01074305 Computer Security

Chapter 7

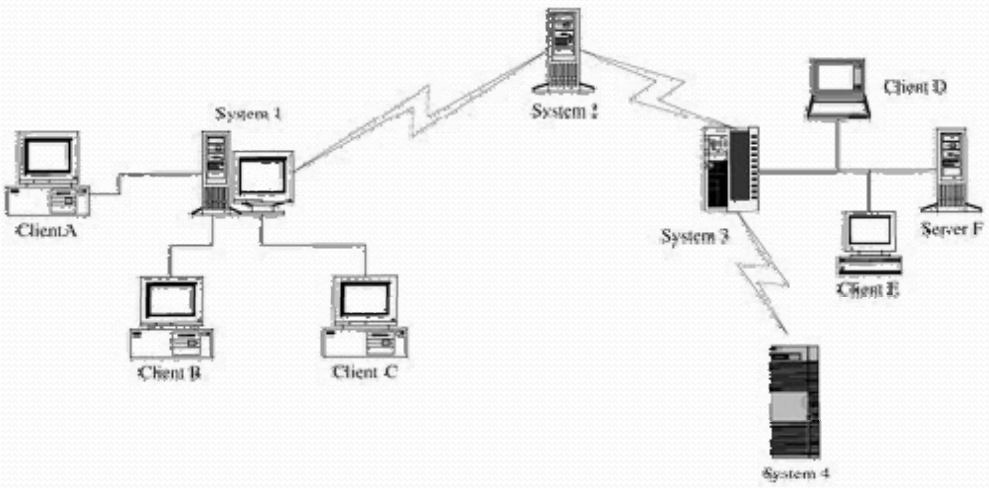
Security in Networks

Charles P. Pfleeger & Shari Lawrence Pfleeger, Security in Computing, 4th Ed., Pearson Education, 2007

- **In this chapter**
  - Networks vs. stand-alone applications and environments: differences and similarities
  - Threats against networked applications, including denial of service, web site defacements, malicious mobile code, and protocol attacks
  - Controls against network attacks: physical security, policies and procedures, and a range of technical controls
  - Firewalls: design, capabilities, limitations
  - Intrusion detection systems
  - Private e-mail: PGP and S/MIME

7.1. Network Concepts

- The Network
  - A network in its simplest form



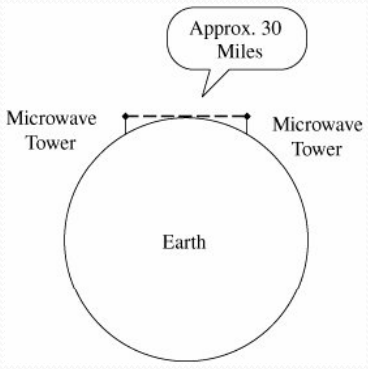
More Complex but More Typical View of Networks.

- The network (Cont'd)
  - Environment of Use
    - Networks can be described by several typical characteristics:
      - *Anonymity*. "On the Internet, nobody knows you're a dog."
      - *Automation*. One or both endpoints, as well as all intermediate points, involved in a given communication may be machines with only minimal human supervision.
      - *Distance*. Many networks connect endpoints that are physically far apart.
      - *Opaqueness*. users cannot tell if the current communication involves the same host with which they communicated the last time.
      - *Routing diversity.* To maintain or improve reliability and performance, routings between two endpoints are usually dynamic.

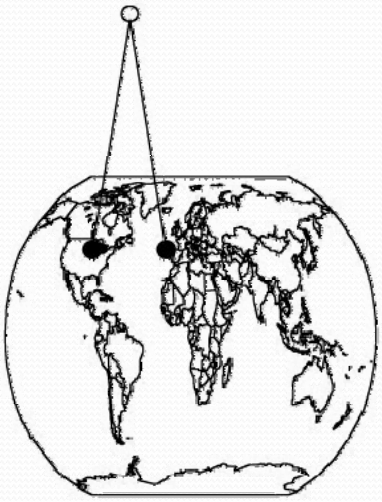
- The network (Cont'd)
  - Shape and Size
    - The way a network is configured is called the network **topology**.
    - Three dimensions of networks that have particular bearing on a network's security.
      - *Boundary*. The boundary distinguishes an element of the network from an element outside it.
      - *Ownership*. It is often difficult to know who owns each host in a network.
      - *Control*. Finally, if ownership is uncertain, control must be, too.

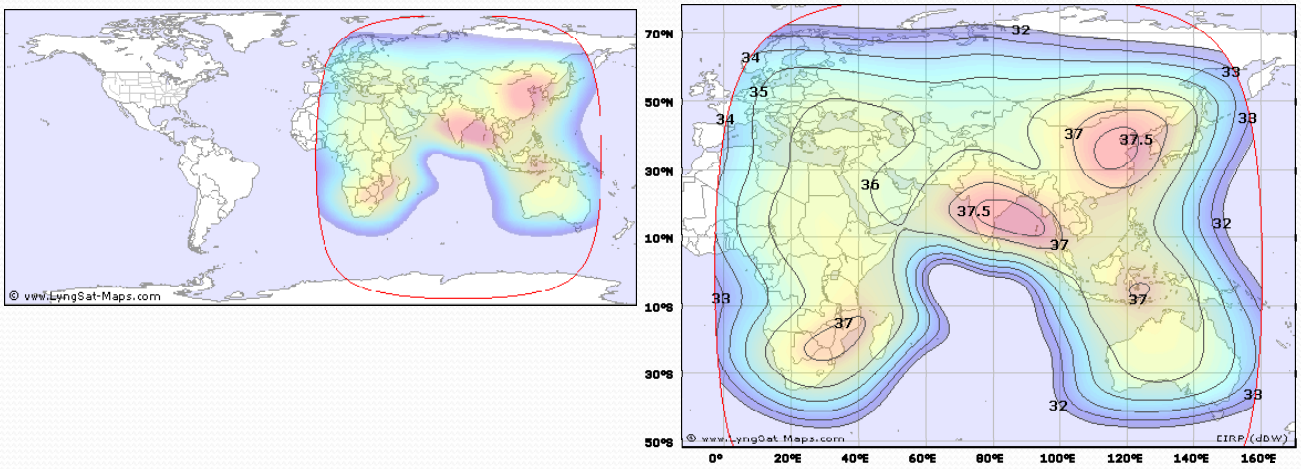
- The network (Cont'd)
  - Media
    - Cable
      - **Twisted pair** or **unshielded twisted pair (UTP)**.
      - **Coaxial (coax) cable**
        - **Ethernet**, carrying up to 100 Mbps over distances of up to 1500 feet.
        - Coax cable also suffers from degradation of signal quality over distance.
        - Repeaters (for digital signals) or amplifiers (for analog signals)
    - Optical Fiber
      - Less interference, less crossover between adjacent media, lower cost, and less weight than copper

- The network (Cont'd)
  - Media
    - Wireless
      - A protocol developed for short-range telecommunications, designated the802.11 family of standards.
    - Microwave



- The network (Cont'd)
  - Media
    - Infrared
      - Carries signals for short distances (up to 9 miles)
    - Satellite
      - Geosynchronous orbits
      - A rather narrow angle of dispersion from the satellite's transmitter produces a fairly broad pattern (called the **footprint**) on the surface of the earth



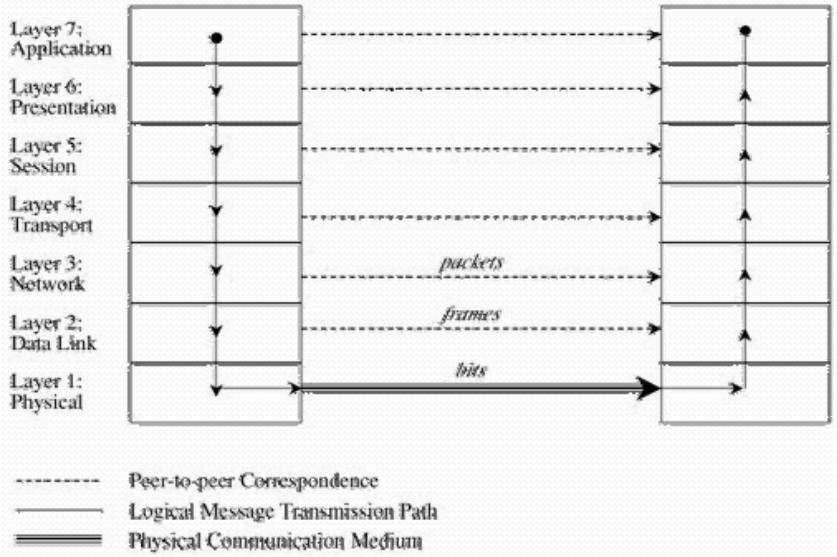


Footprint of the ThaiCom 5 at 78.5°E

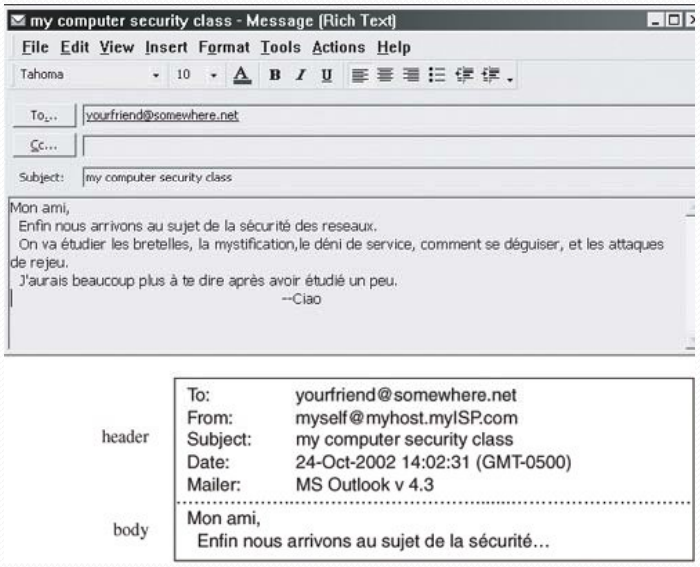
- The network (Cont'd)
  - Protocols
    - When we use a network, the communication media are usually transparent to us.
    - Most of us do not know whether our communication is carried over copper wire, optical fiber, satellite, microwave, or some combination.
    - This ambiguity is actually a positive feature of a network: its ***independence***.
    - Independence is possible because we have defined **protocols** that allow a user to view the network at a high, abstract level of communication (viewing it in terms of user and data)
    - The software and hardware enable us to implement a network according to a **protocol stack**, a layered architecture for communications.

