

# Unit 6

## Network Security

**NOTE : THIS PRESENTATION SHOULD BE CONSIDERED AS SUPPORTING MATERIAL ONLY.  
FOR DETAILED STUDY STUDENTS MUST REFER THE TEXT BOOKS AND REFERENCE BOOKS  
MENTIONED IN SYLLABUS.**

# Eavesdropping and Wiretapping

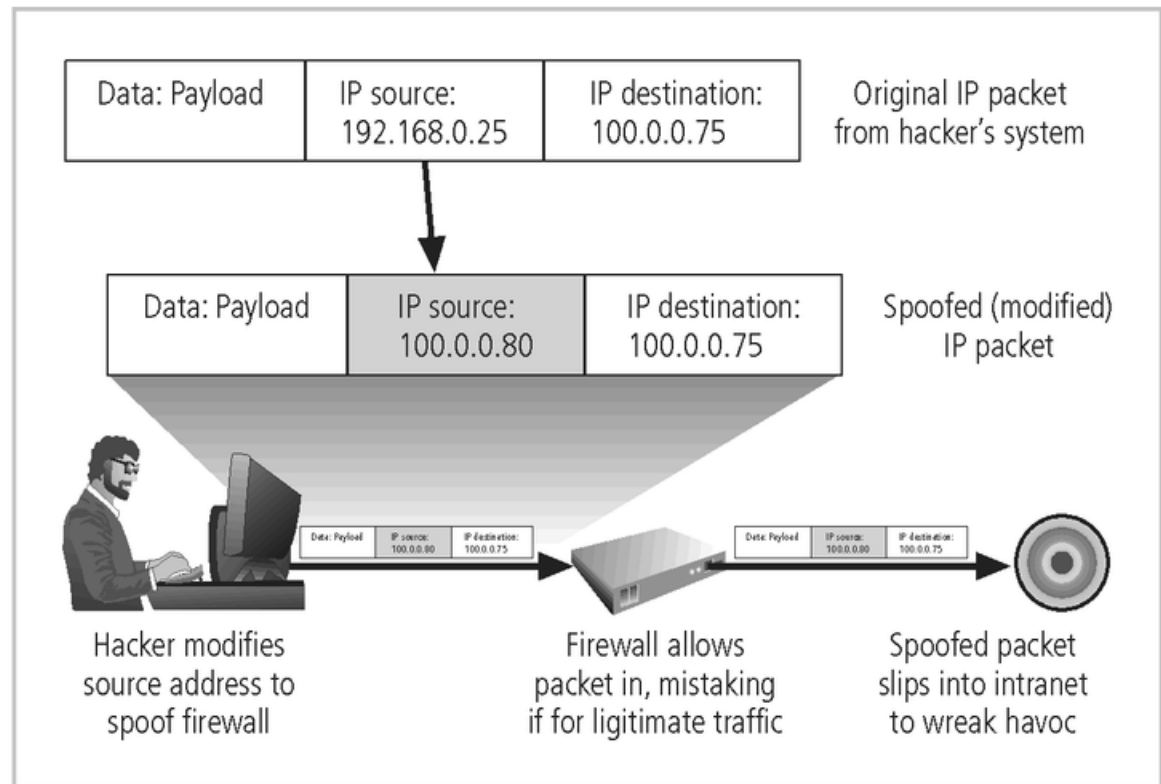
- Threats to data in transit:
  - 1) Eavesdropping
    - = overhearing *without any extra effort*
  - 2) Wiretapping
    - = overhearing *with some extra effort*
    - a) Passive wiretapping
      - Pretty similar to eavesdropping but some extra effort*
    - b) Active wiretapping – injecting msgs
- Wiretapping technique depends on the communication medium

# Spoofing

**Spoofing** is a technique used to gain unauthorized access to computers, wherein the intruder sends messages with a source IP address that has been forged to indicate that the messages are coming from a trusted host.

■ Three types of spoofing:

- 1) Masquerading
- 2) Session hijacking
- 3) Man-in-the middle



**FIGURE 2-10** IP Spoofing

## Spoofing

1) **Masquerading** = a host pretends to be another

- Masquerading - **Example 1**:
  - Real web site: Blue-Bank.com for Blue Bank Corp.
  - Attacker puts a masquerading host at: BlueBank.com
    - It mimics the look of original site as closely as possible
  - A mistyping user (who just missed „-”) is asked to login, to give password => sensitive info disclosure
  - Can get users to masquerading site by other means
    - E.g., advertise masquerading host with banners on other web sites
- Similar typical masquerades:
  - xyz.org *and* xyz.net masquerade as xyz.com
  - 10pht.com masquerades as lOpht.com (1-I, 0-O)
  - citicar.com masquerades as citycar.com

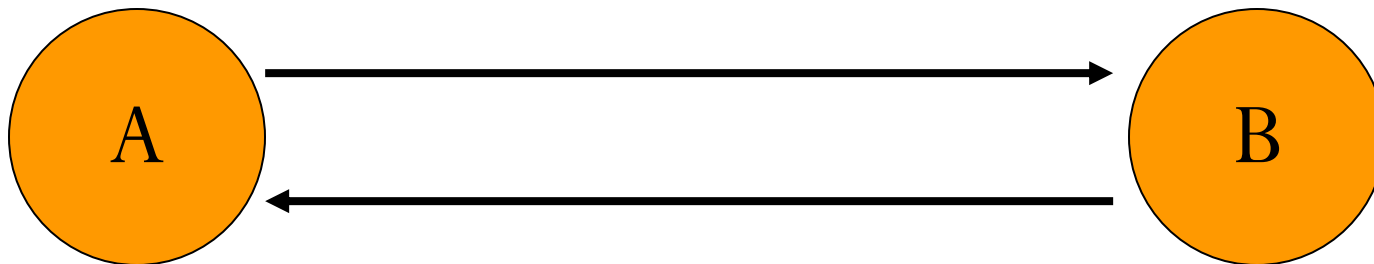
## Spoofing

2) **Session hijacking** = attacker intercepting and carrying on a session begun by a legitimate entity

