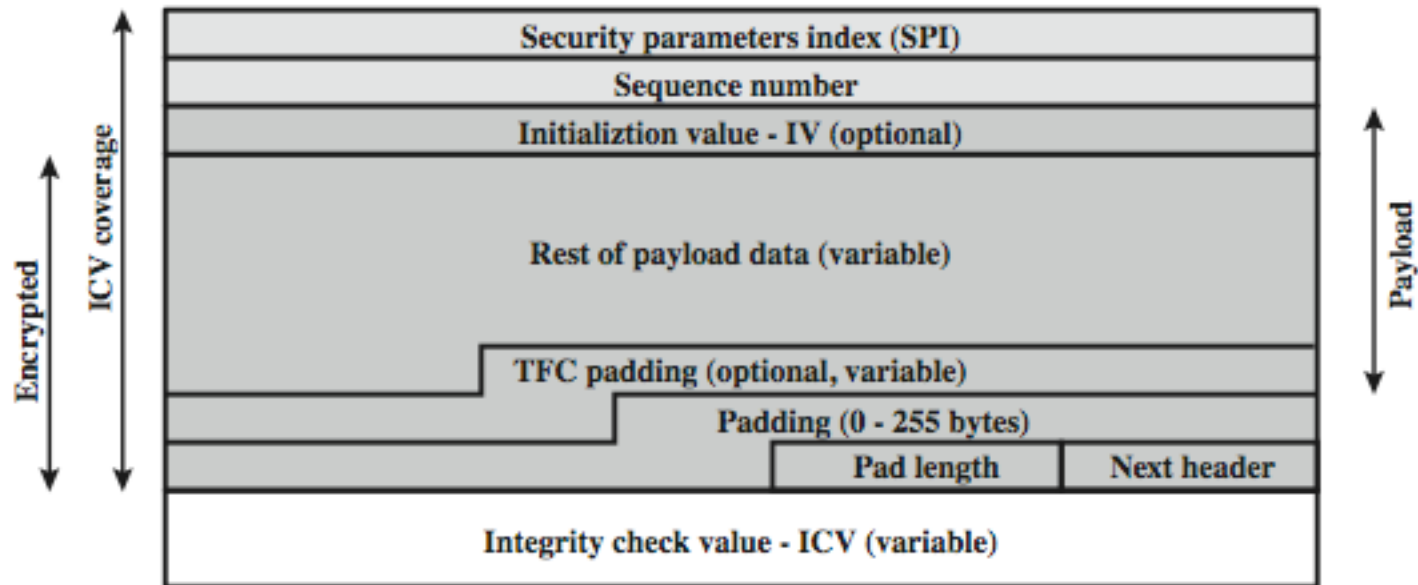
- ❑ RFC4302, December 2005 (V2 in RFC2402, November 1998, V1 in RFC1826, August 1995)
- ❑ Uniform algorithm for Security Parameter Index (SPI) for unicast and multicast
- ❑ Unicast: SPI alone, or SPI+protocol may be used to select SA
- ❑ Multicast: SPI+DA or SPI+DA+SA
- ❑ Extended 64-bit sequence numbers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

Encapsulating Security Payload (ESP)

Provides:

- ❑ Message content confidentiality,
- ❑ Data origin authentication,
- ❑ Connectionless integrity,
- ❑ Anti-replay service,
- ❑ Limited traffic flow confidentiality
- ❑ Services depend on options selected when establish Security Association (SA), net location
- ❑ Can use a variety of encryption & authentication algorithms

