

CS 547: Foundation of Computer Security

S. Tripathy
IIT Patna

Previous Classes

- Security in Networks
 - Threats in Networks & Security Controls
 - Threats in Layer 1 & Layer 2
 - Threats in Layer Network (IP) Layer
 - Threats in Transport Layer
- Network Security Controls
 - Link Encryption & End to End Encryption
 - IP-Sec

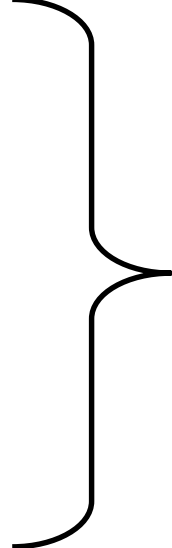
Present class

- Security in Networks
 - Network Security Controls
 - IPSec
 - IKE
 - VPN
 - TLS

Security Issues in IP

Fundamental Issue:

Networks are not (and will never be) fully secure

- source spoofing
 - replay packets
 - no data integrity or confidentiality
- 
- DOS attacks
 - Replay attacks
 - Spying
 - and more...

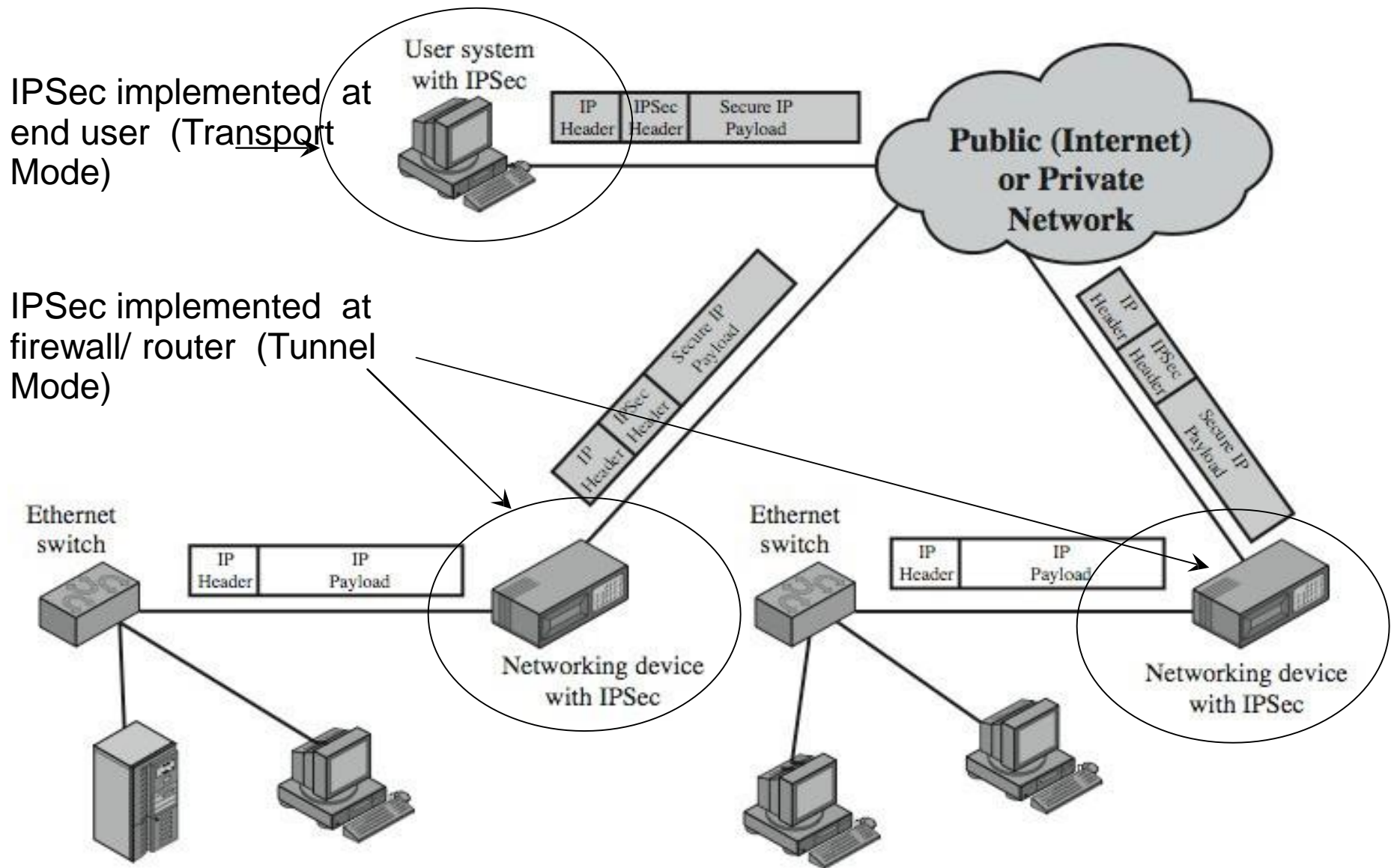
Goals of IPSec

- to verify sources of IP packets
 - *authentication*
- to prevent replaying of old packets
- to protect integrity and/or confidentiality of packets
 - *data Integrity/Data Encryption*

IPSec

- A collection of protocols (RFC 2401)
 - Authentication Header (AH)
 - RFC 2402
 - Encapsulating Security Payload (ESP)
 - RFC 2406
 - Internet Key Exchange (IKE)
 - RFC 2409
 - IP Payload Compression (IPcomp)
 - RFC 3137

Typical IPSec Scenario



Source: Figure 19.1 from William Stallings – Cryptography and Network Security, 5th Edition

IPSec

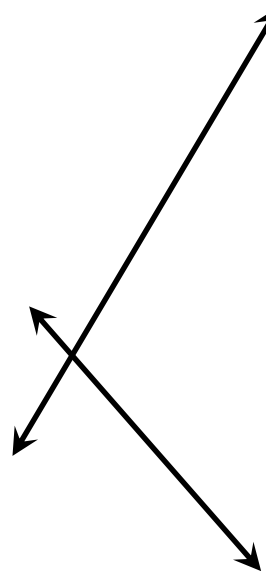
