COMPUTER SECURITY AND CYBER LAW (CSCL)

LECTURER: ROLISHA STHAPIT/ DIKSHYA SINGH

UNIT 3

Unit 3: Introduction to Network Security LH 4

- Fundamentals of Network security, Principal methods of protecting Network (Encryption, Decryption, Encryption in network), Network organization (Firewalls and proxies, Analysis of the network infrastructure), DMZ, Types of Firewalls(Packet Filtering, State-full Packet Filtering Circuit Level Gateway, Application level/proxy), IPSec, VPN.

- **Network Security:** The network security is required to protect data during transmission.
- **OSI Security Architecture TU-T X.800 —**Security Architecture for OSI‖ defines a systematic way of defining and providing security requirements
- The OSI security architecture is useful to managers as a way of organizing the task of providing security.
- The OSI security architecture focuses on security attacks, mechanisms, and services. These can be defined briefly as follows:
- **Security attack**: Any action that compromises the security of information owned by an organization.
- **Security mechanism**: A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.

- **Security service**: A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms.
- Security Services
- X.800: It is a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers
- RFC 2828: RFC 2828 is a processing or communication service provided by a system to give a specific kind of protection to system resources

Security Mechanisms in X.800:

- Two types of Security mechanism (X.800)
- Specific security mechanisms may be incorporated into the appropriate protocol layer in order to provide some of the OSI security services

  E.g. encryption used for authentication

- Pervasive security mechanisms which are general mechanisms incorporated into the system and not specific to any particular OSI security services or protocol layer

  E.g. security audit trail

Why Networks Need Security

- Organizations becoming vulnerable
  - Becoming increasingly dependent on computers, networks
  - Becoming increasingly vulnerable to due widely available Internet access to its computers and networks
- Huge losses due to security breaches
  - $2 M average loss + losses related to less consumer confidence as a result of publicity of breaches
  - Potential losses from disruption of applications
- Protecting consumer privacy
  - Strong laws against unauthorized disclosures (California: $250 K for each such incident)
- Protecting organizations' data and application swoftware

    - Value of data and applications >> network cost

Fundamentals of Network Security

- Computer networks are typically a shared resource used by many applications representing different interests.
- The Internet is particularly widely shared, being used by competing businesses, mutually antagonistic governments, and opportunistic criminals.
- Unless security measures are taken, a network conversation or a distributed application may be compromised by an opponent.
- Network security is required to protect data during transmission.

Who is vulnerable?

- Financial institutions and banks
- Internet service providers
- Pharmaceutical companies
- Government and defense agencies
- Contractors to various government agencies
- Multinational corporations
- ANYONE ON THE NETWORK

Common security attacks and their countermeasures

- Finding a way into the network
  - Firewalls
- Exploiting software bugs, buffer overflows
  - Intrusion Detection Systems
- Denial of Service
  - Access filtering, IDS
- TCP hijacking
  - IPSec
- Packet sniffing
  - Encryption (SSH, SSL, HTTPS)
- Social problems
  - Education

Principal Methods of Protecting Network

Network Encryption (Network Layer or Network Level Encryption)

- Network encryption (sometimes called network layer, or network level encryption) is a network security process that applies crypto services at the network transfer layer - above the data link level, but below the application level.
- The network transfer layers are layers 3 and 4 of the Open Systems Interconnection (OSI) reference model, the layers responsible for connectivity and routing between two end points.
- Using the existing network services and application software, network encryption is invisible to the end user and operates independently of any other encryption processes used. Data is encrypted only while in transit, existing as plaintext on the originating and receiving hosts.

- Network encryption is implemented through Internet Protocol Security (IPSec), a set of open Internet Engineering Task Force (IETF)standards that, used in conjunction, create a framework for private communication over IP networks.
- IPSec works through the network architecture, which means that end users and applications don't need to be altered in any way.
- Encrypted packets appear to be identical to unencrypted packets and are easily routed through any IP network.
- Network encryption products and services are offered by a number of companies, including Cisco, Motorola, and Oracle.

Model for Network Security

The network security model defines some terms:

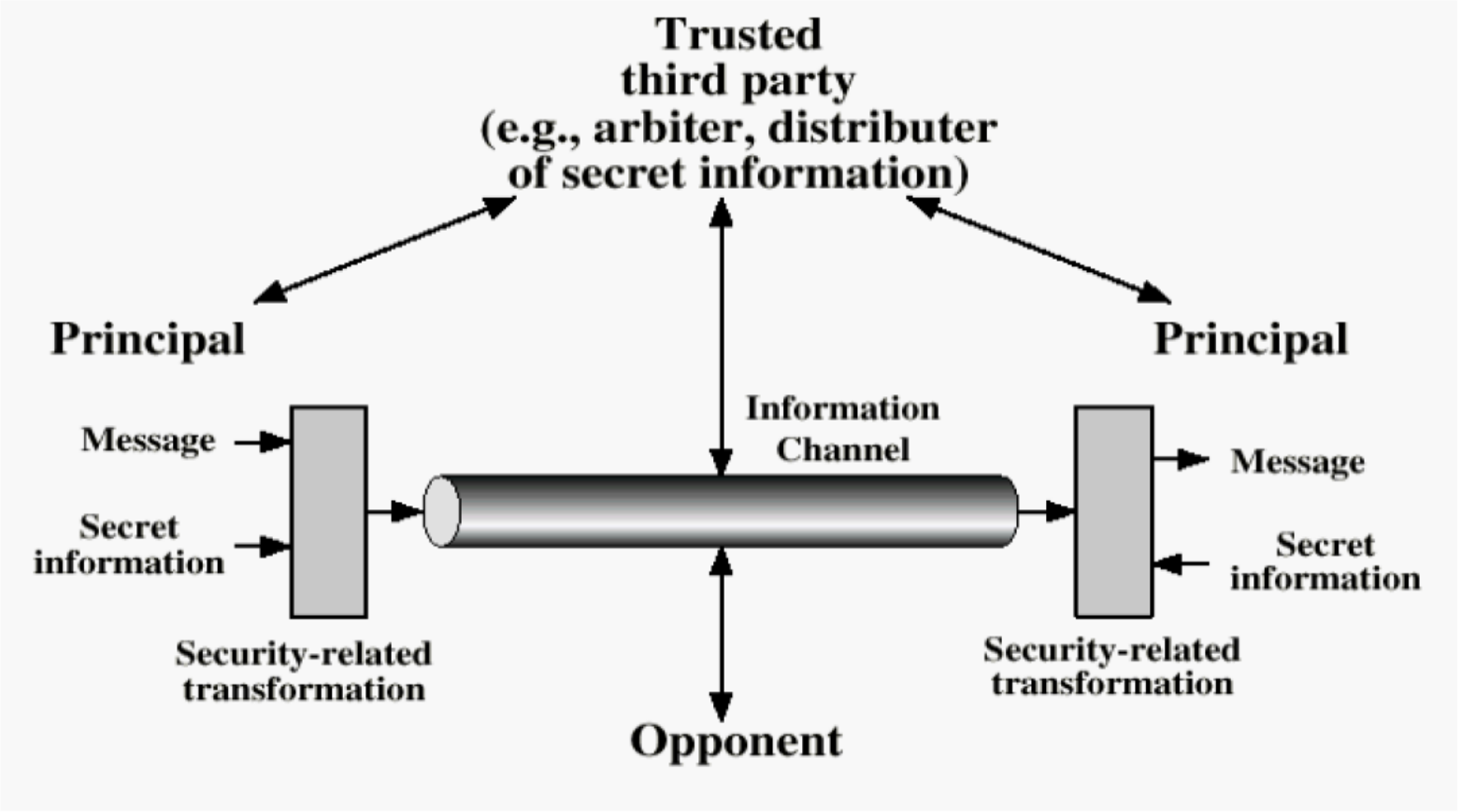
- Principals: Two parties who are involved transmission of message
- Opponent: who give potential threats to confidentiality, authenticity etc.

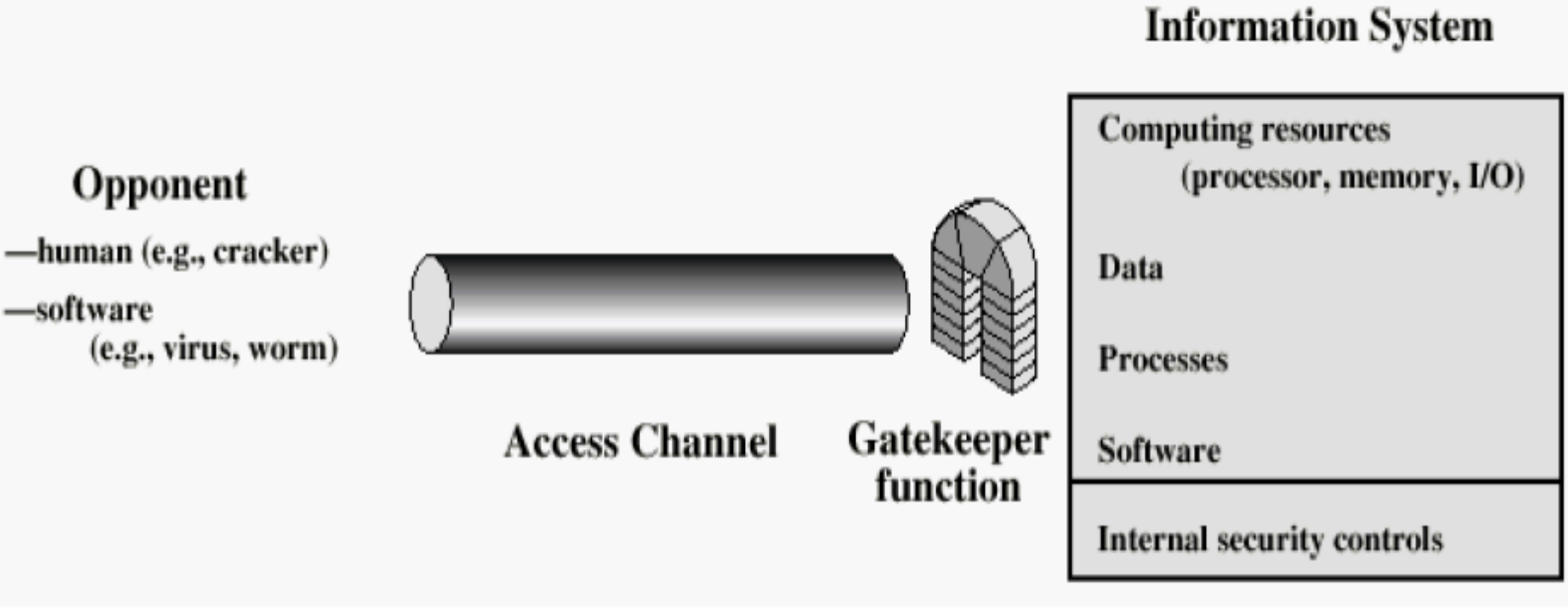
All technique for providing security has two components:

- A security-related transformation on information to be sent (E.g. encryption)
- Some secrete information (Key) shared by the two principals and , it is hoped , unknown to the opponent.(E.g. encryption key)

The General model shows the four basic tasks in designing the particular security service:

- Design an algorithm for performing the security related transformation that opponent cannot defeat its purpose
- Generate the secret information to be used with the algorithm
- Develop methods for distributing and sharing of the secret information
- Specify a protocol to be used by the two principals
- Trusted third party may be needed to achieve secured transmission


Trusted
third party
(e.g., arbiter, distributer
of secret information)
Principal
Principal
Information
Channel
Message
Secret
information
Message
Secret
information
Security-related
transformation
Security-related
transformation
Opponent



- **Gatekeeper function:** The gatekeeper function are designed to deny access to all but authorized users and screening logic that is designed to detect and reject worm, virus, and other similar attacks.
- Virus and worms are two kinds of software attacks

- Using this model requires us to:

  - Select appropriate gatekeeper functions to identify users

  - Implement security controls to ensure only authorised users access designated information or resources

- Trusted computer systems can be used to implement this model

Disruptions, Destruction, Disasters

- Disruptions: Disruptions are the loss or reduction in network service. Some disruptions may also be caused by or result in the destruction of data.

  Could be minor or temporary (a circuit failure)

- Destructions of Data: Viruses destroying files, crash of hard disk
- Natural (or manmade) disasters: Human or natural catastrophe may destroy host computers or large sections of the network.

Preventing Disruption, Destruction and Disaster

- Using Redundant Hardware
- Preventing Natural Disaster
- Preventing Theft
- Preventing Viruses
- Preventing Denial of Service

Using Redundant Hardware: A key principal in preventing disruption, destruction and disaster is redundancy. Examples of components that provide redundancy are:

- Uninterruptible power supplies (UPS)
  - A separate battery powered power supply
  - Can supply power for minutes or even hours
- Fault-tolerant servers (with redundant components)
- Disk mirroring
  - A redundant second disk for every disk on the server
  - Every data on primary disk is duplicated on mirror
- Disk duplexing (redundant disk controllers)

Preventing Natural Disasters

- It is more difficult to do, since the entire site can be destroyed by a disaster
- Fundamental principle:
  - Decentralize the network resources
  - Store critical data in at least two separate locations (in different part of the country)
- Best solution
  - Have a completely redundant network that duplicates every network component, but in a different location
- Other steps depends on the type of disaster to be prevented
  - Flood: Locate key components away from rivers
  - Fire: Install fire suppression system

Preventing Theft

- Security plan must include:
  - An evaluation of ways to prevent equipment theft
  - Procedures to execute the plan
- Equipment theft
  - A big problem: about $1 billion lost each year to theft of computers and related equipment
  - Attractive good second hand market: making the m valuable to steal

Preventing Computer Viruses

- Viruses (Macro viruses)
  - Attach themselves to other programs and spread when they are executed (files are opened)
- Worms
  - Special type of virus that spread itself without human intervention (copies itself from computer to computer)
- Anti-virus software packages
  - Check disks and files to ensure that they are virus-free
- Incoming e-mail messages
  - Most common source of viruses
  - Attachments to e-mails to be checked for viruses
  - Use of filtering programs that ‘clean’ incoming e-mail

Preventing Denial of Service Attacks

- DoS attacks: Network disrupted by a flood of messages (prevents messages from normal users)
  - Flooding web servers, email servers
- Distributed DoS (DDoS)
  - Places DDoS agents into many computers
  - Controls them by DDoS handler

Example: Issues instructions to computers to send simultaneous messages to a target computer

- Difficult to prevent DoS and DDoS attacks
  - Setup many servers around the world
  - Use Intrusion Detection Systems
  - Require ISPs to verify that all incoming messages have valid IP addresses

Disaster Recovery Plans (DRP)

- The goal of the disaster recovery plan (DRP) is to plan responses to possible disasters, providing for partial or complete recovery of all data, application software, network components, and physical facilities.
- Critical to the DRP are backup and recovery controls that enable an organization to recover its data and restart its application software should some part of the network fail.
- The DRP should also address what to do in a variety of situations, such as, if the main database is destroyed or if the data center is destroyed.

Network Control Mechanism

- It is a mechanism to reduce or eliminate the threats for network security. Types of network controls are:
- Preventative Control Mechanism

  Mitigate or stop a person from acting or an event from occurring (e.g., locks, passwords, backup circuits)

  Act as a limiting by discouraging or retraining
- Detective Control Mechanism

  Reveal or discover unwanted events (e.g., auditing)

  Documenting events for potential evidence
- Corrective Control Mechanism

  Repair an unwanted event or a intrude (e.g., reinitiating a network circuit)

Location of Encryption Function (Device)

- The most powerful and most common to countering the threats in network security is encryption
- In using the encryption we need to decide what to encrypt and where the encryption gear (device or function) should be located.
- There are two fundamental alternatives:
  - Link Encryption
  - End-to-End Encryption

Link Encryption: In link encryption, each vulnerable communication link is equipped on both end with the communication devices, thus all traffic over all communication link is secured.

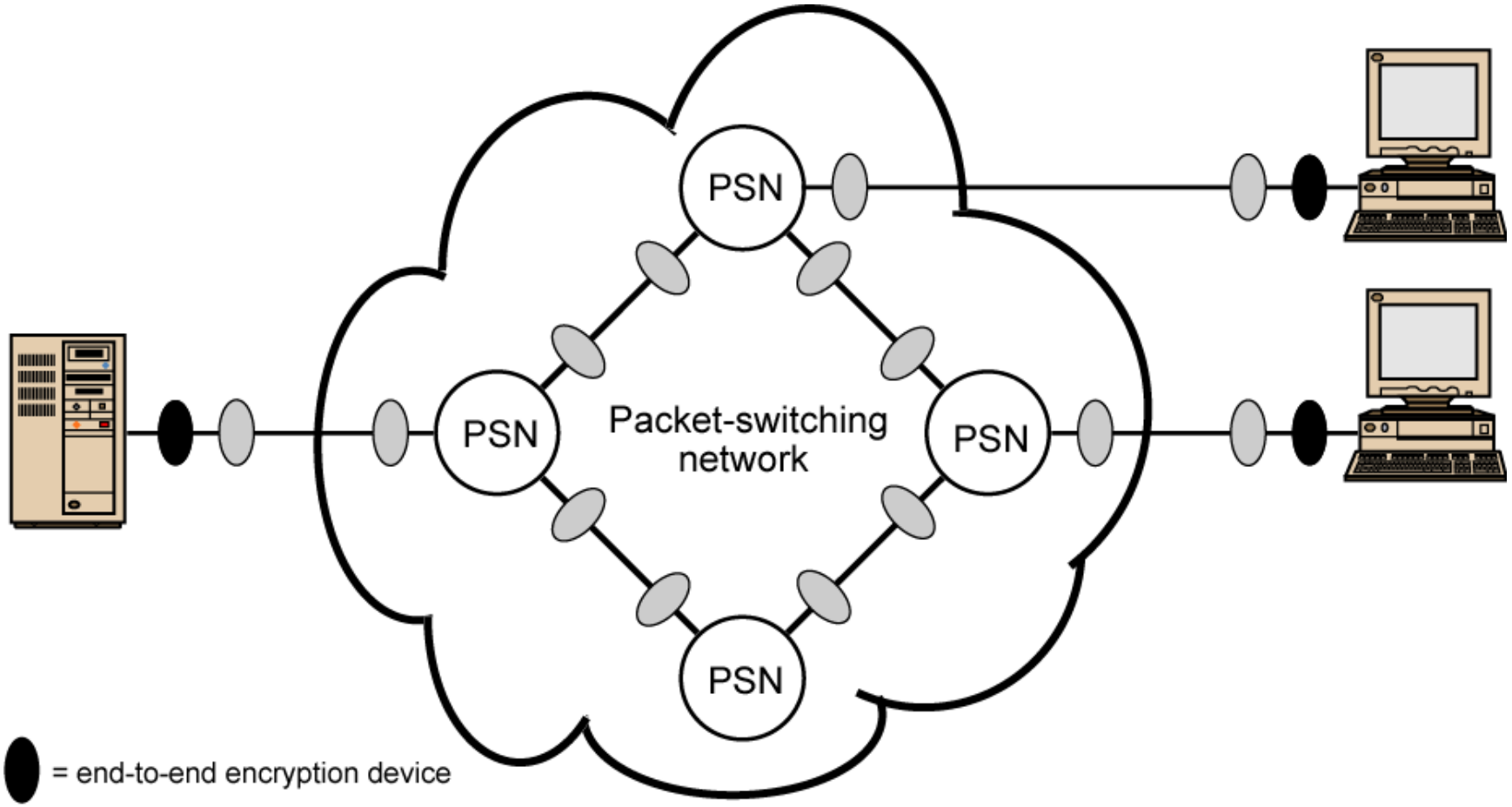
- Encryption occurs independently on every link
- Must decrypt traffic between links in order to route the frames
- Requires many encryption devices
- It provides the high level of security

