UNIT 2

# NETWORK SECURITY AND FIREWALLS

## 2.1 INTRODUCTION

- Network Security and Firewalls the ability to conduct business on a public network has strong attraction- and the potential for big savings.
- Security and confidentiality are essential, however, before business can conduct financial transaction over the Internet and a lack of widespread security measures remains at this time.
- At present, credit card number, financial records and other important information are not encrypted and can be intercepted by any savvy Internet hacker.

A security threat is defined as a circumstance, condition, or event with the potential to cause economic hardship to data or net-work resources in the from of destruction, disclosure, modification of data, denial of service, and / or fraud, waste, and abuse.

The discussion of security concerns in electronic commerce can be divided into two broad types:

1. ***Client-server security:*** uses various authorization methods to make sure that only valid users and programs have access to information resources such as databases. Such mechanisms include pass-word protection , encrypted smart cards, biometrics, and firewalls.

2 ***Data and transaction security:*** ensures the privacy and confidentiality in electronic messages and data packets, including the authentication of remote users in network transaction for activities such as on-line payments.

## 2.2 CLIENT-SERVER NETWORK SECURITY

Client-server network security is one of the biggest headaches system admin-iterators face as they balance the opposing goals of user maneuverability and easy access and site security and confidentiality of local information.

Network security on the internet is a major concern for commercial organizations, especially top management.

Client-server network security problems manifest themselves in three ways:

1. ***Physical security holes*** result when individuals gain unauthorized physical access to a computer.

   On the network, this is also a common problem, as hackers gain access to network systems by guessing by passwords of various users.

2. ***Software security holes*** result when badly written programs "privy-leged" software are "compromised" into doing this they shouldn't.

   This is the highest level of access possible and could be used to delete the entire file system, or create a new account or password file resulting in incalculable damage.

3. ***Inconsistent usage holes*** result when a system administrator assembles a combination of hardware and software such that the system is seriously flawed from a security point of view. The incompatibility of attempting two unconnected but useful things creates the security hole.

To reduce these security threats, various protection methods are used. At the file level, operating systems typically offer mechanisms such as access control lists that specify the resources various users and groups are entitled to access. Protection – also called authorization or access control – grants privileges to the system or resource by checking user-specific information such as passwords.

Over the years, several protection methods have been developed, including *Trust-based security, security through obscurity, password schemes, and biometric systems.*

**1. Trust – Based Security**

- Quite simply, trust – based security means to trust every one and do nothing extra for protection. It is possible not be provide access restrictions of any kind and to assume that all users are trustworthy and competent in their use of the shared network.
- This approach worked in the past, when the system administrator had to worry about a limited threat. Today, this is no longer the case.

**2. Security Through Obscurity**

- Most organizations is the mainframe era practiced a philosophy known as Security Through Obscurity (STO)

- STO provides a false sense of security in computing systems by hiding information.
- This method was quite successful with stand/alone system that ran operating systems such as IBM MVS or CMS and DEC VAX.
- But its usefulness is minimal in the UNIX world, where users are free to move around the file system, have a great understanding of programming techniques, and have immense computing power at their fingertips.
- Widespread networking necessitates greater need for details of how the system works, rendering STO less effective.

### 3. Password Schemes

One straightforward security solution a, password scheme, erects a first-level barrier to accidental intrusion. In actuality, however, password schemes do little about deliberate attack, especially when common words or proper names are selected as passwords.

For instance, network administrators at a Texas air force discovered that they could crack about 70 percent of the passwords on their UNIX network with tools resembling those used by hackers.

### 4. Biometric Systems

Biometric systems, the most secure level of authorization, involve some unique aspect of a person's body. Past biometric authentication was based on comparisons of

fingerprints, palm prints, retinal partial patterns, or on signature verification or voice recognition. Biometric systems are very expensive to implement. Biometric controls provide access procedures that match every valid user identifier(UDI).

They also provide authentication method to verify that users requesting access are really the ones who claim to be.

- Provide some password, which only user knows.
- Present something like a smart card or a token which only the user has
- Identify something only the user is, like signature, voice, fingerprint or retinal (eye) scan. It is implemented by biometric controls.

It a cost of several thousand dollars per reader station, they may be better suited for controlling physical access – where one biometric units can serve for many workers – than for network or workstations access.

**Biometric Authentication**

(1) Biometric authentication is the automatically recognition of a living being using suitable body characteristics.

(2) By measuring an individual's physical features in an authentication inquiry and comparing this data with stored biometric reference data, the identity of a specific user is determined.

The most common biometrics is the following:

***Face geometry (Photo)***

The computer takes the picture of your face & matches it with a Pre stored picture.