- Session hijacking - **Example 1**
  - Books Depot wiretaps network and intercepts packets
  - After buyer finds a book she wants at a search engine and starts ordering it, the order is taken over by Books Depot
- Session hijacking - **Example 2**
  - Sysadmin starts Telnet session by remotely logging in to his privileged account
  - Attacker uses hijacking utility to intrude in the session
    - Can send his own commands between admin's commands
    - System treats commands as coming from sysadmin

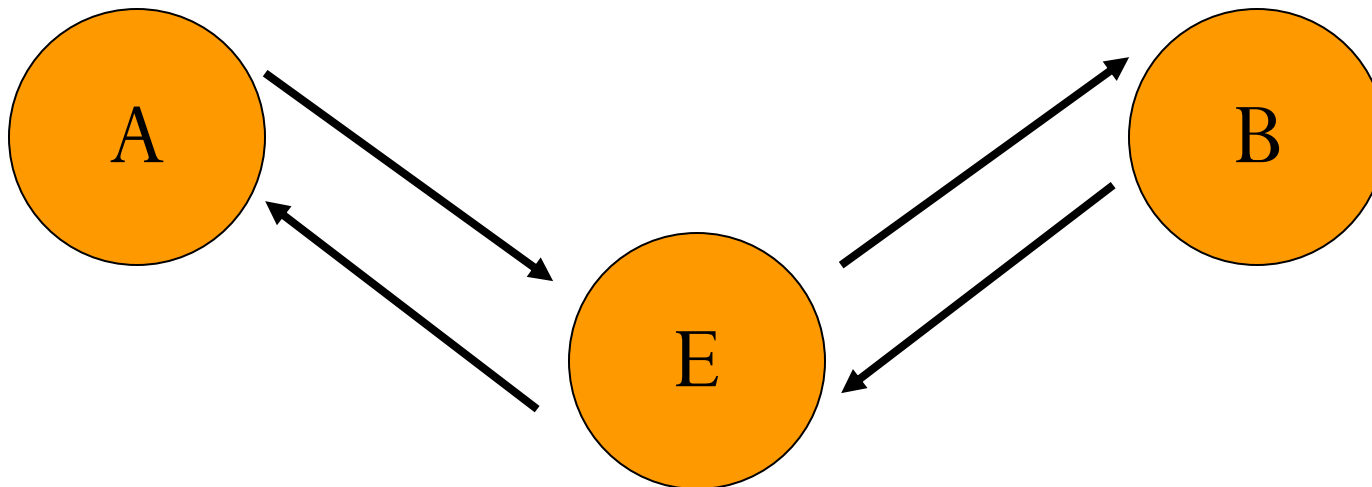
# Man-in-the-Middle

- In a Man-in-the-Middle attack the attacker gets in the middle of a real run of a protocol.



# Man-in-the-Middle

- In a Man-in-the-Middle attack the attacker gets in the middle of a real run of a protocol.



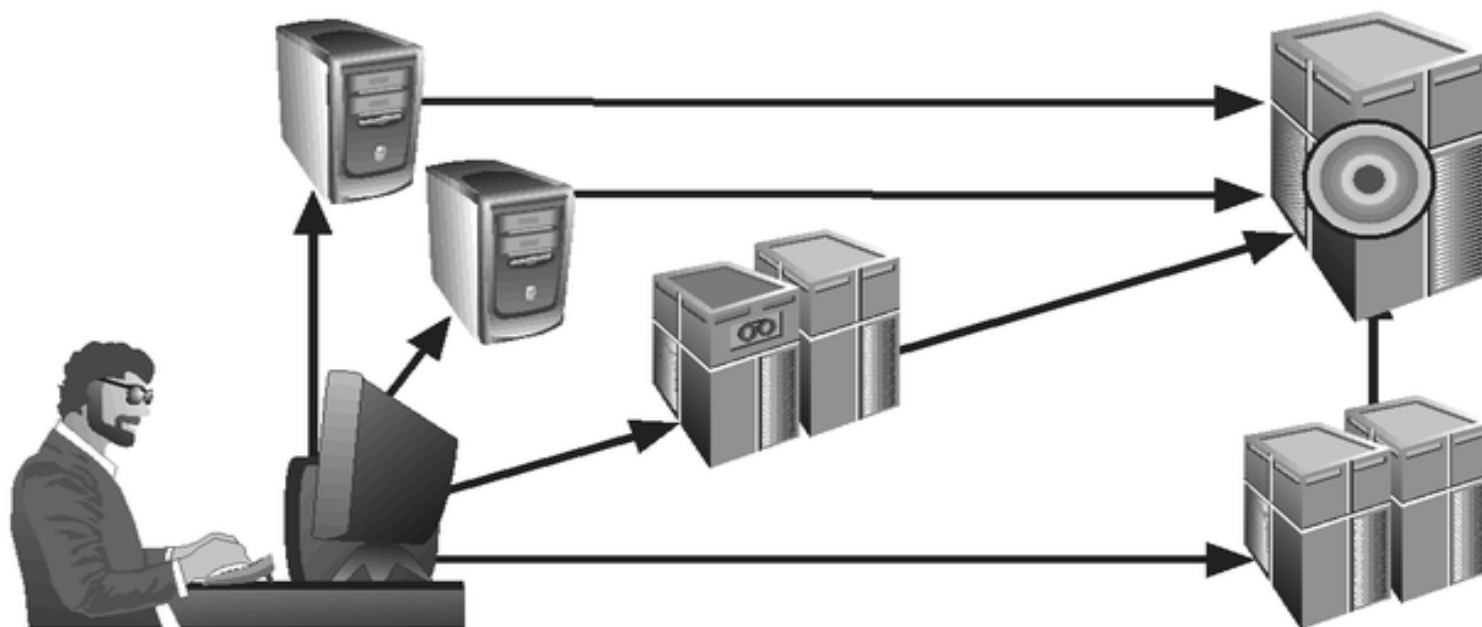
# Denial of service

- Denial-of-service (DoS): attacker sends large number of connection or information requests to a target
  - Target system cannot handle successfully along with other, legitimate service requests
  - May result in system crash or inability to perform ordinary functions
- Distributed denial-of-service (DDoS): coordinated stream of requests is launched against target from many locations simultaneously



In a denial-of-service attack, a hacker compromises a system and uses that system to attack the target computer, flooding it with more requests for services than the target can handle.