ESP Packet



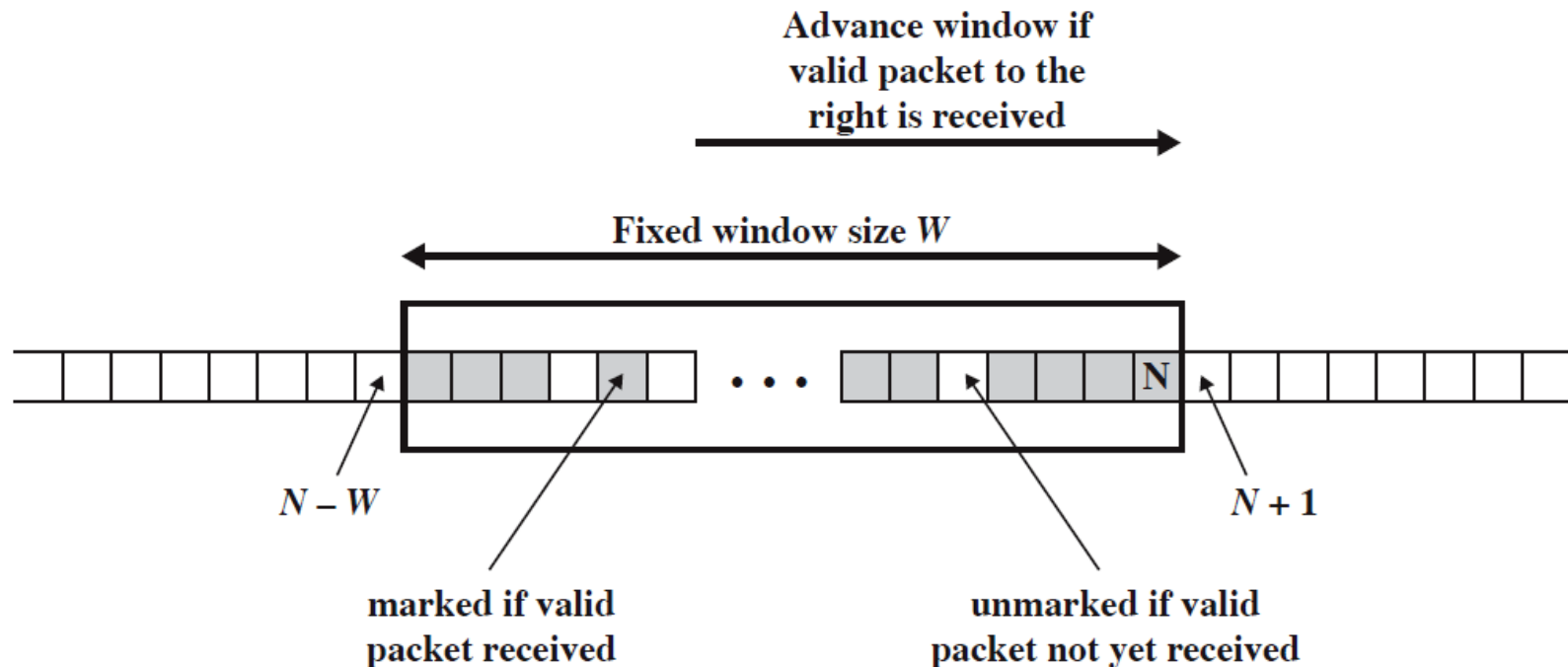
- ❑ Payload data: IP, TCP, UDP packet
- ❑ Pad Length in bytes
- ❑ Next Header: Type of payload (TCP, UDP, ...)
- ❑ Authentication Data: Integrity Check Value over ESP packet

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

Anti-Replay Service

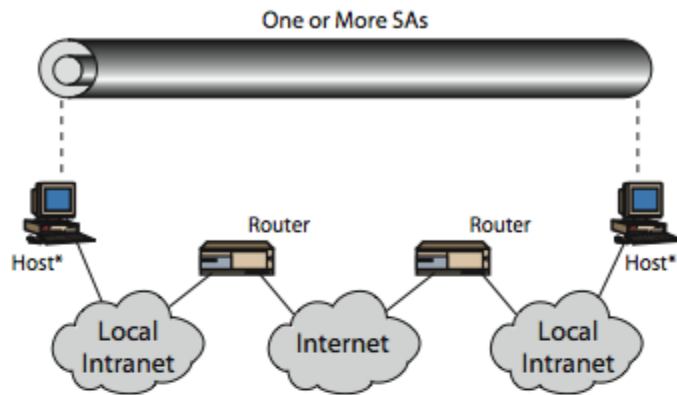
- ❑ Sender initializes sequence number to 0 when a new SA is established. Increment for each packet
- ❑ Receiver then accepts packets with sequence # within window of $(N - W + 1)$