***Fingerprints (Fingerscan)***

Whenever a user wants access, matching fingerprint against a template containing authorized person's fingerprints.

***Hand Geometry***

Like fingerprints except the verifier uses a TV like camera to take the picture of the user's hand.

***Blood vessel pattern in the retina of a person's eye***

A match is done between the pattern of the blood vessels in retina that is being scanned & pre stored picture of retina.

***Voice (Voice Print)***

A match between users voice & voice pattern stored on templates.

***Signature***

Matched against the pre stored authentication signature.

***Key stoke Dynamics***

Match of person's keyboard pressure & speed against pre stored information.

***Others***

Like Thermo graphy, using a PIN & iris scan.

## 2.3 EMERGING CLIENT – SERVER SECURITY THREATS

Another security threat that is emerging in the electronic commerce world is mobile code (Software agents), which in many ways resembles a more traditional virus threat.

Mobile code is an executable program that has the ability to move from machine to machine and also to invoke itself without external influence.

### Software Agents and Malicious Code Threat

- The major threat to security from running client software results because of the nature of the Internet: Client programs interpret data downloaded from arbitrary servers on the Internet.
- In the absence of checks on imported data, the potential exists for this data to subvert programs running on the systems.
- The security threat arises when the downloaded data passes through local interpreters (Such as post script) on the client system without the user's knowledge.

### Threats to Servers

Hackers have potential access to a large numbers of systems. As a result, computers that are not properly configured and / or are running programs with security holes are particularly vulnerable.

Hackers can use popular UNIX Programs like Finger, rsh, or user to discover account names and then try to guess

simple passwords using a dictionary or more sophisticated password guessing methods (e.g., a hacker could use a password guessing program in which multiple computer systems are used simultaneously for comparison purpose).

Hackers can use electronic eavesdropping to trap user names and unencrypted passwords sent over the network. They can monitor the activity on a system continuously and impersonate a user when the impersonation attack is likely to be detected.

Hackers can spoof, or configure, a system to masquerade as another systems, thus gaining unauthorized access to resources or information on systems that "trust" the systems being mimicked.

## 2.4 NETWORK SECURITY AND FIREWALLS

A ***firewall*** is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules.

A firewall typically establishes a barrier between a trusted, secure internal network and another outside network, such as the Internet, that is assumed to not be secure or trusted.

Firewalls are often categorized as either network firewalls or host-based firewalls. Network firewalls are a software appliance running on general purpose hardware or hardware-based firewall computer appliances that filter traffic between two or more networks.

Host-based firewalls provide a layer of software on

one host that controls network traffic in and out of that single machine.

Routers that pass data between networks contain firewall components and can often perform basic routing functions as well,Firewall appliances may also offer other functionality to the internal network they protect such as acting as a DHCP or VPN server for that network

- The most commonly accepted network protection is a barriers – a firewall – between the corporate network and the outside world (un trusted network).
- The term firewall can mean many things to many people, but basically it is a method of placing a device – a computer or a router – between the network and the Internet to control and monitor all traffic between the outside world and the local network.

Generally speaking, a firewall is a protection device to shield vulnerable areas from some form of danger. In the context of the Internet, a firewall is a system – a router, a personal computers a host, or a collection of hosts – set up specifically to shield a site or subnet form protocols and services that can be abused from hosts on the outside of the subnet.