In a distributed denial-of-service attack, dozens or even hundreds of computers (known as zombies) are compromised, loaded with DoS attack software and then remotely activated by the hacker to conduct a coordinated attack.



**FIGURE 2-9** Denial-of-Service Attacks

# Network Security Controls

- Previous chapters have presented several strategies for addressing security concerns,
  - such as encryption for confidentiality and integrity ,access control mechanisms
  - These strategies are also useful in protecting networks.
- Subsequent sections provide detailed explanations for three particularly important controls
  - firewalls, intrusion detection systems, and encrypted e-mail.

# Encryption

- Encryption is probably the most important and versatile tool for a network security expert.
- We have seen in earlier chapters that encryption is powerful for providing privacy, authenticity, integrity, and limited access to data.
- However, let us consider these points
  - First, a flawed system design with encryption is still a flawed system design.
  - Second, notice that encryption protects only what is encrypted
    - Data are exposed before encryption and after decryption
  - Finally, encryption is no more secure than its key management
    - If an attacker can guess or deduce a weak encryption key, the game is over.
- In network applications, encryption can be applied either between
  - two hosts (called link encryption)
  - two applications (called end-to-end encryption)

# Link Encryption

- In **link encryption**, data are encrypted *just* before the system places them on the physical communications link.
  - at layer 1 or 2 in the OSI model.
  - Similarly, decryption occurs just as the communication arrives at and enters the receiving computer

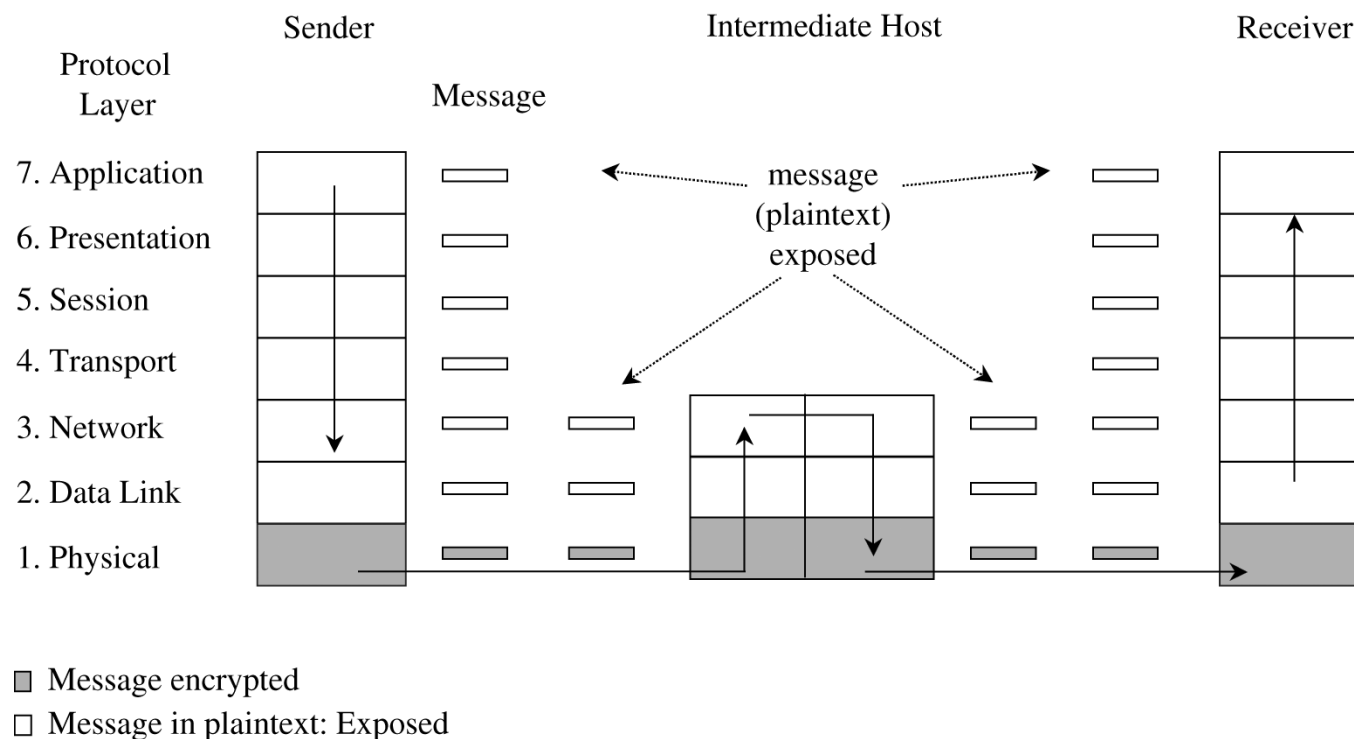
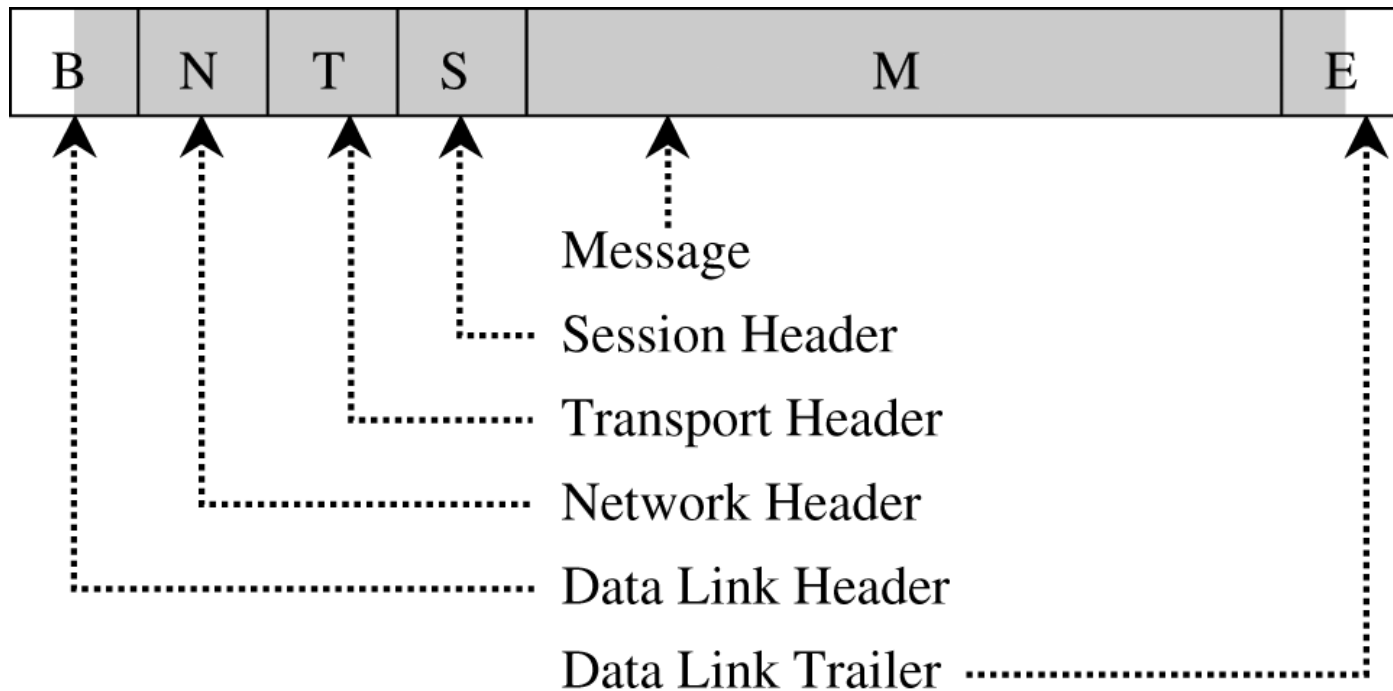


