

CS 547: Foundation of Computer Security

S. Tripathy
IIT Patna

Previous Class

- Security in Networks
- Network Security Controls
 - (Wifi Security) WEP

Kinds of Threats

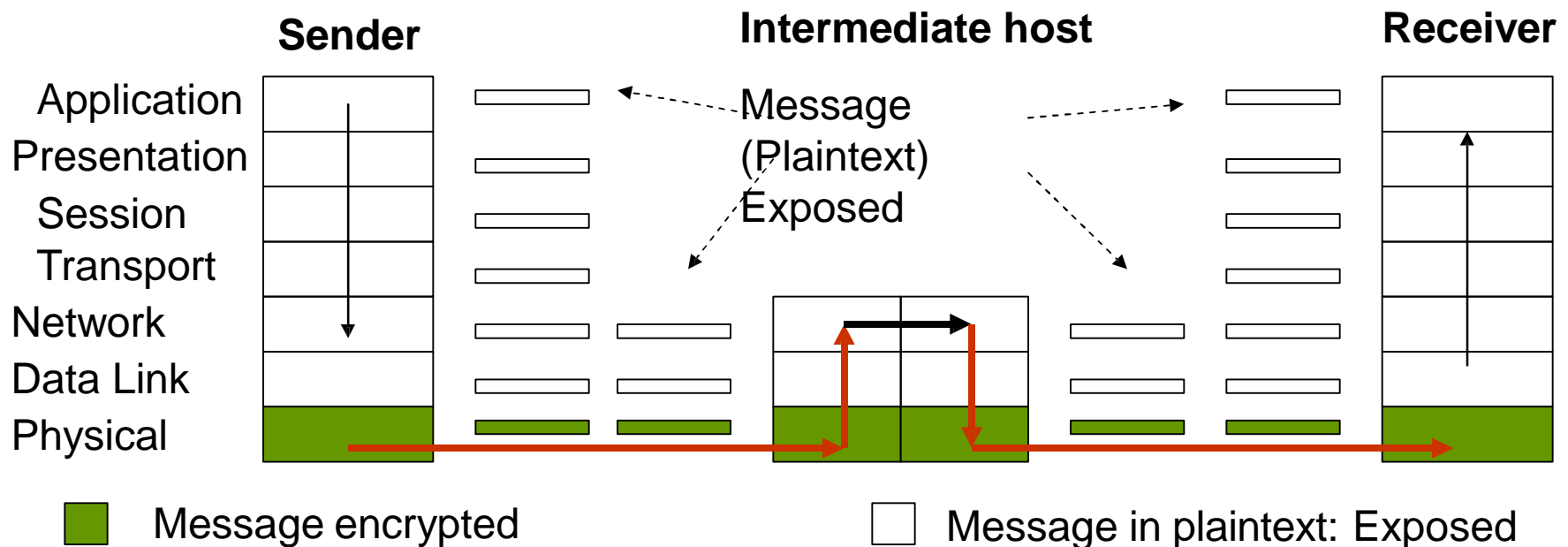
- Intercepting data in traffic
 - Modifying data in transit
 - Inserting communications
 - Impersonating a user
 - Inserting a repeat of a previous communication
 - Blocking selected traffic
 - Blocking all traffic
-
- Accessing programs or data at remote hosts
 - Modifying programs or data at remote hosts
 - Running a program at a remote host

Encryption

- Encryption is the most important & versatile tool for a network security expert.
- Encryption is used for providing:
 - Privacy
 - Authenticity
 - Integrity
 - Limited access to data
- NB: Encryption protects only what is encrypted