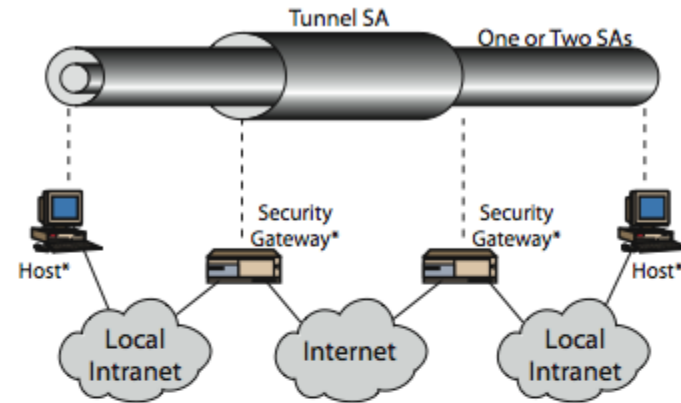
Combining Security Associations

- ❑ SAs can implement either AH or ESP
- ❑ To implement both need to combine SAs to form a security association bundle
- ❑ Transport adjacency: Outer AH over Inner ESP
- ❑ Iterated tunneling: Multiple with different end points
 - 1. All security between end-systems: AH Transport, ESP Transport, ESP inside AH transport, any one of the first 3 inside AH or ESP Tunnel
 - 2. Between gateways (routers or firewalls): Single SA. No nesting.
 - 3. Case 1 inside Case 2
 - 4. Tunnel between a remote host and firewall. One or two SAs may be used as in Case 1.

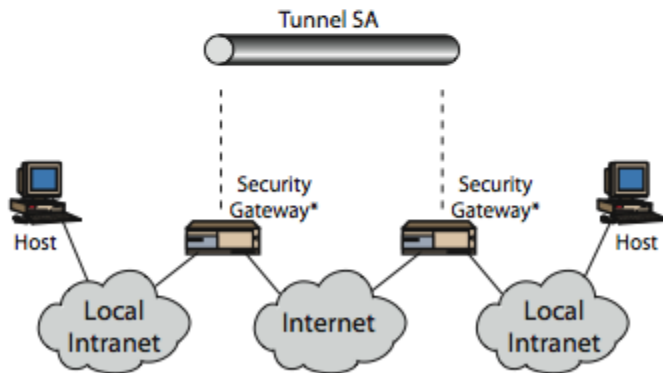
Combining Security Associations



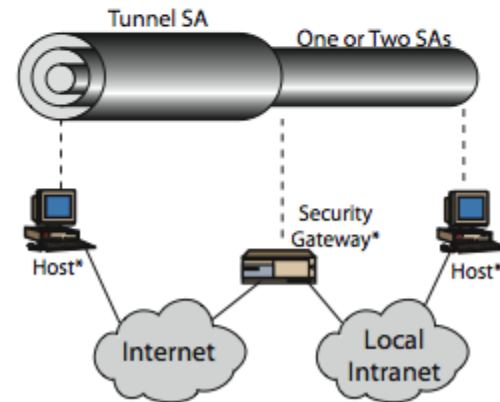
(a) Case 1



(c) Case 3



(b) Case 2



(d) Case 4

IPSec Key Management (IKE)

- ❑ Handles key generation & distribution
- ❑ Typically need 2 pairs of keys
 - 2 per direction for integrity and confidentiality
- ❑ Manual key management
 - Sys admin manually configures every system
- ❑ Automated key management
 - Automated system for on demand creation of keys for SA's in large systems
 - Oakley key exchange and ISAKMP key management
 - IKEv2 no longer uses Oakley & ISAKMP terms, but basic functionality is same