Figure 7-20 Link Encryption.

# Link Encryption

- Encryption protects the message in transit between two computers, but the message is in plaintext (in the clear) inside the hosts.
  - Notice that because the encryption is added at the bottom protocol layer, the message is exposed in all other layers of the sender and receiver.
  - Link encryption is invisible to the user.
    - The encryption becomes a transmission service performed by a low-level network protocol layer
    - just like message routing or transmission error detection
  - Hardware encryption devices operate quickly and reliably;
    - in this case, link encryption is invisible to the operating system as well as to the operator
  - Link encryption is especially appropriate when the transmission line is the point of greatest vulnerability

# Link Encryption




 Encrypted

Figure 7-21 Message Under Link Encryption.

# End-to-End Encryption

- provides security from one end of a transmission to the other
  - Can be done by hardware or software
  - performed at the highest network levels (layer 7, application, or perhaps at layer 6, presentation) of the OSI model

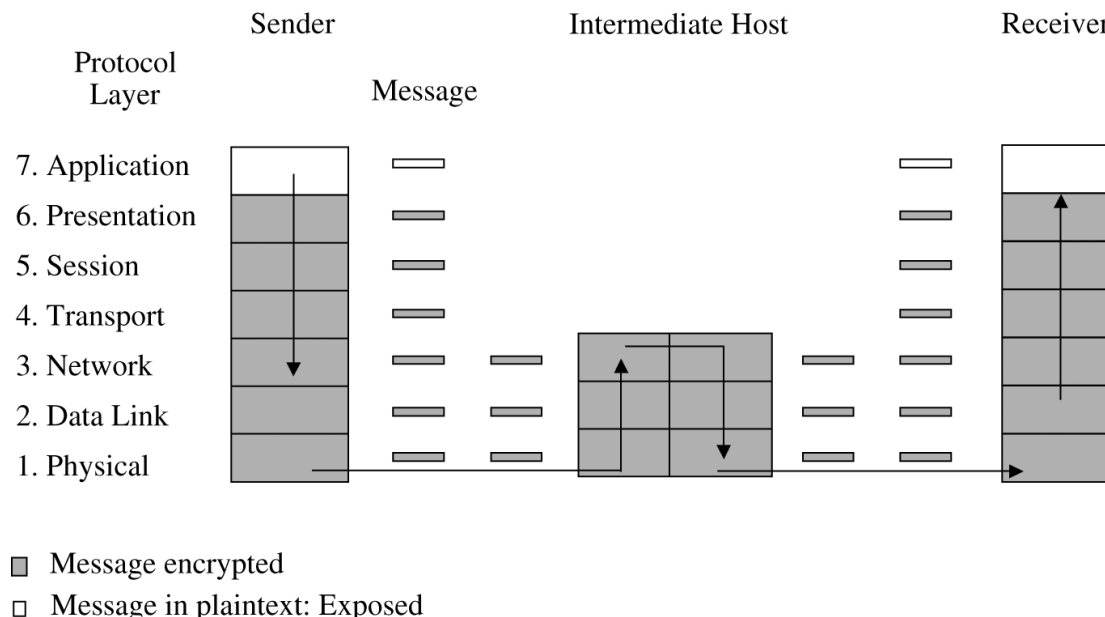


Figure 7-22 End-to-End Encryption.