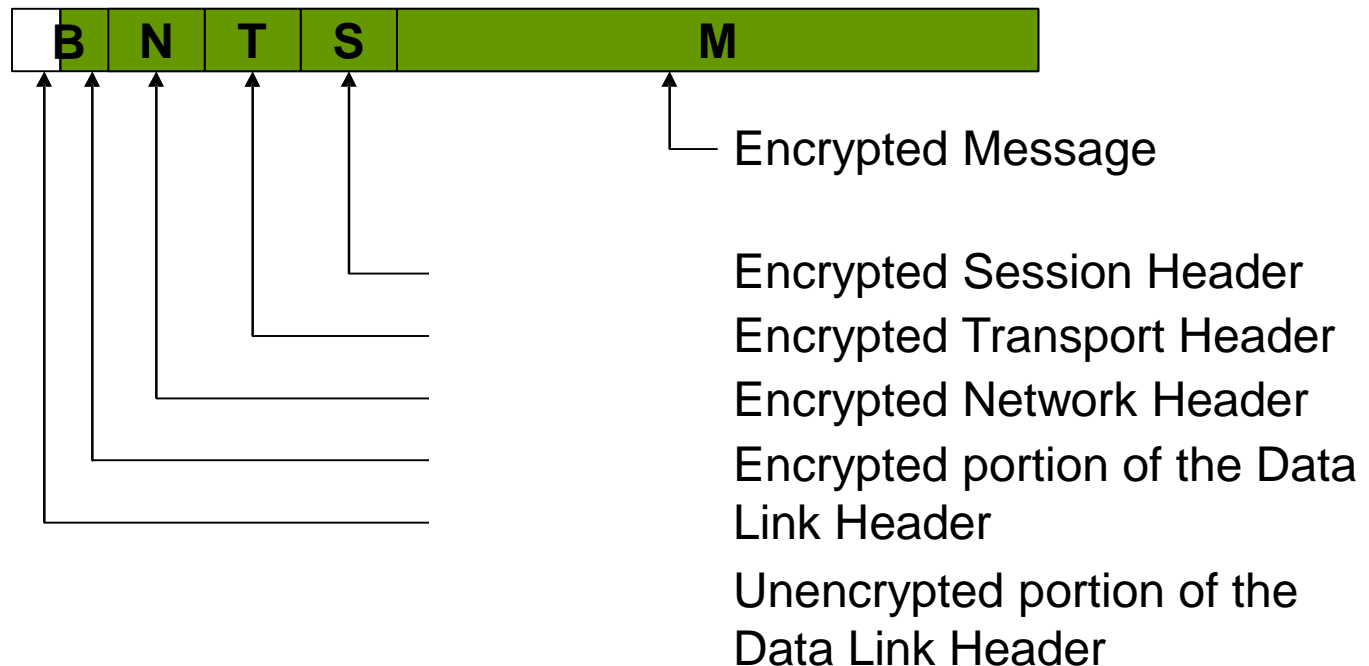
Link Encryption

- Data is encrypted just before the system places them on the physical communications link and decryption occurs just as the communication arrives at and enters the receiving computer.
- Encryption occurs at layer 1 or 2 of the ISO OSI model.



Link Encryption

- Encryption protects the message in transit between two computers
- This kind of encryption is invisible to user
- It is most appropriate when the transmission line is the point of greatest vulnerability