- The network (Cont'd)
  - Protocols
    - ISO OSI Reference Model

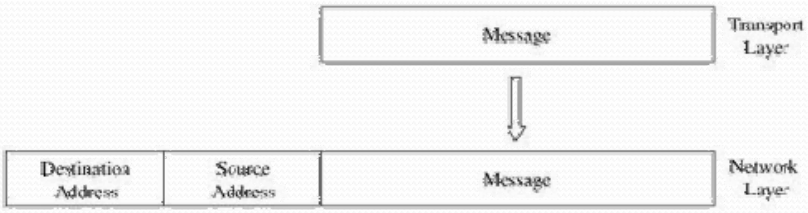
Layer	Name	Activity
7	Application	User-level data
6	Presentation	Standardized data appearance, blocking, text compression
5	Session	Sessions or logical connections between parts of an application; message sequencing, recovery
4	Transport	Flow control, end-to-end error detection and correction, priority service
3	Network	Routing, message blocking into uniformly sized packets
2	Data Link	Reliable data delivery over physical medium; transmission error recovery, separating packets into uniformly sized frames
1	Physical	Actual communication across physical medium; individual bit transmission



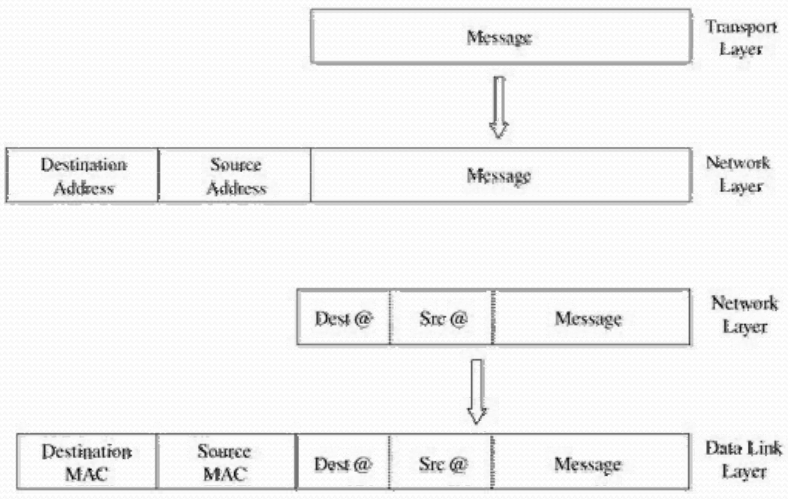
- The network (Cont'd)
  - Protocols (Cont'd)
    - ISO OSI Reference Model
      - Each layer passes data in three directions:
        - *above* with a layer communicating more abstractly,
        - *parallel* or *across* to the same layer in another host,
        - *below* with a layer handling less abstract (that is, more fundamental) data items.
        - The communications above and below are actual interactions, while the parallel one is a virtual communication path. Parallel layers are called "**peers**."



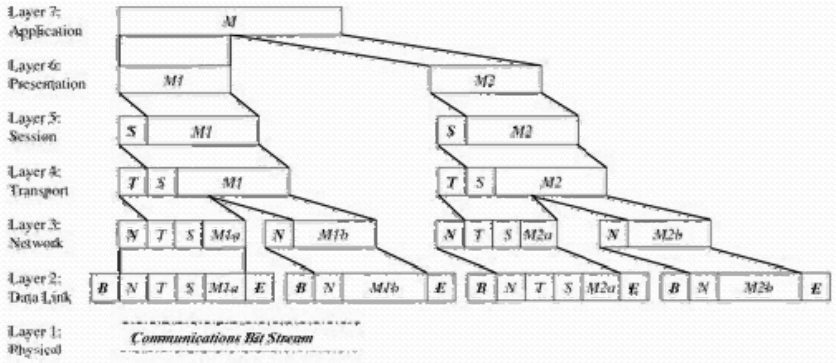
- The network (Cont'd)
  - Protocols (Cont'd)
    - Addressing
      - Suppose your message is addressed to yourfriend@somewhere.net.
      - At the network layer, a **router** actually sends the message from your network to a router on the network somewhere.net.
      - Together, the network layer structured with destination address, source address, and data is called a **packet**.



- The network (Cont'd)
  - Protocols (Cont'd)
    - Addressing (Cont'd)
      - Every computer connected to a network has a **network interface card (NIC)** with a unique physical address, called a **MAC address** (for Media Access Control).
      - At the data link level, two more headers are added, one for your computer's NIC address (the source MAC) and one for your router's NIC address.
      - A data link layer structure with destination MAC, source MAC, and data is called a **frame**.



- The network (Cont'd)
  - Protocols (Cont'd)
    - Layering
      - Each layer reformats the transmissions and exchanges information with its peer layer. Let us summarize what each layer contributes.



- The network (Cont'd)
  - Protocols (Cont'd)
    - TCP/IP
      - The OSI model is a conceptual one; it shows the different activities required for sending a communication.
      - However, full implementation of a seven-layer transmission carries too much overhead for megabit-per-second communications.
      - The OSI protocol slows things down to unacceptable levels.

- The network (Cont'd)
  - Protocols (Cont'd)
    - TCP/IP
      - TCP/IP is defined by protocols, not layers, but we can think of it in terms of four layers:
        - Application
        - Host-to-host (end-to-end) transport
        - Internet
        - Physical.

- The network (Cont'd)
  - Protocols (Cont'd)
    - TCP/IP
      - TCP/IP is often used as a single acronym, it really denotes two different protocols:
        - **TCP** implements a connected communications session on top of the more basic **IP** transport protocol.
        - **UDP** (user datagram protocol) is also an essential part of the suite.

Layer	Action	Responsibilities
Application	Prepare messages from	user interactions User interaction, addressing
Transport	Convert messages to packets	Sequencing, reliability (integrity), error correction
Internet	Convert packets to datagrams	Flow control, routing
Physical	Transmit datagrams as individual bits	Data communication

- The network (Cont'd)
  - Protocols (Cont'd)
    - TCP/IP
      - The TCP protocol must ensure the correct sequencing of packets as well as the integrity (correct transmission) of data within packets.
      - A TCP packet is a data structure that includes a sequence number, an acknowledgment number for connecting the packets of a communication session, flags, and source and destination port numbers.
      - A port is a number designating a particular application running on a computer.
      - The UDP protocol does not provide the error-checking and correcting features of TCP, but it is a much smaller, faster protocol.

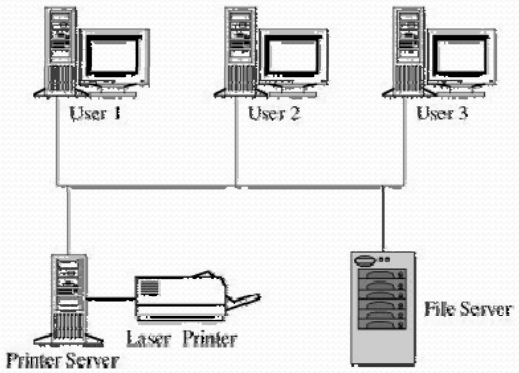
Layer	TCP Protocols	UDP Protocols
Application Protocol	SMTP (Simple Mail Transfer Protocol): used for communicating e-mail HTTP (Hypertext Transfer Protocol): used for communicating web pages FTP (File Transfer Protocol): used for receiving or sending files Telnet (Terminal Emulation Protocol): used for performing remote operations as if directly connected to the host from a terminal and others	SNMP (Simple Network Monitoring Protocol): used for controlling network devices Syslog (System Audit Log): used for entering records in the system log Time: used for communicating and synchronizing time among network devices and others
Transport	TCP	UDP
Internet	IP	IP
Physical	Data communication	Data communication

- The network (Cont'd)
  - Protocols (Cont'd)
    - Addressing Scheme
      - All networks use an addressing scheme so that data can be directed to the expected recipient.
      - All network models implement an addressing scheme.
      - An address is a unique identifier for a single point in the network.
      - A host on a TCP/IP wide area network has a 32-bit address called an **IP address**.

- The network (Cont'd)
  - Protocols (Cont'd)
    - Addressing Scheme (Cont'd)
      - An IP address is expressed as four 8-bit groups in decimal notation, separated by periods, such as 100.24.48.6. (Note: The world's networks are running out of unique addresses. This 32-bit standard address is being increased to 128 bits in a scheme called IPv6.)
      - People prefer speaking in words or pseudowords, so network addresses are also known by **domain names**, such as ATT.COM

- The network (Cont'd)
  - Protocols (Cont'd)
    - Routing Concepts
      - A host needs to know how to direct a packet from its own IP address.
      - Each host knows to what other hosts it is directly connected
      - Hosts communicate their connections to their neighbors.
      - Hosts advertise to their neighbors to describe to which hosts (addresses) they can route traffic and at what cost (number of hops).
      - Each host routes traffic to a neighbor that offers a path at the cheapest cost.

- The network (Cont'd)
  - Types of Networks
    - Local Area Networks
      - *Small.*
      - *Locally controlled.*
      - *Physically protected.*
      - *Limited scope.*
    - Wide Area Networks
      - *Single control.*
      - *Covers a significant distance.*
      - *Physically exposed* (often, but not always).

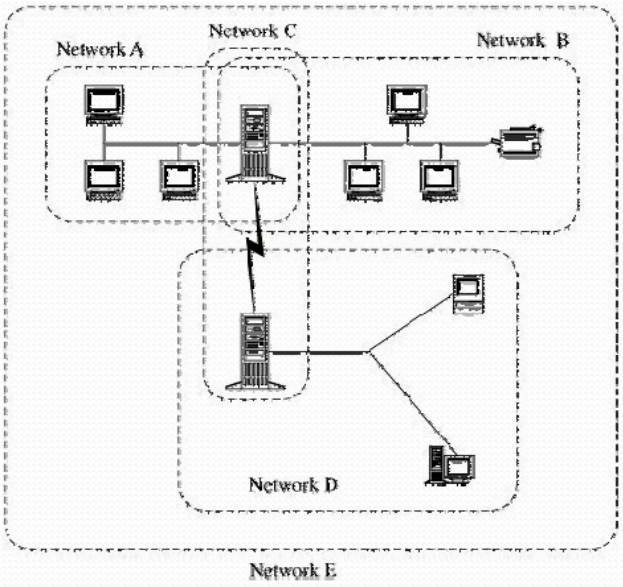


- The network (Cont'd)
  - Types of Networks
    - Internetworks (Internets)
      - Networks of networks, or internetwork networks, are sometimes called **internets**.
      - An internet is a connection of two or more separate networks, in that they are separately managed and controlled.
      - The most significant internetwork is known as the **Internet**, because it connects so many of the other public networks.

