IP Security

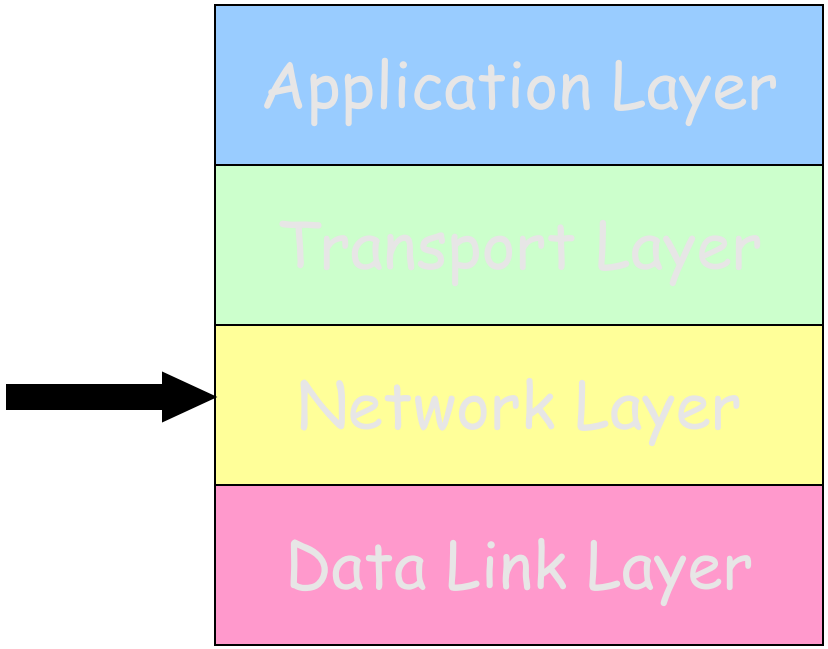
Cunsheng Ding
HKUST, Kong Kong, China

Outlines of the Two Lectures

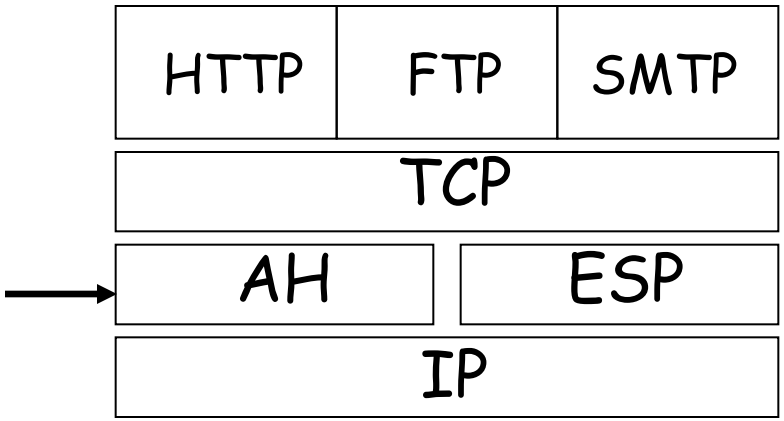
- Network layer security
- Brief introduction of IPSec
- IPSec building blocks
  - Security association database
  - Security policy database
  - Sub-protocols
    - AH and ESP
    - Two modes of AH and ESP
  - The outline of the key management (IKE)
- IPSec workflow
- Anti-replay in IPSec (see Appendix 1)

Network Layer and Its Security

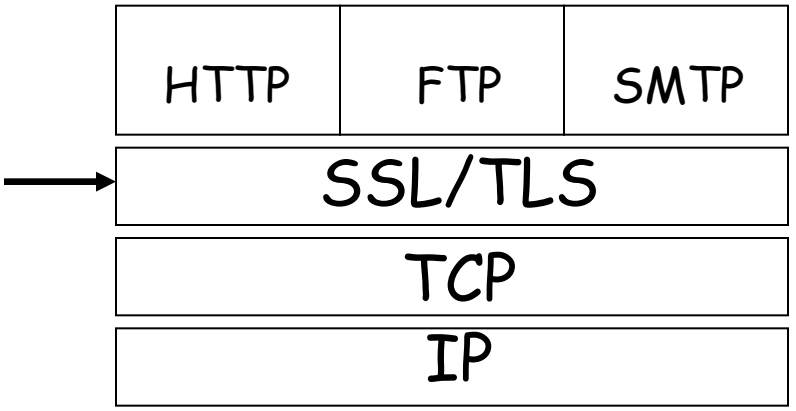
TCP/IP Protocol Stack



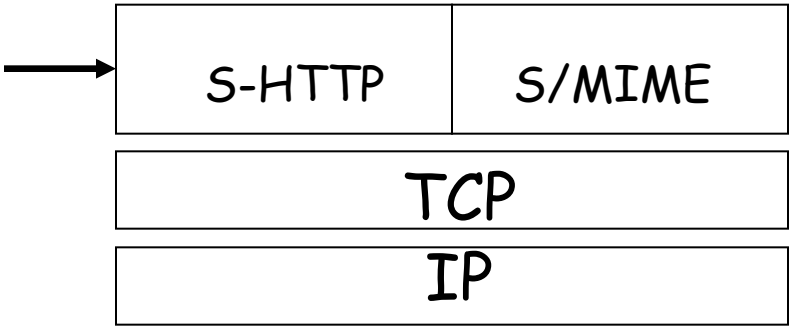
Where can we put security?



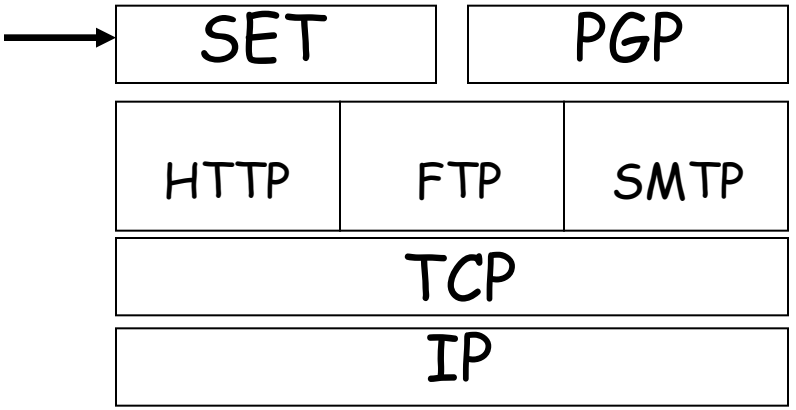
Network approach



Transport approach



Application approach



Presentation approach

Network Layer

- Provides connectionless service
- Routing (routers): determine the path: a path has to traverse to reach its destination
- Defines addressing mechanism
  - Hosts should conform to the addressing mechanism

Network Layer and Security

In most network architecture and corresponding communication protocol stack: *network layer protocol data units are transmitted in the clear*:

- Easy to inspect the data content
- Easy to forge source or destination address
- Easy to modify content
- Easy to replay data

$\Rightarrow$ Need network layer security protocol
IPSec is designed for this purpose

Brief Introduction to IPSec

Internet Engineering Task Force Standardization

- 1992: IPSEC WG (IETF)
  - Define security architecture
  - Standardize IP Security Protocol and Internet Key Management Protocol
- **1998: revised version of IPSec Architecture**
  - *IPsec protocols* (two sub-protocols AH & ESP)
  - *Internet Key Exchange* (IKE)
- 2005: updated version (RFC4301-4306
- Implementation: Windows 7, XP, 2000, Vista; Mac OS X, Free BSD, HP-UX

IPSec: Network Approach

- Provides security for IP and upper layer protocols
- Suit of algorithms:
  - Mandatory-to-implement
    - Assures interoperability
  - Easy to add new algorithms

IP Security Overview

IPSec provides the following:

- Data origin authentication
- Connectionless data integrity
- Data content confidentiality
- Anti-replay protection
- Limited traffic flow confidentiality

Building Blocks:
Security Association Database

Security Association

- It is a one-way relationship between a sender and a receiver, stored in the SAD.
- It associates security services and keys with the traffic to be protected.
- It is uniquely identified by three parameters:
  - Security Parameter Index (SPI)
    - A bit string assigned to this SA
    - The SPI is carried in AH or ESP headers to enable the receiving system to select the SA under which a receiving packet will be processed.
  - IPSec protocol identifier (AH or ESP)
  - Destination address (direction, firewall, router)

Security Association

- Defines *security services* and *mechanisms* between two end points (or IPsec modules):
  - Hosts
  - Network security gateways (e.g., routers, application gateways)
  - Hosts and security gateways
- Defines parameters, mode of operation, and initialization vector
  - e.g., Confidentiality using ESP with DES in CBC mode with IV initialization vector
- May use either Authentication Header (AH) or Encapsulating Security Payload (ESP).