# End-to-End Encryption

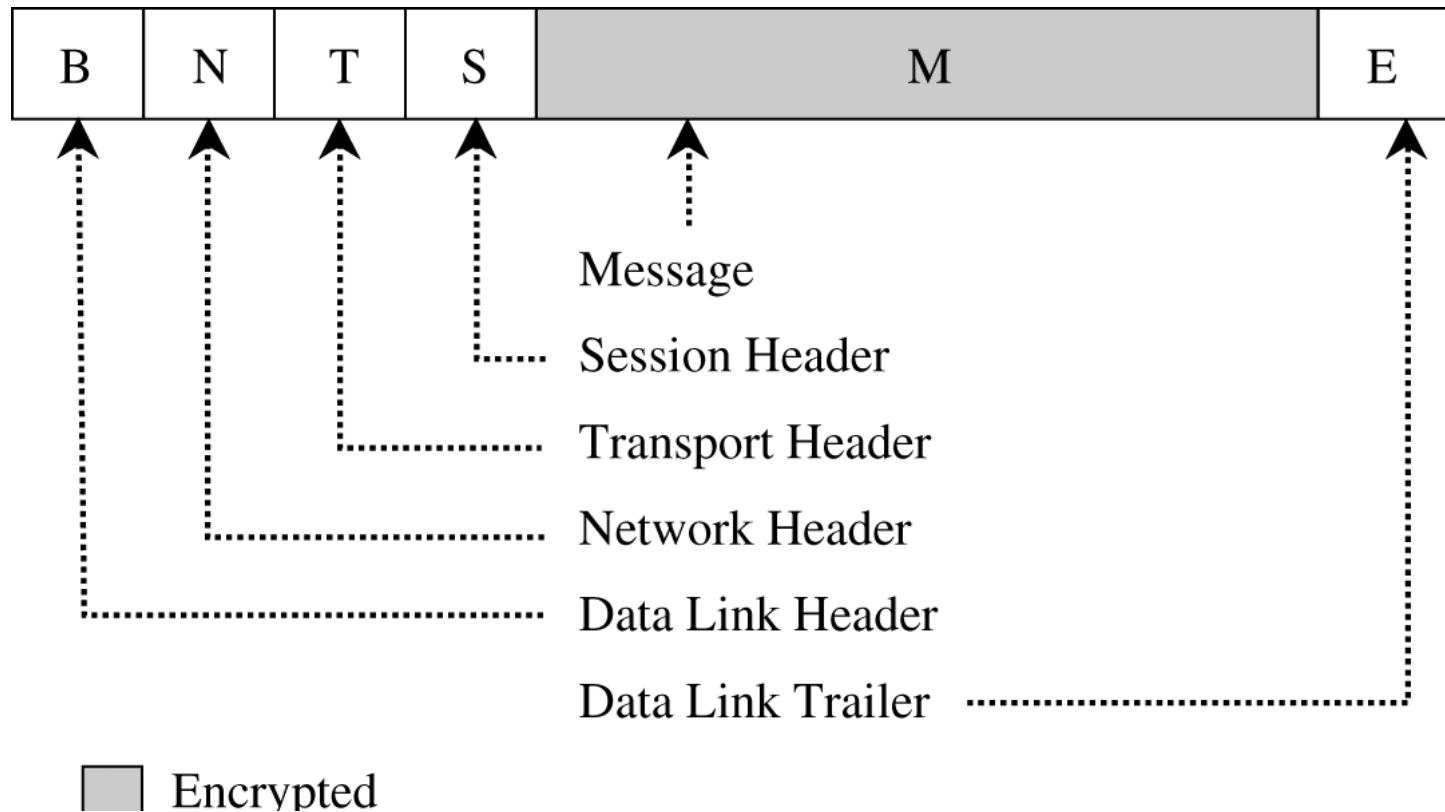


Figure 7-23 End-to-End Encrypted Message.



# Comparison of Encryption Methods

**Table 7-5. Comparison of Link and End-to-End Encryption.**

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

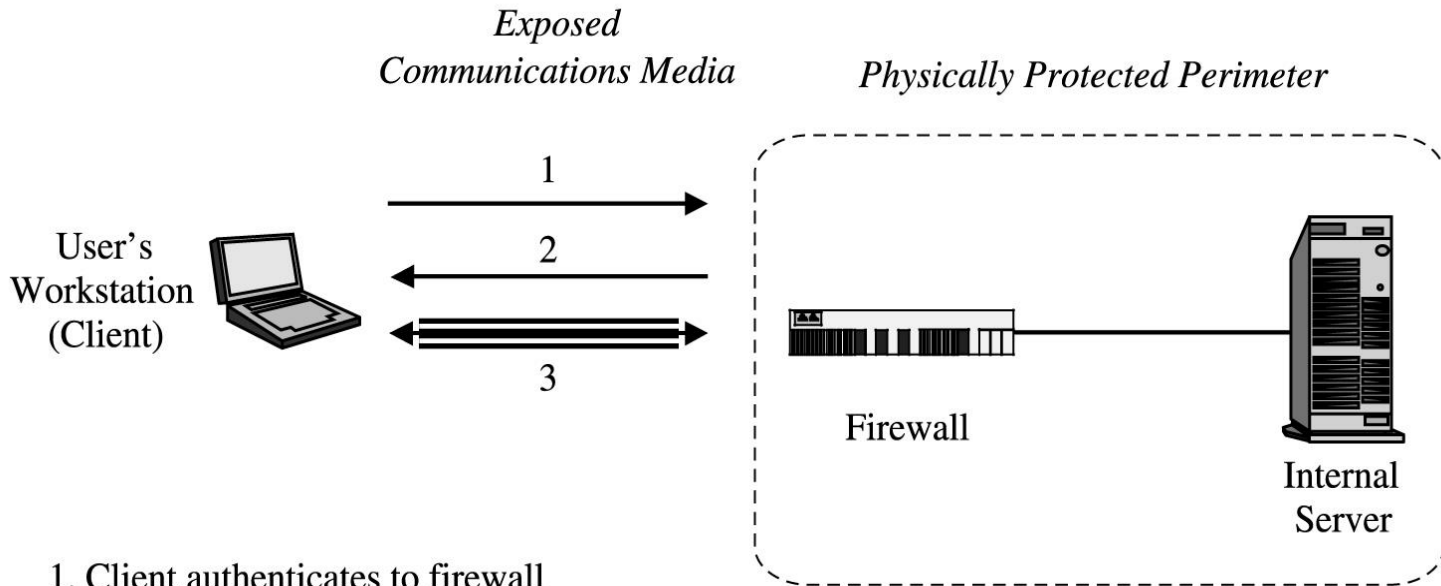
# Virtual Private Networks (VPN)

- Link encryption can be used to give a network's users the sense that they are on a private network
  - even when it is part of a public network
- For this reason, the approach is called a **virtual private network** (or VPN).
- Typically, physical security and administrative security are strong enough to protect transmission inside the perimeter of a network.
  - the greatest exposure for a user is between the user's workstation or client and the perimeter of the host network or server.