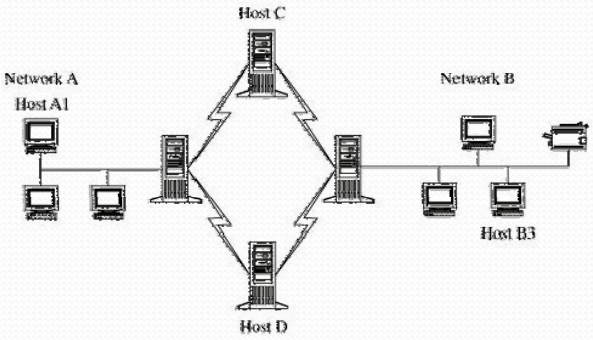
- The network (Cont'd)
  - Types of Networks (Cont'd)
    - Internetworks (Internets) (Cont'd)
      - The characteristics of the Internet.
        - *Federation*. Almost no general statements can be made about Internet users or even network service providers.
        - *Enormous*.
        - *Heterogeneous*.
        - *Physically and logically exposed*.

7.2. Threats in Networks

- What Makes a Network Vulnerable?
  - Consider how a network differs from a stand-alone environment:
    - *Anonymity*. An attacker can mount an attack from thousands of miles away and never come into direct contact with the system
    - *Many points of attack both targets and origins*
    - *Sharing*.
    - *Complexity of system*.
    - *Unknown perimeter*.
    - *Unknown path*.



Unclear Network Boundaries



Uncertain Message Routing in a Network

- **Who Attacks Networks?**
  - Four important motives are challenge or power, fame, money, and ideology.
  - **Challenge -** Some attackers enjoy the intellectual stimulation of defeating the supposedly undefeatable.
  - **Fame -** Seek recognition for their activities
  - **Money and Espionage**
  - **Ideology -** Attacks are perpetrated to advance ideological ends.

- **Reconnaissance**
  - A clever attacker investigates and plans before acting.
  - A network attacker learns a lot about a potential target before beginning the attack.

- **Reconnaissance (Cont'd)**
  - **Port Scan**
    - A program that, for a particular IP address, reports which ports respond to messages and which of several known vulnerabilities seem to be present.
    - Port scanning tells an attacker three things:
      - which standard ports or services are running and responding on the target system,
      - what operating system is installed on the target system
      - what applications and versions of applications are present.

- Reconnaissance (Cont'd)
  - Social Engineering
    - The port scan gives an external picture of a networkwhere are the doors and windows, of what are they constructed, to what kinds of rooms do they open? The attacker also wants to know what is inside the building.
    - Social engineering involves using social skills and personal interaction to get someone to reveal security-relevant information and perhaps even to do something that permits an attack.
    - Because the victim has helped the attacker (and the attacker has profusely thanked the victim), the victim will think nothing is wrong and not report the incident.

- Reconnaissance (Cont'd)
  - Intelligence
    - From a port scan the attacker knows what is open.
    - From social engineering, the attacker knows certain internal details.
    - But a more detailed floor plan would be nice.
    - **Intelligence** is the general term for collecting information.
    - In security it often refers to gathering discrete bits of information from various sources and then putting them together

- Reconnaissance (Cont'd)
  - Operating System and Application Fingerprinting
    - The port scan supplies the attacker with very specific information.
    - The attacker is likely to have many related questions, such as which commercial server application is running, what version, and what the underlying operating system and version are.
    - A new version will implement a new feature but an old version will reject the request. All these peculiarities, sometimes called the operating system or application **fingerprint**, can mark the manufacturer and version.

- Reconnaissance (Cont'd)
  - Operating System and Application Fingerprinting (Cont'd)
    - Ports such as 80 (HTTP), 25 (SMTP), 110 (POP), and 21 (FTP) may respond with something like

```
Server: Netscape-Commerce/1.12 Your browser
sent a non-HTTP compliant message.
```

Or

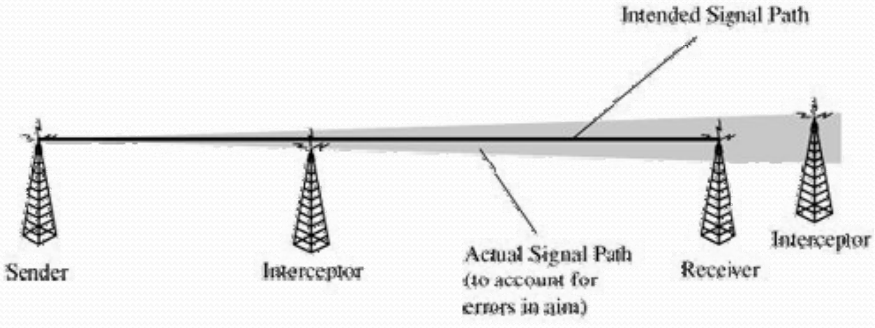
```
Microsoft ESMTP MAIL Service, Version:
5.0.2195.3779
```

- Reconnaissance (Cont'd)
  - Bulletin Boards and Chats
  - Availability of Documentation
  - Concluding Remarks
    - A good thief, that is, a successful one, spends time understanding the context of the target.
    - To prepare for perpetrating a bank theft, the thief might monitor the bank, seeing how many guards there are, when they take breaks, when cash shipments arrive, and so forth.

- Threats in Transit: Eavesdropping and Wiretapping
  - The term **eavesdrop** implies overhearing without expending any extra effort.
  - A more hostile term is **wiretap**, which means intercepting communications through some effort.
    - **Passive wiretapping** is just "listening," much like eavesdropping.
    - But **active wiretapping** means injecting something into the communication.

- Threats in Transit: Eavesdropping and Wiretapping (Cont'd)
  - Cable
    - A **packet sniffer** can retrieve all packets on the LAN. Alternatively, one of the interface cards can be reprogrammed to have the supposedly unique address of another existing card on the LAN so that two different cards will both fetch packets for one address.
    - By a process called **inductance** an intruder can tap a wire and read radiated signals without making physical contact with the cable.
    - The easiest form of intercepting a cable is by direct cut. If a cable is severed, all service on it stops. As part of the repair, an attacker can easily splice in a secondary cable that then receives a copy of all signals along the primary cable.

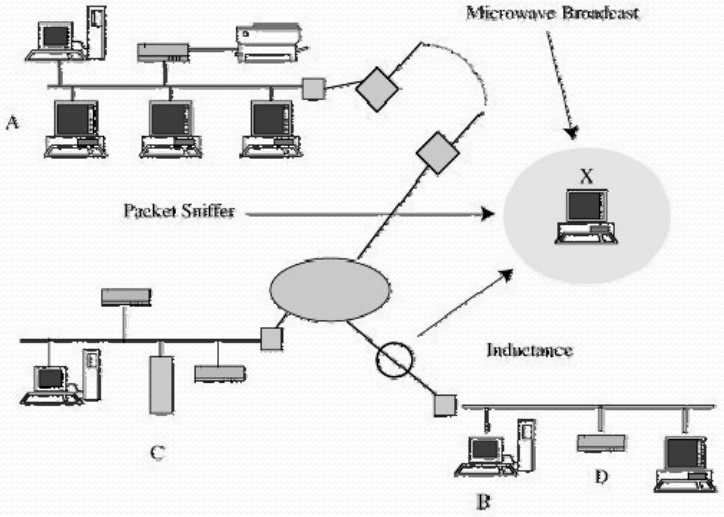
- Threats in Transit: Eavesdropping and Wiretapping (Cont'd)
  - Microwave



- Threats in Transit: Eavesdropping and Wiretapping (Cont'd)
  - Satellite Communication
  - Optical Fiber
    - Optical fiber offers two significant security advantages over other transmission media.
      - First, the entire optical network must be tuned carefully each time a new connection is made.
      - Second, optical fiber carries light energy, not electricity. Light does not emanate a magnetic field as electricity does.

- Threats in Transit: Eavesdropping and Wiretapping (Cont'd)
  - Wireless
    - The major threat is not interference; it is interception.
    - Interception
    - Theft of Service

- Threats in Transit: Eavesdropping and Wiretapping (Cont'd)
  - Summary of Wiretapping



- Summary of Wiretapping (Cont'd)
  - Protocol Flaws
    - Internet protocols are publicly posted for scrutiny by the entire Internet community. Each accepted protocol is known by its Request for Comment (**RFC**) number.

- Summary of Wiretapping (Cont'd)
  - Impersonation
    - Guess the identity and authentication details of the target.
    - Pick up the identity and authentication details of the target from a previous communication or from wiretapping.
    - Circumvent or disable the authentication mechanism at the target computer.
    - Use a target that will not be authenticated.
    - Use a target whose authentication data are known.

- Summary of Wiretapping (Cont'd)
  - Impersonation (Cont'd)
    - **Authentication Foiled by Guessing**
      - Easy-to-guess passwords.
      - Default passwords.
      - Dead accounts offer a final source of guessable passwords.
    - **Authentication Thwarted by Eavesdropping or Wiretapping**
    - **Authentication Foiled by Avoidance**
      - A weak or flawed authentication allows access to any system or person who can circumvent the authentication.

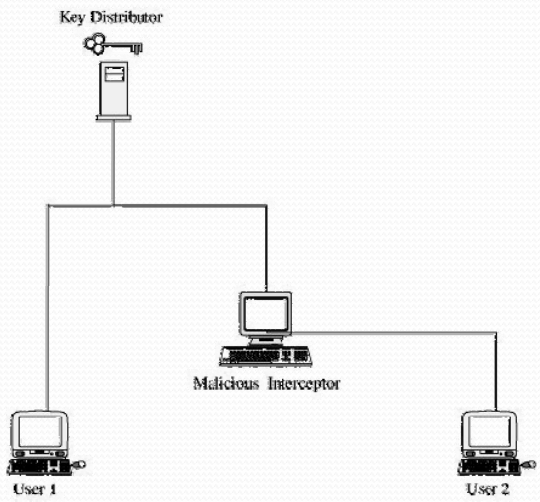
- Summary of Wiretapping (Cont'd)
  - Impersonation (Cont'd)
    - Nonexistent Authentication
      - If two computers are used by the same users to store data and run processes and if each has authenticated its users on first access, you might assume that computer-to-computer or local user-to-remote process authentication is unnecessary.

- Summary of Wiretapping (Cont'd)
  - Impersonation (Cont'd)
    - Well-Known Authentication
      - Authentication data should be unique and difficult to guess.
      - But the convenience of one well-known authentication scheme sometimes usurps the protection.
      - For example, one computer manufacturer planned to use the same password to allow its remote maintenance personnel to access any of its computers belonging to any of its customers throughout the world.

- Summary of Wiretapping (Cont'd)
  - Impersonation (Cont'd)
    - Trusted Authentication
      - Authentication can become a problem when identification is delegated to other trusted sources.
    - Spoofing
      - an attacker falsely carries on one end of a networked interchange.

- Summary of Wiretapping (Cont'd)
  - Impersonation (Cont'd)
    - Masquerade
      - One host pretends to be another.
      - A common example is URL confusion. E.g., xyz.com, xyz.org, and xyz.net might be three different organizations
      - A variation of this attack is called **phishing**. You send an e-mail message, perhaps with the real logo of Blue Bank, and an enticement to click on a link, supposedly to take the victim to the Blue Bank web site.