Security Association

- **Host A Security Association:**

```
# ipsecadm new esp -spi 1000 -src HostA \
  -dst HostB -forcetunnel -enc 3des -auth sha1 \
  -key 7762d8707255d974168cbb1d274f8bed4cbd3364 \
  -authkey 6a20367e21c66e5a40739db293cf2ef2a4e6659f
```

- **Host B Security Association:**

```
# ipsecadm new esp -spi 1001 -src HostB \
  -dst HostA -forcetunnel -enc 3des -auth sha1 \
  -key 7762d8707255d974168cbb1d274f8bed4cbd3364 \
  -authkey 6a20367e21c66e5a40739db293cf2ef2a4e6659f
```

RemarK: src = source, dst = destination, keysize = 160 bits

spi is a binary string at most 32 bits, used to create and delete SA, the spi values between 0 and 100 are reserved.

SA Parameters

- Sequence Number counter (defined later)
- Sequence Counter Overflow (defined later)
- Anti-replay Window (defined later)
- AH information (defined later)
- ESP information (defined later)
- Lifetime of this SA
- IPSec Protocol Mode (Tunnel, Transport)
- Path MTU: maximum size of a packet that can be transmitted without fragmentation

SA -- Lifetime

- Amount of traffic protected by a key and time frame the same key is used
  - Manual creation: no lifetime
  - Dynamic creation: may have a lifetime

Building Blocks:
Security Policy Database

Security Policy Database (SPD)

- Defines:
  - What traffic to be protected
  - How to protect
  - With whom the protection is shared
- For each packet entering or leaving an IPsec implementation, SPD is used to determine security mechanism to be applied
- Actions:
  - Discard: do not let packet in or out
  - Bypass: do not apply or expect security services
  - Protect: apply/expect security services on packets

Building Blocks:
IPSec Protocols

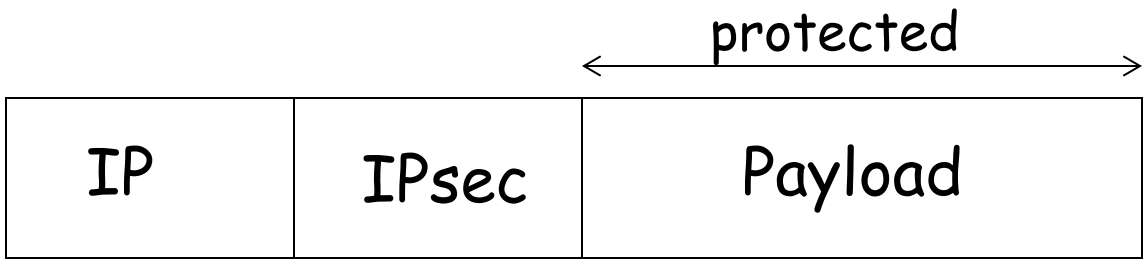
IPSec Protocols

- *Encapsulating Security Payload (ESP)*
  - Data confidentiality and limited traffic flow confidentiality
  - Anti-replay protection
  - Proof of data origin, data integrity (optional)
- *Authentication Header (AH)*
  - Proof of data origin, data integrity
  - Anti-replay protection

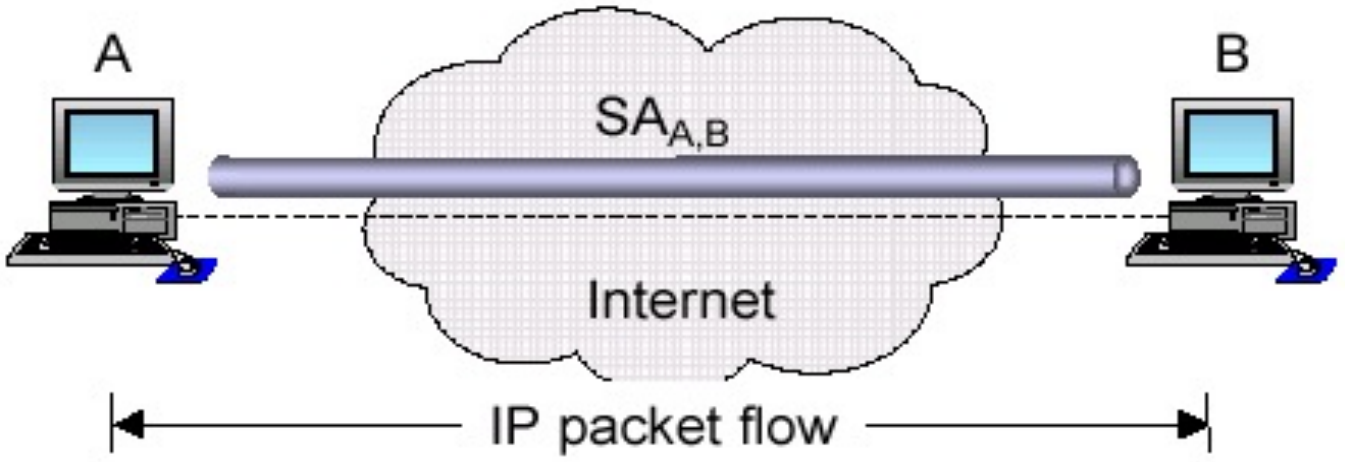
Transport and Tunnel Modes

Transport Mode: AH & ESP

- **Usage:** protect upper layer protocols
  - IPSec header is inserted between the IP header and the upper-layer protocol header
  - Communication endpoints must be cryptographic endpoints (for end-to-end authentication)



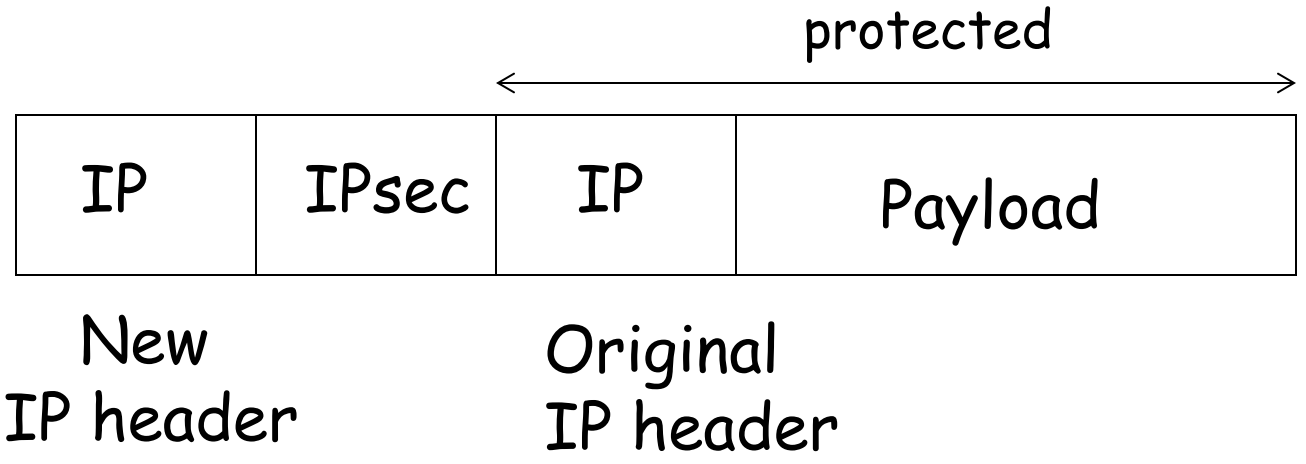
When is Transport Mode Used



Both endpoints are cryptographic endpoints, i.e. they generate / process an IPSec header (AH or ESP)