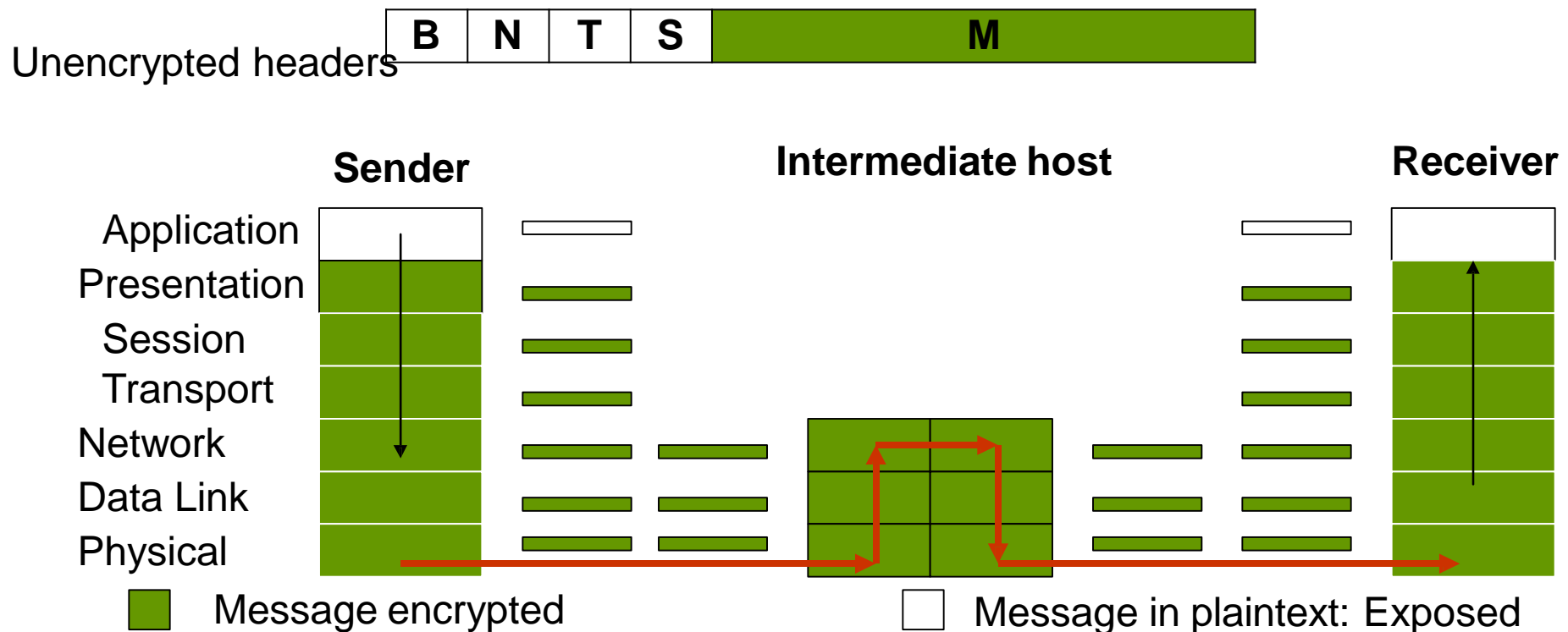


Network-layer security

- Suppose every link in our network had strong link-layer security
 - Why would this not be enough?
 - We need security **across** networks
 - Ideally, **end-to-end**
- At the network layer, this is usually accomplished with a Virtual Private Network (VPN)

End-to-End Encryption

- ⑩ Encryption is performed at the highest level (application layer).
- ⑩ Provides security for a message from one end of transmission to the other.
- ⑩ Since encryption precedes all the routing and transmission processing, the message is transmitted in encrypted form throughout the network.
- The message could go through potentially insecure intermediate nodes. The message is protected against disclosure while in transit.



Comparison of Encryption Methods

- ⑩ Link encryption
 - ⑩ The two end hosts of a link should share a key to facilitate link-level encryption.
 - ⑩ it should be performed on all links in the network. Otherwise, a message could go through certain links in clear text.
- ⑩ End-to-end encryption:
 - ⑩ It is basically applied to “logical links”, which are channels between two processes, at a level well above the physical path.
 - ⑩ Since the intermediate hosts along a transmission path do not need to encrypt or decrypt a message, they have no need for cryptographic facilities.

Comparison of Encryption Methods

- ⑩ With end-to-end encryption, there is a virtual cryptographic channel between each pair of users.
- ⑩ If we use symmetric cryptography,
 - ✎ Each pair of users should share a unique cryptographic key.
 - ✎ For n users, the number of unique keys required is $n(n-1)/2$.
- ⑩ If we use public key cryptography,
 - ✎ We need a pair of keys (public & private) per user. So, $2n$ keys for n users.
- ⑩ The number of keys required in link-level encryption is normally far less than the number of keys required for end-to-end encryption.
 - ⑩ If there are N hosts in a network, the number of link-level keys required would be $N(N-1)/2$.
 - ⑩ Each host can support several applications run by several users.
 - ✎ So, $N \ll n$.
- ⑩ Neither form of encryption is right for all situations.
 - ✎ A user who does not trust the quality of the link-level encryption provided by the system can apply end-to-end encryption as well.
 - ✎ A system administrator who is concerned about the security of an end-to-end encryption scheme supplied by an application program can also apply link-level encryption.

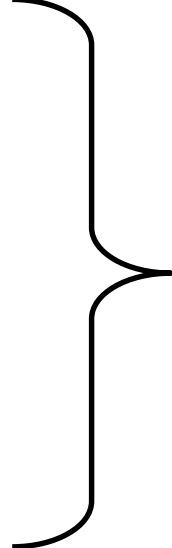
Comparison of Encryption Methods

Link Encryption	End-to-end Encryption
Security within hosts	
Data exposed in sending host	Data encrypted in sending host
Data exposed in intermediate hosts	Data encrypted in intermediate hosts
Role of user	
Applied by sending host	Applied by sending process
Invisible to user	User applies encryption
Host maintains encryption	User must find algorithm
One encryption algorithm for all users / link	User selects encryption algorithm
Typically done in hardware	Either hardware or software implementation
All or no data encrypted	User chooses to encrypt or not for each data item
Implementation concerns	
Requires one key per host pair	Requires one key per user pair
Provides node authentication	Provides user authentication