- Summary of Wiretapping (Cont'd)
  - Impersonation (Cont'd)
    - Session Hijacking
      - Intercepting and carrying on a session begun by another entity.
    - Man-in-the-Middle Attack
      - A **man-in-the-middle** attack is a similar form of attack, in which one entity intrudes between two others.



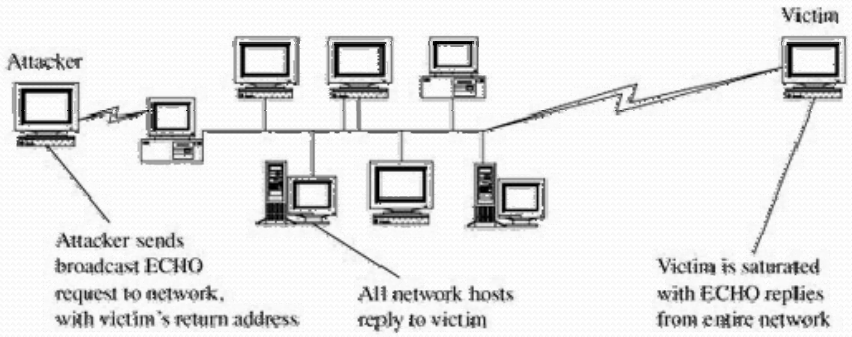
Key Interception by a Man-in-the-Middle Attack.

- Message Confidentiality Threats
  - Misdelivery
  - Exposure
    - To protect the confidentiality of a message, we must track it all the way from its creation to its disposal.
    - Along the way, the content of a message may be exposed in temporary buffers; at switches, routers, gateways, and intermediate hosts throughout the network; and in the workspaces of processes that build, format, and present the message.
  - Traffic Flow Analysis
    - Sometimes not only is the message itself sensitive but the fact that a message *exists* is also sensitive.

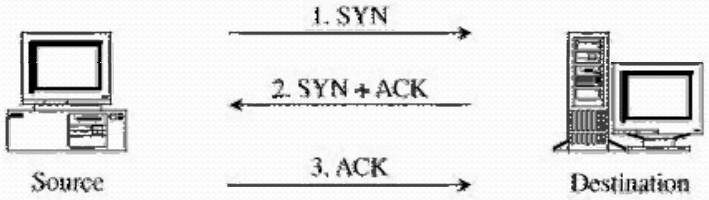
- Message Integrity Threats
  - Falsification of Messages
  - Noise
- Format Failures
  - Malformed Packets
  - Protocol Failures and Implementation Flaws

- Web Site Vulnerabilities
  - Web Site Defacement
  - Buffer Overflows
  - Dot-Dot-Slash
    - E.g, `http://yoursite.com/webhits.htw?CiWebHits&File=../../../../../winnt/system32/autoexec.nt`
  - Application Code Errors

- Denial of Service
  - Transmission Failure
  - Connection Flooding
  - Echo-Chargen
    - Chargen is a protocol that generates a stream of packets; it is used to test the network's capacity.
  - Ping of Death



- Denial of Service (Cont'd)
  - Smurf
    - First, the attacker chooses a network of unwitting victims.
    - The attacker spoofs the source address in the ping packet so that it appears to come from the victim.
    - Then, the attacker sends this request to the network in **broadcast mode**



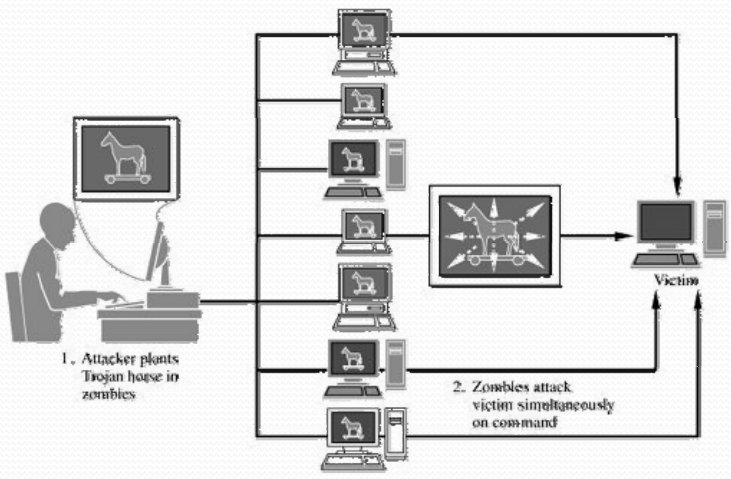
- Denial of Service (Cont'd)
  - Syn Flood
    - A session is established with a three-way TCP handshake.
    - Occasionally packets get lost or damaged in transmission.
    - The destination maintains a queue called the **SYN_RECV** connections, tracking those items for which a SYNACK has been sent but no corresponding ACK has yet been received.
    - The attacker can deny service to the target by sending many SYN requests and never responding with ACKs, thereby filling the victim's SYN_RECV queue.

- Denial of Service (Cont'd)
  - Teardrop
    - The **teardrop** attack misuses a feature designed to improve network communication.
    - The attacker sends a series of datagrams that cannot fit together properly.
    - One datagram might say it is position 0 for length 60 bytes, another position 30 for 90 bytes, and another position 41 for 173 bytes.
    - These three pieces overlap, so they cannot be reassembled properly.
    - In an extreme case, the operating system locks up with these partial data units it cannot reassemble, thus leading to denial of service.

- Denial of Service (Cont'd)
  - Traffic Redirection
    - If an attacker can corrupt the routing, traffic can disappear.
    - Suppose a router advertises to its neighbors that it has the best path to every other address in the whole network.
    - Soon all routers will direct all traffic to that one router.
    - The one router may become flooded, or it may simply drop much of its traffic.
    - In either case, a lot of traffic never makes it to the intended destination.

- Denial of Service (Cont'd)
  - DNS Attacks
    - By overtaking a name server or causing it to cache spurious entries (called **DNS cache poisoning**), an attacker can redirect the routing of any traffic, with an obvious implication for denial of service.
    - .

- Distributed Denial of Service (DDoS)



- Threats in Active or Mobile Code
  - **Active code** or **mobile code** is a general name for code that is pushed to the client for execution.
  - Cookies
    - A **cookie** is a data object that can be held in memory (a **per-session** cookie) or stored on disk for future access (a **persistent** cookie).

- Threats in Active or Mobile Code (Cont'd)
  - Scripts
    - Clients can invoke services by executing scripts on servers.
    - The server cannot distinguish between commands generated from a user at a browser completing a web page and a user's handcrafting a set of orders.
    - The malicious user can monitor the communication between a browser and a server to see how changing a web page entry affects what the browser sends and then how the server reacts.

- Threats in Active or Mobile Code (Cont'd)
  - Active Code
    - Java Code
      - A **hostile applet** is downloadable Java code that can cause harm on the client's system.
    - ActiveX Controls
      - Using ActiveX controls, objects of arbitrary type can be downloaded to a client. If the client has a viewer or handler for the object's type, that viewer is invoked to present the object.

- Threats in Active or Mobile Code (Cont'd)
  - Bots
    - **Bots**, hackerese for robots, are pieces of malicious code under remote control.
    - A network of bots, called a **botnet**,

- **Complex Attacks**
  - **Script Kiddies**
    - An underground establishment has written scripts for many of the popular attacks.
    - With a script, attackers need not understand the nature of the attack or even the concept of a network.
    - The attackers merely download the attack script and execute it.
    - People who download and run attack scripts are called **script kiddies**.

7.3. Network Security Controls

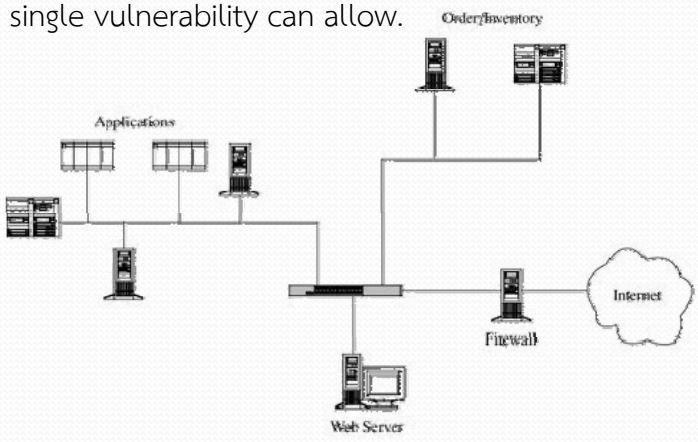
- **Security Threat Analysis**
  - The three steps of a security threat analysis in other situations.
    - First, we scrutinize all the parts of a system so that we know what each part does and how it interacts with other parts.
    - Next, we consider possible damage to confidentiality, integrity, and availability.
    - Finally, we hypothesize the kinds of attacks that could cause this damage.

- **Security Threat Analysis (Cont'd)**
  - Individual parts of a network:
    - *local nodes* connected via
    - *local communications links* to a
    - *local area network,* which also has
    - *local data storage,*
    - *local processes,* and
    - *local devices.*

- **Security Threat Analysis (Cont'd)**
  - The local network is also connected to a
    - *network gateway* which gives access via
    - *network communications links* to
    - *network control resources,*
    - *network routers,* and
    - *network resources*, such as databases.

- Security Threat Analysis (Cont'd)
  - Summarize these threats with a list:
    - intercepting data in traffic
    - accessing programs or data at remote hosts
    - modifying programs or data at remote hosts
    - modifying data in transit
    - inserting communications
    - impersonating a user
    - inserting a repeat of a previous communication
    - blocking selected traffic
    - blocking all traffic
    - running a program at a remote host

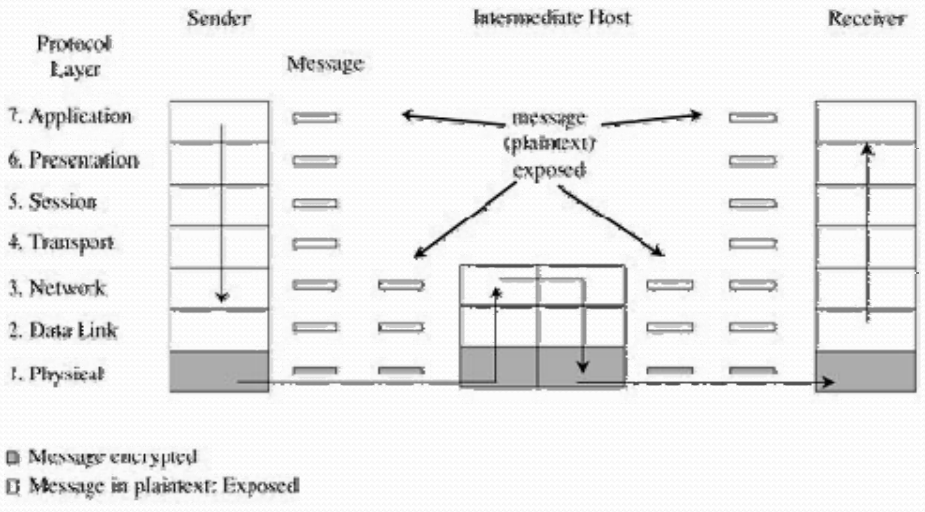
- Design and Implementation
  - Architecture
    - Segmentation
      - Segmentation reduces the number of threats, and it limits the amount of damage a single vulnerability can allow.