Ref: http://en.wikipedia.org/wiki/Internet_Key_Exchange

Oakley

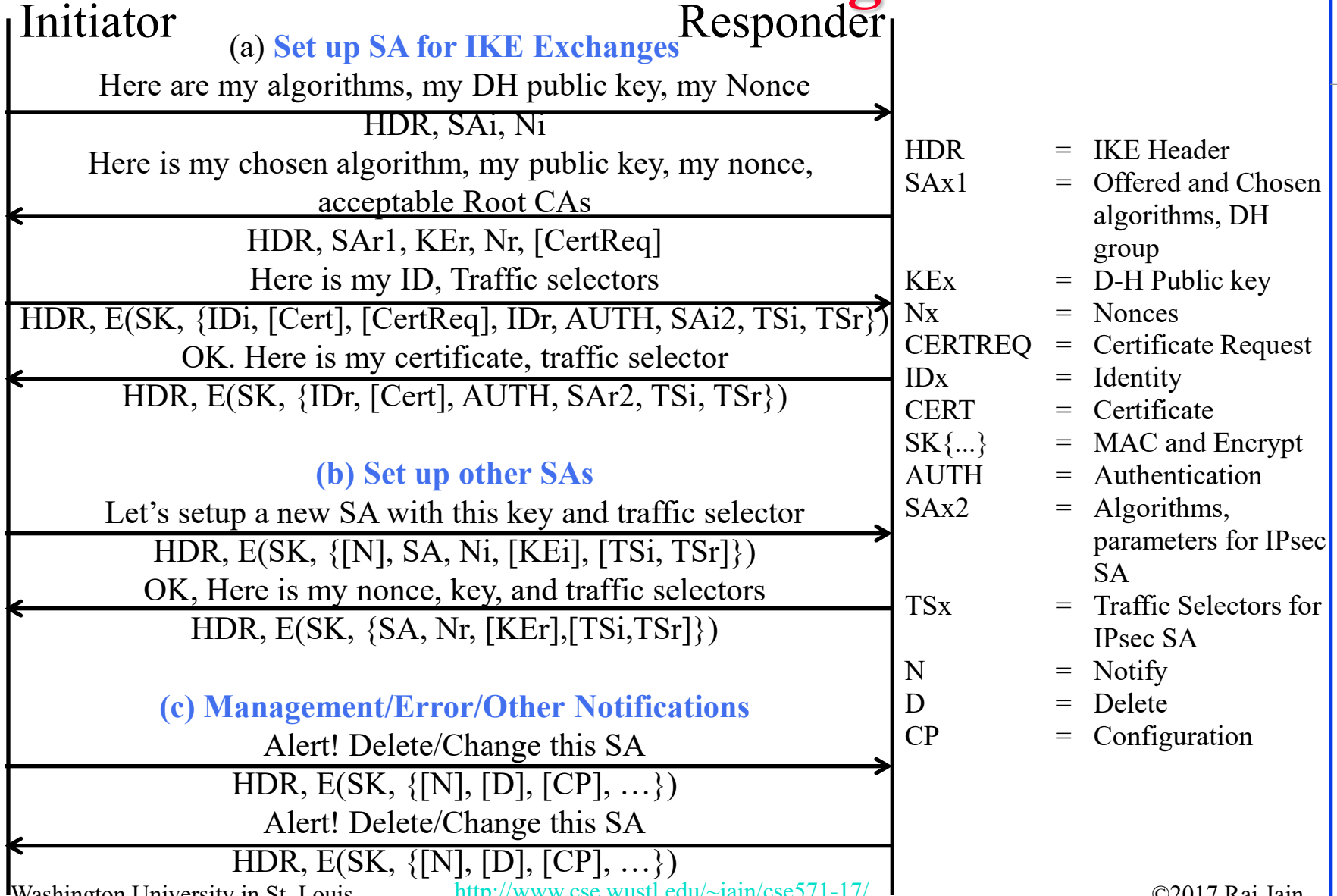
- ❑ A key determination protocol based on D-H key exchange
- ❑ Adds features to address weaknesses of D-H.
D-H has no info on identities of parties, is subject to man-in-middle attack, is computationally expensive
- ❑ Oakley adds
 - Cookies to thwart DoS attacks
 - Several groups of pre-specified global parameters
 - Nonces to protect against replay
 - DH public key exchange with authentication using Digital signature, Public Key Encryption, or Symmetric Key Encryption
- ❑ 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, and delete SAs
- ❑ Independent of key exchange protocol, encryption algorithm, and authentication method

Ref: http://en.wikipedia.org/wiki/Internet_Security_Association_and_Key_Management_Protocol