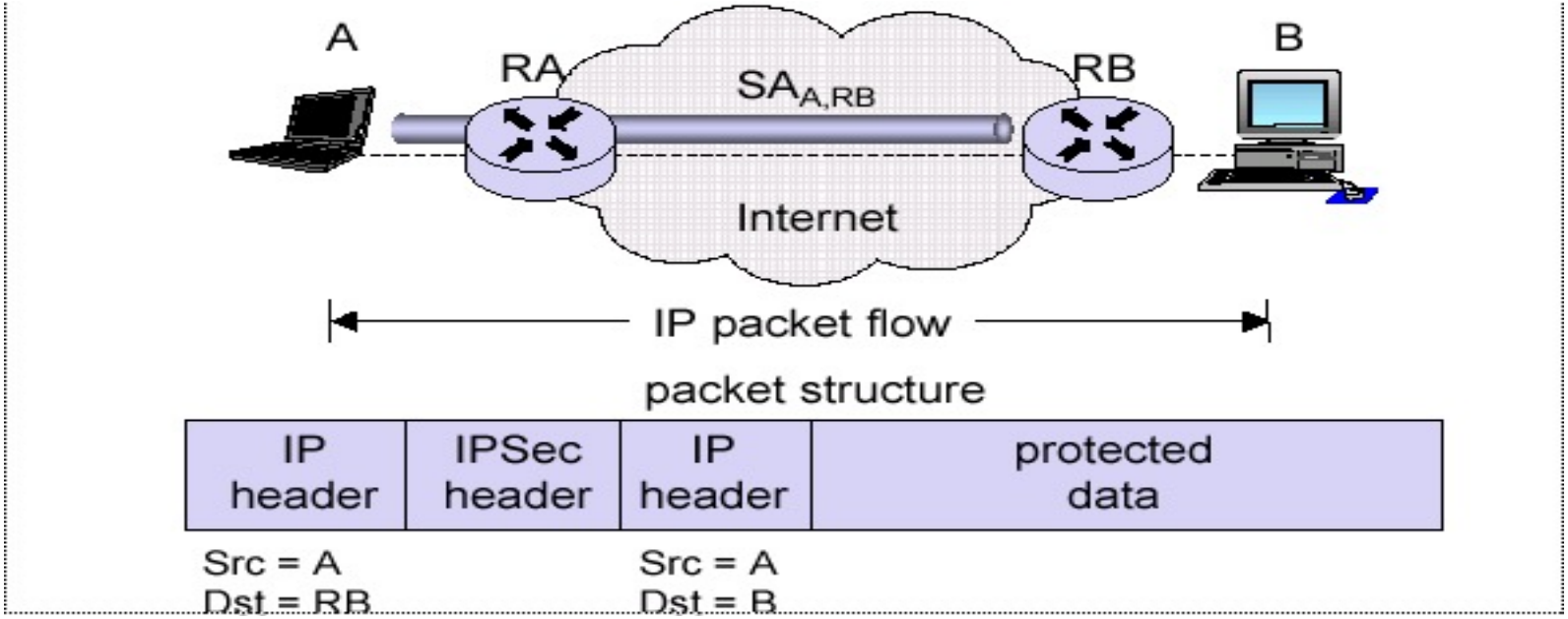
Tunnel Mode: AH & ESP

- **Usage:** protect entire IP datagram
  - Entire IP packet to be protected is encapsulated in another IP datagram and an IPsec header is inserted between the outer and inner IP headers



When Is Tunnel Mode Used

Tunnel mode is used when at least one cryptographic endpoint is not a communication endpoint of the secured IP packets.



Outer IP Header – Destination for the router.

Inner IP Header – Ultimate Destination

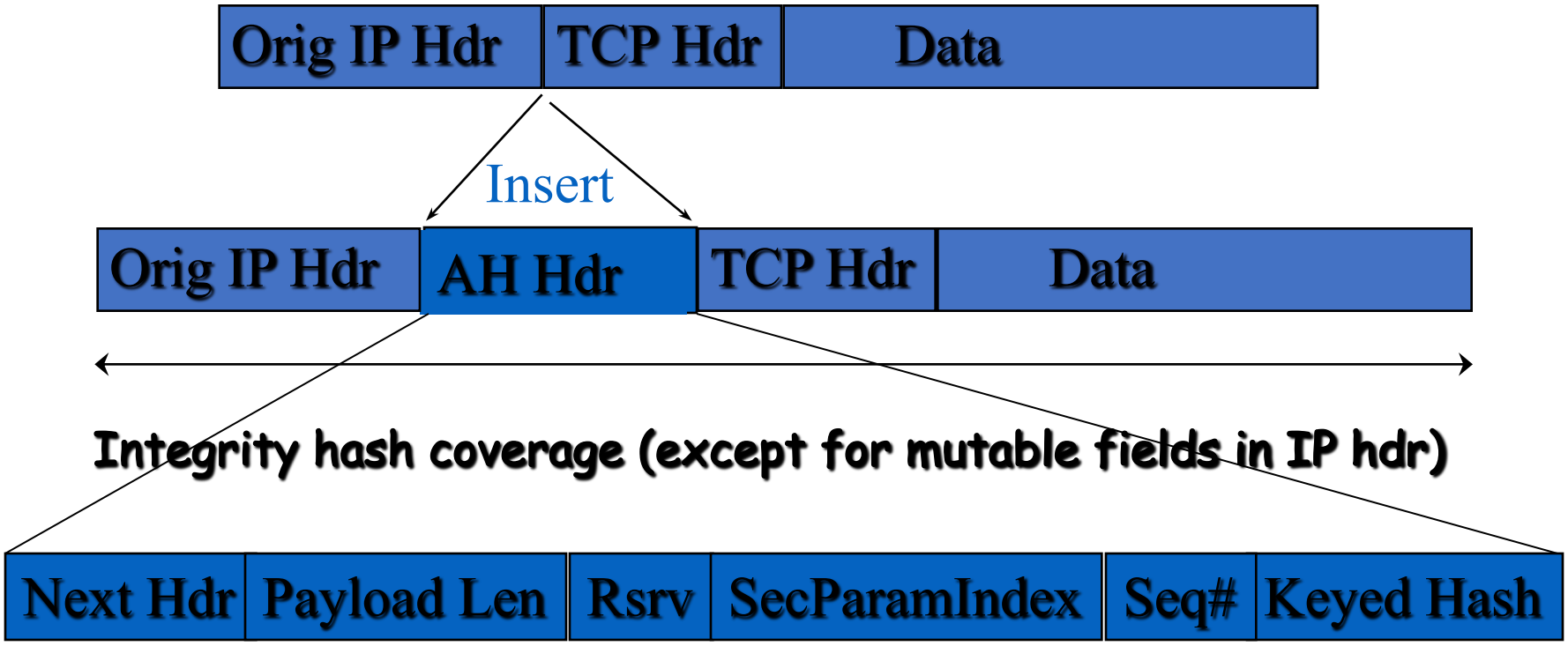
AH in Transport and Tunnel Modes

Authentication Header (AH)

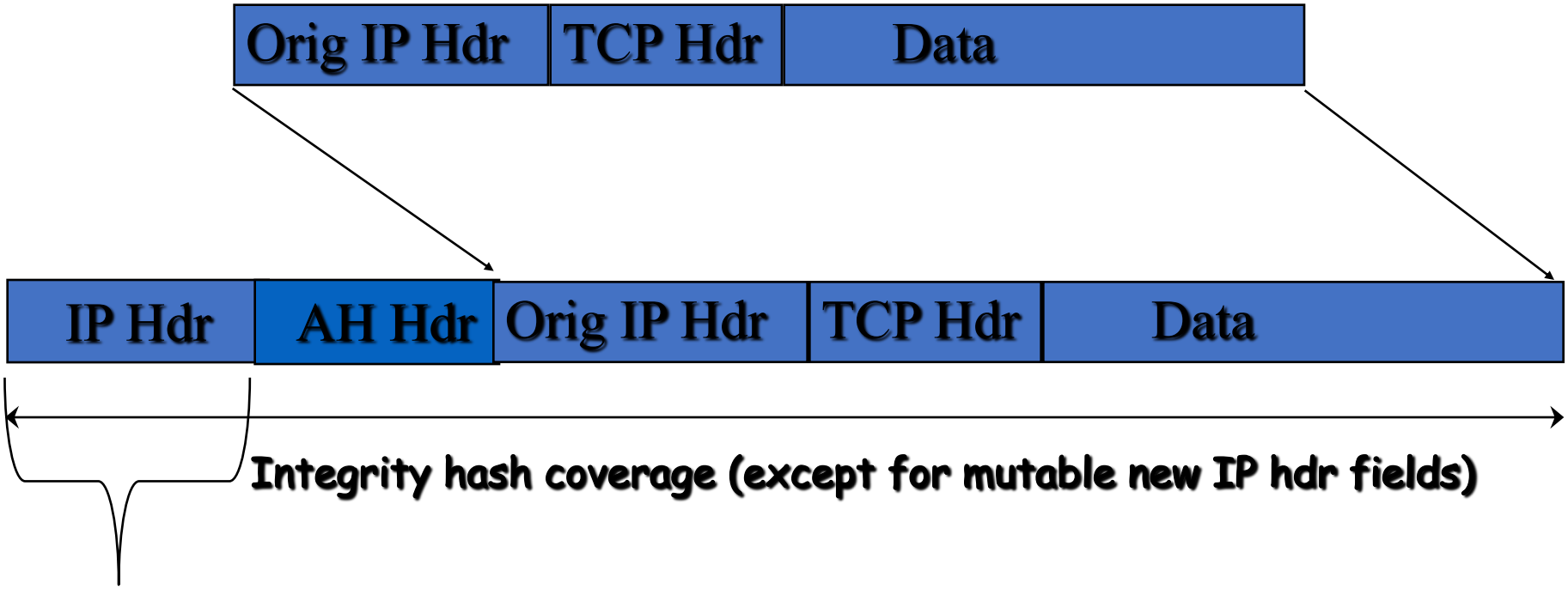
- Does NOT provide confidentiality
- Provides:
  - Data origin authentication
  - Connectionless data integrity
- May provide:
  - Non-repudiation (depends on cryptographic alg.)
  - Anti-replay protection

IPSec AH in Transport Mode

Question: Why insert AH there?