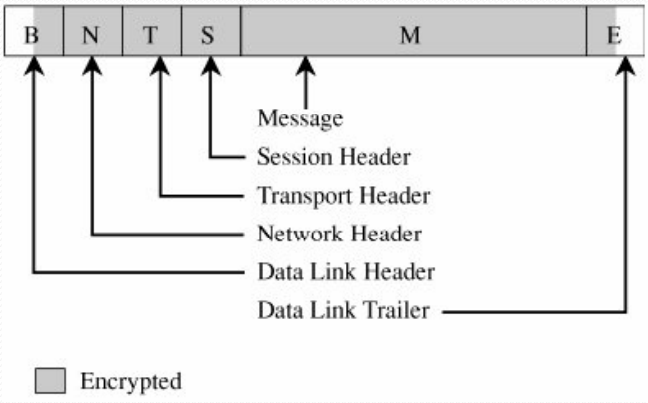


- Design and Implementation (Cont'd)
  - Architecture (Cont'd)
    - Redundancy
      - Another key architectural control is redundancy: allowing a function to be performed on more than one node, to avoid "putting all the eggs in one basket."
      - In **failover mode** the servers communicate with each other periodically, each determining if the other is still active. If one fails, the other takes over processing for both of them.

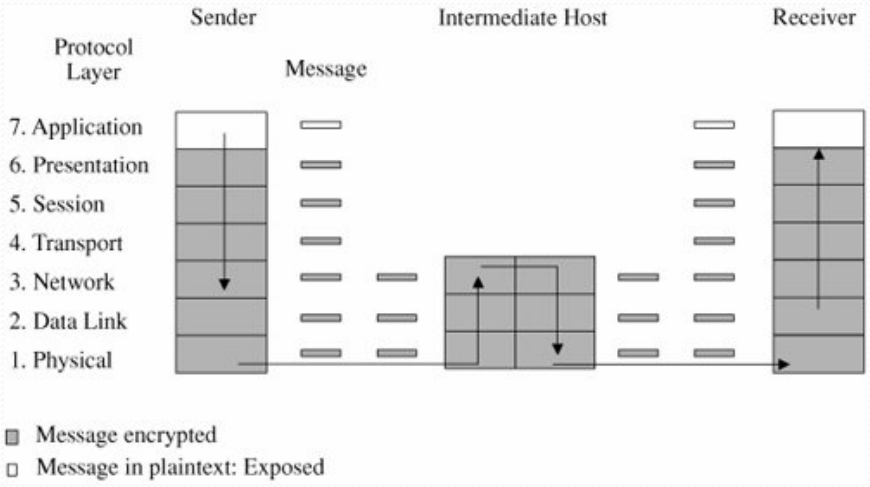
- Design and Implementation (Cont'd)
  - Architecture (Cont'd)
    - Single Points of Failure
      - One way to evaluate the network architecture's tolerance of failure is to look for **single points of failure**.

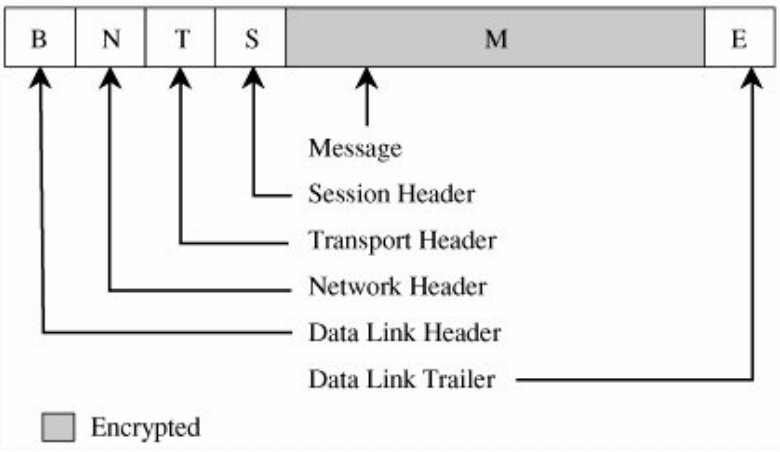
- Design and Implementation (Cont'd)
  - Encryption
    - Link Encryption
      - Data are encrypted just before the system places them on the physical communications link.

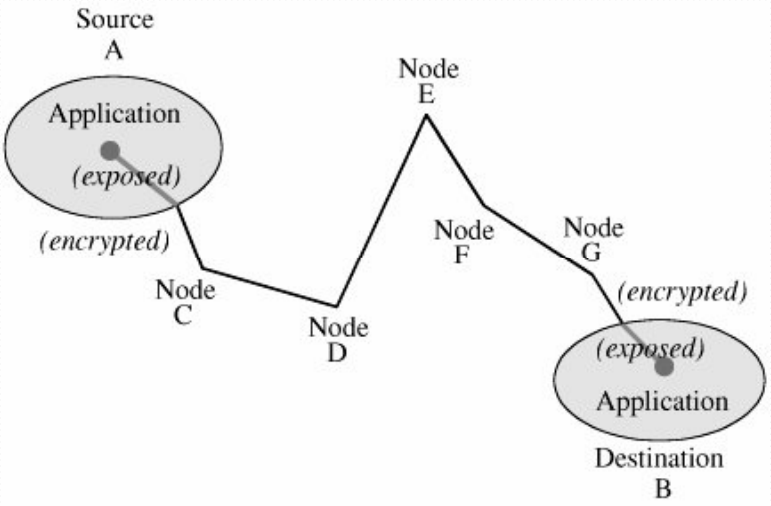




- Design and Implementation (Cont'd)
  - Encryption
    - End-to-End Encryption
      - **End-to-end encryption** provides security from one end of a transmission to the other.

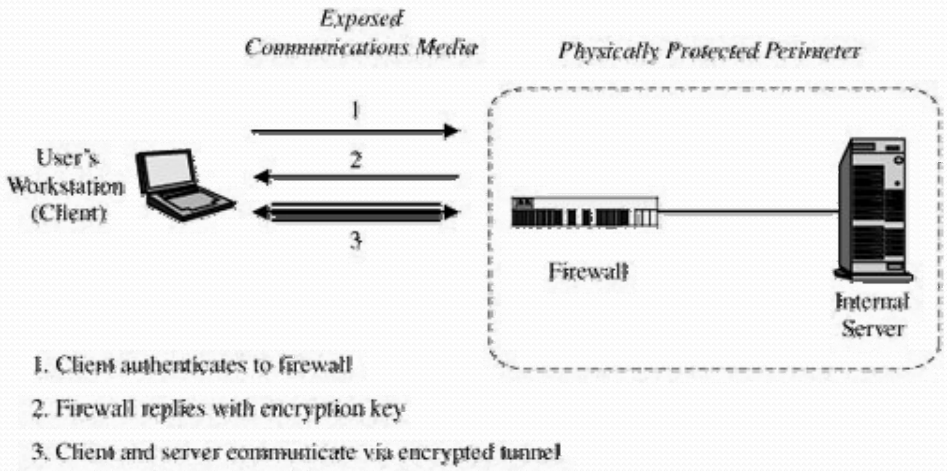

Sender
Intermediate Host
Receiver
Protocol Layer
Message
7. Application
6. Presentation
5. Session
4. Transport
3. Network
2. Data Link
1. Physical
Message encrypted
Message in plaintext: Exposed

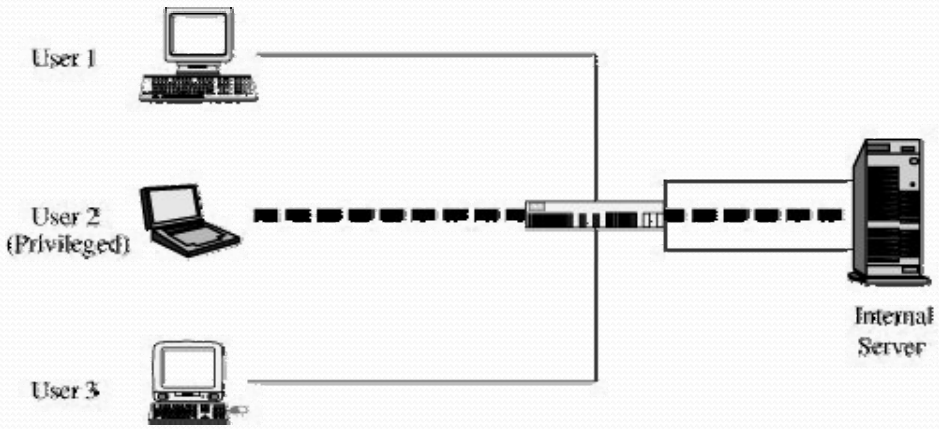

B
N
T
S
M
E
Message
Session Header
Transport Header
Network Header
Data Link Header
Data Link Trailer
Encrypted



Link Encryption	End-to-End Encryption
Security within hosts	
Data exposed in sending host	Data encrypted in sending host
Data exposed in intermediate nodes	Data encrypted in intermediate nodes
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 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
Implementation concerns	
Requires one key per host pair	Requires one key per user pair
Provides node authentication	Provides user authentication

- Design and Implementation (Cont'd)
  - Encryption
    - Virtual Private Networks
      - With the VPN, we say that the communication passes through an **encrypted tunnel** or **tunnel**.





- Design and Implementation (Cont'd)
  - Encryption
    - PKI and Certificates
      - A **public key infrastructure,** or **PKI**, is a process created to enable users to implement public key cryptography, usually in a large (and frequently, distributed) setting.

- Design and Implementation (Cont'd)
  - Encryption
    - PKI and Certificates
      - PKI offers each user a set of services, related to identification and access control, as follows: Create certificates associating a user's identity with a (public) cryptographic key :
        - Give out certificates from its database,
        - Sign certificates, adding its credibility to the authenticity of the certificate,
        - Confirm (or deny) that a certificate is valid,
        - Invalidate certificates for users who no longer are allowed access or whose private key has been exposed

- Design and Implementation (Cont'd)
  - Encryption
    - PKI and Certificates
      - PKI sets up entities, called **certificate authorities**, that implement the PKI policy on certificates.
      - The specific actions of a certificate authority include the following:
        - managing public key certificates for their whole life cycle
        - issuing certificates by binding a user's or system's identity to a public key with a digital signature
        - scheduling expiration dates for certificates
        - ensuring that certificates are revoked when necessary by publishing certificate revocation lists

- Design and Implementation (Cont'd)
  - Encryption
    - SSH Encryption
      - **SSH** (secure shell) is a pair of protocols (versions 1 and 2), originally defined for Unix but also available under Windows 2000, that provides an authenticated and encrypted path to the shell or operating system command interpreter.
      - The SSH protocol involves negotiation between local and remote sites for encryption algorithm (for example, DES, IDEA, AES) and authentication (including public key and Kerberos).