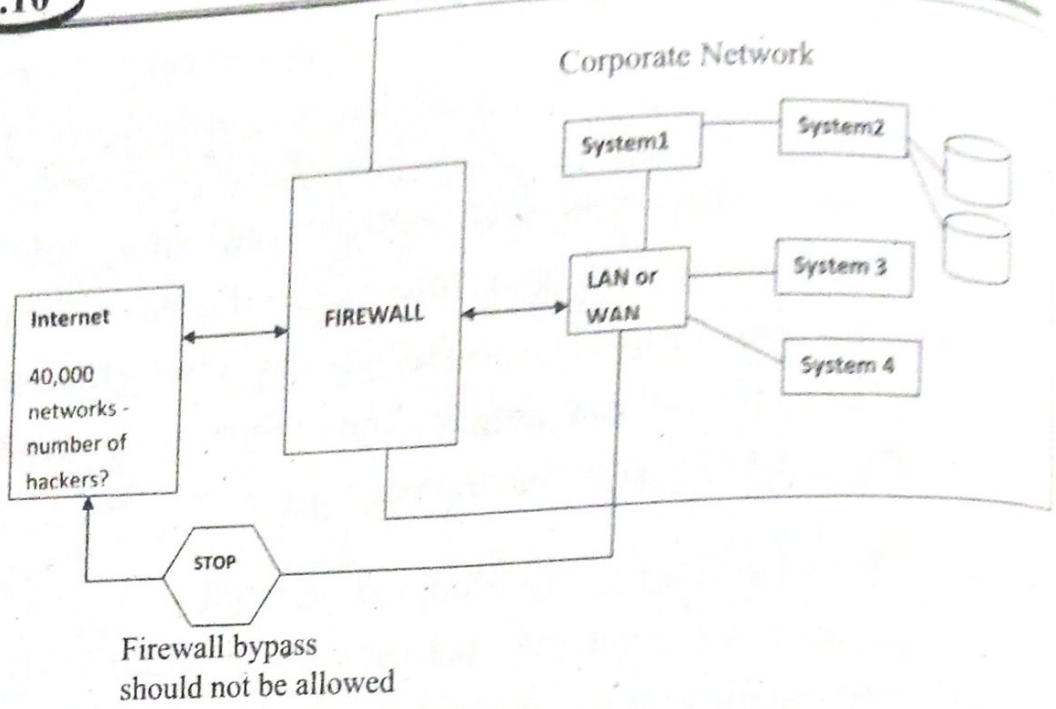


***Figure – Firewall-secured Internet connection***

## Firewalls In Practice

Firewalls range from simple traffic logging systems that record all network traffic flowing through the firewall in a file or database for auditing purposes to more complex methods such as IP packet screening routers, hardened firewall hosts, and proxy application gateways.

The simplest firewall is a packet-filtering gateway or screening router.

## IP Packet Screening Routers

This is a static traffic routing service placed between the network service provider's router and the internal network. The traffic routing service may be implemented at an IP level via screening rules in a router or at an application leven via proxy gateways and services.

The firewall router filters incoming packers to pertmit or deny IP packers based on several screening rules.

Rules include target interface to which the packet is routed, known source IP address, and incoming packet protocol (TCP, UDP, ICMP).

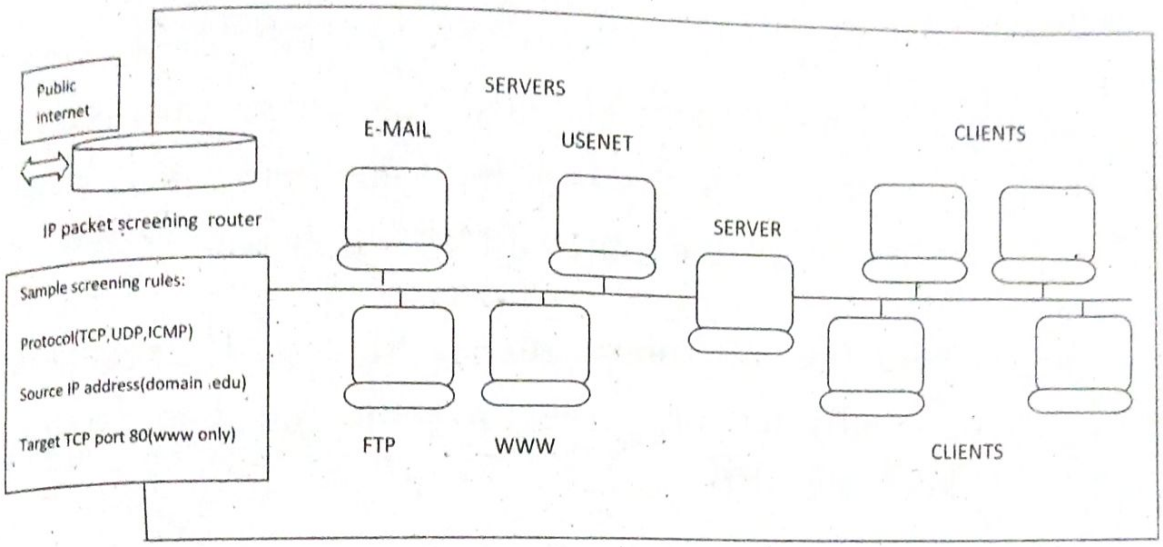


***Fig: Secure firewall with IP Packet Screening Routers***

## Proxy Application Gateways

A proxy application gateway is a special server that typically runs on a firewall machine. Their primary use is access to applications such as the World Wide Web from within a secure perimeter Instead of talking directly to external WWW servers, each request from the client would be routed to a proxy on the firewall that is defined by the user.

The proxy knows how to get through the firewall. All application – level proxy makes a firewall safely permeable for users in an organization, without creating a potential security hole through which hackers can get into corporate networks.