Security Issues in IP

Fundamental Issue:

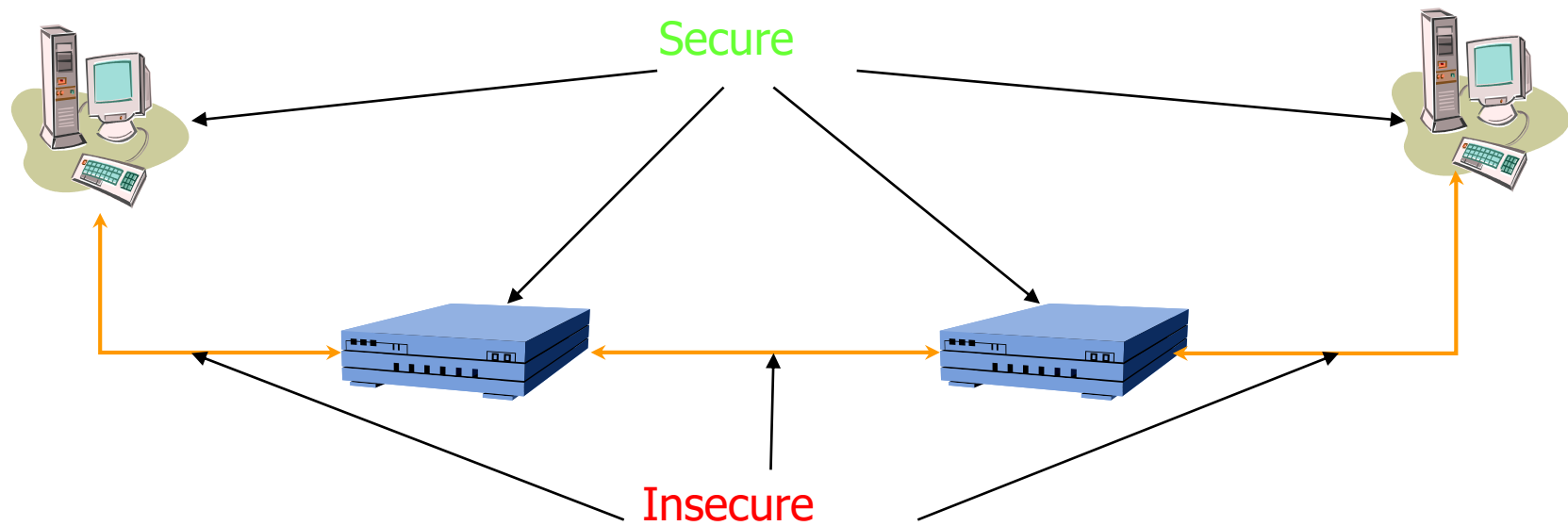
Networks are not (and will never be) fully secure