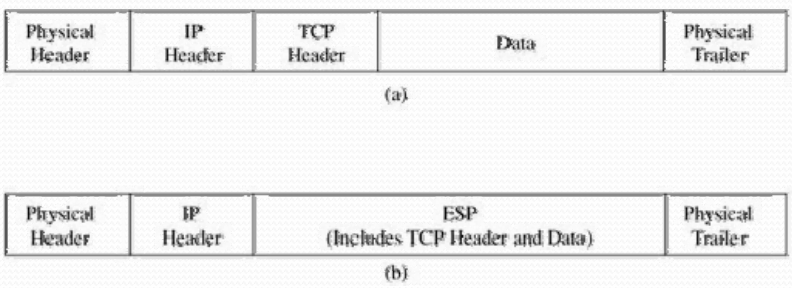
- Design and Implementation (Cont'd)
  - Encryption
    - **SSL Encryption -** Originally designed by Netscape to protect communication between a web browser and server.
      - It is also known now as **TLS,** for **transport layer security**.
      - To use SSL, the client requests an SSL session.
      - 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, and then they switch to encrypted communication, using the shared session key.

- Design and Implementation (Cont'd)
  - Encryption
    - IPSec
      - As a part of the IPv6 suite, the IETF adopted **IPSec**, or the **IP Security Protocol Suite**.
      - IPSec is somewhat similar to SSL, in that it supports authentication and confidentiality in a way that does not necessitate significant change either above it (in applications) or below it (in the TCP protocols).
      - The basis of IPSec is what is called a **security association**, which is essentially the set of security parameters for a secured communication channel. It

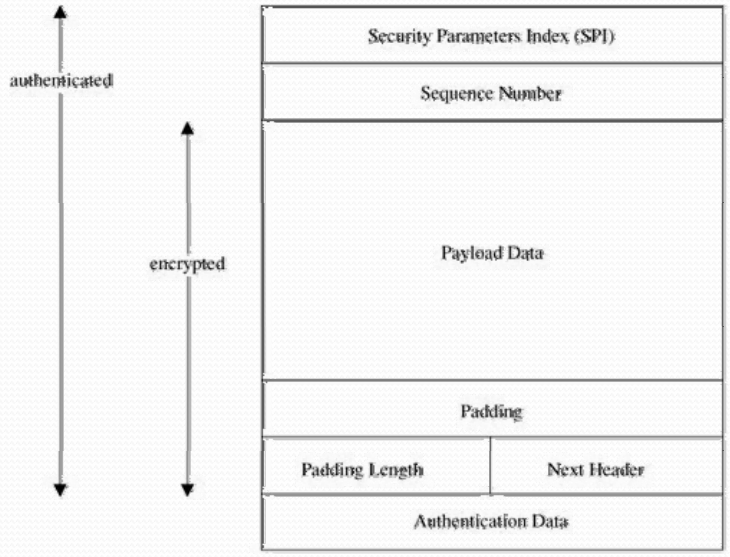
- Design and Implementation (Cont'd)
  - Encryption
    - IPSec
      - A security association includes
        - encryption algorithm and mode (for example, DES in block-chaining mode)
        - encryption key
        - encryption parameters, such as the initialization vector
        - authentication protocol and key

- Design and Implementation (Cont'd)
  - Encryption
    - IPSec
      - A security association includes
        - lifespan of the association, to permit long-running sessions to select a new cryptographic key as often as needed
        - address of the opposite end of association
        - sensitivity level of protected data (usable for classified data)

- Design and Implementation (Cont'd)
  - Encryption
    - IPSec
      - The fundamental data structures of IPSec are the **AH (authentication header)** and the**ESP (encapsulated security payload)**. T



Packets: (a) Conventional Packet; (b) IPSec Packet.

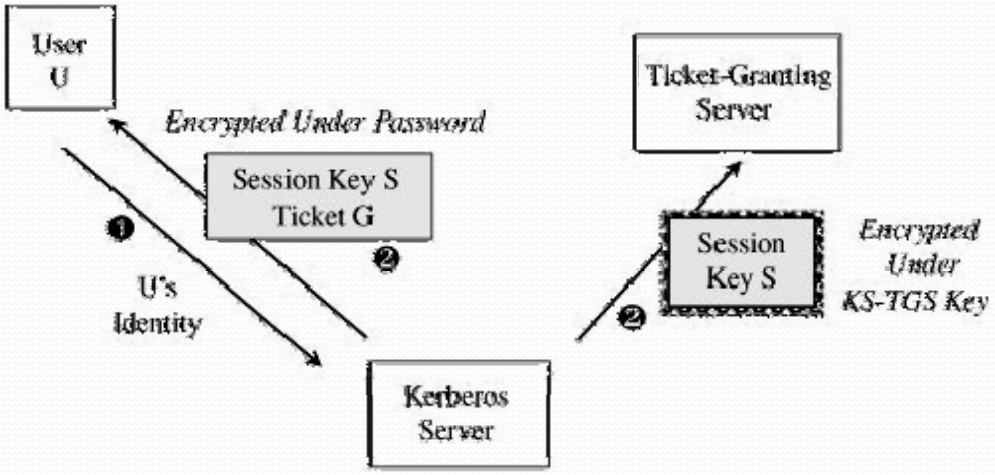


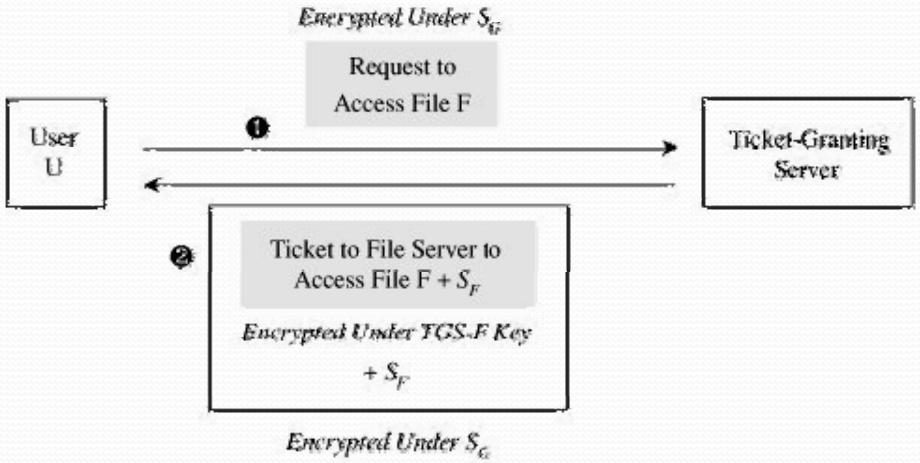
Encapsulated Security Packet.

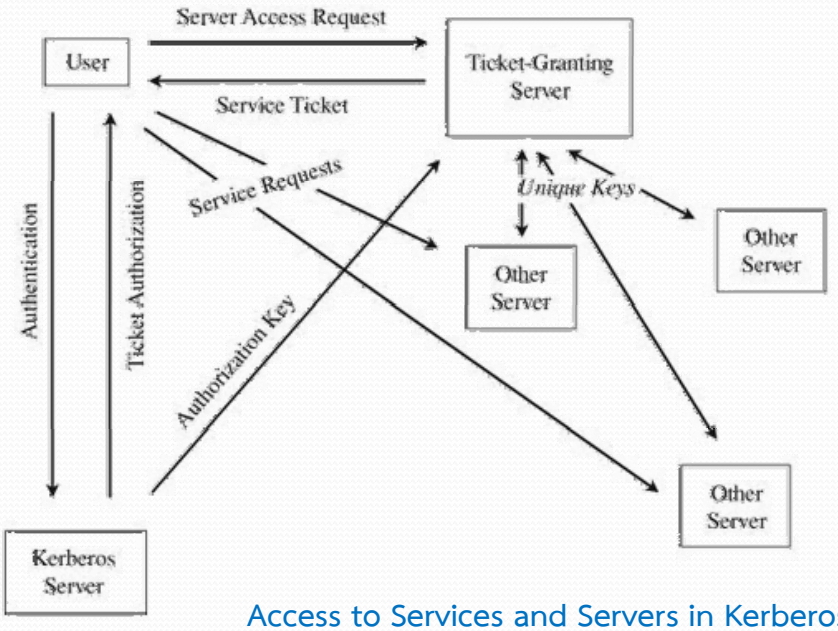
- Design and Implementation (Cont'd)
  - Encryption
    - Signed Code
      - A partial (not complete) approach to reducing this risk is to use **signed code**.
      - A trustworthy third party appends a digital signature to a piece of code, supposedly connoting more trustworthy code.
      - A signature structure in a PKI helps to validate the signature.

- Design and Implementation (Cont'd)
  - Encryption
    - **Encrypted E-mail**
    - **Content Integrity -** as a bonus with cryptography. No one can change encrypted data in a meaningful way without breaking the encryption.
    - **Error Correcting Codes**
    - **Cryptographic Checksum -** (sometimes called a **message digest**) is a cryptographic function that produces a checksum.

- Design and Implementation (Cont'd)
  - Strong Authentication
    - Kerberos
      - a system that supports authentication in distributed systems.
      - Kerberos is based on the idea that a central server provides authenticated tokens, called **tickets**, to requesting applications.
      - A ticket is an unforgeable, nonreplayable, authenticated object.
      - That is, it is an encrypted data structure naming a user and a service that user is allowed to obtain.
      - It also contains a time value and some control information.


User
U
Encrypted Under Password
Session Key S
Ticket G
1
U's
Identity
2
Kerberos
Server
Ticket-Granting
Server
Session
Key S
2
Encrypted
Under
KS-TGS Key


Encrypted Under S_G
Request to
Access File F
User
U
1
Ticket-Granting
Server
2
Ticket to File Server to
Access File F + S_F
Encrypted Under TGS-F Key
+ S_F
Encrypted Under S_G



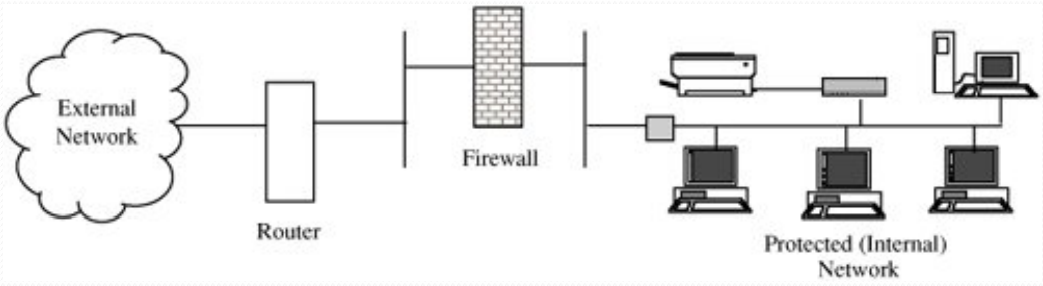
Access to Services and Servers in Kerberos.