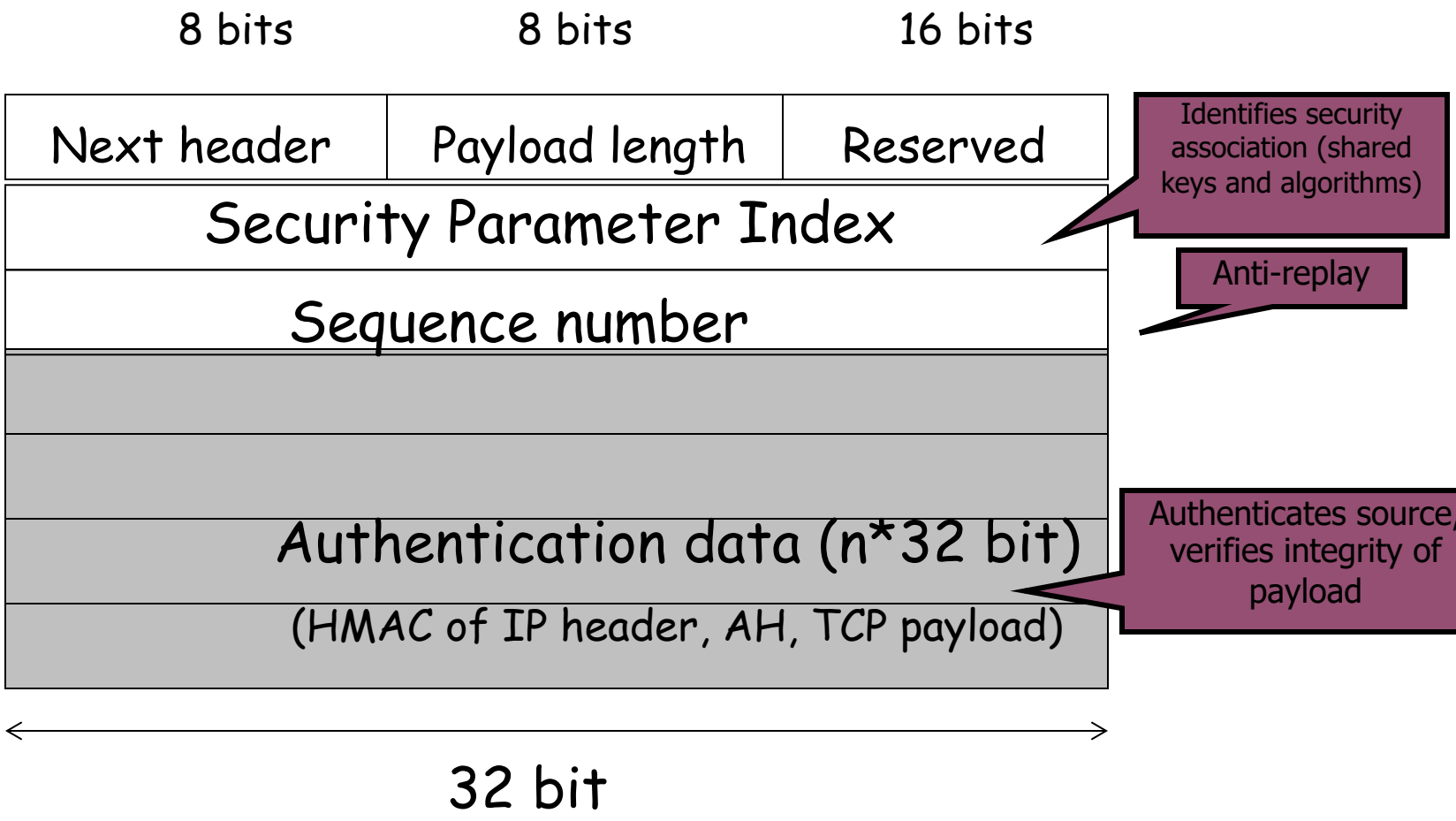


IPSec AH in Tunnel Mode



New IP header with source & destination IP address

AH Header Format



AH Header Format

- Next Header (8 bits): identifies the type of header immediately following this head.
- Payload Length (8 bits): Length of Authentication Header in 32-bit words.
- Reserved (16 bits): For future use.
- Security Parameters Index (32 bits): identifies a security association.
- Sequence Number (32 bits): A monotonically increasing counter value, discussed earlier.
- Authentication Data (variable): 32*n, contains ICV (integrity check value) or MAC for this packet.

Authentication Data

- Computed by using
  - authentication algorithm (MD5, SHA-1, SHA-2, SHA-3)
  - cryptographic key (authentication key)
- Sender: computes authentication data
- Recipient: verifies data

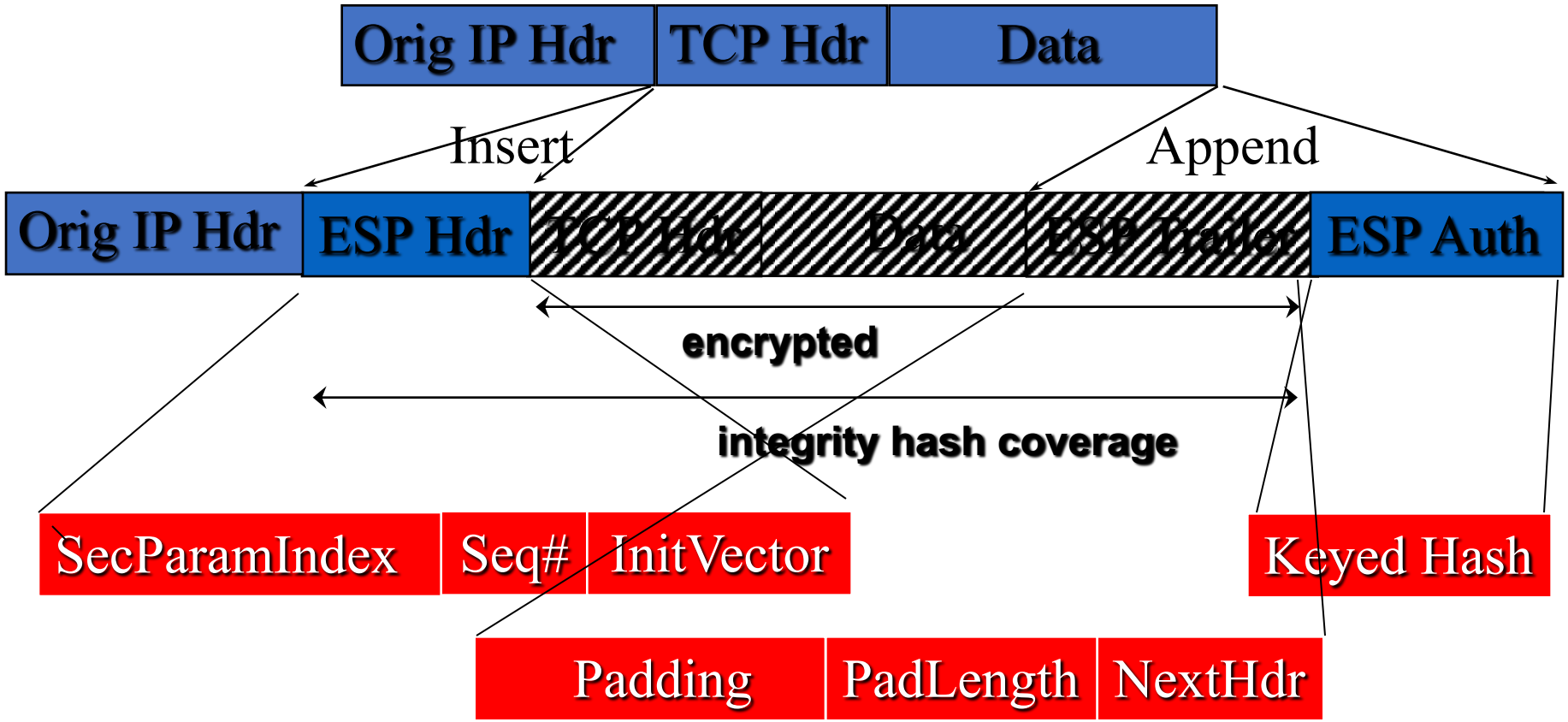
ESP in Transport and Tunnel Modes

Encapsulating Security Payload (ESP)