**Hardened Firewall Hosts**

A hardened firewall host is a stripped-down machine that has been configured for increased security.

Creating a hardened host requires several steps, among them.

- Removing all user accounts except those necessary for operation of the firewall, the logic being that, if users cannot log in to the firewall host, they cannot subvert
- Removing all non crucial files and executables, especially network server programs and client programs like FTP and Telnet.
- Extending traffic logging and monitoring to check remote access.
- Disabling IP forwarding to prevent the firewall form forwarding unauthorized packets between the Internet and the enterprise network.
- The hardened firewall host method can provide a greater level of audit and security, in return for increased configuration cost and decreased cost and " level of service (because a proxy needs to be developed for each desired service).
- Hardened firewall hosts also offer specific advantages. for example.
- Concentration of security. All modified software and logging is located on the firewall system as opposed to being distributed on many hosts.

- Centralized and simplified network services management. Services such as FIP, e-mail, Gopher, and other similar services are located on the firewall system(S) as opposed to being maintained on many systems.

### Security Policies And Firewall Management

The firewall method of protection spans a continuum between ease of use and paranoid security. Before putting a firewall in place, the administrator who has the responsibility of designing, specifying, and implementing or overseeing the installation of a firewall must address a numbers of management issues.

## 2.5 DATA AND MESSANGE SECURTY

### Data and Message Security

The lack of data and messages security on the Internet has become a higher profile problem due to increasing number of merchants trying to spur commerce on the global network.

For instance, credit card numbers in their plain text form create a risk when transmitted across the Internet where the possibility of the number falling into the wrong hands is relatively high.

Would you be willing to type in your credit card number knowing the risk? Even worse, would you expose your customers to that risk? Just the thought of "sniffer" programs that collect credit card numbers en masse is enough to keep merchants away from on-line shopping given the possible

lawsuits and other liability issues. In short, the lack of business transaction security is widely acknowledged as a major implement to widespread e- commerce.

The lack of data and message security on the Internet has become a high profile problem due to the increasing number of merchants trying to spur commerce on the global network.

**Data Security**

Electronic data security is of paramount importance at a time when people are considering banking and other financial transactions by PCs. Also, Computer industry trends toward distributed computed computing, and nomadic or mobile computer users, only exacerbate security challenges.

**Message Security**

Threats to message security fall into three categories: confidentiality, integrity, and authentication.

**Message Confidentially**

Confidentiality is important for uses involving sensitive data such as credit card numbers.

The environment must protect all message traffic. After successful delivery to their destination gateways, messages must be removed (expunged) from the public environment.

**Message and System Integrity**

Business transactions require that their contents remain unmodified during transports. In other words, information

received must have the same content and organizations as information's sent. It must be clear that no one has added, deleted, or modified any part of the massage.

### Message Sender Authentication/Identification

For e-commerce, it is important that clients authenticate themselves to servers, that servers authenticate to clients, that both authenticate to each others.

### Encryption As The Basis For Data And Massage Security

Encrypt, or encipher, the message, which means that Anne can scramble it in a hopelessly complicated way, rendering it unreadable to anyone except you, the intended recipient.

### Secret-Key Cryptography

Secret-key cryptography involves the use of a shared key for both encryption by the transmitter and decryption by the receiver. Shared-key techniques suffer from the problem of key distribution, since shared keys must be securely distributed to each pair of communicating parties. Secure-key distribution becomes cumbersome in large networks.

### Data Encryption Standard (DES)

A widely-adopted implementation of secret-key cryptography is Data Encryption Standard (DES).

### Public-Key Cryptography

- A cryptographic system that uses two keys- a public key known to everyone and a private or secret key known only to the recipient of the message.

- An important element to the public key system is that the public and private keys are related in such a way that only the public key can be used to encrypt messages and only the corresponding private key can be used to decrypt them. Moreover, it is virtually impossible to deduce the private key if you know the public key.
- A more powerful from of cryptography involves the use of public keys.
- Public-key techniques involve a pair of keys; a private key and a public key associated with each user. Information encrypted by the private key can be decrypted only using the corresponding public key.
- The private-key used to encrypt transmitted information by the user, is kept secret.

**RSA and Public-Key Cryptography**

RSA is a public-key cryptosystem for both encryption and authentication developed in 1977. RSA's system uses a matched pair of encryption and decryption keys, each performing a one-way transformation of the date.

**Digital Public-Key Certificates**

The most difficult aspect of creating an effective multiparty transaction system is the distribution of public keys. Because the keys are intended to be public and widely distributed, secrecy is not a concern; anyone should be able to get a copy of a public key. Rather, the primary concern is authenticity.