- Design and Implementation (Cont'd)
  - Access Controls
    - ACLs on Routers
    - Firewalls

- Design and Implementation (Cont'd)
  - Wireless Security
    - **SSID (Service Set Identifier)**
    - **WEP (Wired equivalent privacy)**
      - WEP uses an encryption key shared between the client and the access point.
      - To authenticate a user, the access point sends a random number to the client, which the client encrypts using the shared key and returns to the access point.
      - From that point on, the client and access point are authenticated and can communicate using their shared encryption key.

- Design and Implementation (Cont'd)
  - Wireless Security
    - **WPA and WPA2 (WiFi Protected Access)**
      - WPA has a key change approach, called **Temporal Key Integrity Program (TKIP)**, by which the encryption key is changed automatically on each packet.
      - WPA employs the extensible authentication protocol (EAP) by which authentication can be done by password, token, certificate, or other mechanism.

- Alarms and Alerts



Layered Network Protection.

- Alarms and Alerts
  - An **intrusion detection system** is a device that is placed inside a protected network to monitor what occurs within the network.
  - If an attacker passes through the router and passes through the firewall, an intrusion detection system offers the opportunity to detect the attack at the beginning, in progress, or after it has occurred.
  - Intrusion detection systems activate an alarm, which can take defensive action.

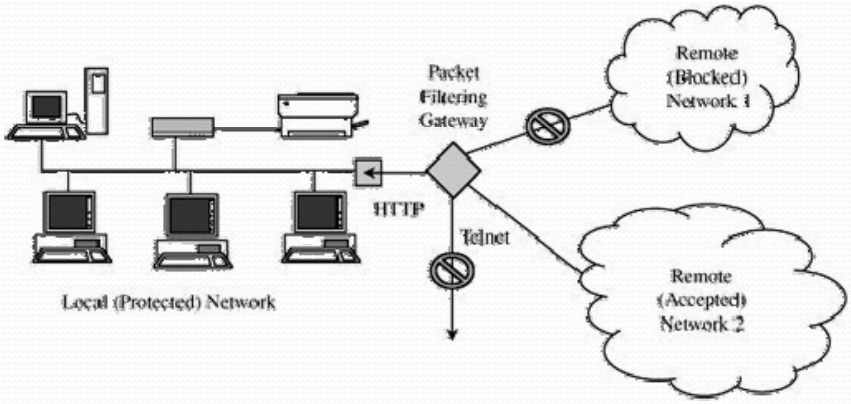
- **Honeypots**
  - You put up a honeypot for several reasons:
    - to watch what attackers do, in order to learn about new attacks (so that you can strengthen your defenses against these new attacks)
    - to lure an attacker to a place in which you may be able to learn enough to identify and stop the attacker
    - to provide an attractive but diversionary playground, hoping that the attacker will leave your real system alone

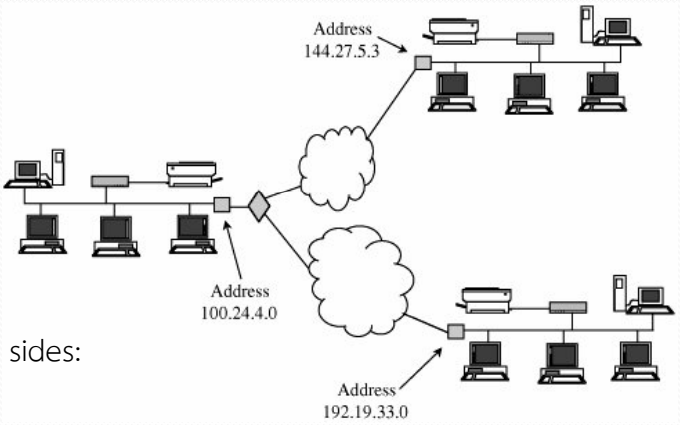
7.4. Firewalls

- **What Is a Firewall?**
  - A device that filters all traffic between a protected or "inside" network and a less trustworthy or "outside" network.
  - The purpose of a firewall is to keep "bad" things outside a protected environment.

- **Types of Firewalls**
  - packet filtering gateways or screening routers
  - stateful inspection firewalls
  - application proxies
  - guards
  - personal firewalls

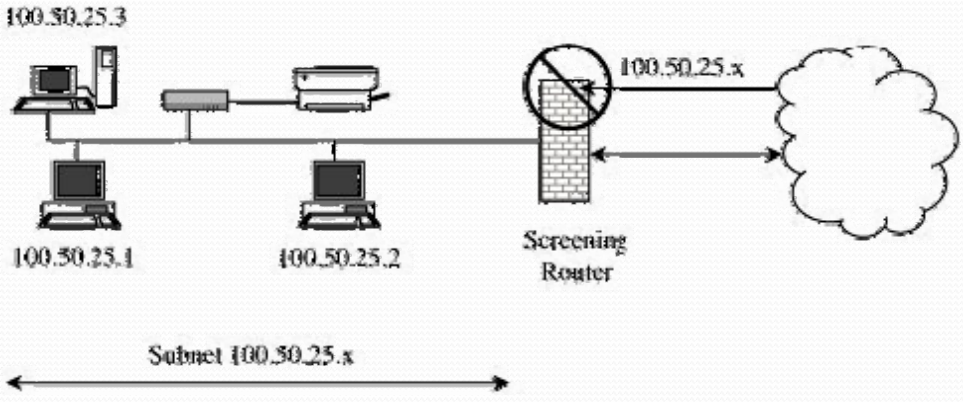
- **Packet Filtering Gateway**
  - A packet filtering gateway or screening router is the simplest, and in some situations, the most effective type of firewall.





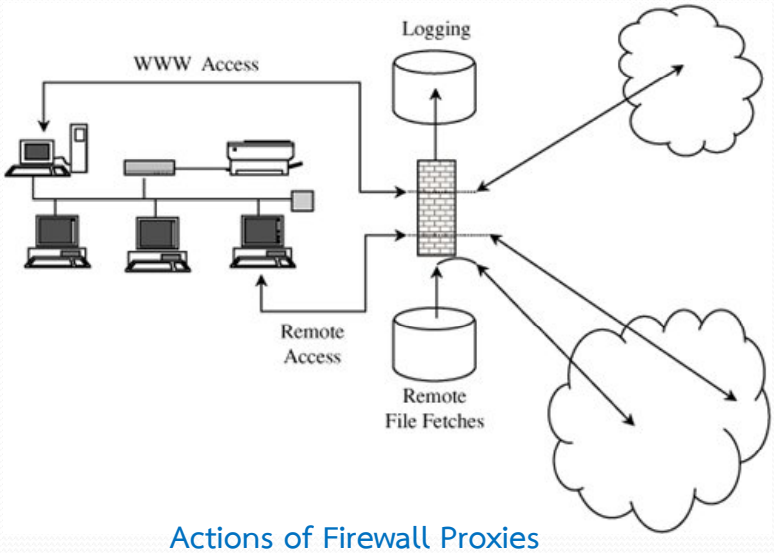
Three Connected LANs

- In this example, the router has two sides: inside and outside.
- We say that the local LAN is on the inside of the router, and the two connections to distant LANs through wide area networks are on the outside.



Filter Screening Outside Addresses

- **Stateful Inspection Firewall**
  - A **stateful inspection firewall** maintains state information from one packet to another in the input stream.
- **Application Proxy**
  - An **application proxy gateway**, also called a **bastion host**, is a firewall that simulates the (proper) effects of an application so that the application receives only requests to act properly.
  - A proxy gateway is a two-headed device: It looks to the inside as if it is the outside (destination) connection, while to the outside it responds just as the insider would.

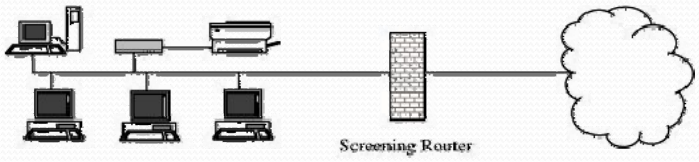


Actions of Firewall Proxies

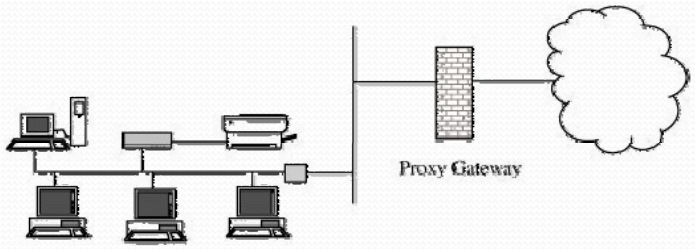
- **Guard**
  - A sophisticated firewall.
  - Like a proxy firewall, it receives protocol data units, interprets them, and passes through the same or different protocol data units that achieve either the same result or a modified result.
  - The guard decides what services to perform on the user's behalf in accordance with its available knowledge, such as whatever it can reliably know of the (outside) user's identity, previous interactions, and so forth.
  - The degree of control a guard can provide is limited only by what is computable.
  - But guards and proxy firewalls are similar enough that the distinction between them is sometimes fuzzy.

- **Personal Firewalls**
  - An application program that runs on a workstation to block unwanted traffic, usually from the network.

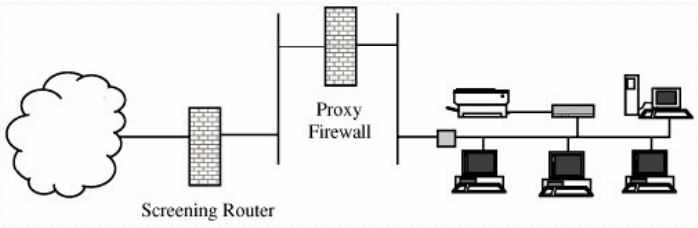
- Example Firewall Configurations



Firewall with Screening Router.



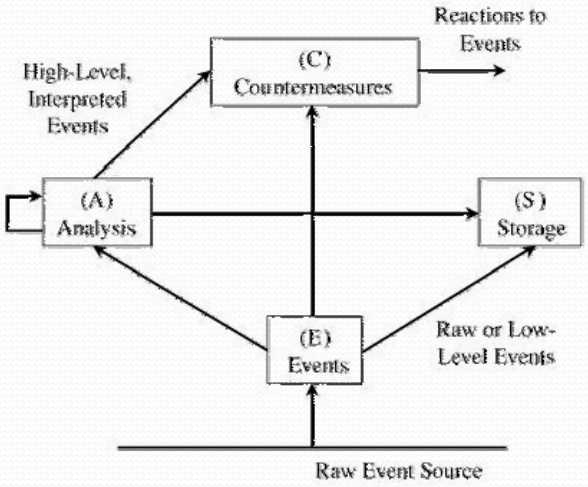
Firewall on Separate LAN



Firewall with Proxy and Screening Router.