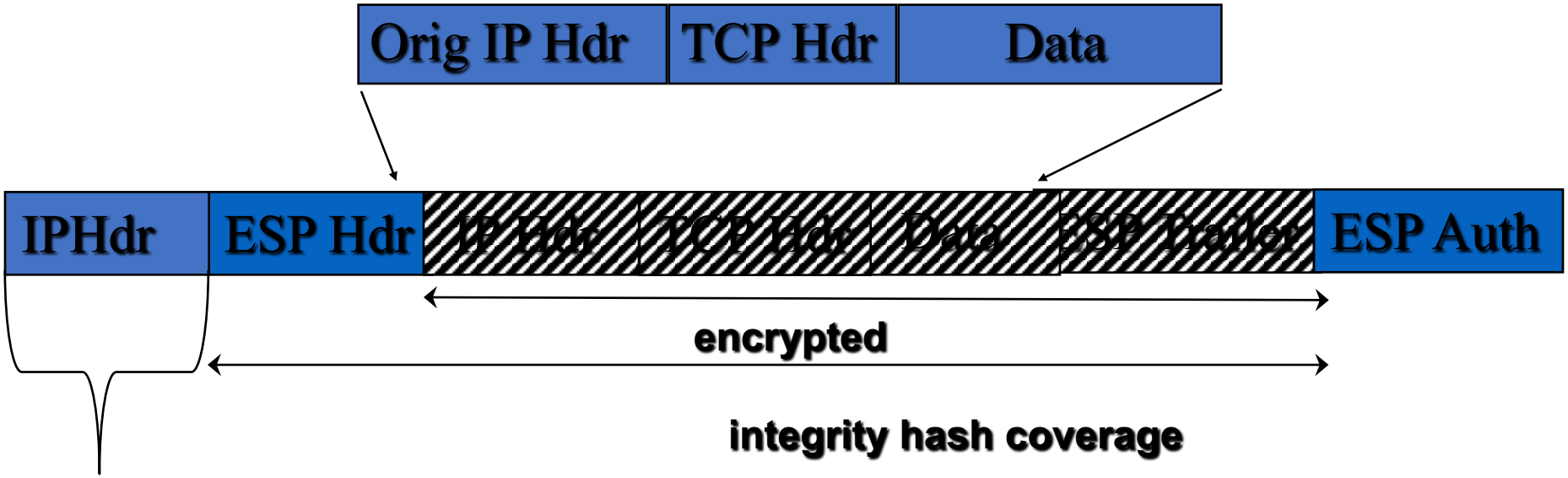
- Provides:
  - Confidentiality
  - Authentication
    - optional
    - not as strong as AH
  - Limited traffic flow confidentiality (in tunnel mode only)
  - Anti-replay protection

IPSec ESP in Transport Mode

Question: ESP Hdr, ESP trailer, ESP Auth. There?



IPSec ESP Tunnel Mode



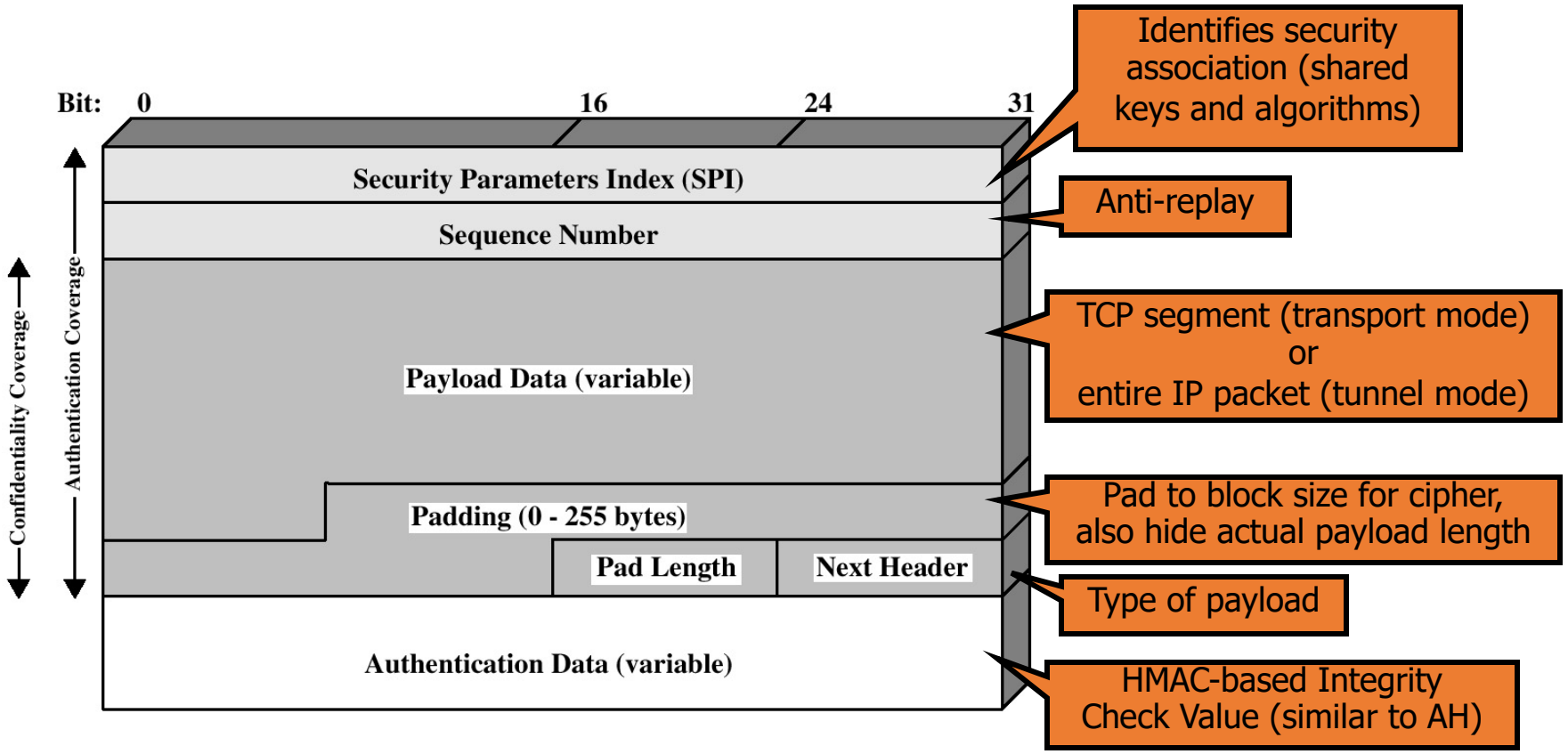
New IP header with source & destination IP address

Question: Why a new IP Hdr is generated?

ESP header and trailer

- ESP packet processing:
  1. Verify sequence number
  2. Verify integrity
  3. Decrypt
- ESP header: not encrypted (why?)
  - Contains: SPI and sequence number
- ESP trailer: usually encrypted
  - Contains: padding, length of padding, next protocol

ESP Format


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)
Confidentiality Coverage
Authentication Coverage
Identifies security association (shared keys and algorithms)
Anti-replay
TCP segment (transport mode) or entire IP packet (tunnel mode)
Pad to block size for cipher, also hide actual payload length
Type of payload
HMAC-based Integrity Check Value (similar to AH)

ESP Format ctd.

- Security Parameters Index (32 bits): identifies a security association.
- Sequence Number (32 bits): A monotonically increasing counter value, same as in AH.
- Payload Data (variable): A transport-level segment (transport mode) or IP packet (tunnel mode) that is protected by encryption.
- Padding (0-255 bytes): for encryption and others.
- Pad Length (8 bits): indicating the number of pad bytes immediately proceeding this field.

ESP Format ctd.

- Next Header (8 bits): Identifies the type of data contained in the payload data field by identifying the first header in that payload.

  E.g., an extension header in IPv6, or an upper layer protocol such as TCP.
- Authentication Data (variable): 32*n, contains the Integrity Check Value computed over the ESP packet minus Authentication Data Field.