- ⑩ Implemented at the IP layer, so it does not require any change to existing TCP, UDP and application layer protocols.
- ⑩ Designed to address the fundamental shortcomings of the IP layer such as being subjected to **spoofing, eavesdropping and session hijacking**.
- ⑩ The basis of IPSec is security association (SA)
 - ⑩ SA is basically the set of security parameters for a secured communication channel.
 - ⑩ Each host can have several SAs in effect for current communications with different remote hosts.
- ⑩ A SA is identified using a security parameter index (SPI)
 - ⑩ SPI is a 32-bit identifier used to identify SA
 - ⑩ The SPI and the partner IP address are used to index to the security association database (SADB) that has information about the other characteristics of the different security associations
- ⑩ Two protocols have been developed to provide packet-level security for both IPv4 and IPv6:
 - ⌘ **IP Authentication Header**, AH (Next Header protocol ID: 51) provides integrity, authentication and non-repudiation.
 - ⌘ **IP Encapsulating Security Payload**, ESP provides confidentiality, along with authentication and integrity protection.

IPSEC Processing

- Use SPI to look up security association (SA)
- Perform authentication check using SA

spi	SA's
1	
2	
...	
13	Alice to Bob Bob's spi: 17
...	
21	Bob to Alice Bob's spi: 2

spi	SA's
1	
2	Bob to Alice Alice's spi: 21
...	
...	
...	
17	Alice to Bob Alice's spi: 13