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

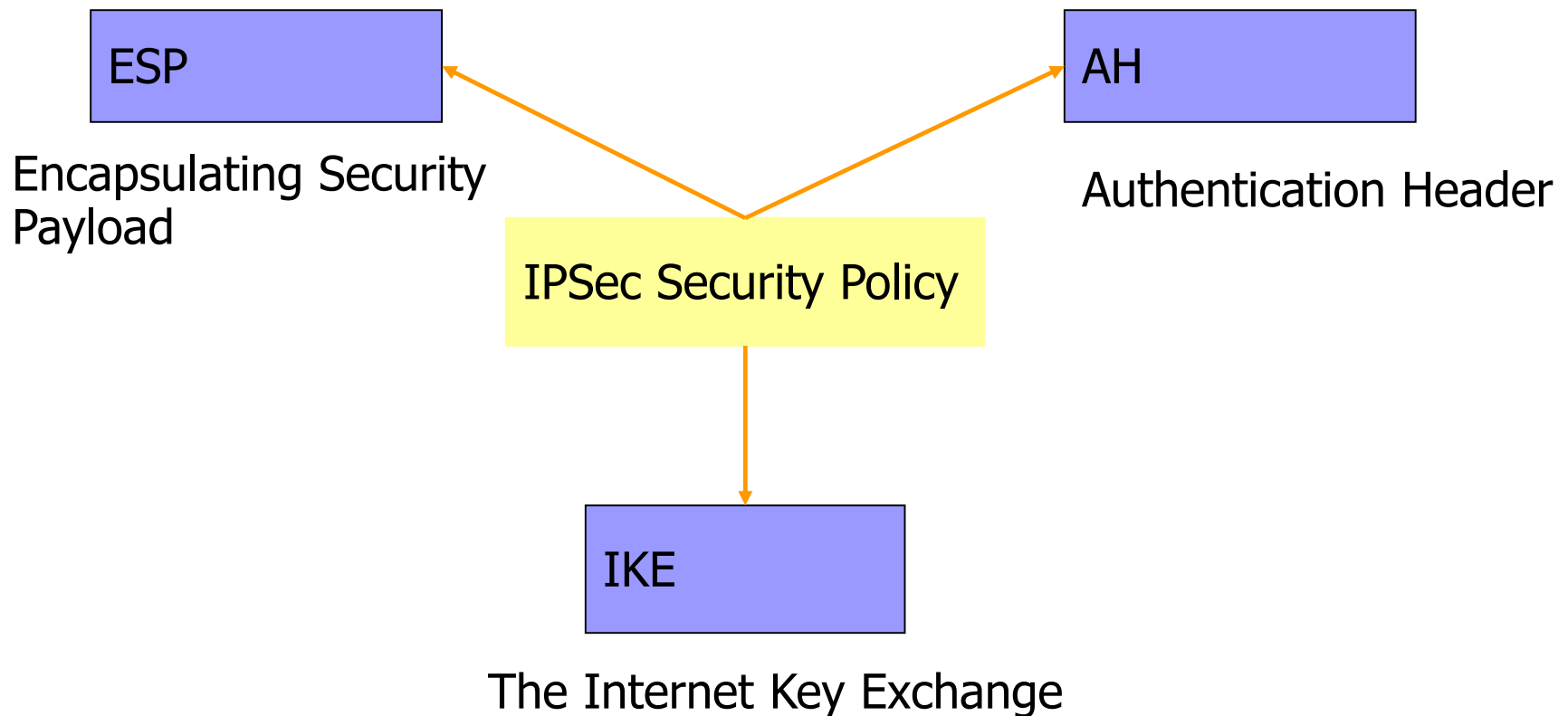
Goals of IPSec

- 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*

The IPSec Security Model