IKEV2 Exchanges

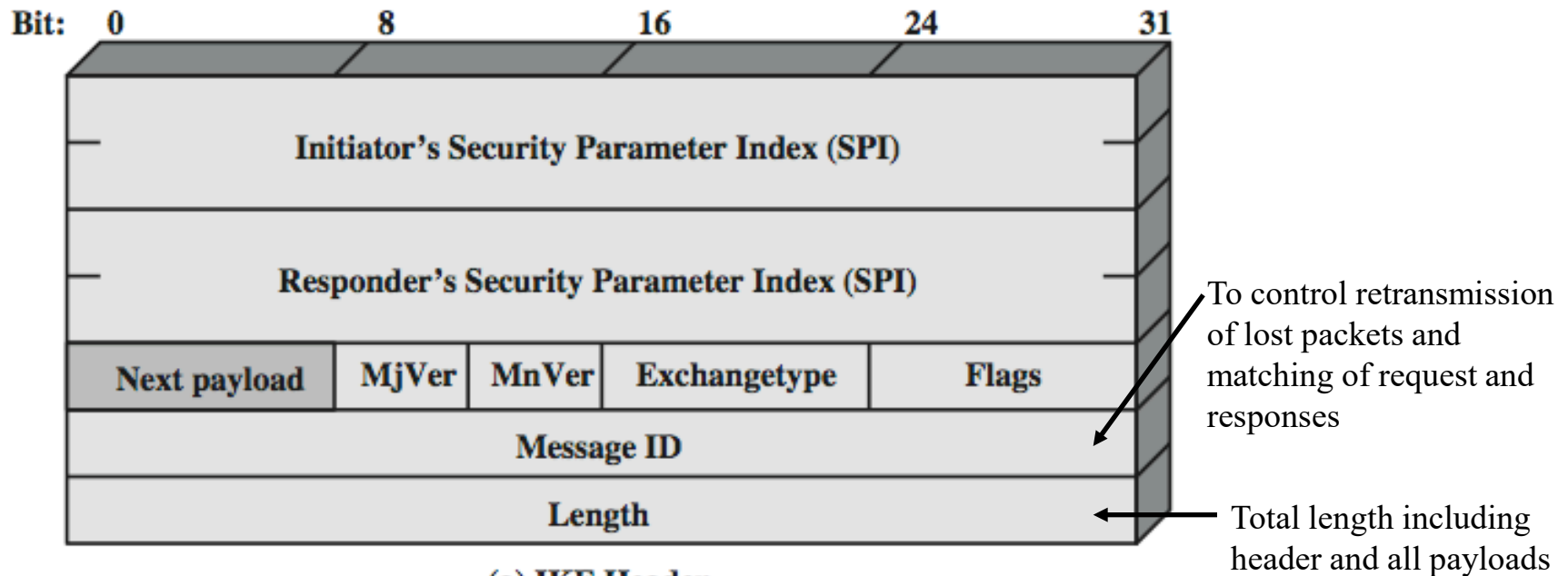


IKEv2 Exchanges (Cont)

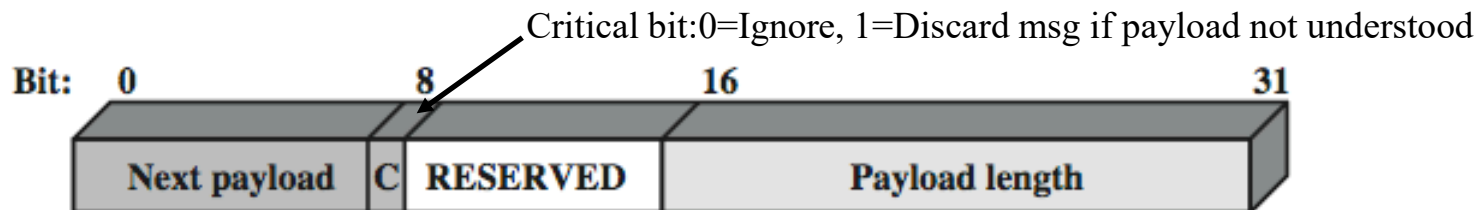
- ❑ KeySeed SK is generated by D-H exchange
- ❑ A Pseudo Random Function (PRF) is used with SK to generate all other keys
- ❑ Encryption Key + Integrity Key per side
⇒ Four keys/SA
- ❑ Traffic selectors specify the IP address range, ports, and IP protocol type for the SA