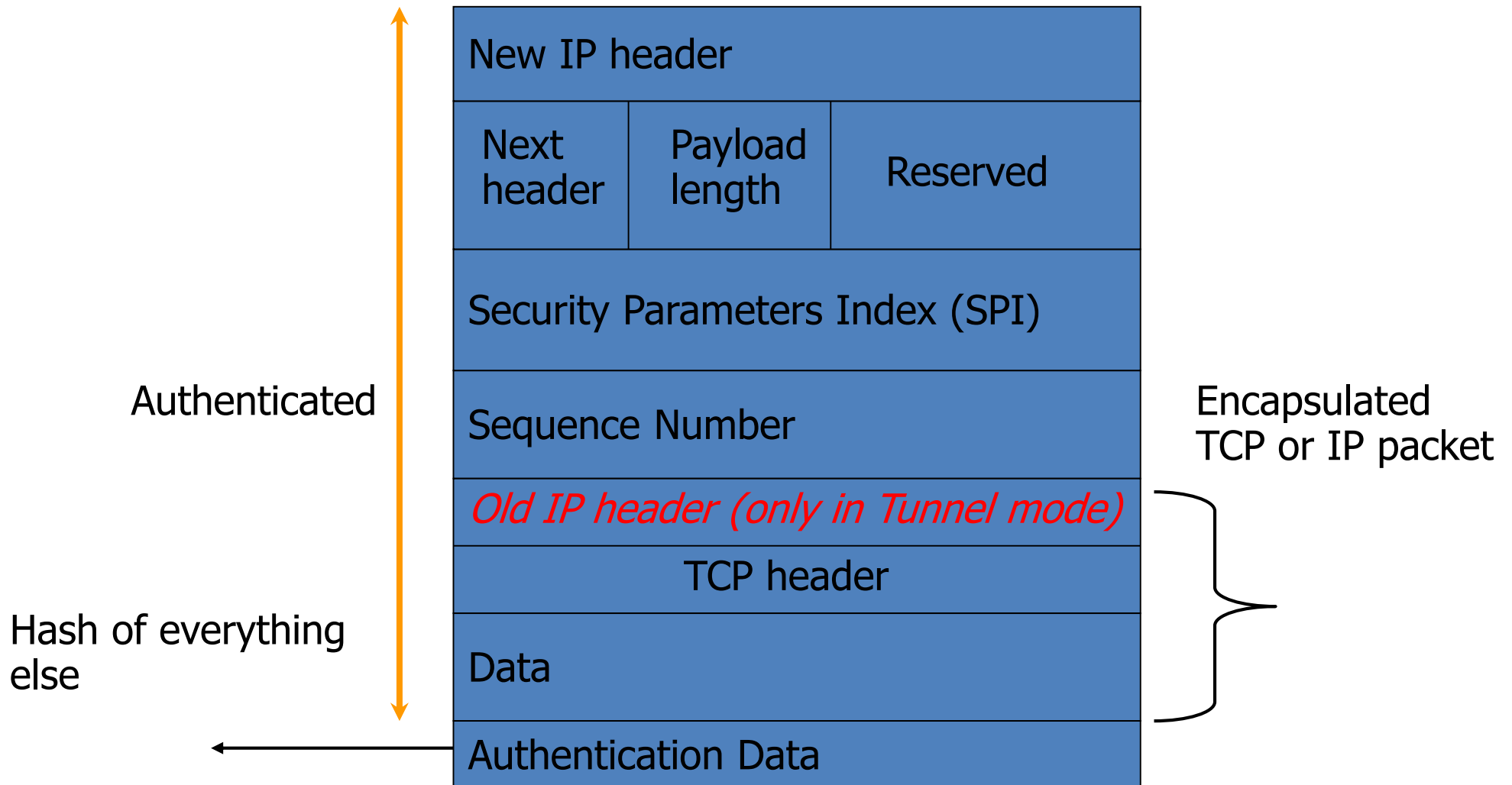
IPSEC Processing

- Operates in two modes
 - Transport mode (secure IP), protects payload
 - Tunneling mode (secure IP inside standard IP), protects entire packet
 - Popular in routers
 - Communicating hosts don't have to implement IPSEC themselves
 - Nested tunneling possible

Authentication Header (AH)

- Protects against source spoofing
 - Provides source authentication
- Protects against data manipulation
 - Use cryptographically strong hash algorithms
- Protects against replay attacks
 - Use 32-bit monotonically increasing sequence number to avoid replay attacks
 - Protects against denial of service attacks
- NO protection for confidentiality!