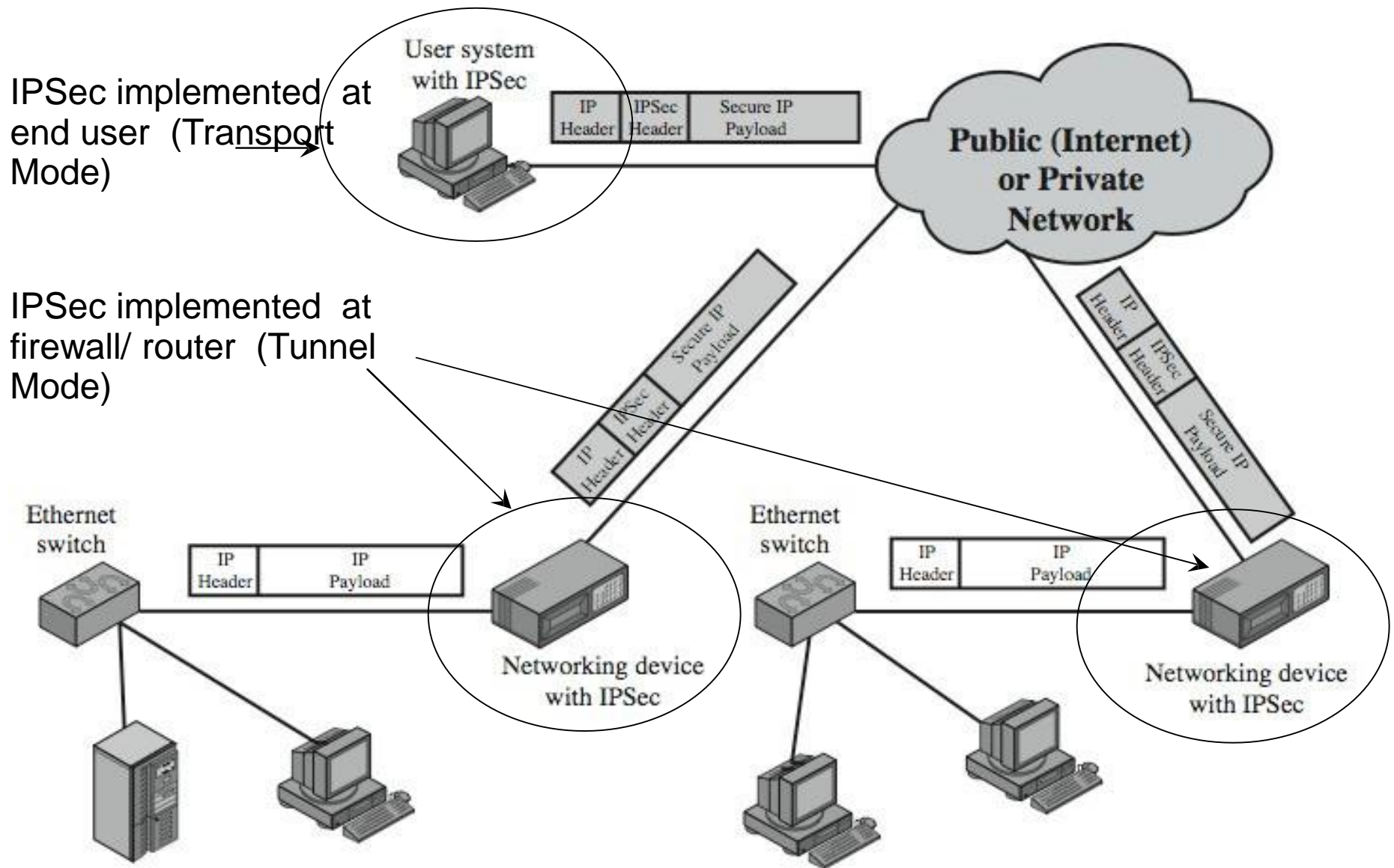
IPSec Architecture



IPSec Architecture

- IPSec provides security in three situations:
 - Host-to-host, host-to-gateway and gateway-to-gateway