Disadvantage:

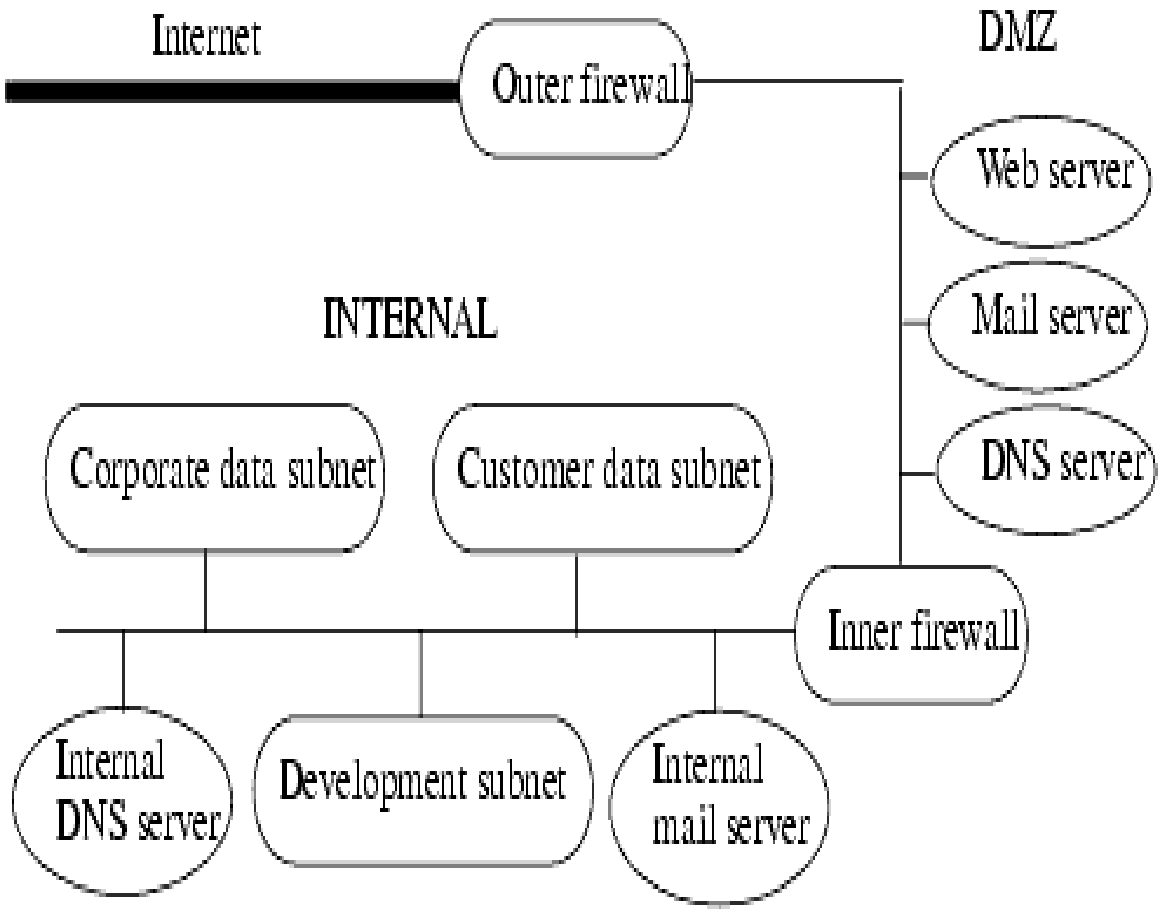
- The main disadvantage of link encryption approach is that the message must be decrypted each time it entered a packet switch; this is necessary because the switch must read the address (virtual circuit number) in the packet header to route the packet.

End-to-end Encryption With end-to- end encryption, the encryption process is carried out at two end systems. The source host or terminal encrypts the data and the encrypted data are then transmitted unaltered across the network to the destination host and destination host shares a key with the source and decrypt the data.

- Encryption occurs between original source and final destination
- Needs devices at each end with shared keys
- Must leave headers in clear so that network correctly routes information
- Contents are protected, but traffic pattern flows are not


PSN
PSN
Packet-switching
network
PSN
PSN
= end-to-end encryption device
= link encryption device
PSN = packet switching node

Network Organization



- The network designed for the Dribble Corporation.
- The "outer firewall" sits between the Internet and the company network.
- The subnet labeled "DMZ" or demilitarized zone provides limited public access to various servers.
- The "inner firewall" sits between the DMZ and the subnets that are not to be accessed by the public.
- These subnets share common mail and DNS servers that, like the other hosts, are not publicly accessible.
- Four servers reside in the DMZ. They are the mail, WWW, DNS, and log servers. The mail server in the DMZ performs address and content checking on all electronic mail messages. The goal is to hide internal information from the outside while being transparent to the inside.

Firewalls and Proxies

- A firewall is a host that mediates access to a network, allowing and disallowing certain types of access on the basis of a configured security policy.
- This firewall accepts or rejects messages on the basis of external information, such as destination addresses or ports, rather than on the basis of the contents of the message.
- A ***filtering firewall*** performs access control on the basis of attributes of the packet headers, such as destination addresses, source addresses, and options.
- Routers and other infrastructure systems are typical examples of filtering firewalls.
- They allow connections through the firewall, usually on the basis of source and destination addresses and ports.
- Access control lists provide a natural mechanism for representing these policies.

- Firewall is hardware device or software applications that act as filters between a company’s private network and the internet.
- It protects networked computers from intentional hostile intrusion that could compromise confidentiality or result in data corruption or denial of service by enforcing an access control policy between two networks.
- A firewall system is usually located at a higher level gateway, such as a site's connection to the Internet, however firewall systems can be located at lower-level gateways to provide protection for some smaller collection of hosts or subnets.
- The main function of a firewall is to centralize access control. A firewall serves as the gatekeeper between the untrusted Internet and the more trusted internal networks. The earliest firewalls were simply routers.

- This contrasts with the second type of firewall, which never allows such a direct connection.
- Instead, special agents called ***proxies*** control the flow of information through the firewall.
- A proxy is an intermediate agent or server that acts on behalf of an endpoint without allowing a direct connection between the two endpoints.
- A proxy (or applications level) firewall uses proxies to perform access control. A proxy firewall can base access control on the contents of packets and messages, as well as on attributes of the packet headers.
- A proxy firewall adds to a filtering firewall the ability to base access on content, either at the packet level or at a higher level of abstraction.

- A different point of view is to see the firewall as an audit mechanism. It analyzes the packets that enter. Firewalls can then base actions on this analysis, leading to traffic shaping (in which percentages of bandwidth are reserved for specific types of traffic), intrusion response, and other controls.

Analysis of the Network Infrastructure

- The benefits of this design flow from the security policy and the principle of least privilege.
- The security policy distinguishes "public" entities from those internal to the corporation, but recognizes that some corporate resources must be available to the public.
- The network layout described above provides this functionality.
- The public entities may enter the corporate perimeter (bounded by the "outer firewall") but are confined to the DMZ area (bounded inside by the "inner firewall").
- The key decision is to limit the flow of information from the internal network to the DMZ.

- .The public cannot communicate directly with any system in the internal network, nor can any system in the internal network communicate directly with other systems on the Internet (beyond the "outer firewall").
- The systems in the DMZ serve as mediators, with the firewalls providing the guards.
- Firewalls and the DMZ systems make up the pump, because they control all access to and from the Internet and filter all traffic in both directions.

Outer Firewall Configuration

- The goals of the outer firewall are to restrict public access to the Drib's corporate network and to restrict the Drib's access to the Internet.
- In the Bell-LaPadula Model, for example, one cannot read information from a higher level (here, by restricting public access to the Drib's network), but one cannot write information to a lower level, either (here, by restricting the Drib's employees' access to the Internet).
- Certain sanitized exchanges, however, are allowed.
- To implement the required access control, the firewall uses an access control list, which binds source addresses and ports and destination addresses and ports to access rights.
- The public needs to be able to access the Web server and mail server, and no other services.
- The firewall therefore presents an interface that allows connections to the WWW services (HTTP and HTTPS) and to electronic mail (SMTP). Sites on the Internet see the addresses of the Web and mail servers as the same—that of the firewall. No other services are provided to sites on the Internet.

Inner Firewall Configuration

- The internal network is where the Drib's most sensitive data resides.
- It may contain data, such as proprietary information, that the Drib does not want outsiders to see.
- For this reason, the inner firewall will block all traffic except for that specifically authorized to enter (the principle of fail-safe defaults). All such information will come from the DMZ, and never directly from the Internet.

DMZ

- “DMZ” stands for “demilitarized zone.”
- The DMZ is a portion of a network that separates a purely internal network from an external network.
- When information moves from the Internet to the internal network, confidentiality is not at issue. However, integrity is.
- The guards between the Internet and the DMZ, and between the DMZ and the internal network, must not accept messages that will cause servers to work incorrectly or to crash.
- When information moves from the internal network to the Internet, confidentiality and integrity are both at issue.
- A DMZ is an optional and more secure approach to a firewall and effectively acts as a proxy server as well.

In the DMZ

DMZ Mail Server

- performs address and content checking on all electronic mail messages
- When it receives a letter from the Internet, it performs the following Steps

reassembles the message into a set of headers, a letter, and any attachments

scans the letter and attachments for any computer virus or malicious logic.

- Restore the attachments to transmit

- Rescan it for any violation of SMTP specification

Scans the recipient address lines.