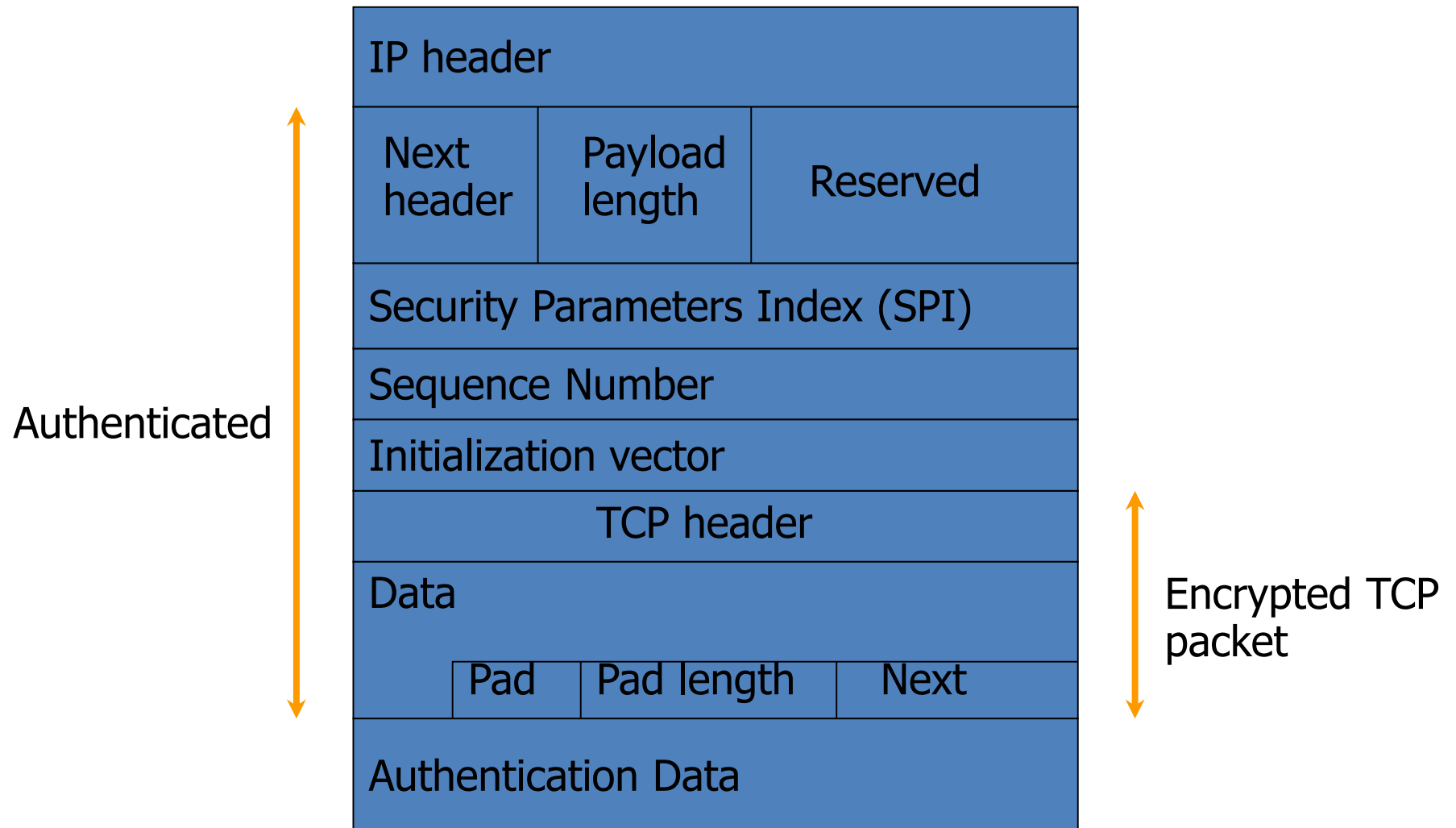
AH Packet Details



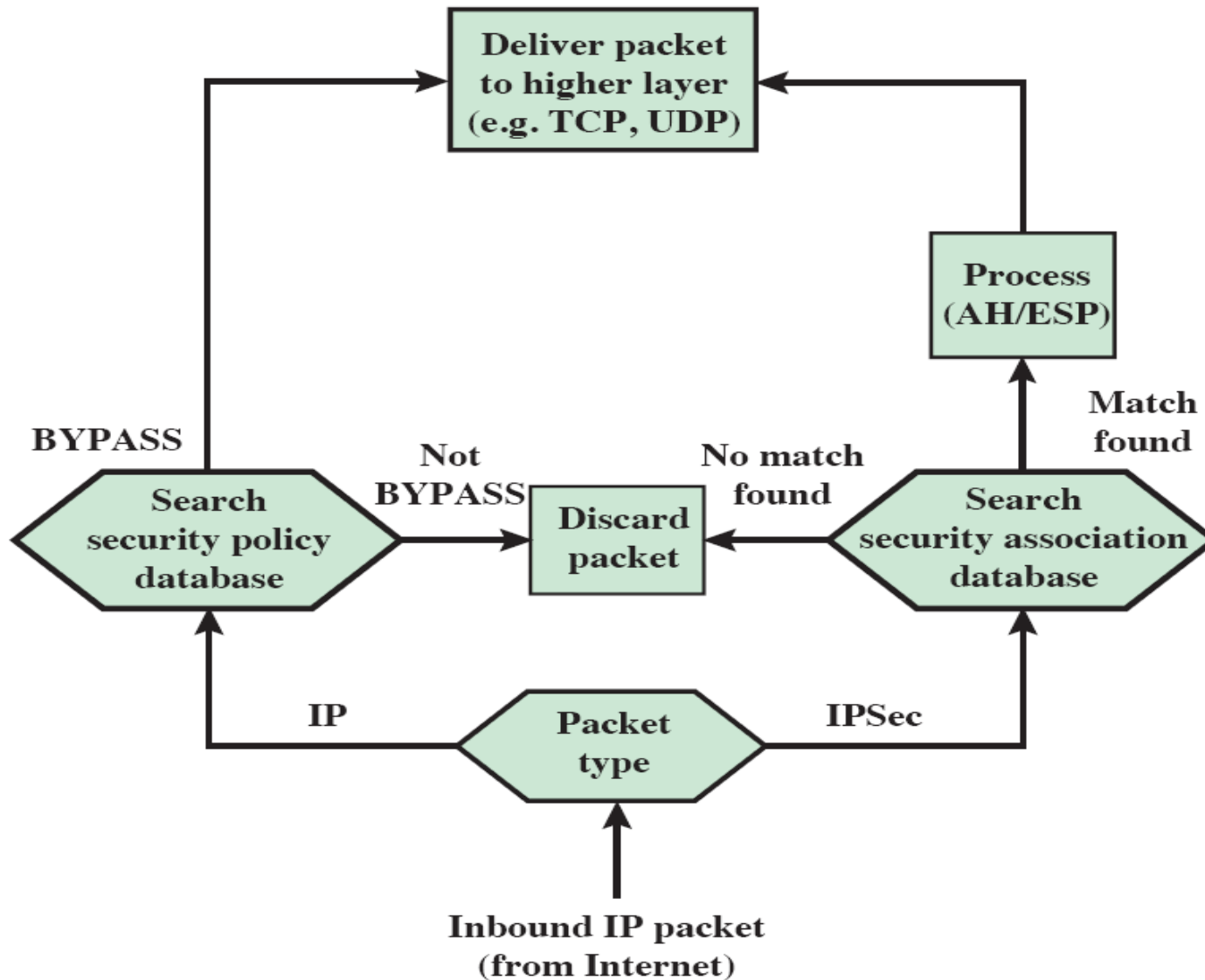
Encapsulating Security Payload (ESP)

- Provides all that AH offers
 - Same as AH:
 - Use 32-bit sequence number to counter replaying attacks
 - Use integrity check algorithms
- in addition provides
 - Data confidentiality:
 - Uses symmetric key encryption algorithms to encrypt packets