IKE Header and Payload Formats

- IKE messages= Header + one or more payloads



(a) IKE Header



(b) Generic Payload Header

IKE Payload Types

| Type | Parameters |
|------------------------------------|--|
| Security Association | Proposals = {Proposal={Protocol={Transform={Attribute}}}} |
| Key Exchange | DH Group #, Key Exchange Data = Data required to generated a session key |
| Identification | ID Type, ID Data |
| Certificate | Cert Encoding, Certificate Data |
| Certificate Request | Cert Encoding, Certification Authority |
| Authentication | Auth Method, Authentication Data |
| Nonce | Nonce Data |
| Notify | Protocol-ID, SPI Size, Notify Message Type, SPI, Notification Data =Errors or status |
| Delete | Protocol-ID, SPI Size, # of SPIs, SPI (one or more) = SAs that have been deleted |
| Vendor ID | Vendor ID |
| Traffic Selector | Number of TSs, Traffic Selectors |
| Encrypted | IV, Encrypted IKE payloads, Padding, Pad Length, ICV |
| Configuration | CFG Type, Configuration Attributes |
| Extensible Authentication Protocol | EAP Message |

Cryptographic Suites: VPN

- ❑ RFC 4308: VPN-A: Older, VPN-B: Stronger

| | VPN-A | VPN-B |
|----------------|---------------|-----------------------|
| ESP encryption | 3DES-CBC | AES-CBC (128-bit key) |
| ESP integrity | HMAC-SHA1-96 | AES-XCBC-MAC-96 |
| IKE encryption | 3DES-CBC | AES-CBC (128-bit key) |
| IKE PRF | HMAC-SHA1 | AES-XCBC-PRF-128 |
| IKE Integrity | HMAC-SHA1-96 | AES-XCBC-MAC-96 |
| IKE DH group | 1024-bit MODP | 2048-bit MODP |

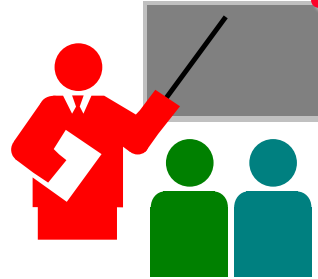
Cryptographic Suites: NSA Suite B

- Specified by NSA for use with sensitive information

| | GCM-128 | GCM-256 | GMAC-128 | GMAC-256 |
|------------------------------|-----------------------|-----------------------|------------------------|------------------------|
| ESP encryption/ Integrity | AES-GCM (128-bit key) | AES-GCM (256-bit key) | Null | Null |
| ESP integrity | Null | Null | AES-GMAC (128-bit key) | AES-GMAC (256-bit key) |
| IKE encryption | AES-CBC (128-bit key) | AES-CBC (256-bit key) | AES-CBC (128-bit key) | AES-CBC (256-bit key) |
| IKE PRF | HMAC-SHA-256 | HMAC-SHA-384 | HMAC-SHA-256 | HMAC-SHA-384 |
| IKE Integrity | HMAC-SHA-256-128 | HMAC-SHA-384-192 | HMAC-SHA-256-128 | HMAC-SHA-384-192 |
| IKE DH group | 256-bit random ECP | 384-bit random ECP | 256-bit random ECP | 384-bit random ECP |
| IKE authentication | ECDSA-256 | ECDSA-384 | ECDSA-256 | ECDSA-384 |

Ref: http://en.wikipedia.org/wiki/NSA_Suite_B_Cryptography

Summary



1. IPSec provides authentication, confidentiality, and key management at Layer 3. Applies to all traffic.
2. Security associations are one-way and can be bundled together.
3. Authentication header for message authentication using HMAC
4. Encapsulating security protocol (ESP) for confidentiality and/or integrity
5. Both can be used end-to-end with original IP header inside (Tunnel) or without original IP header (Transport) mode
6. Oakley is the IKE key determination protocol
7. ISAKMP is the IKE key management protocol

Homework 20

- ❑ A. For each of the fields in IPv4 header, indicate whether the field is immutable, mutable but predictable, or mutable (zeroed prior to ICV calculation).
- ❑ B. Suppose the current replay window spans from 60 to 124. What will the receiver do with a packet and what will the parameters of the window be if the next incoming packet has a sequence number:
 - a. 50
 - b. 100
 - c. 150