ESP

- SA has multiple algorithms defined:
  - Cipher: for confidentiality
  - Authenticator: for authenticity
  - Each ESP has:
    - one cipher and one authenticator, or
    - one cipher and zero authenticator.
    - Disallowed: zero cipher and zero authenticator

Encryption, Authentication, Compression

Encryption and Authentication Algorithms

- Encryption:
  - Triple DES in CBC mode (MUST)
  - AES in CBC mode (SHOULD+)
  - AES in CTR (counter) mode (SHOULD)
- Authentication:
  - HMAC-MD5-96 (MAY)
    - 96 truncated bits from 128 bits
  - HMAC-SHA-1-96 (MUST)
    - 96 truncated bites from 160 bits
  - AES-XCBC-96 (SHOULD)

Summary of IPSec Services

	AH	ESP (encrp. Only)	ESP (encrp + auth)
Connectionless integrity	√		√
Data origin authentication	√		√
Anti-replay	√	√	√
Confidentiality		√	√
Limited traffic flow confidentiality		√	√

The Outline of the Key Management Protocol

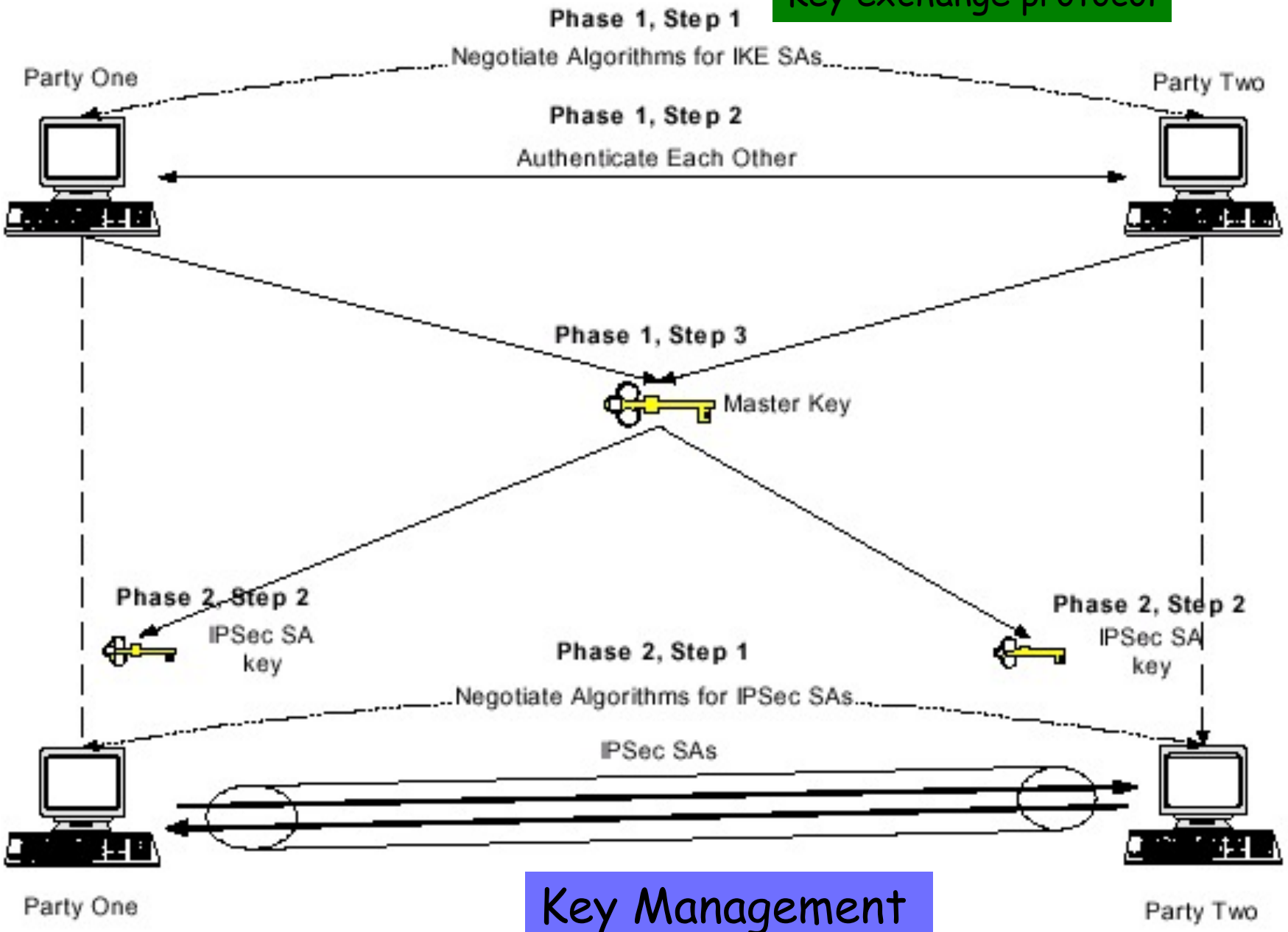
Key Management

- IPSec needs secret keys:
  - for transmitting and receiving both AH and ESP
- It supports two types of key management:
  - **Manual:** A system administrator manually configures each system with its own keys and with the keys of other communicating systems.
  - **Automated**: An automated system enable the on-demand creation of keys for SAs and facilitates the use of keys in a large distributed system with an evolving configuration.

Key Management Protocol

- The management protocol is called "Internet Key Exchange (IKE)".
- It has two versions.
  - IKE 1998, IKEv2 2005, revised IKEv2 2014
- It is the most complicated sub-protocol of IPSec.
- Outline of IKE 1998 will be given in this lecture.
- LKEv2 will be covered in Lecture 20.

Key exchange protocol



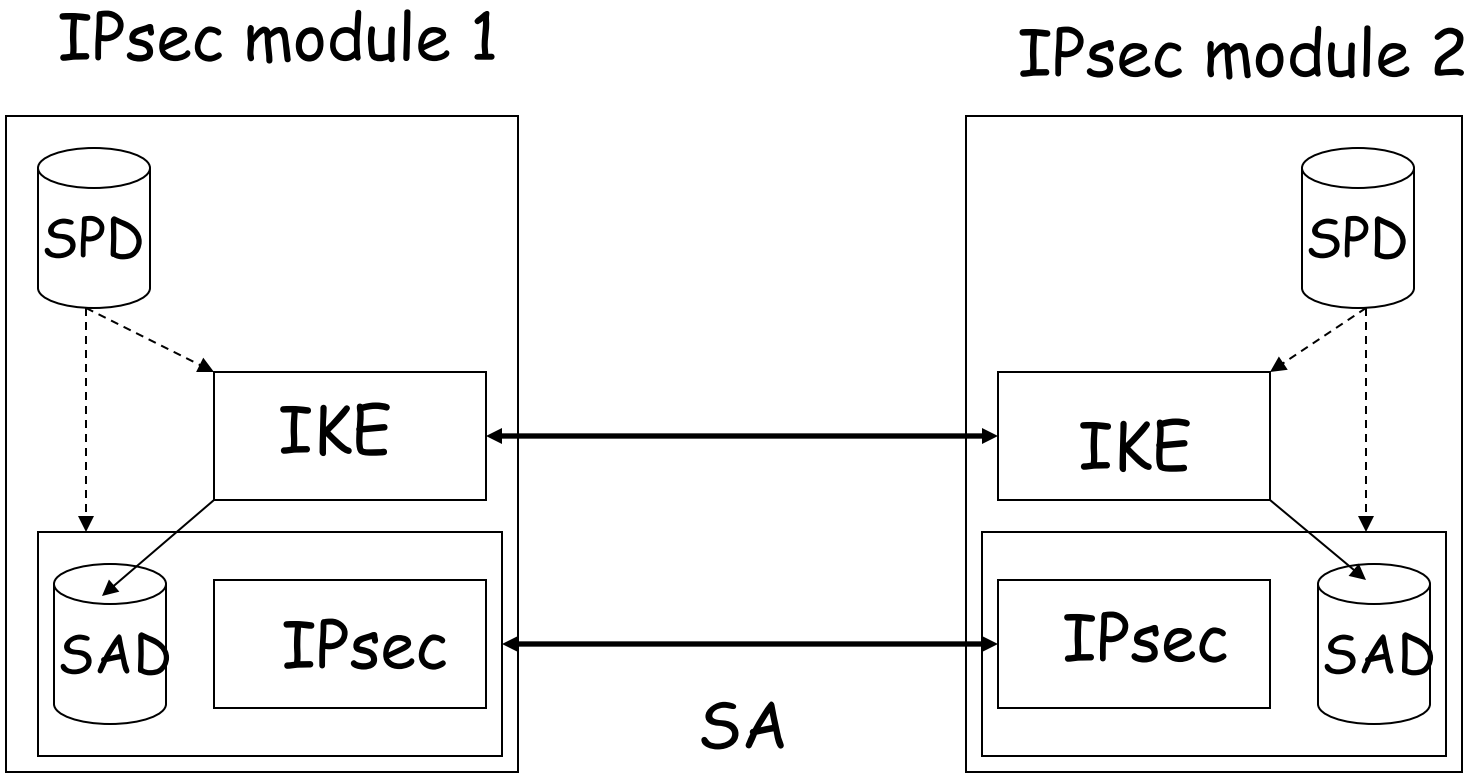
Key Management

Some Entries in an IKE SA

- A mutual authentication method, which is one of:
  - A protocol based on a pre-shared secret key
  - A challenge-response protocol based on a public-key cipher
- A key-establishment method, which is one of:
  - The digital envelop protocol
  - The Diffie-Hellman key exchange protocol
- A cipher and a hash function
- Encryption and authentication keys