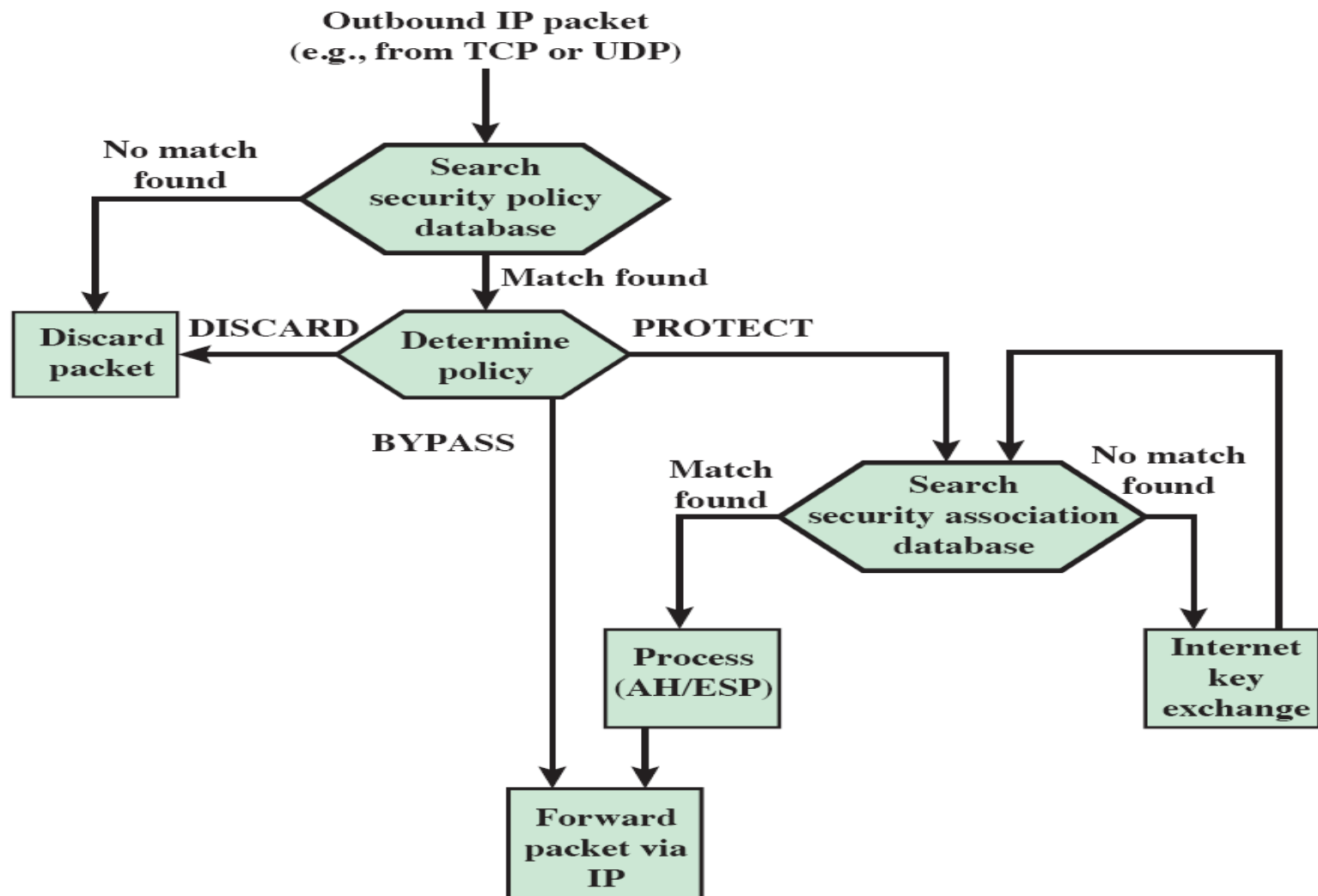
ESP Packet Details



Inbound Processing Model



Outbound Processing Model

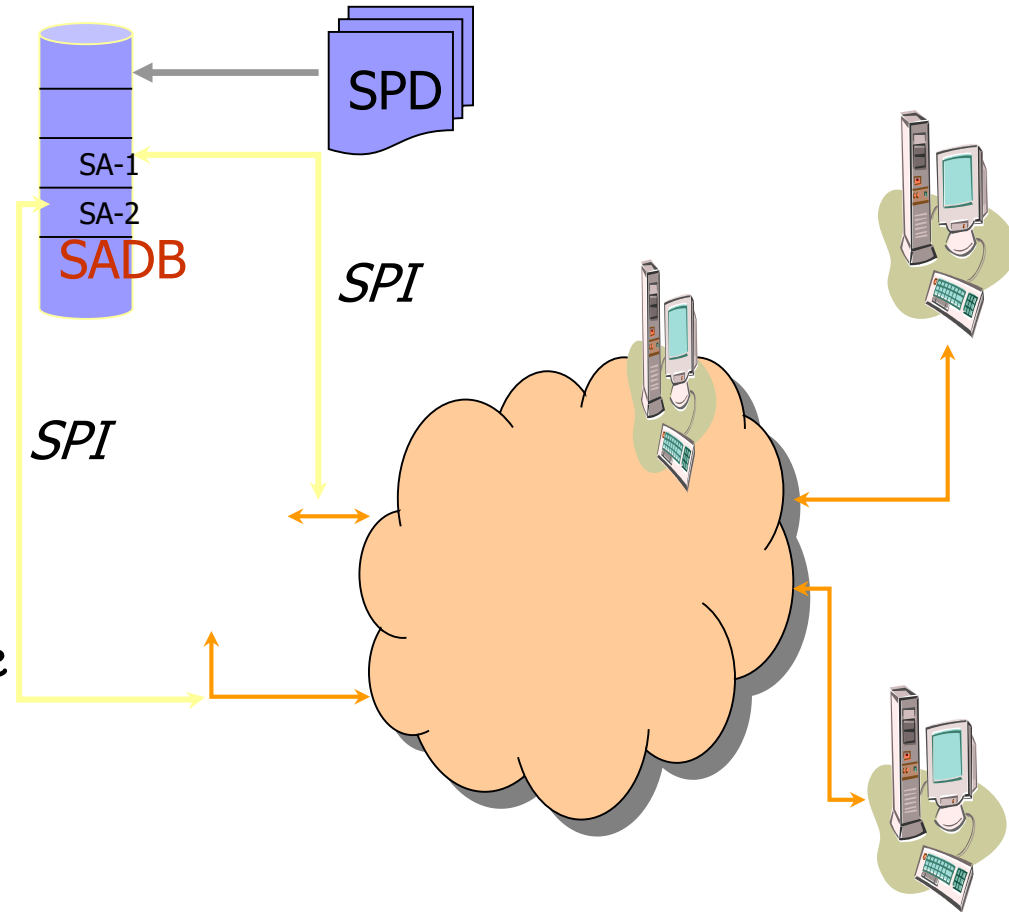


Internet Key Exchange (IKE)