Lab 20: Create Certificates

- ❑ In this lab, you will learn how to create public-key certificates yourself using OpenSSL. You will generate 3 certificates: One for yourself as a certificate authority (CA) and then one for a Web server and another for a web client
- ❑ Download OpenSSL
 - Mac users: brew install openssl
 - Windows users:
<http://gnuwin32.sourceforge.net/packages/openssl.htm>
- ❑ Get familiar with OpenSSL
 - Windows users: cd to openssl directory and openssl --help
 - Mac users: openssl --help
- ❑ Create a directory to store your keys and certificates

Lab 20: Create Certificates (Cont)

1. Create a CA certificate:

- ❑ Create a certificate private key using OpenSSL
 - Hint: openssl genrsa -help
 - We need des3 and 2048 key length
- ❑ Remove the passphrase from yourkey.key
 - Hint: use openssl rsa --help
- ❑ Create a self-signed certificate for yourself as a CA
 - Hint: use openssl req --help
 - We need --x509 option and --day 999 plus some others

Lab 20: Create Certificates (Cont)

2. Create a Certificate for a Server

- ❑ Create a private key for the localhost server
 - Use `openssl genrsa --help`
 - Options: `des3`, `password`, `output key`
- ❑ Remove the passphrase from the key.
- ❑ Create a certificate signing request (CSR) for the created key
 - Hint: `openssl req --help`
- ❑ Create a certificate for the localhost server
 - Hint: Edit `openssl.cnf` file to reflect your directory (certificate locations)
 - `openssl ca -day ... -in (your CSR) -out (your.crt) -keyfile (CA key) -cert (CA cert) -policy policy_anything`

Lab 20: Create Certificates (Cont)

3. Create a certificate for a client

- ❑ Repeat all steps for part 2 for for the client
 - Create private key for a client
 - Remove passphrase
 - Create CSR for the client.
 - Create client certificate.
- ❑ Export the SSL client certificate in PKCS12 format
 - Hint: `openssl pkcs12 --help`
 - You need the options for each of the following: password, input certificate file (client), input key (client), certificate generated and the output PKCS12 file

Acronyms

- ❑ AH Authentication Header
- ❑ DA Destination Address
- ❑ DH Diffie-Hellman
- ❑ DoS Denial of Service
- ❑ ESP Encapsulating Security Payload
- ❑ HMAC Hybrid Message Authentication Code
- ❑ ICV Integrity Check Value
- ❑ IETF Internet Engineering Task Force
- ❑ IKE Internet Key Exchange
- ❑ IKEv2 Internet Key Exchange version 2
- ❑ IP Internet Protocol
- ❑ IPsec Internet Protocol Security
- ❑ IPv4 Internet Protocol version 4
- ❑ IPv6 Internet Protocol version 6
- ❑ ISAKMP Internet Security Association and Key Management Protocol
- ❑ MIB Management Information Base

Acronyms (Cont)

- ❑ MTU Maximum Transmission Unit
- ❑ NSA National Security Agency
- ❑ RFC Request for Comments
- ❑ SA Source Address
- ❑ SPI Security Parameters Index
- ❑ TCP Transmission Control Protocol
- ❑ TTL Time to Live
- ❑ UDP User Datagram Protocol
- ❑ VPN Virtual Private Network

Scan This to Download These Slides



Raj Jain

<http://rajjain.com>

Related Modules



CSE571S: Network Security (Spring 2017),
<http://www.cse.wustl.edu/~jain/cse571-17/index.html>

CSE473S: Introduction to Computer Networks (Fall 2016),
<http://www.cse.wustl.edu/~jain/cse473-16/index.html>



Wireless and Mobile Networking (Spring 2016),
<http://www.cse.wustl.edu/~jain/cse574-16/index.html>

CSE571S: Network Security (Fall 2014),
<http://www.cse.wustl.edu/~jain/cse571-14/index.html>



Audio/Video Recordings and Podcasts of
Professor Raj Jain's Lectures,
<https://www.youtube.com/channel/UCN4-5wzNP9-ruOzQMs-8NUw>