Whole Picture of IPSec

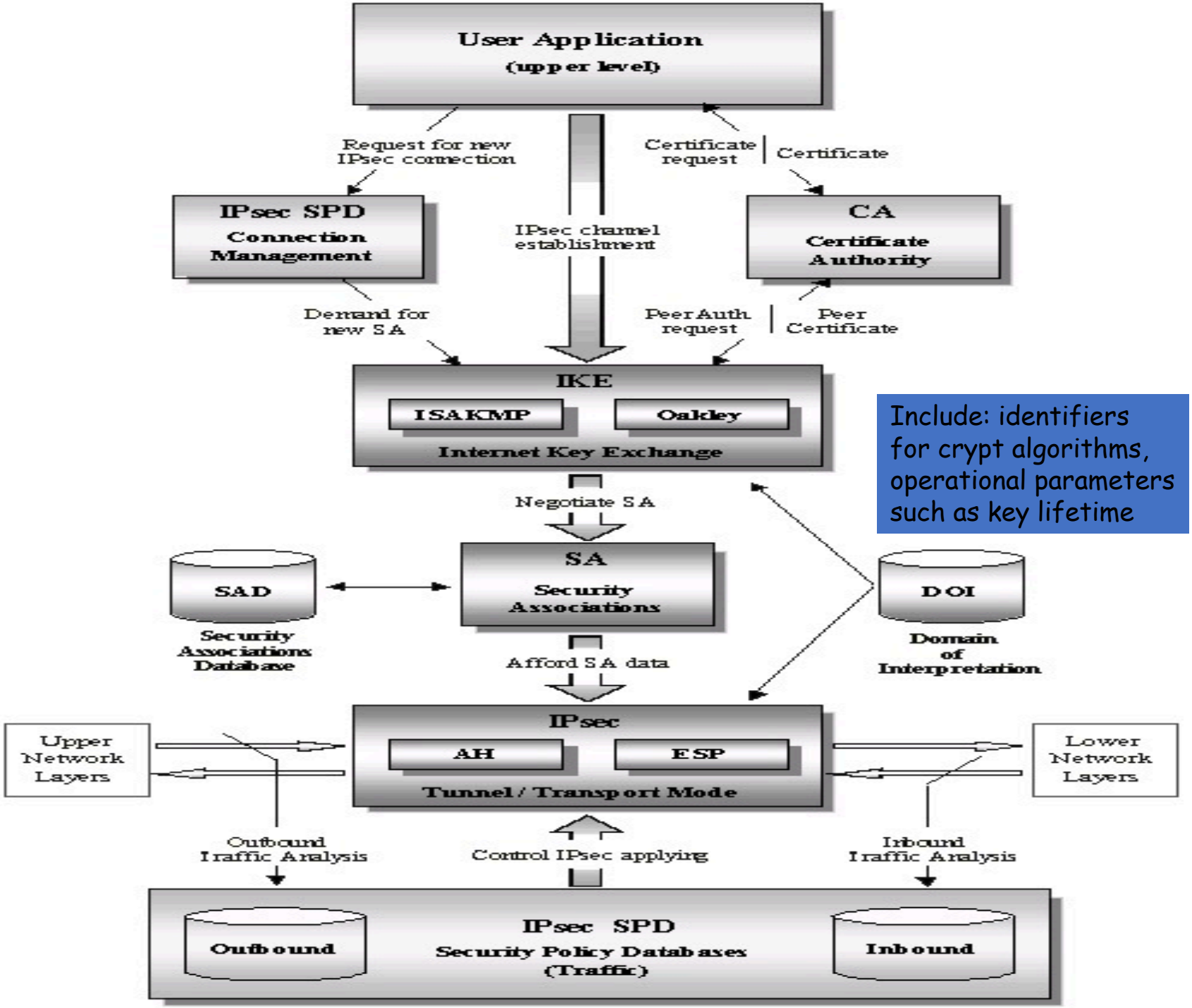
IP Security Architecture



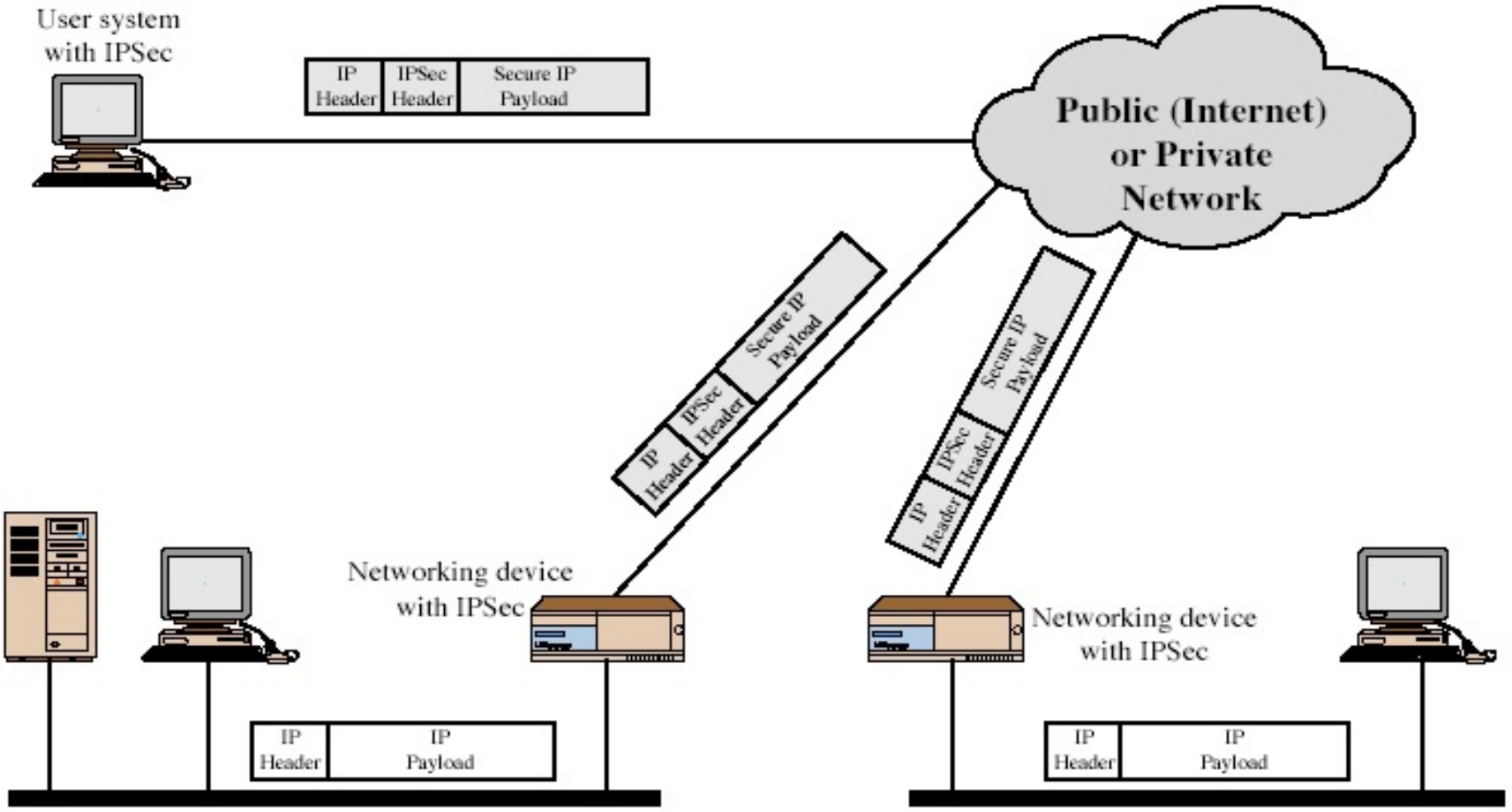
SAD: Security Association Database

SPD: Security Policy Database

IKE: Internet Key Exchange


User Application
(upper level)
Request for new IPsec connection
Certificate request
Certificate
IPsec SPD
Connection Management
IPsec channel establishment
CA
Certificate Authority
Demand for new SA
PeerAuth. request
Peer Certificate
IKE
ISAKMP
Oakley
Internet Key Exchange
Include: identifiers for crypt algorithms, operational parameters such as key lifetime
Negotiate SA
SAD
Security Associations Database
SA
Security Associations
DOI
Domain of Interpretation
Afford SA data
IPsec
AH
ESP
Tunnel / Transport Mode
Upper Network Layers
Lower Network Layers
Outbound Traffic Analysis
Control IPsec applying
Inbound Traffic Analysis
Outbound
IPsec SPD
Security Policy Databases (Traffic)
Inbound

IPSec Uses


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

Applications of IPSec

- Using IPSec all distributed applications can be secured,
  - Remote logon,
  - client/server,
  - e-mail,
  - file transfer,
  - Web access
  - etc.