7.5. Intrusion Detection Systems

- An **intrusion detection system (IDS)** is a device, typically another separate computer, that monitors activity to identify malicious or suspicious events.



- IDSs perform a variety of functions:
  - monitoring users and system activity
  - auditing system configuration for vulnerabilities and misconfigurations
  - assessing the integrity of critical system and data files
  - recognizing known attack patterns in system activity
  - identifying abnormal activity through statistical analysis
  - managing audit trails and highlighting user violation of policy or normal activity
  - correcting system configuration errors
  - installing and operating traps to record information about intruders

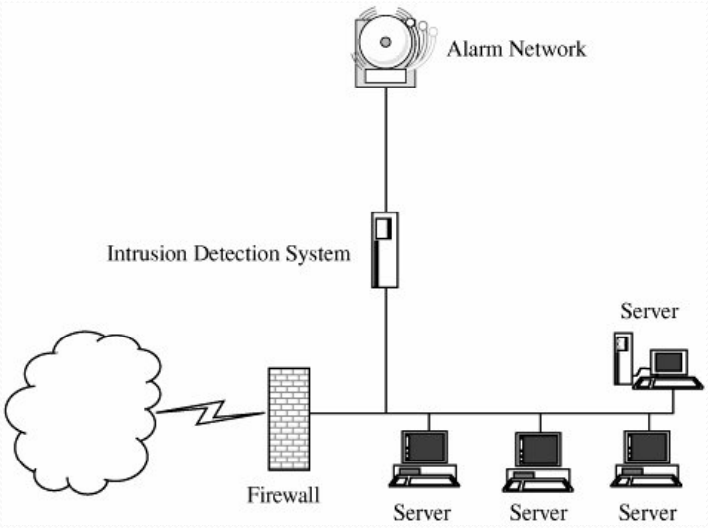
- Types of IDSs
  - The two general types of intrusion detection systems
    - **Signature-based** intrusion detection systems perform simple pattern-matching and report situations that match a pattern corresponding to a known attack type.
    - **Heuristic** intrusion detection systems, also known as **anomaly based**, build a model of acceptable behavior and flag exceptions to that model
  - Intrusion detection devices
    - A **network-based** IDS is a stand-alone device attached to the network to monitor traffic throughout that network;
    - A **host-based** IDS runs on a single workstation or client or host, to protect that one host.

- Signature-Based Intrusion Detection
  - The problem with signature-based detection is the signatures themselves.
  - An attacker will try to modify a basic attack in such a way that it will not match the known signature of that attack.
  - Signature-based IDSs cannot detect a new attack for which a signature is not yet installed in the database.
  - Tend to use **statistical analysis**

- **Heuristic Intrusion Detection**
  - Instead of looking for matches, heuristic intrusion detection looks for behavior that is out of the ordinary.
  - The inference engine of an intrusion detection system performs continuous analysis of the system, raising an alert when the system's dirtiness exceeds a threshold.

- **Heuristic Intrusion Detection (Cont'd)**
  - Inference engines work in two ways.
    - **state-based** intrusion detection systems, see the system going through changes of overall state or configuration.
    - **model-based** intrusion detection systems, try to map current activity onto a model of unacceptable activity and raise an alarm when the activity resembles the model.

- **Stealth Mode**
  - most IDSs run in **stealth mode**, whereby an IDS has two network interfaces:
    - one for the network (or network segment) being monitored and
    - the other to generate alerts and perhaps other administrative needs.



Stealth Mode IDS Connected to Two Networks

- **Goals for Intrusion Detection Systems**
  - Filter on packet headers
  - Filter on packet content
  - Maintain connection state
  - Use complex, multipacket signatures
  - Use minimal number of signatures with maximum effect
  - Filter in real time, online
  - Hide its presence
  - Use optimal sliding time window size to match signatures

- **Responding to Alarms**
  - Whatever the type, an intrusion detection system raises an alarm when it finds a match
  - In general, responses fall into three major categories (any or all of which can be used in a single response):
    - Monitor, collect data, perhaps increase amount of data collected
    - Protect, act to reduce exposure
    - Call a human

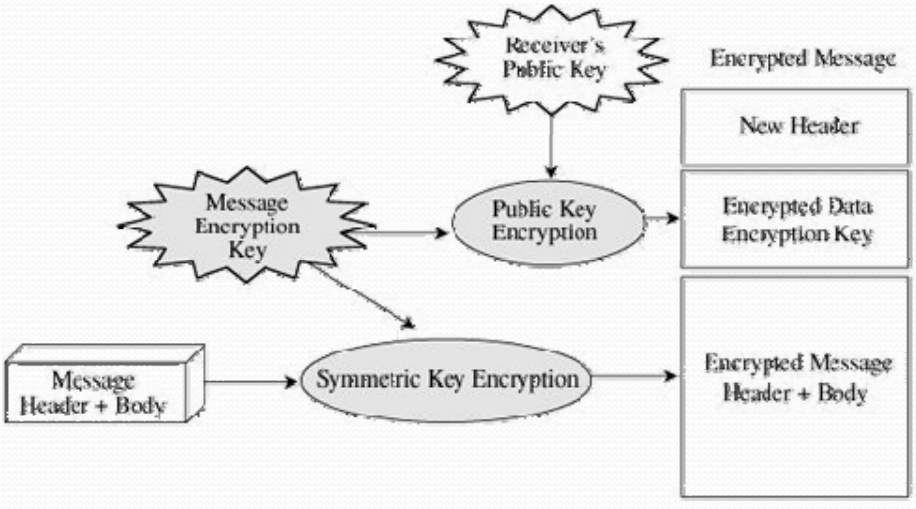
- **False Results**
  - Although an IDS might detect an intruder correctly most of the time, it may stumble in two different ways:
    - Raising an alarm for something that is not really an attack (called a **false positive**, or **type I error** in the statistical community)
    - Not raising an alarm for a real attack (a **false negative**, or **type II error**).
    - Too many false positives means the administrator will be less confident of the IDS's warnings, perhaps leading to a real alarm's being ignored.
    - But false negatives mean that real attacks are passing the IDS without action.
    - We say that the degree of false positives and false negatives represents the sensitivity of the system.

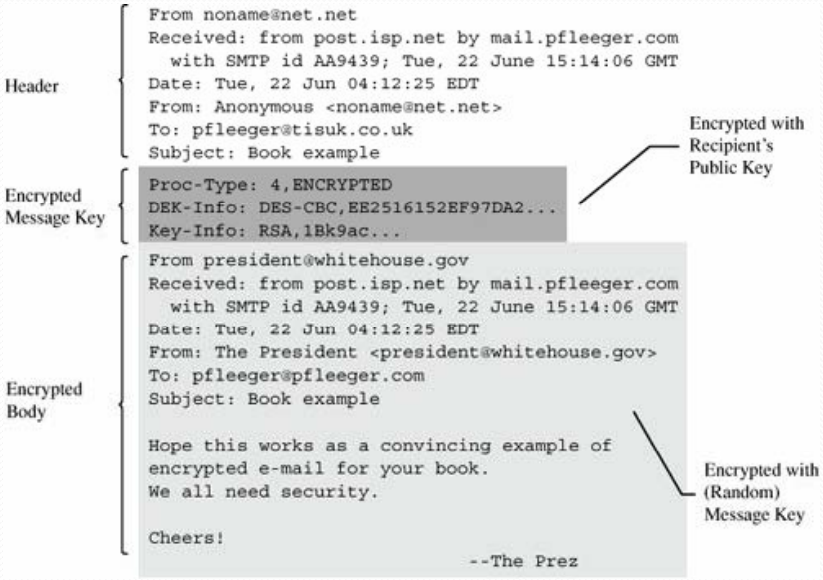
7.6. Secure E-Mail

- Consider threats to electronic mail:
  - message interception (confidentiality)
  - message interception (blocked delivery)
  - message interception and subsequent replay
  - message content modification
  - message origin modification
  - message content forgery by outsider
  - message origin forgery by outsider
  - message content forgery by recipient
  - message origin forgery by recipient
  - denial of message transmission

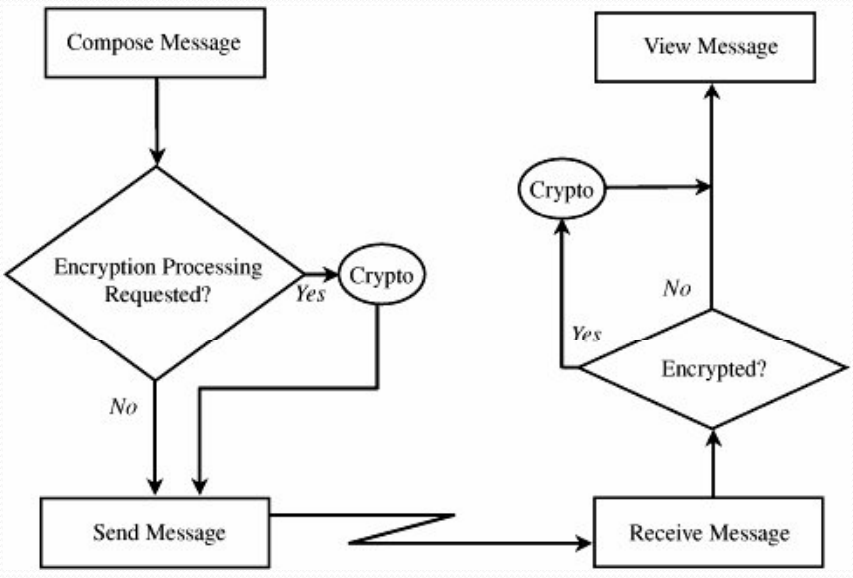
- Requirements and Solutions
  - If we were to make a list of the requirements for secure e-mail, our wish list would include the following protections.
    - *Message confidentiality* (the message is not exposed en route to the receiver)
    - *Message integrity* (what the receiver sees is what was sent)
    - *Sender authenticity* (the receiver is confident who the sender was)
    - *Non-repudiation* (the sender cannot deny having sent the message)

- Designs





Encrypted E-mail Secured Message



Encrypted E-mail Processing in Message Transmission

7.7. Summary of Network Security

- Security issues for networks are visible and important, but their analysis is similar to the analysis done for other aspects of security.
- That is, we ask questions about what we are protecting and why we are protecting it.
- In particular, we ask
  - What are the assets?
  - What are the threats?
  - Who are the threat agents?
  - What are the controls?
  - What is the residual, uncontrolled risk?