## Digital Signatures

- A digital signature is an electronic rather than a written signature that can be used by Someone to authenticate the identity of the sender of a message or of the signer of a document.
- It can also be used to ensure that the original content of the message or document that has been conveyed is unchanged.
- Additional benefits to the use of a digital signature are that it is easily transportable, cannot be easily repudiated, cannot be imitated by someone else, and can be automatically time-stamped.
- A digital signature can be used with any kind of message, whether it is encrypted or not, simply so that the receiver can be sure of the sender's identity and that the message arrived intact.
- A digital certificate contains the digital signature of the certificate-issuing authority so that anyone can verify that the certificate is real.
- The signature is an unforgivable piece of data asserting that a named person wrote or otherwise agreed to the document to which the signature is attached.
- Digital signatures are a recent development the need for which has arisen with the proliferation of electronic commerce.
- A secure digital signature system thus consists to two parts; a method of signing a document such that forgery is infeasible, and a method of verifying that a signature

was actually generated by whomever it represents. Furthermore, secure digital signatures cannot be repudiated; that is, the signer of a document cannot later disown it by claiming it was forged.

**Digital Signature Standard (DSS)**

The digital signature standard specifies a digital signature algorithm (DSA) as part of the U.S. governments capstone project.

## 2.6 ENCRYPTED DOCUMENTS AND ELECTRONIC MAIL

Encrypted Documents and Electronic Mail: E-mail users who desire confidentiality and sender authentication are using encryption.

Encryption is simply intended to keep personal thoughts personal. Some users are already using Pretty Good Privacy (PGP); others are starting to use Privacy Enhanced Mail (PEM).

Electronic data security is important at a time when people are considering banking and other financial transaction by PCs.

E-mail is typically encrypted for the reason that all network correspondence is open for eavesdropping Internet e-mail is obviously for less secure then the postal systems. where envelops protect correspondence from casual snooping.

- If electronic mail systems are to replace the existing paper mail system for business transactions, "signing" an electronic message must be possible.

- The recipient of a signed message has proof that the message originated from the sender. This quality is stronger than mere authentication (where the recipient can verify that the message came from the sender); the recipient can convince a "judge" that the signer sent the message.

- To do so, he must convince the judge that he did not forge the signed message himself! In an authentication problem the recipient does not worry about this possibility, since he only wants to satisfy himself that the message came from the sender.

- A glance at the header area of any e-mail message, by contrast, will show that it has passed through a number of nodes on its way to you. Every one of these nodes presents the opportunity for snooping..

**Advantages**

- No can figure out the private key from the corresponding public key. Hence, the key management problems is mostly confined to the management of private keys The need for sender and receiver to share secret information over public channels is completely eliminated.

- E-mail users who desire confidentiality and sender authentication are using encryption. Encryption is simply intended to keep personal thoughts personal.

- E-mail us typically encrypted for the reason that all

network correspondence is open for eavesdropping. A glance at the header area of any e-mail message, by contrast, will show that it has passed through a number of nodes on its way to you.

- Every one of these nodes presents the opportunity for snooping. Everyday communication over phone and fax lines entails security risks.
- Electronic data security is important at a time when people are considering banking and other financial transaction by PCs.
- E-mail software is increasingly incorporating specific options that simplify encryption and decryption. Examination of encrypted information is non-trivial; each file must be decrypted even before it can be examined.
- If the file itself proves to contain embedded, compressed, encrypted files, those too must be expanded and decrypted.
- This process may need repeating several times before the innermost fills contents are discernible. Lets look at two e-mail encryption schemes that are being deployed on the internet.

**Privacy Enhanced Mail Standard(PEM)**

PEM is the internet privacy enhanced mail standard, designed, proposed, but not yet officially adopted, by the internet activities board to provide secure electronic mail over the internet.

Designed to work with current Internet e-mail formats. PEM includes encryption, authentication, and key management, and allows use of both public-key and secret-key cryptosystems.

### Pretty Good Privacy (PGP)

- Pretty Good privacy (PGP) is an implementation of public-key cryptography based on RSA. It is a free software package developed by Phillip Zimmerman that encrypts e-mail.
- PGP provides secure encryption of documents and data files that even advanced supercomputers are hard pressed to CRACK.
- Public key cryptography is computationally very expensive. It takes a lot of computing power to decrypt and encrypt a message.
- Therefore, PGP can be done by encrypting your message with a conventional algorithm (the IDEA algorithm), and then use the recipient's public key to encrypt just the IDEA key needed to decrypt the message.

The digital signature is then encrypted with RSA using the senders private key, and the result is pretended to the e-mail.