# Virtual Private Networks (VPN)

- A firewall is an access control device that sits between two networks or two network segments.
  - It filters all traffic between the protected or "inside" network and a less trustworthy or "outside" network or segment
- Many firewalls can be used to implement a VPN.
  - the user can request a VPN session with the firewall
  - The user's client and the firewall negotiate a session encryption key
  - the firewall and the client subsequently use that key to encrypt all traffic between the two
  - it feels to the user that the network is private, even though it is not.
- With the VPN, we say that the communication passes through an **encrypted tunnel** or tunnel.

# Virtual Private Networks (VPN)



1. Client authenticates to firewall
2. Firewall replies with encryption key
3. Client and server communicate via encrypted tunnel

Figure 7-25 Establishing a Virtual Private Network.

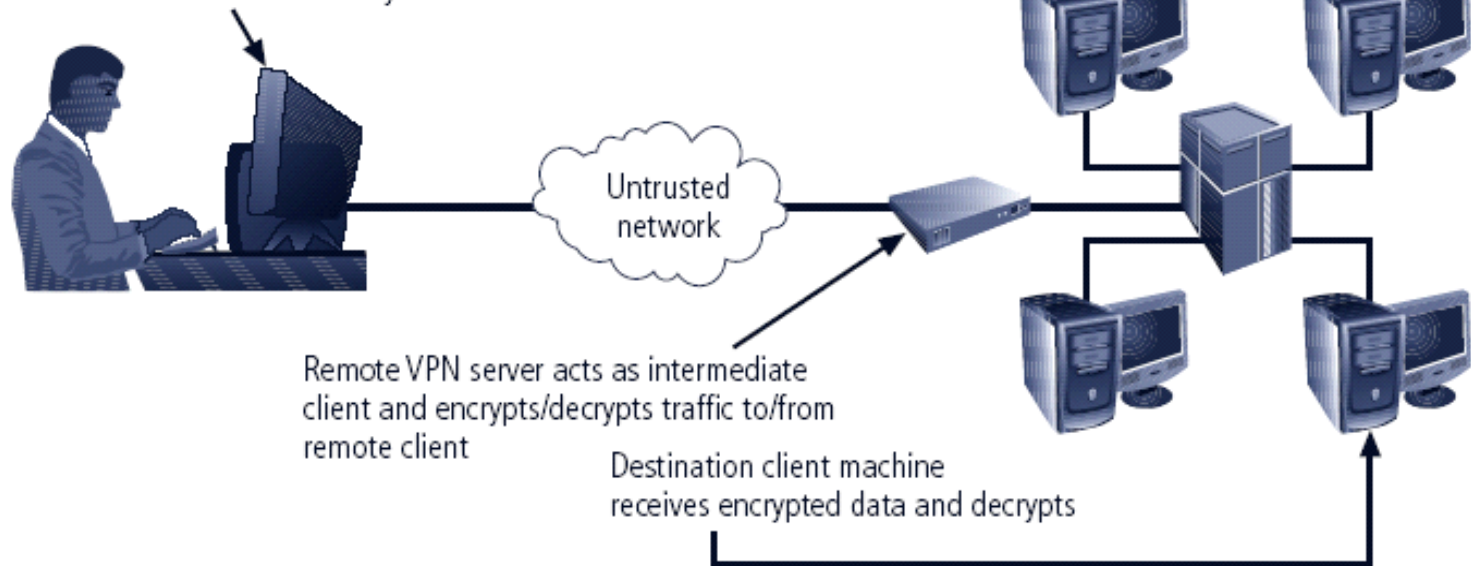
# Transport Mode

- Data within IP packet is encrypted, but header information is not
- Allows user to establish secure link directly with remote host, encrypting only data contents of packet
- Two popular uses:
  - End-to-end transport of encrypted data
  - Remote access worker connects to office network over Internet by connecting to a VPN server on the perimeter

Teleworker client machine encrypts data and sends to destination system with unencrypted header