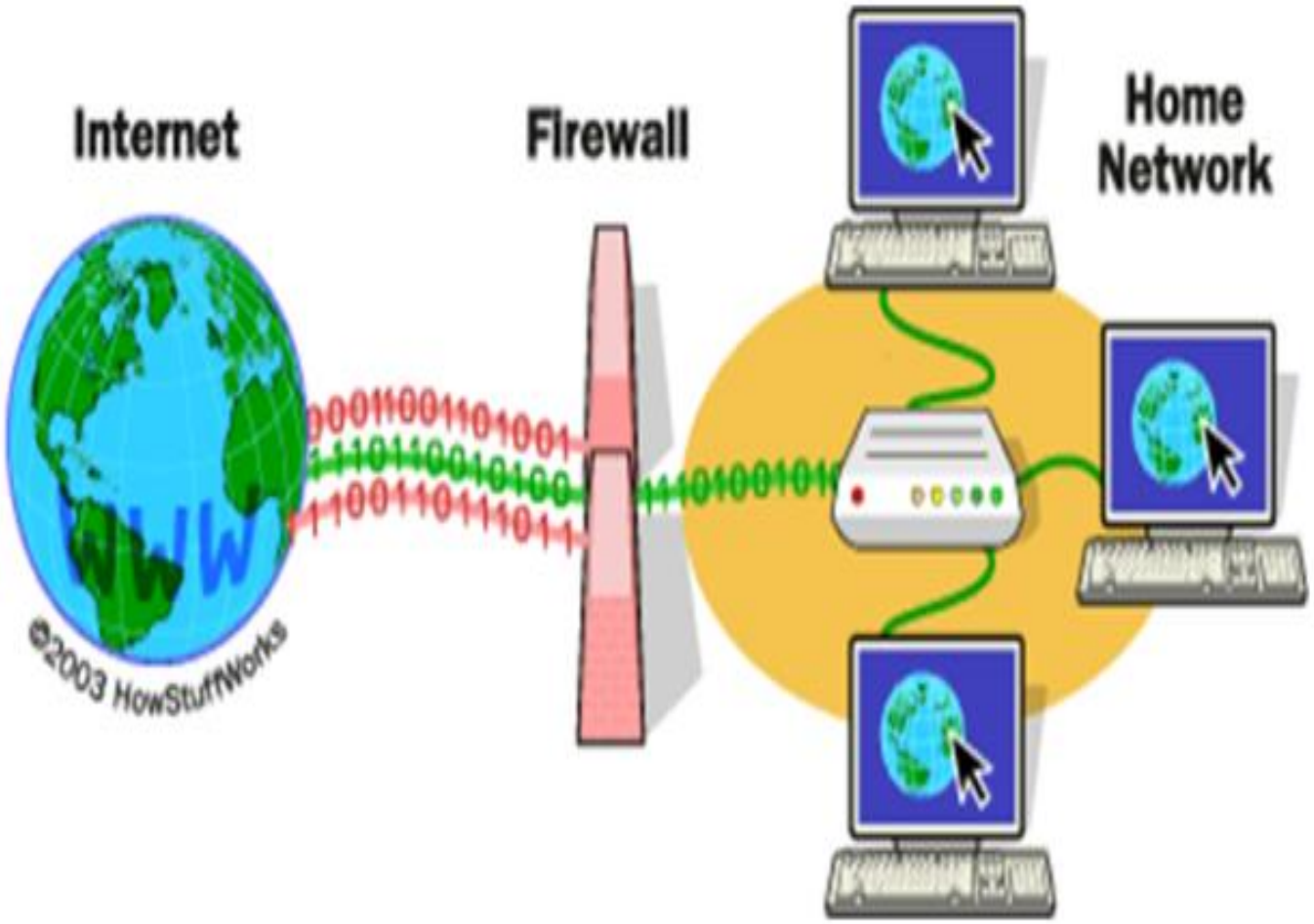
- Addresses that directed the mail to the drib are rewritten to direct the mail to the internal mail server

- When it receives a outgoing letter from the internal mail server
  - Steps 1 and 2 are the same
  - In step 3 the mail proxy scans the header lines.
  - All lines that mention internal hosts are rewritten to identify the host as “drib.org”, the name of the outside firewall.

- DMZ WWW Server
    - Identifies itself as “www.drib.org” and uses IP address of the outside firewall
- DMZ DNS Server
    - It contain entries for
        - DMZ mail, Web and log hosts
        - Internal trusted administrative host
        - Outer firewall
        - Inner firewall
- DMZ Log Server

Firewalls in Detail

- A firewall is a dedicated computer (device) that interfaces with computers outside a network and has special security precautions built into it in order to protect sensitive files on computers within the network
- It is used to service outside the network, specially internet connection and dial-in lines.
- A firewall is a “choke point/guard box” of controlling and monitoring the network traffic.
- It imposes restrictions on network services (only authorized traffic is allowed).
- It enforces auditing and controlling access (alarms of abnormal behavior can be generated).


Internet
Firewall
Home
Network
WWW
©2003 HowStuffWorks

Firewall Characteristics

All firewalls must have the following three properties:

- All traffic between the networks must pass through it.
- Only authorized traffic, as defined by the local security policy, is allowed to pass through a firewall.
- The firewall machine/system itself should be immune to penetration that is the use of a trusted operating system

Firewall Control

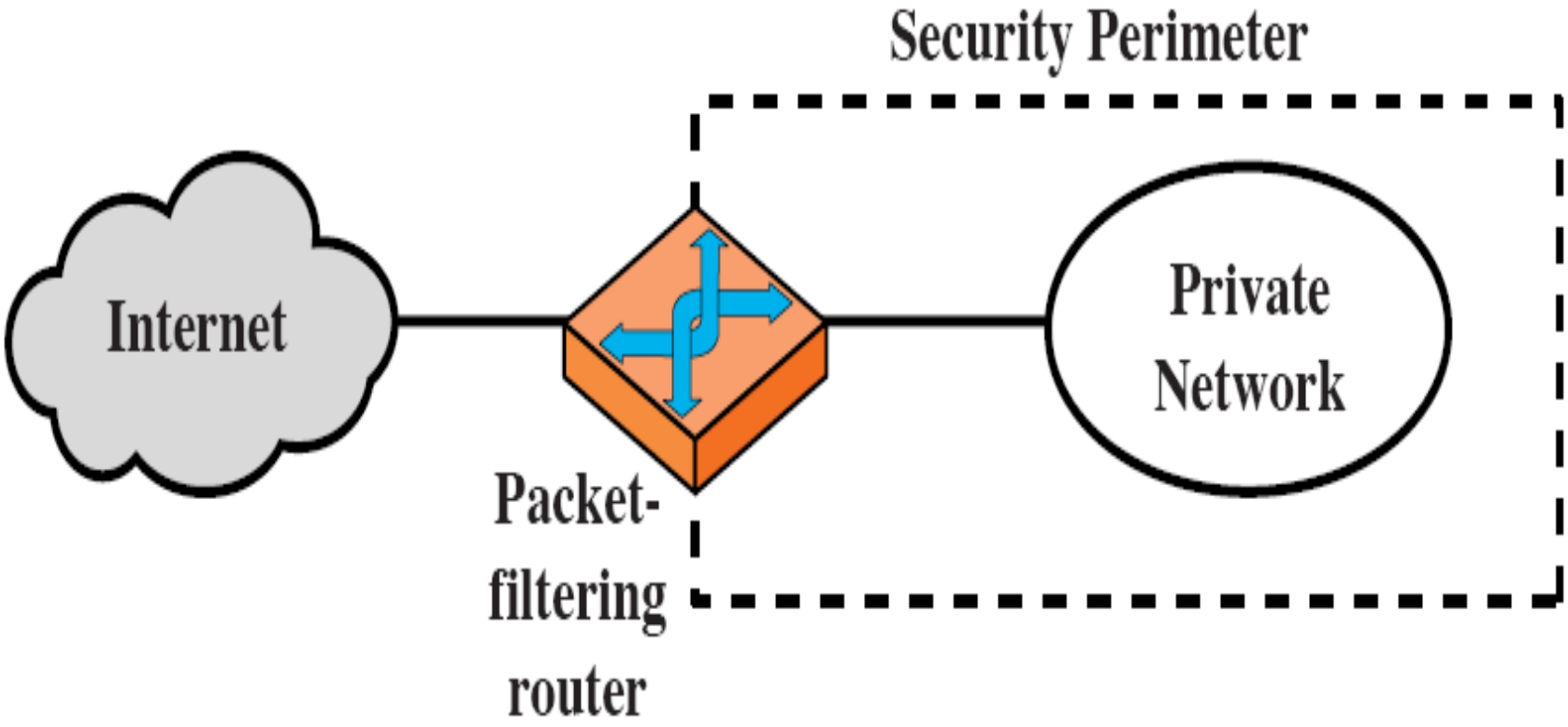
- **Service Control:** Determine the type of Internet service that can be accessed , inbound or outbound; the firewall may filter IP Address and TCP port
- **Direction Control:** Determine the direction in which particular service request may be initialized and allowed to follow through the firewall.
- **User Control:** Controls access to a service according to which user is attempting to access it. Typically used in local users
- **Behavior Control:** Control how particular services are used.

Types of Firewall

- Packet Filtering,
- State-full Packet Filtering
- Circuit Level Gateway,
- Application level/proxy

Packet Filtering

- Packet filtering firewalls work at the network layer (OSI model), or the IP layer (TCP/IP).
- In this each packet is compared to a set of criteria before it is forwarded.
- Depending on the packet and the criteria, the firewall can drop, forward the packet or send a message to the originator.
- Rules can be source and destination IP address, source and destination port number and protocol used.
- The advantages of packet filtering firewalls are their low cost and low impact on network performance.