Benefits of Using IPSec

- The benefits of IPSec include:
  - IPSec can be transparent to end users.
  - There is no need to train users on security mechanisms
  - IPSec can provide security for individual application
    - By configuration, IPSec is applied to only one specified application.

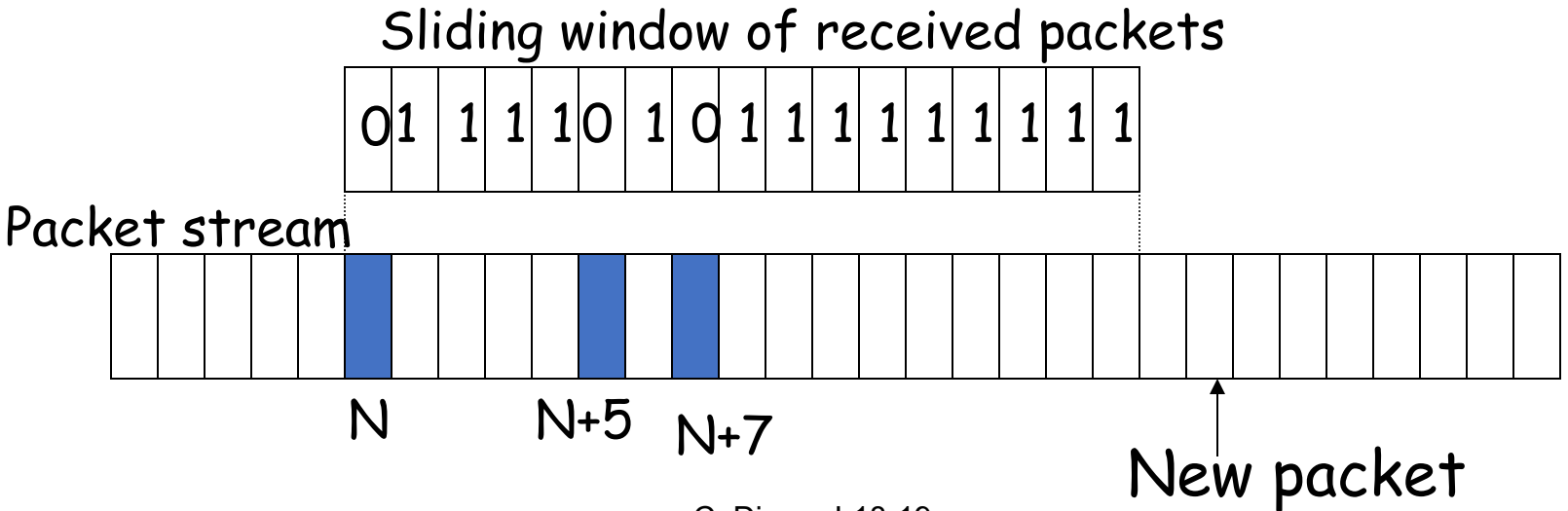
Appendix 1:
Anti-replay Service

SA Parameters for Anti-replay

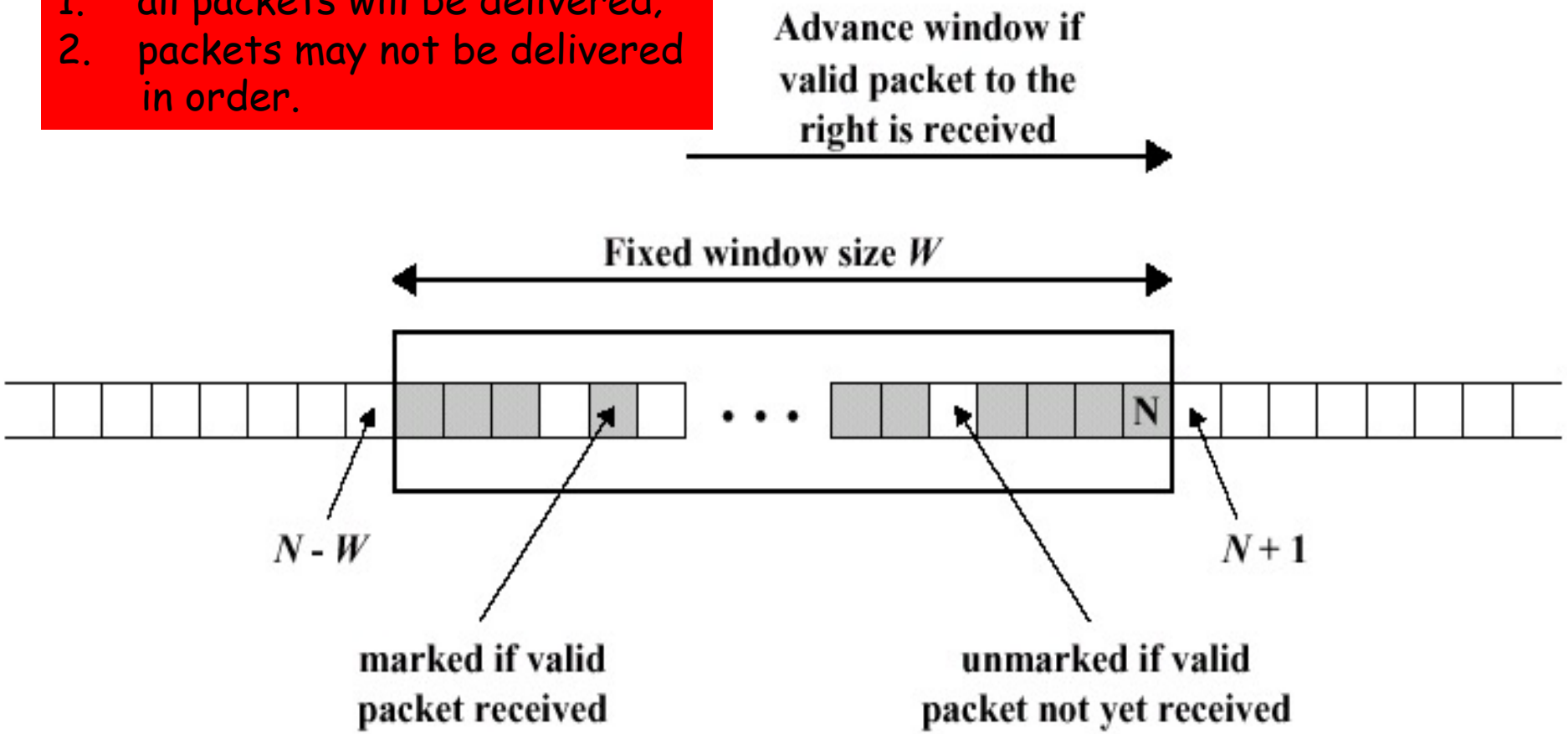
- Sequence Number Counter
  - A 32-bit value used to generate the sequence number field in AH or ESP headers.
- Sequence Counter Overflow
  - A flag indicating whether overflow of the sequence number counter should generate an auditable event and prevent further transmission of packets on this SA
- Anti-Replay Window
  - Used to determine whether an inbound AH or ESP packet is a replay.

Anti-replay Protection

- Protection by sequence number (32-bits) and sliding receive window (64-bits)
- When SA is created: sequence number is initiated to 0
- Prior to IPsec output processing: sequence number is incremented. Thus the first value to be used is 1



Problems: No guarantee that
1. all packets will be delivered;
2. packets may not be delivered in order.



Guards against replay attacks.

- IPSec dictates that the receiver implements a window of size W, default W=64.
  - If a received packet falls within window and is new, the MAC is checked. If not new, a replay attack. Disable it.
  - If the received packet is to the right of the window, and is authentic, window is advanced so that this packet is the right-most in this window. If not authentic, disable it.
  - If received packet is to the left of the window, the packet is disabled. [left => possible replay attack]

Appendix 2: SPD Entry

- Destination IP address
- Source IP address
- User ID: a user identifier from the operating system
- Data sensitivity level
- Transport layer protocol
- IPSec protocol (AH or ESP)
- Source and destination ports
- IPv6 class
- IPv6 flow label
- IPv4 type of service

Appendix 3: SA Selectors

- Each SPD entry is defined by a set of IP and upper-layer protocol field values, called ***selectors.***
- These selectors are used to filter outgoing traffic in order to map it into a particular SA.
- How is an outbound packet processed?
  - Compare the values of the appropriate fields in the packet (the selector fields) against the SPD to find a matching SPD entry, which will point to zero or more SAs.
  - Determine the SA if any for this packet and its associated SPI.
  - Do the required IPSec processing (i.e., AH or ESP processing).