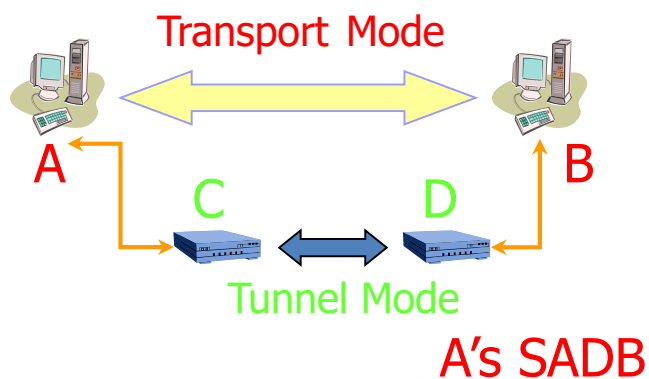
- Exchange and negotiate security policies
- Establish security sessions
 - Identified as *Security Associations*
- Key exchange
- Key management

IPsec/IKE Acronyms

- Security Association (SA)
 - Collection of attributes associated with a connection
 - Is *asymmetric*!
 - One SA for inbound traffic, other SA for outbound
- Security Association Database (SADB)
 - A database of SAs
- Security Parameter Index (SPI)
 - A unique index for each entry in the SADB
 - Identifies the SA associated with a packet
- Security Policy Database (SPD)
 - Store policies used to establish SAs



SPD and SADB Example



A's SPD

From	To	Protocol	Port	Policy
A	B	Any	Any	AH[HMAC-MD5]

From	To	Protocol	SPI	SA Record
A	B	AH	12	HMAC-MD5 key

From	To	Protocol	Port	Policy	Tunnel Dest
A _{sub}	B _{sub}	Any	Any	ESP[3DES]	D

C's SPD

From	To	Protocol	SPI	SA Record
A _{sub}	B _{sub}	ESP	14	3DES key

C's SADB

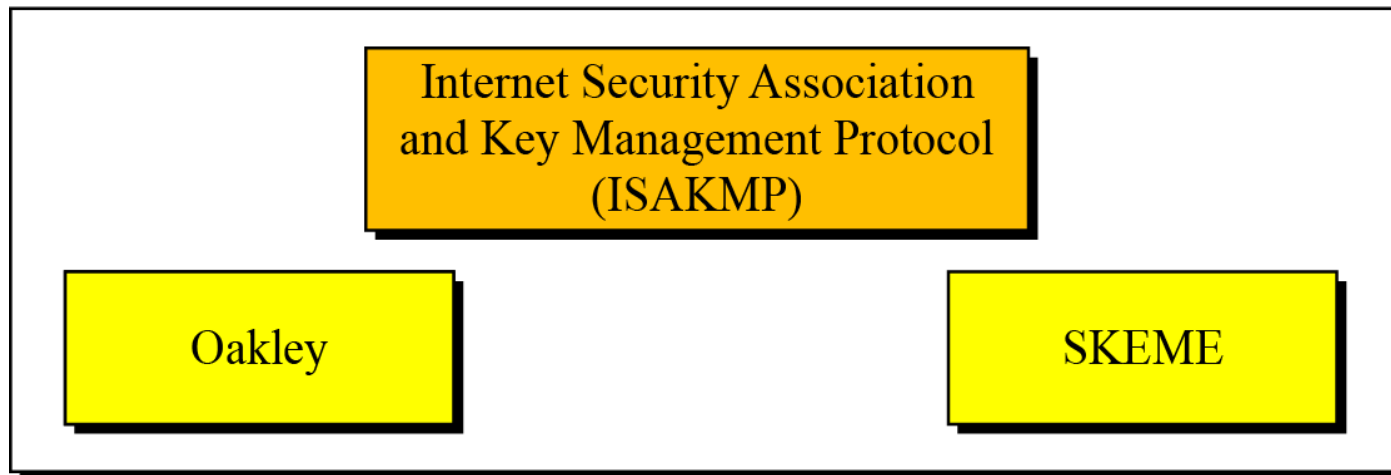
Key Management in IPSec

- Ultimate aim
 - generate and manage SAs for AH and ESP
 - asymmetric
 - receiver and initiator have different SAs
- can be manual or automated
 - manual key management
 - sysadmin manually configures every system
 - automated key management
 - on demand creation of keys for SA's in large systems