Security Perimeter
Internet
Private
Network
Packet-
filtering
router

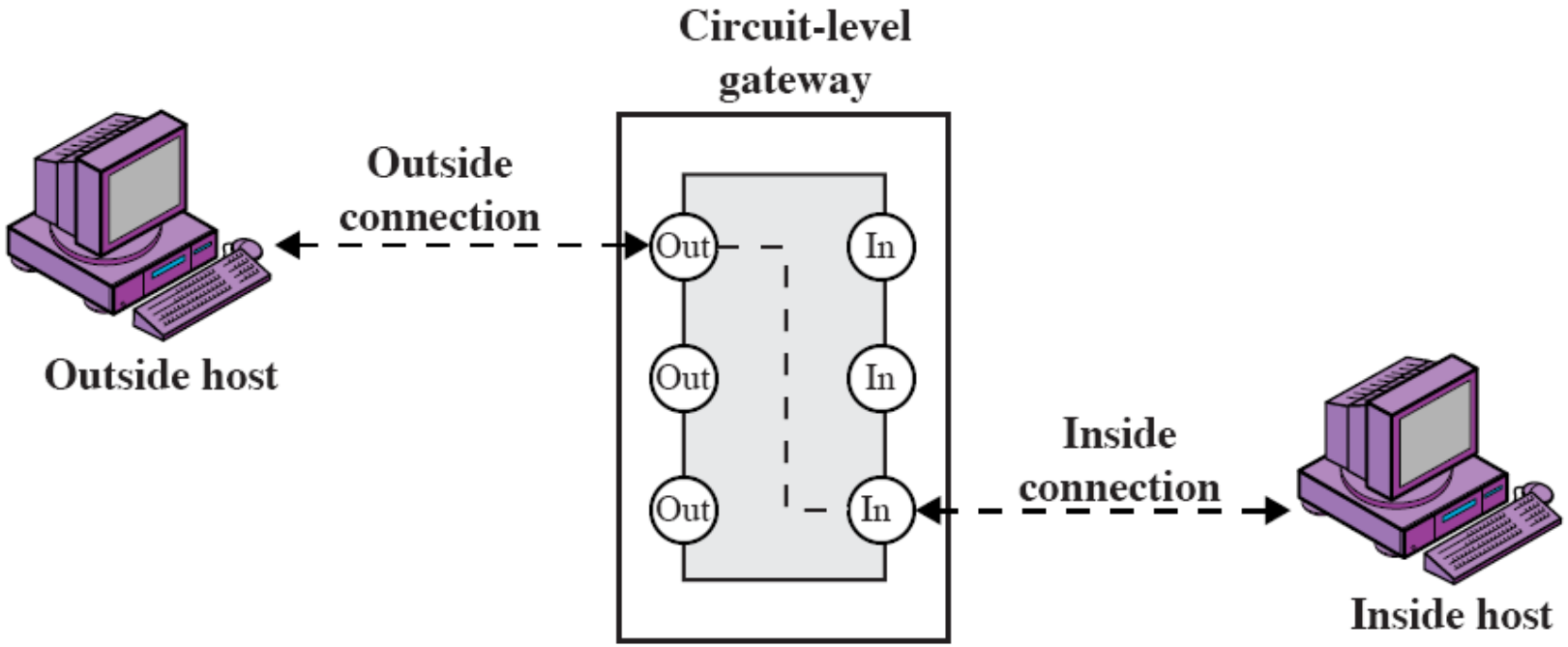
State-full Packet Filtering

- A traditional packet filter makes filtering decisions on an individual packet basis and does not take into consideration any higher layer context .
- A simple packet filtering firewall must permit inbound network traffic on all these high-numbered ports for TCP-based traffic to occur.
- This creates a vulnerability that can be exploited by unauthorized users.
- A stateful inspection packet firewall tightens up the rules for TCP traffic by creating a directory of outbound TCP connections.
- There is an entry for each currently established connection.
- The packet filter will now allow incoming traffic to high-numbered ports only for those packets that fit the profile of one of the entries in this directory.
- A stateful packet inspection firewall reviews the same packet information as a packet filtering firewall, but also records information about TCP connections

- A stateful packet filtering firewall (SPFF) looks at each packet and applies rules or tests, but the rules or tests applied to each packet may be modified depending on packets that have already been processed or in the case of an application relay it will maintain state by definition.
- It can keep track of individual TCP sessions and even their sequence numbers to be able to make packet decisions based more on the previous record, overall behavior and context rather than the content of individual packet only

Circuit Level Gateway Filtering

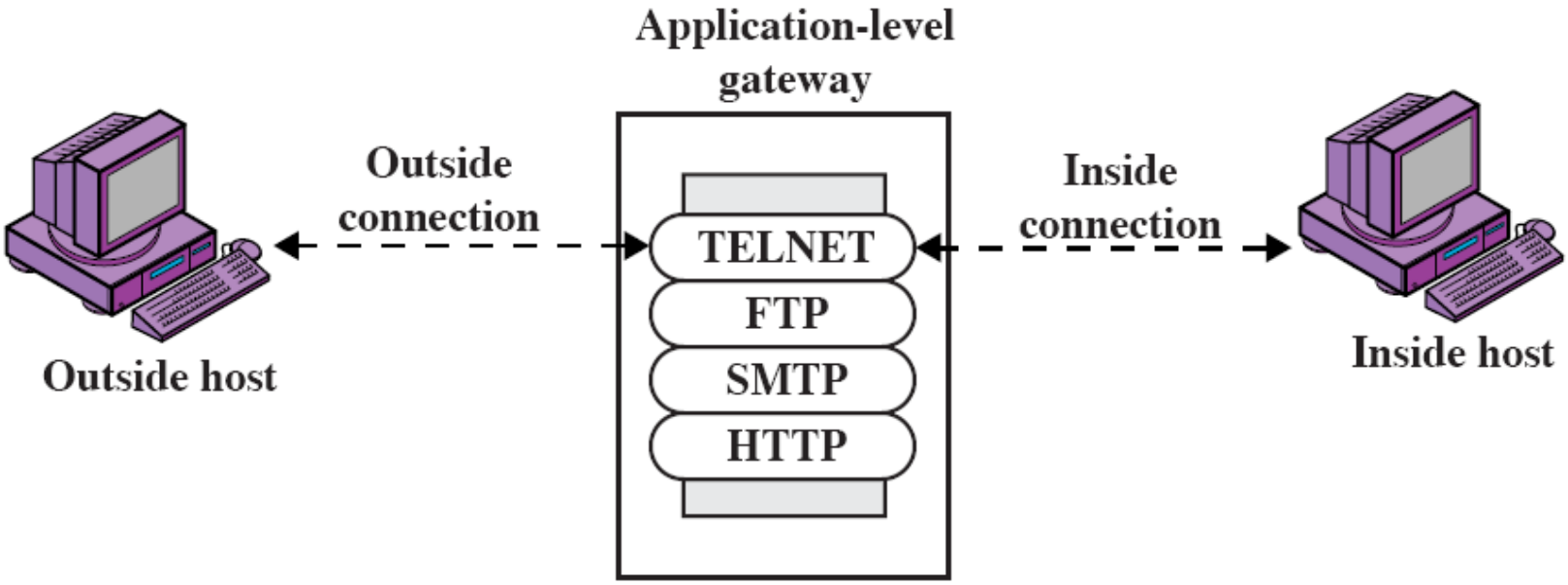
- It work at the session layer (OSI model), or the TCP layer (TCP/IP).
- They monitor TCP handshaking between packets to determine whether a requested session is legitimate.
- Information passed to a remote computer through a circuit level gateway appears to have originated from the gateway.
- This is useful for hiding information about protected networks. Circuit level gateways are relatively inexpensive and have the advantage of hiding information about the private network they protect.
- On the other hand, they do not filter individual packets.
- The gateway establishes separate connection with client and servers and relays the application requests and response between the two.



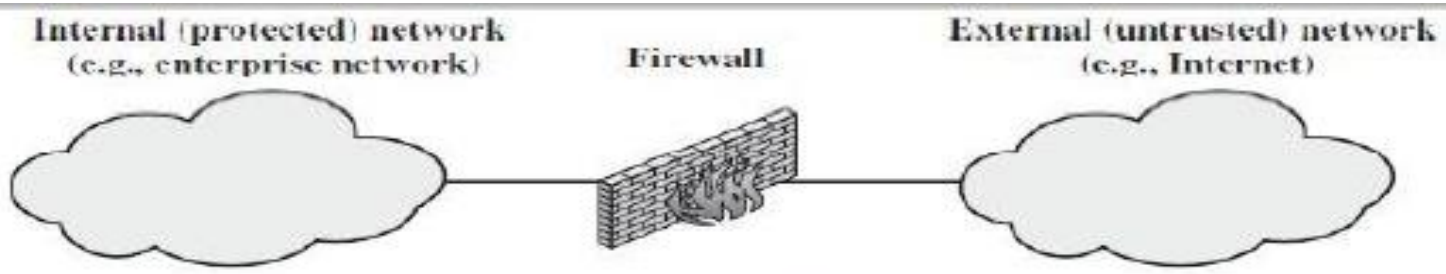
There is no way for a remote computer or a host to determine the internal private IP addresses of an organization, for example. This technique is also called Network Address Translation where the private IP addresses originating from the different clients inside the network are all mapped to the public IP address available through the internet service provider and then sent to the outside world (Internet).

Application level/proxy Filtering

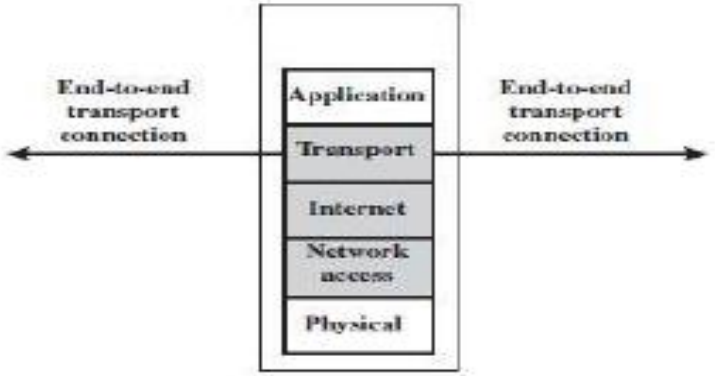
- Application level gateways, also called proxies, are similar to circuit-level gateways except that they are application specific.
- They can filter packets at the application layer of the OSI model.
- Incoming or outgoing packets cannot access services for which there is no proxy.
- In plain terms, an application level gateway that is configured to be a web proxy acts as the server to the internal network and client to the external network.
- Because they examine packets at application layer, they can filter application specific commands such as http: post and get, etc.
- Application level gateways can also be used to log user activity and logins. They offer a high level of security, but have a significant impact on network performance.