OR

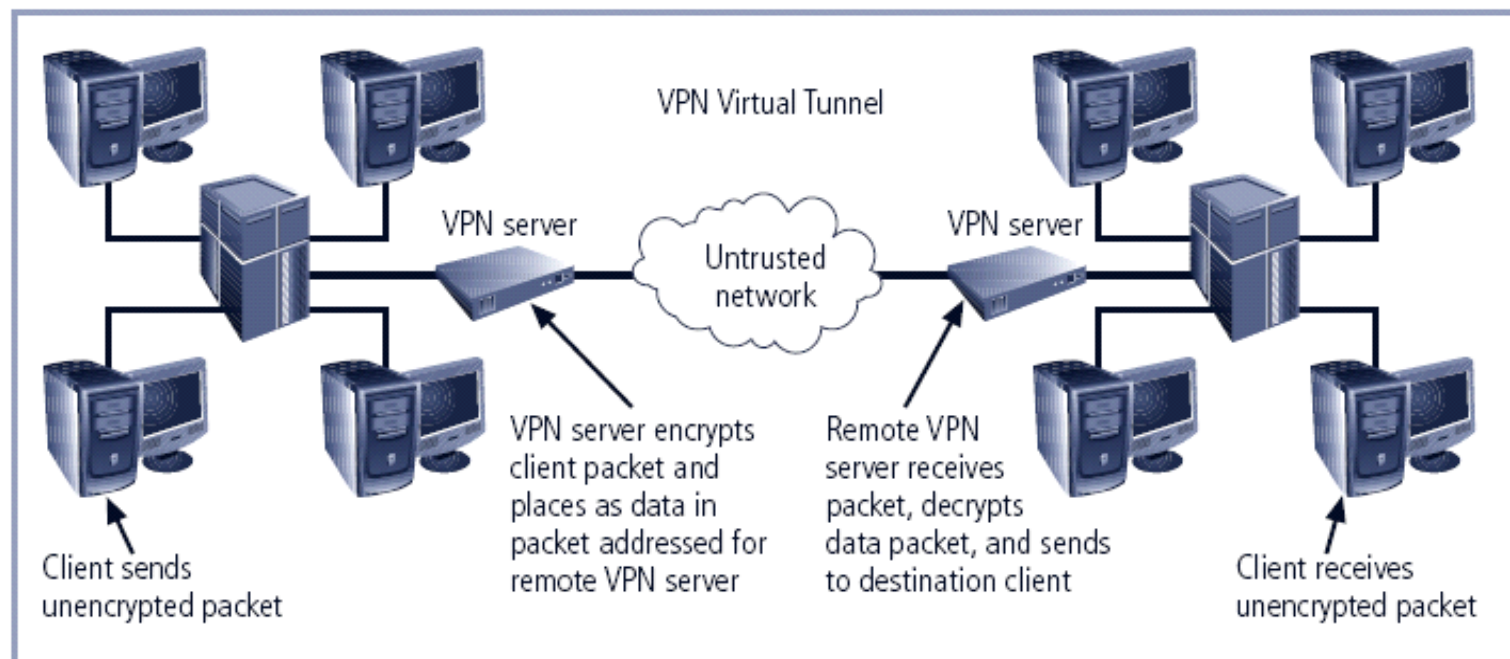
Teleworker client machine requests intranet connection using transport mode VPN then the client machine acts as if locally connected



**FIGURE 6-18** Transport Mode VPN

# Tunnel Mode

- Organization establishes two perimeter tunnel servers
- These servers act as encryption points, encrypting all traffic that will traverse unsecured network
- Primary benefit to this model is that an intercepted packet reveals nothing about true destination system
- Example of tunnel mode VPN: Microsoft's Internet Security and Acceleration (ISA) Server



**FIGURE 6-19** Tunnel Mode VPN



# SSL Encryption(Secure Sockets Layer)

- Originally designed by Netscape to protect communication between a web browser and server
  - It is also known now as TLS, for **transport layer security**
  - Most widely used secure communication protocol on the Internet
  - SSL interfaces between applications (such as browsers) and the TCP/IP protocols to provide server authentication, optional client authentication, and an encrypted communications channel between client and server
  - Client and server negotiate a mutually supported suite of encryption for session encryption and hashing
    - possibilities include triple DES and SHA1, or RC4 with a 128-bit key and MD5.

# SSL Encryption(Secure Sockets Layer)

- To use SSL,
  - the client requests an SSL session
  - The server responds with its public key certificate so that the client can determine the authenticity of the server.
  - The client returns part of a symmetric session key encrypted under the server's public key
  - Both the server and client compute the session key
  - then they switch to encrypted communication, using the shared session key

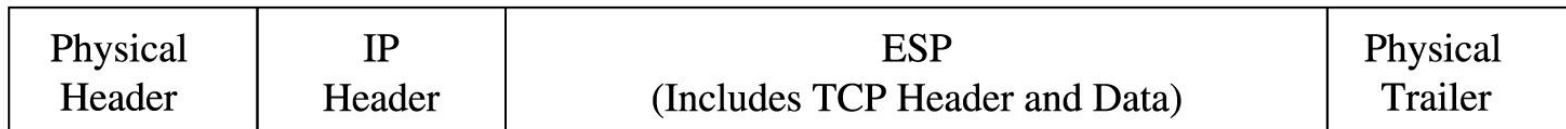
# IPSec

- As a part of the IPv6 suite, the IETF adopted **IPSec**, or the IP Security Protocol Suite.
- Designed to address fundamental shortcomings
  - spoofing, eavesdropping, and session hijacking
  - defines a standard means for handling encrypted data.
  - IPSec requires no change to the existing large number of TCP and UDP protocols
- Like SSL, it was designed to be independent of specific cryptographic protocols and to allow the two communicating parties to agree on a mutually supported set of protocols.

# IPSec



(a)



(b)

Figure 7-27 Packets: (a) Conventional Packet;  
(b) IPSec Packet.

**ESP** (encapsulated security payload).

# Firewalls

- A firewall is a device or, software, or a combination of both designed to prevent unauthorised users from accessing a network and/or a single workstation.
- Networks usually use hardware firewalls which are implemented on the router level. These firewalls are expensive, and it is difficult to configure them.
- Software Firewalls are used in single workstations and are usually less expensive and it is easier to configure them

# Firewalls

- Inspect each individual inbound or outbound packet of data to or from the system
- Check if it should be allowed to enter or otherwise it should be blocked

# Types of firewalls

- Packet filtering gateways or screening routers
- Stateful inspection firewalls
- Application proxies
- Guards
- Personal firewalls

# Packet filtering gateways

- Control is based on packet address or a specific transport protocol (e.g. HTTP).
- Example: a packet filter can block traffic using Telnet protocol but allows HTTP traffic.



# Stateful inspection firewalls

- Keeps a history of *previously seen packets* to make better decisions about current and future packets.
- Useful to counter attacks which force very short length packets into, say a TCP packet stream.
  - Remember TCP packets arrive in different order and firewall will not be able to detect the signature of an attack split across 2 or more packets.

# Application Proxies

- Packet filters deal with header information but not data inside the message.
- Also a malicious application that acts on behalf of the user (e.g. an e-mail agent), with all user's privileges can cause damage.