Key Management in IPSec

- The Internet Key Exchange (IKE) is a protocol designed to create both inbound and outbound Security Associations

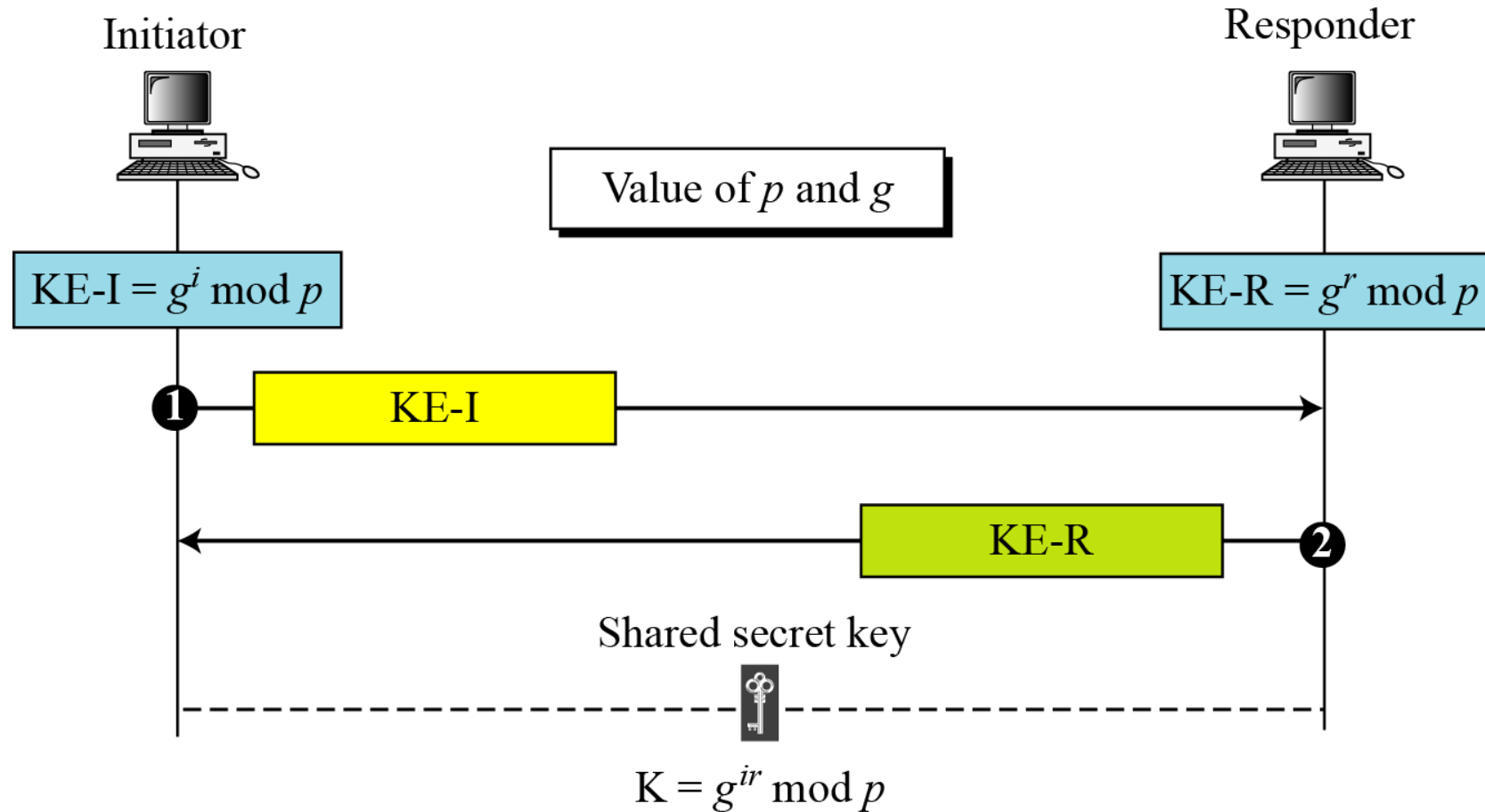
Internet Key Exchange (IKE)



the actual IKE protocol used in IPSec uses parts of Oakley and SKEME (Secure key exchange Mechanism for Internet) .
Uses ISAKMP messages to exchange authenticated keying material

Basis of IKE:

Diffie-Hellman key exchange



Vulnerable!

- Thanks