Application-level
gateway
Outside
connection
Inside
connection
TELNET
FTP
SMTP
HTTP
Outside host
Inside host

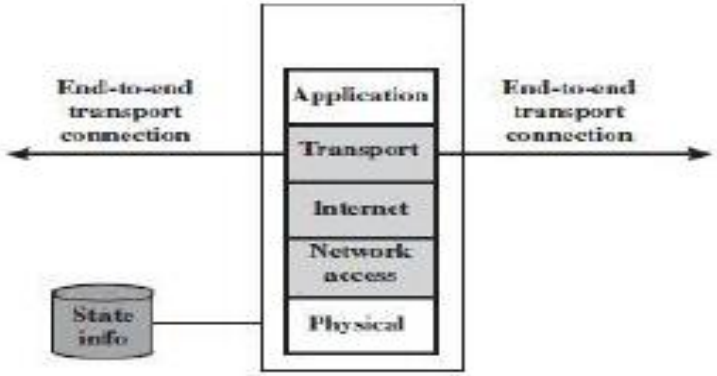
- An application-level gateway, also called an application proxy, acts as a relay of application-level traffic.
- The user contacts the gateway using a TCP/IP application, such as Telnet or FTP, and the gateway asks the user for the name of the remote host to be accessed.
- When the user responds and provides a valid user ID and authentication information, the gateway contacts the application on the remote host and relays TCP segments containing the application data between the two endpoints.
- If the gateway does not implement the proxy code for a specific application, the service is not supported and cannot be forwarded across the firewall.