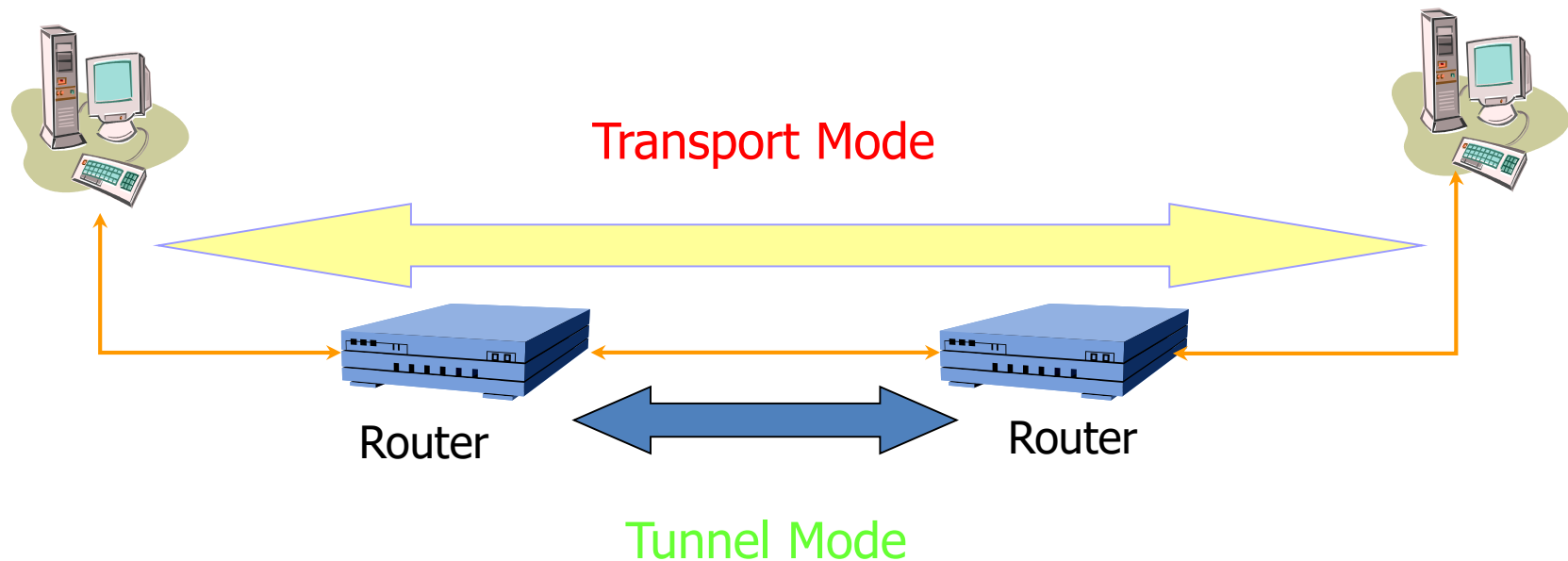
Typical IPSec Scenario



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

IPsec Architecture

IPSec operates in two modes:
Transport mode (for end-to-end)
Tunnel mode (for VPN)

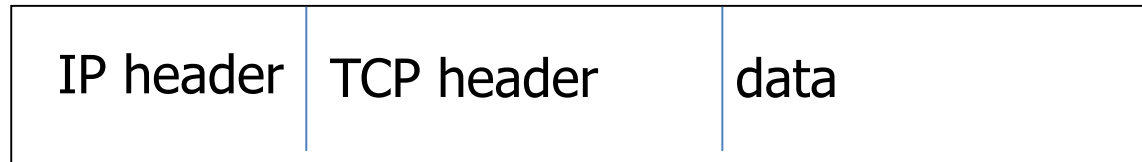


IPSec

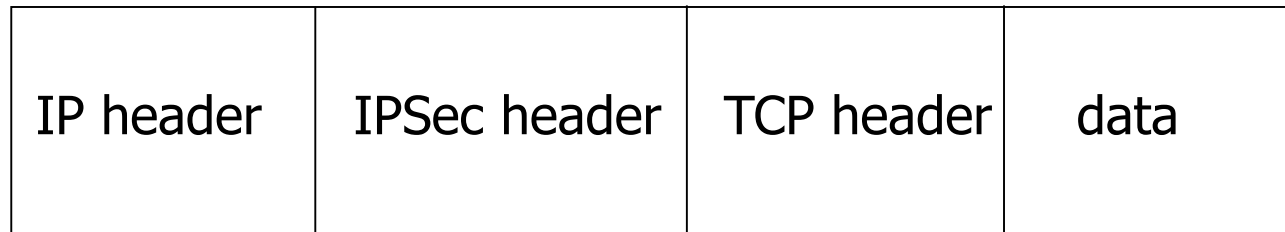
- ⑩ Implemented at the IP layer, so it does not require any change to existing TCP, UDP and application layer protocols.
- ⑩ Designed to address the fundamental shortcomings of the IP layer such as being subjected to **spoofing, eavesdropping and session hijacking**.
- ⑩ The basis of IPSec is security 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.

Various Packets

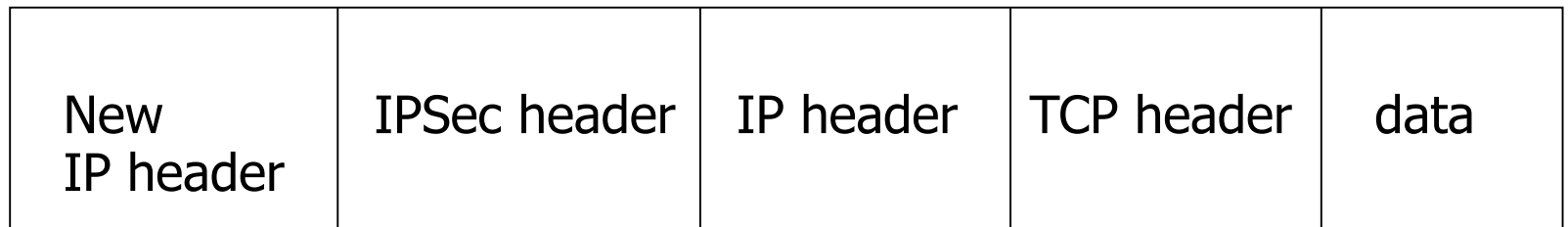
Original



Transport mode



Tunnel mode



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

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!

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

- Thanks