# Application Proxies

- Application Proxies have access to the entire range of information in the network stack. They can also filter harmful or disqualified commands in the data stream.
- The proxy controls actions through the firewall on the basis of the data visible *inside* the protocol, and not just on external header information

# comparison

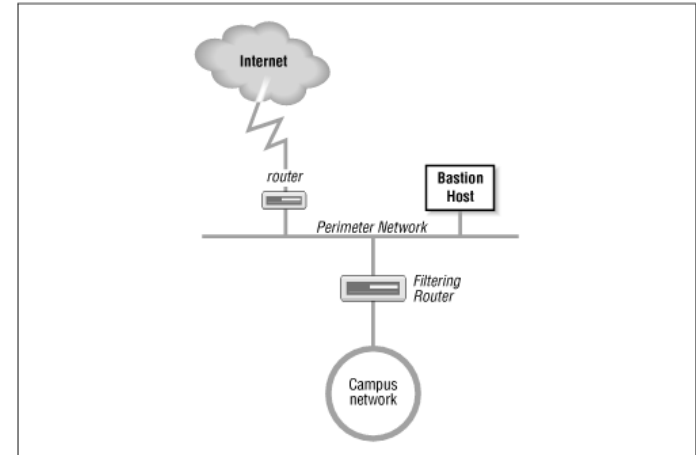
Packet Filtering	Stateful Inspection	Application Proxy	Guard	Personal Firewall
Simplest	More complex	Even more complex	Most complex	Similar to packet filtering firewall
Sees only addresses and service protocol type	Can see either addresses or data	Sees full data portion of packet	Sees full text of communication	Can see full data portion of packet
Auditing difficult	Auditing possible	Can audit activity	Can audit activity	Can and usually does audit activity
Screens based on connection rules	Screens based on information across packets in either header or data field	Screens based on behavior of proxies	Screens based on interpretation of message content	Typically, screens based on information in a single packet, using header or data
Complex addressing rules can make configuration tricky	Usually preconfigured to detect certain attack	Simple proxies can substitute for complex addressing	Complex guard functionality can limit assurance	Usually starts in "deny all inbound" mode, to which user

# DMZ

- Portion of network separating purely internal network from external network
  - Allows control of accesses to some trusted systems inside the corporate perimeter
  - If DMZ systems breached, internal systems still safe
  - Can perform different types of checks at boundary of internal,DMZ networks and DMZ,Internet network

# Screened Subnet or Demilitarized Zone (DMZ)

- Created between two packet filtering routers.
- The exterior router is the **only connection between the enterprise network and the outside world**
- **The interior router does the** bulk of the access control work. It filters packets
- The bastion host is a secure server. It provides an interconnection point between the enterprise network and the outside world for the restricted services
- The perimeter network connects the servers together and connects the exterior router to the interior router



# Intrusion Detection System

# Intrusion and Intrusion Detection

- Intrusion : Attempting to break into or misuse your system.
- Intruders may be from outside the network or legitimate users of the network.
- Intrusion can be a physical, system or remote intrusion.



# Different ways to intrude

- Buffer overflows
- Unexpected combinations
- Unhandled input
- Race conditions

# Intrusion Detection Systems (IDS)

Intrusion Detection Systems look for attack signatures, which are specific patterns that usually indicate malicious or suspicious intent.

# Intrusion Detection Systems (IDS)

- Different ways of classifying an IDS

IDS based on

- anomaly detection
- signature based misuse
- host based
- network based

# Anomaly based IDS

- This IDS models the normal usage of the network as a noise characterization.
- Anything distinct from the noise is assumed to be an intrusion activity.
  - E.g flooding a host with lots of packet.
- The primary strength is its ability to recognize novel attacks.

# Drawbacks of Anomaly detection IDS

- Assumes that intrusions will be accompanied by manifestations that are sufficiently unusual so as to permit detection.
- These generate many false alarms and hence compromise the effectiveness of the IDS.

# Signature based IDS

- This IDS possess an attacked description that can be matched to sensed attack manifestations.
- The question of what information is relevant to an IDS depends upon what it is trying to detect.
  - E.g DNS, FTP etc.

# Signature based IDS (contd.)

- ID system is programmed to interpret a certain series of packets, or a certain piece of data contained in those packets, as an attack. For example, an IDS that watches web servers might be programmed to look for the string “phf” as an indicator of a CGI program attack.
- Most signature analysis systems are based off of simple pattern matching algorithms. In most cases, the IDS simply looks for a sub string within a stream of data carried by network packets. When it finds this sub string (for example, the “phf” in “GET /cgi-bin/phf?”), it identifies those network packets as vehicles of an attack.

# Drawbacks of Signature based IDS

- They are unable to detect novel attacks.
- Suffer from false alarms
- Have to programmed again for every new pattern to be detected.



# Host/Applications based IDS

- The host operating system or the application logs in the audit information.
- These audit information includes events like the use of identification and authentication mechanisms (logins etc.) , file opens and program executions, admin activities etc.
- This audit is then analyzed to detect trails of intrusion.

# Drawbacks of the host based IDS

- The kind of information needed to be logged in is a matter of experience.
- Unselective logging of messages may greatly increase the audit and analysis burdens.
- Selective logging runs the risk that attack manifestations could be missed.

# Strengths of the host based IDS

- Attack verification
- System specific activity
- Encrypted and switch environments
- Monitoring key components
- Near Real-Time detection and response.
- No additional hardware

# Stack based IDS

- They are integrated closely with the TCP/IP stack, allowing packets to be watched as they traverse their way up the OSI layers.
- This allows the IDS to pull the packets from the stack before the OS or the application have a chance to process the packets.

# Network based IDS

- This IDS looks for attack signatures in network traffic via a promiscuous interface.
- A filter is usually applied to determine which traffic will be discarded or passed on to an attack recognition module. This helps to filter out known un-malicious traffic.

# Strengths of Network based IDS

- Cost of ownership reduced
- Packet analysis
- Evidence removal
- Real time detection and response
- Malicious intent detection
- Complement and verification
- Operating system independence

# Commercial ID Systems

- ISS – Real Secure from Internet Security Systems:
  - Real time IDS.
  - Contains both host and network based IDS.
- Tripwire – File integrity assessment tool.
- Bro and Snort – open source public-domain system.