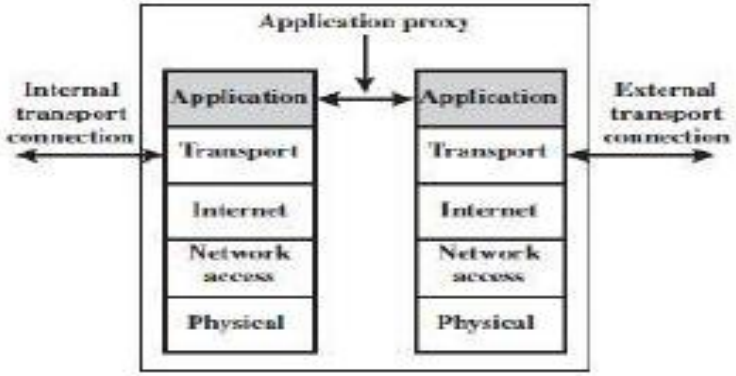
(a) General model



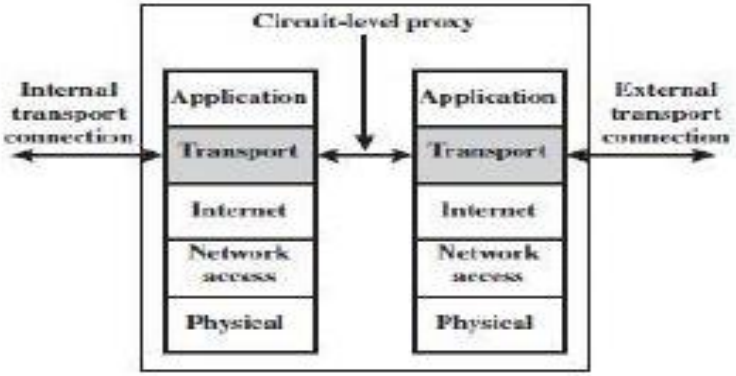
(b) Packet filtering firewall



(c) Stateful inspection firewall



(d) Application proxy firewall



(e) Circuit-level proxy firewall

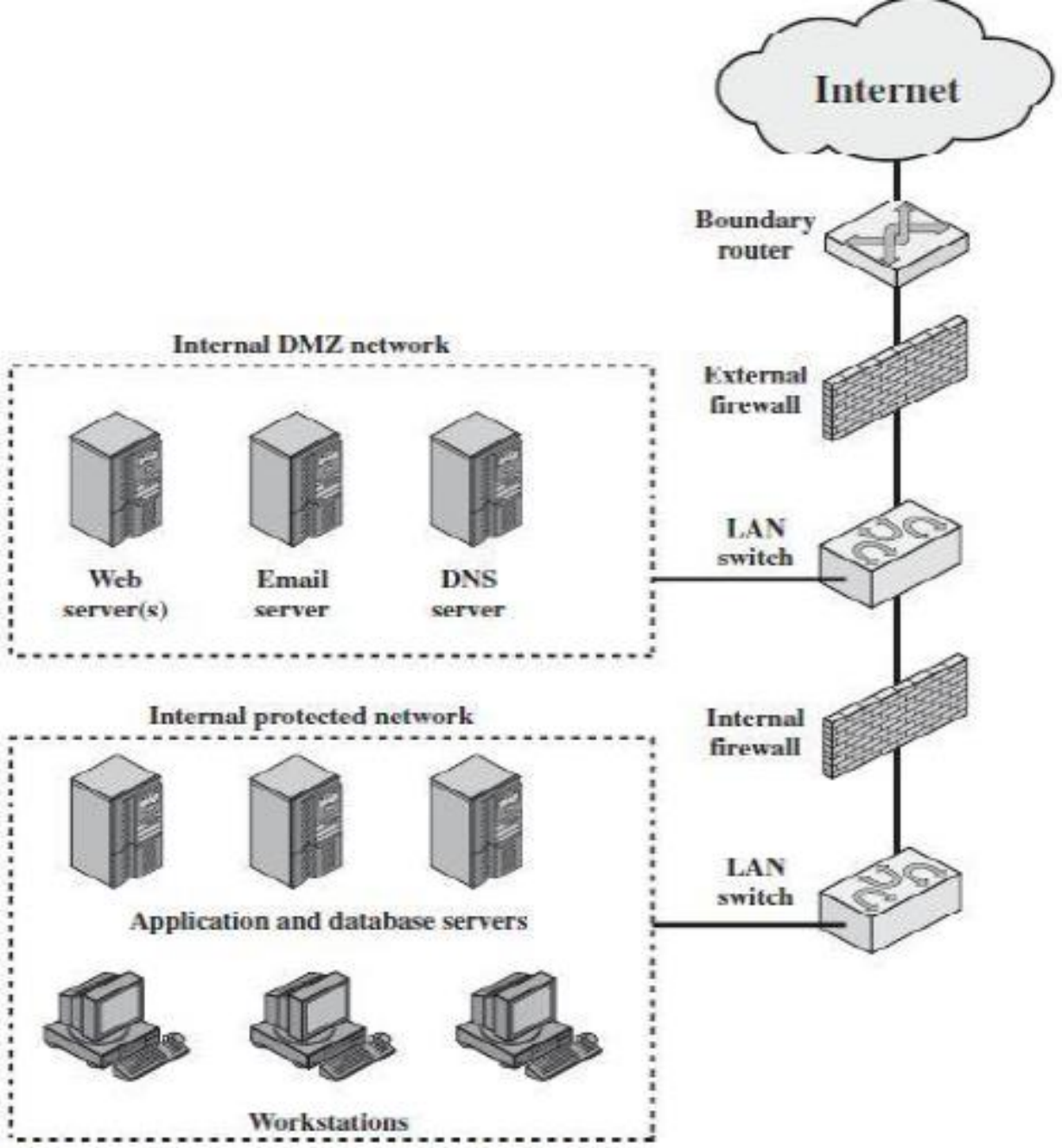


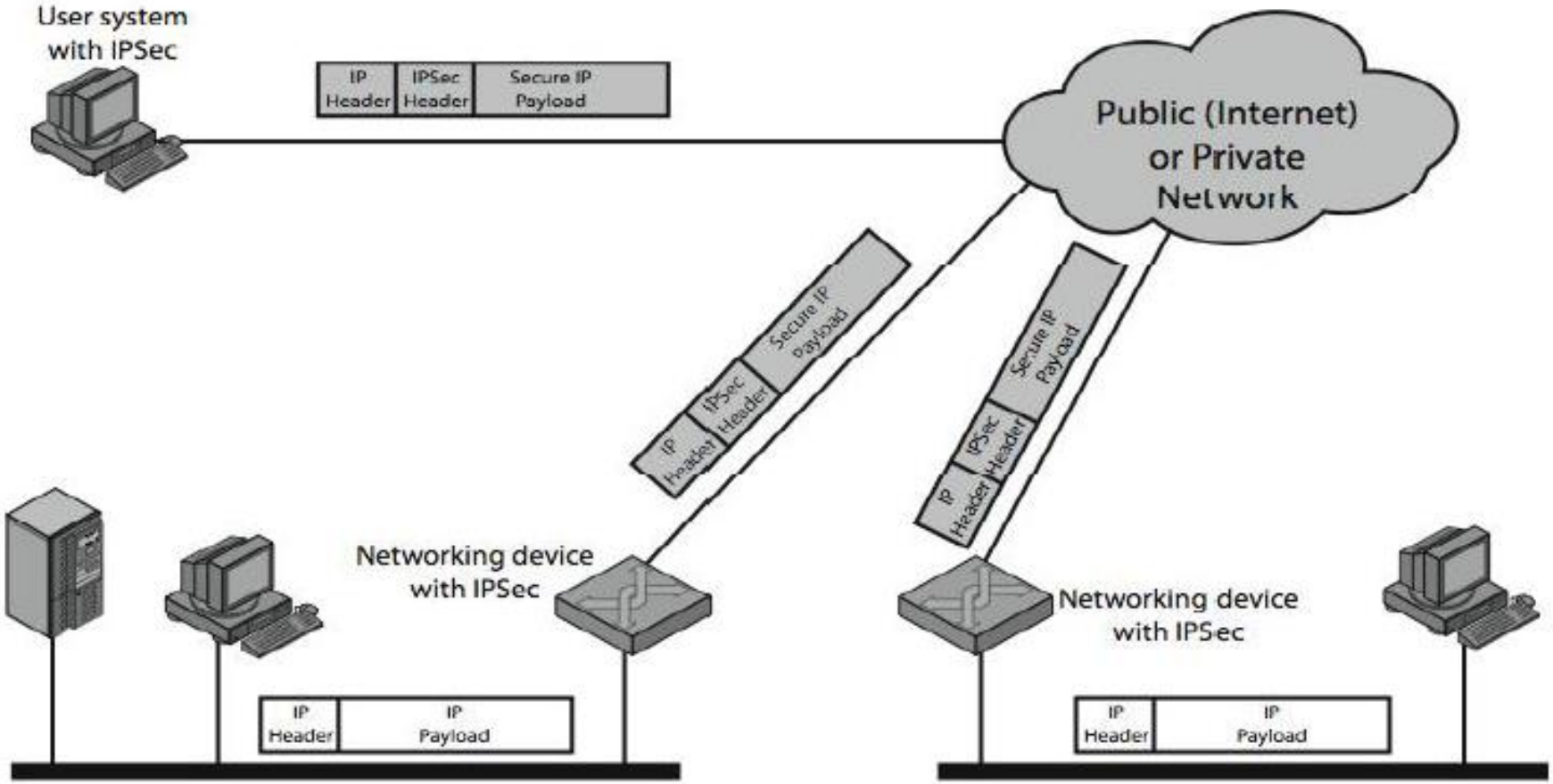
Figure 11.3 Example Firewall Configuration

IP Security (IPSec)

- IP security (IPSec) is a capability that can be added to either current version of Internet Protocol(IPv4 or IPv6) by means of additional headers.
- IP-level security encompasses three functional areas: authentication, confidentiality, and key management.
- The authentication mechanism assures that a received packet was transmitted by the party identified as the source in the packet header, and that the packet has not been altered in transit.
- The confidentiality facility enables communicating nodes to encrypt messages to prevent eavesdropping by third parties.
- The key management facility is concerned with the secure exchange of keys.
- IPSec provides the capability to secure communications across a LAN, across private and public WANs, and across the Internet.

IPSec Uses

- The figure illustrates a typical IP Security scenario. An organization maintains LANs at dispersed locations. Unsecure IP traffic is conducted on each LAN. For traffic offsite, through some sort of private or public WAN, IPSec protocols are used.
- These protocols operate in networking devices, such as a router or firewall, which connect each LAN to the outside world.
- The IPSec networking device will typically encrypt and compress all traffic going into the WAN, and decrypt and decompress traffic coming from the WAN; these operations are transparent to workstations and servers on the LAN. Secure transmission is also possible with individual users who dial into the WAN. Such user workstations must implement the IPSec protocols to provide security.


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

Benefits of IPSec

- When IPSec is implemented in a firewall/router, it provides strong security to all traffic crossing the perimeter
- IPSec in a firewall/router is resistant to bypass if all traffic from outside must use IP, and the firewall is the only means of entrance from the Internet into the organization.
- IPSec is below the transport layer (UDP,TCP), hence transparent to applications
- IPSec can be transparent to end users
- IPSec can provide security for individual users if needed
- IPSec secures routing architecture

IPSec Services

- Access control
- Connectionless integrity
- Data origin authentication
- Rejection of replayed packets (a form of partial sequence integrity)
- Confidentiality (encryption)
- Limited traffic flow confidentiality

Security Associations

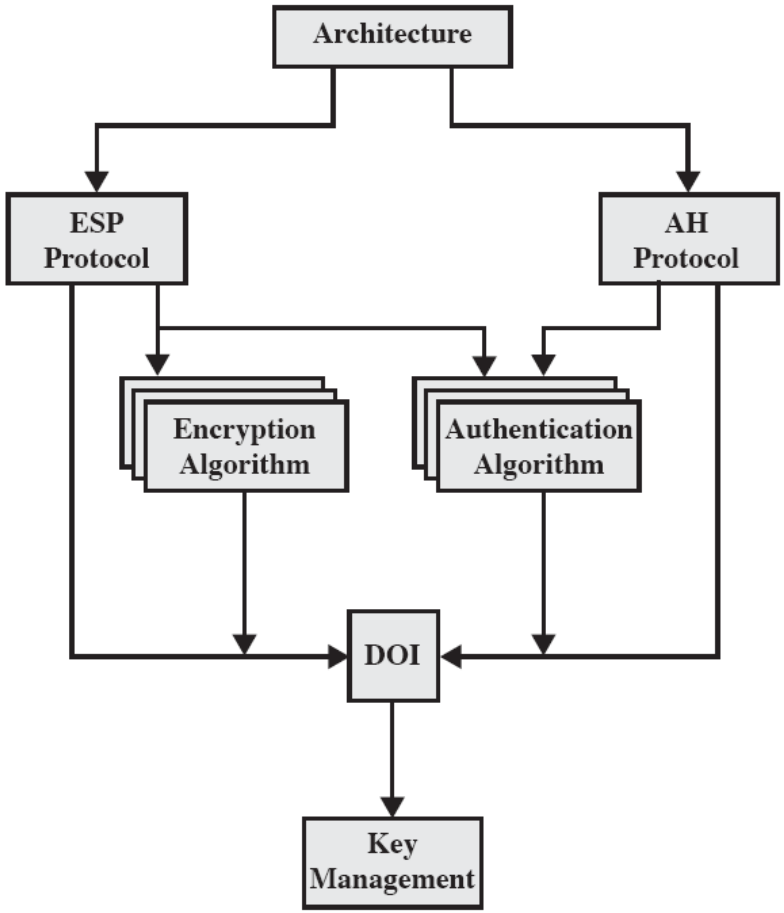
- A key concept that appears in both the authentication and confidentiality mechanisms for IP is the security association (SA).
- An association is a one-way relationship between a sender and a receiver that affords security services to the traffic carried on it. If a peer relationship is needed, for two-way secure exchange, then two security associations are required. Security services are afforded to an SA for the use of AH or ESP, but not both.
- A security association is uniquely identified by three parameters:

  Security Parameters Index (SPI): A bit string assigned to this SA and having local significance only

  IP Destination Address: this is the address of the destination endpoint of the SA

  Security Protocol Identifier: This indicates whether the association is an AH or ESP security association.
- A SA may also have a number of other parameters. In each IPSec implementation, there is a Security Association Database that defines the parameters associated with each SA.

Architecture of IPSec



- Key Management- Documents that describe key management schemes.

- Domain of Interpretation (DOI)- Contains the values needed for the other documents to relate to each other.

Authentication Header

- The Authentication Header provides support for data integrity and authentication of IP packets.
- The data integrity feature ensures that undetected modification to a packet‘s content in transit is not possible.
- The authentication feature enables an end system or network device to authenticate the user or application and filter traffic accordingly; it also prevents address spoofing attacks and replay attacks.

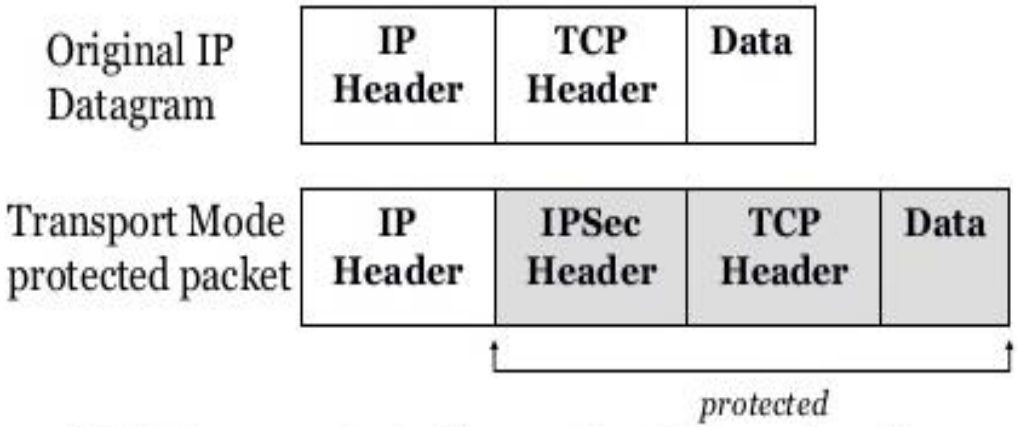
Encapsulating Security Payload

- The Encapsulating Security Payload provides confidentiality services, including confidentiality of message contents and limited traffic flow confidentiality.
- As an optional feature, ESP can also provide an authentication service, with the same MACs as AH. ESP supports range of ciphers, modes, and padding

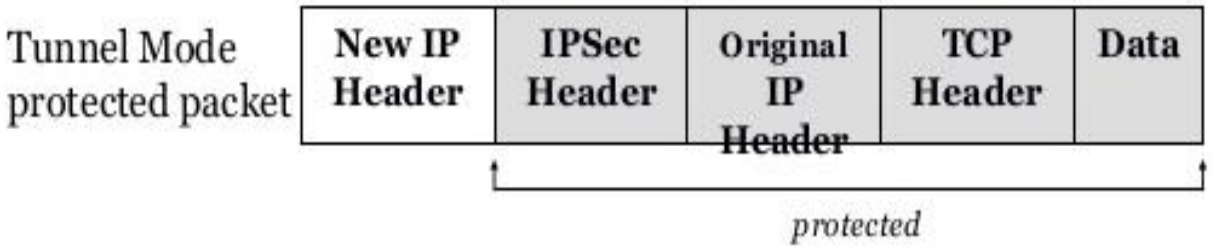
IPSec Operation Modes

- IPsec has two modes.
- **Transport mode** encapsulates the IP packet data area (which is the upper layer packet) in an IPsec envelope, and then uses IP to send the IPsec-wrapped packet. The IP header is not protected.
- **Tunnel mode** encapsulates an entire IP packet in an IPsec envelope and then forwards it using IP. Here, the IP header of the encapsulated packet is protected.
- Transport mode is used when both endpoints support IPsec. Tunnel mode is used when either or both endpoints do not support IPsec but two intermediate hosts do.

- Transport Mode: protect the upper layer protocols



- Tunnel Mode: protect the entire IP payload



Virtual Private Network (VPN)

- A virtual private network (VPN) is a private computer network that interconnects remote (and often geographically separate) networks through primarily public communication infrastructures such as the Internet.
- VPNs provide security through tunneling protocols and security procedures such as encryption.
- For example, a VPN could be used to securely connect the branch offices of an organization to a head office network through the public Internet.
- A VPN can also be used to interconnect two similar networks over a dissimilar middle network; for example, two IPv6 networks over an IPv4 network.

- There are two main types of VPN: remote-access VPNs and site-to-site VPNs.
- Remote-access VPNs allow individual users to connect to a remote network, such as salespeople in the field connecting to their company's intranet.
- Site-to-site VPNs allow inter-connection of networks of multiple users, for example, branch offices to the main company network.
- VPNs hence reduce costs as they eliminate the need for dedicated leased lines between networks, instead use existing infrastructures to connect networks while adding a layer of security.

Secure VPNs use cryptography and tunneling protocols to provide:

- Confidentiality such that even if traffic is sniffed, an attacker would only see encrypted data which they cannot understand
- Allowing sender authentication to prevent unauthorized users from accessing the VPN
- Message integrity to detect any tampering of transmitted messages

- VPN can provide Confidentiality, Integrity, and Authenticity
- Security against determined hacker depends largely upon underlying protocols used
- Assuming security of SSH, IPSec, or other protocol used, should be secure

Secure VPN protocols include the following:

- IPSec (Internet Protocol Security) Its design meets most security goals: authentication, integrity, and confidentiality. IPSec functions through encrypting and encapsulating an IP packet inside an IPSec packet. De-encapsulation happens at the end of the tunnel, where the original IP packet is decrypted and forwarded to its intended destination.
- Microsoft Point-to-Point Encryption (MPPE) works with the Point-to-Point Tunneling Protocol and in several compatible implementations on other platforms.
- Secure Shell (SSH) VPN - OpenSSH offers VPN tunneling (distinct from port forwarding) to secure remote connections to a network or inter-network links..

- Use of a public network exposes corporate traffic to eavesdropping and provides an entry point for unauthorized users.
- To counter this problem, a VPN is needed.
- In essence, a VPN uses encryption and authentication in the lower protocol layers to provide a secure connection through an otherwise insecure network, typically the Internet.
- VPNs are generally cheaper than real private networks using private lines but rely on having the same encryption and authentication system at both ends.
- The encryption may be performed by firewall software or possibly by routers. The most common protocol mechanism used for this purpose is at the IP level and is known as IPsec.

- Tunnel endpoints must authenticate before secure VPN tunnels can be established.
- User-created remote access VPNs may use passwords, biometrics, two-factor authentication or other cryptographic methods.
- Network-to-network tunnels often use passwords or digital certificates, as they permanently store the key to allow the tunnel to establish automatically and without intervention from the user.

Trusted Computer Systems

- Trusted system : A computer and Operating system that can be verified to implement a given security policy is called trusted system
- Another widely applicable requirement is to protect data or resources on the basis of levels of security, as is commonly found in the military where information is categorized as
  - Unclassified (U)
  - Confidential (C)
  - Secret (S)
  - Top secret (TS), or higher.
- Here subjects (people or programs) have varying rights of access to objects (information) based on their classifications. This is known as multilevel security. A system that can be proved to enforce this is referred to as a trusted system

The multilevel secure system must enforce:

 No read up:

A subject can only read an object of less or equal security level - Simple Security Property

 No write down:

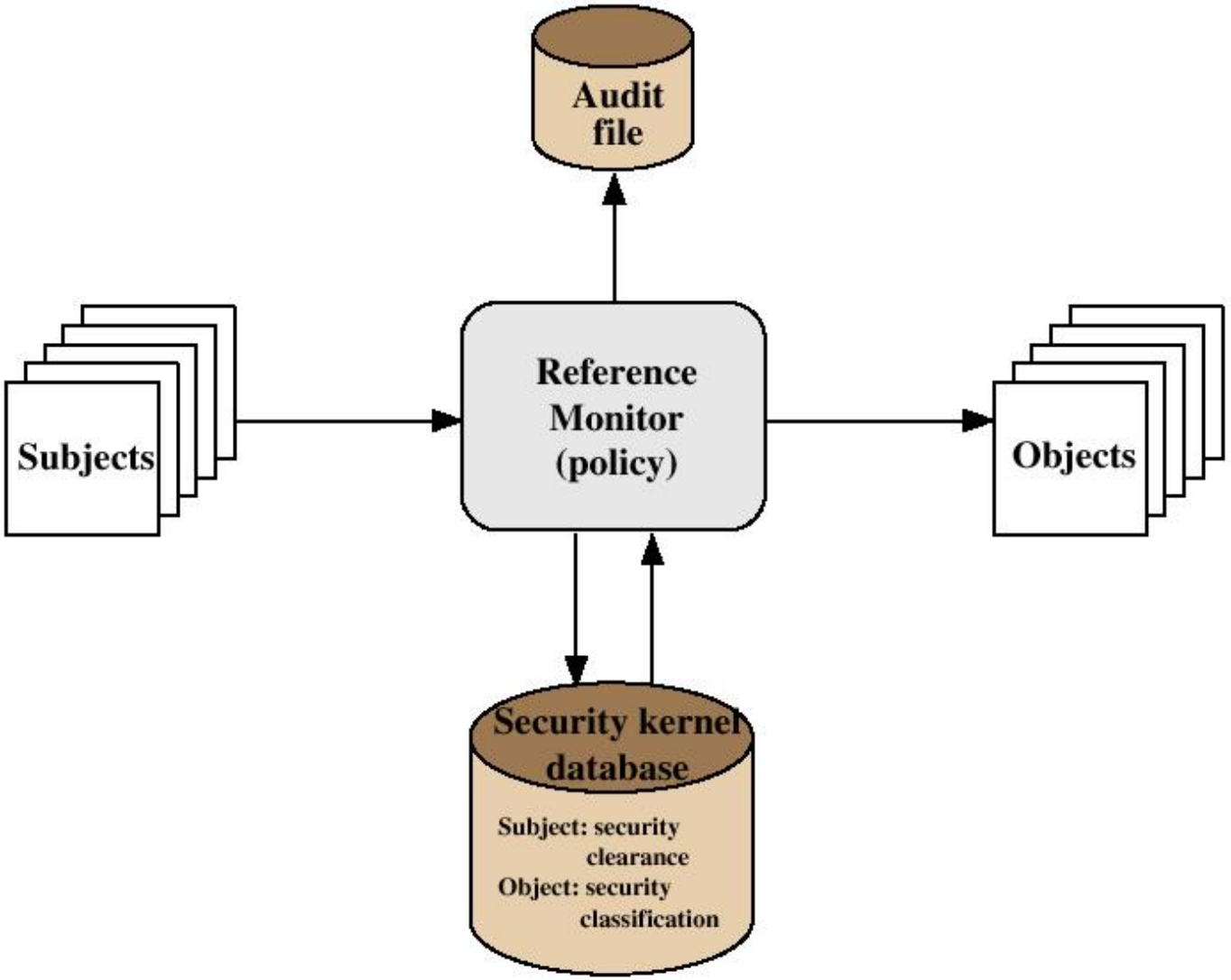
A subject can only write into an object of greater or equal security level - * (star) Property

- These two rules, if properly enforced, provide multilevel security.
- The reference monitor enforces the security rules (no read up, no write down).
- The reference monitor is a controlling element in the hardware and operating system of a computer that regulates the access of subjects to objects on the basis of security parameters of the subject and object.

It must have properties of:

- **Complete mediation:** The security rules are enforced on every access, not just, for example, when a file is opened.
- **Isolation:** The reference monitor and database are protected from unauthorized modification.
- **Verifiability:** The reference monitor's correctness must be provable. That is, it must be possible to demonstrate mathematically that the reference monitor enforces the security rules and provides complete mediation and isolation

Figure Reference Monitor Concept



Notes

- Tunneling is a protocol that allows for the secure movement of data from one network to another.
- Tunneling involves allowing private network communications to be sent across a public network, such as the Internet, through a process called encapsulation.
- The encapsulation process allows for data packets to appear as though they are of a public nature to a public network when they are actually private data packets, allowing them to pass through unnoticed.
- An inbound firewall protects the network against incoming traffic from the internet or other network segments, disallowed connections, malware and denial-of-service attacks. An outbound firewall protects against outgoing traffic originating inside an enterprise network. Often, a single firewall can serve both functions.

Assignment 3

1. What is network security? Differentiate network security with computer security.
2. Why network security is needed?
3. Explain the principal methods of protecting network.
4. Explain the components of network organization.
5. Define firewall and explain how firewall protects the network.
6. List the characteristics of firewall. Explain different types of firewall in brief.
7. What do you mean by DMZ? Explain functions of different DMZ servers
8. What is IPSec? Differentiate between IPSec and VPN.
9. List the capabilities and limitation of firewall.
10. Write advantages and disadvantages of VPN.
11. What is replay attack?
12. What is Bastion Host?

The end of one chapter is just the beginning of another. Read on...the best part is always yet to come.

- Susan Gale

boardofwisdom.com