E-Commerce (Unit - III)

3.1 Need for Computer Security

Computer Security: It is a process of presenting and detecting unauthorized use of your computer. Prevention is measures help you stop unauthorized users (hackers) System often they want to gain control of your computer so they can use it to launch attack on other computer systems.

Need for computer security

- Threats & Count measures
- Introduction to Cryptography
- Authentication and integrity
- Key Management
- Security in Practice – secure email & SMTP
- User Identification
- Trusted Computer System
- CMW
- SECMAN standards.

The Importance of computer security:

A computer security its very important, primarily to keep your information protected. Its also important for your computer overall health, helping to prevent various and malware and allowing program to run more smoothly.

Computer Security – Why?

- Information is a strategic resource.
- A Significant portion of organizational budget is spent on managing information.
- Have several security related objectives.
- Threats to information security.

The Security addressed here to general areas:

- Secure file / information transfers, including secure transactions.
- Security of information's as stored on Internet – connected hosts.
- Secure enterprise networks, when used to support web commerce.

Protecting Resources:

- The term computer and network security refers in a board sense to confidence that information and services available on a network cannot be accessed by unauthorized users.
- Security implies safety, including assurance to data integrity, freedom from unauthorized access, freedom snooping or wiretapping and freedom from distribution of service.

Reasons for information security

The requirements of information's security in an organization have undergone two major changes in the last several decades.

Types of Risks

As the number of peoples utilizing the internet increases, the risks of security violations increases, with it. One can compare the internet to a large department to stored with a lot of entrances, a lot of customers and so security guards to discourage shoplifting.

- Security Threats
- Passive Threats
- Active Threats

Security Threats

Some of the threats that stimulated the upsurge of interest in security.

Passive Threats

Passive threats involve monitoring the transmission data of an organization. The goal of a attackers is to obtain information that in being transmitted.

Active Threats

This involve some modification of the data stream or the creation of a false stream.

3.2 Specific Intruder Approaches

The advantage of such an approach is that it could be made vendor independent and ported to a variety of system.

Bulletin boards

These internet services provider a clearing for information and correspondence about a large variety of subject. Many commercial organizations especially technologies houses, use then to provide customer services. Bulletin boards have been notorious hangouts for hackers and other antisocial types.

Electronic mail

E-Mail is the one of the most commonly used services and is all some origination use. Email poses fewer security problems then over forms of Internet Communication but subject to interception if it is unencrypted.

File Transfer

Using FTP and HTTP users can request and send a variety of bulk data including data bases, files in all formats, documents, software images and voice.

While useful and convincement, file transfer can be insure both in terms of confidentially and virus threats.

IP Spoofing

IP spoofing is a techniques that can load to root access on a system. It is the tool that intruders often use to take over open terminal an login connections after the get root access.

The Intruders create packets with spoofed or impersonated source IP address. The attackers involving forging the source address of packets.

Password guessing

Most host administration have improved their password controls, but group accounts still abound and password dictionary & password cracking programs can easily crack at least 10% of the pass words users these.

The different is enforcement of good passwords.

Password sniffing

CERT estimates that in 1994, thoursands of system were the victims of password sniffers. On LANs internal machine on the network can see the traffic for every machine

on that network. Sniffer programs exploit this characteristic, monitoring all IP traffic and capturing the first 128 bytes or so of every encrypted FTP (or) Telnet session.

Telnet:

Telnet enables users to log on to remote computers. Telnet does little to detect and protect against unauthorized access.

Fortunately, Telnet is generally supported either by using an application gateway or by configuration router to permit outgoing connection using something such as the established screening rules.

Viruses:

A virus is a program that can infect other programs by modifying them to include a copy of itself.

It is possible that any program that comes in contact with virus will become infected with the virus.

Similarly to how virus attacks, humans computer virus can grow, replicate, travel adapts and learn. Attack and defend camouflage themselves and consume resource. The following lists various computer virus information's.

- Alter data in files
- Change disk assignments
- Create bad sectors
- Decrease free space on disk
- Destroy FAT(File Allocation Table)
- Erase specific tracks or entire disk
- Format Specific Tracks or Entire disk
- Hang the System
- Overwrite disk directory
- Suppress Execution of RAM resident programs

Write a volume label on the disk

SATAN (Security Administrator Tool for Analyzing Networks)

SATAN is a powerful tool that can through scan systems and entire networks of systems far a number of common critical security holes.

SATAN can be used by administrator to check their own networks: unfortunately, it is also used by hackers trying to break into a host.

A SATAN is a program available via the Internet.

The primary components are included:

HTTP server that acts at the dedicated SATAN web server.

Policy engine that defines which hosts are allowed to be probed and to what degree.

Inference engine that is driven by a set of rules bases and input from data acquisition.

Report and analysis, based on its findings.

More general information about SATAN and obtaining SATAN is available for anonymous FTP.

3.3 Security strategies:

There are basic security strategies that can be utilized to combat the threats discussed for access control, integrity, confidentiality and authentication.

However, before defenses can be deploy, a security policy must be developed by an organization.

Policy Issue:

Although the need for a policy is obvious, many organizations attempts to make their network secure without first defining what security means.

Before the organization can enforce security, the organization must access risks and develop and unambiguous policy regarding information access and protection.

Policy Guidelines:

A System administrator sets security policies, he or she developing a plan for how to deal with computer security.

One way to approach this task is to do the following.

Look at what it is you are trying to protect.

Look at what you need to protect their data/resource from.

Determine how likely the threats are implement measures which will protect your assets in a cost effective manner.

Review the process continuously and improve process when a weekness is found.

Inadequate management:

Related to the topic of policy is the topic of rational resource management.

Solid procedures and good management of computer system as related to software are critically important.

Mechanisms for Internet Security

Mechanism that help make internet based communication secure can be divided into broad categories.

The First focus is the problems of authorization, authentication and integrity;

The Second focus on the problem of privacy.

Finally the 3rd focus on the problems of availability by controlling access.

First Focus of problems: Authentication and integrity mechanisms:

Authentication mechanisms address the problems of identification of individuals and entities requesting services or access.

Example Configured to reject a request unless the request originates from an authorized client. When a client makes contact the server must various that the client is to undertake the specific task before granting service.

There are three types of authentication:

User to Host : A Host identifies a user before providing services.

Host to Host : Host validate the identity of their hosts.

User to User : User validate that data is beginning transmitted by the true sender and not an importer posing as the sender.

User to Host:

A Host identifies a user before providing services for which uses are authorized and deny those services for which they are not authorized.

Host to Host : Host to host authentication is concerned with the verification of the identity of computer system.

This method is employed by host on the internet.

User to User : This authentication establish proof of one uses identity to another user. This can be employed as a form of digital signature with electronic mail.

Second Focus Problems:

Privacy mechanism:

Confidentiality is the assurance of privacy, option achieved on the internet through the use of encryption as previously discussed in the context of integrity.

The 3rd Focus of problems: Controlling Access

The purpose of access control is to ensure that only authorized user have access to a particular system and / or specific resources, that access to end modification of a particular portion of data is limited authorized individuals and programs.

i. **User oriented access control**

User access control on a time sharing system is the user logon, which requires both a user identifier (ID) and password.

ii. **Data oriented access control**

Following successful logon, the user is generated access to a host or set of hosts and applications.

This generally not sufficient for a system that include sensitive data in the database.

3.4 Security Tools:

The section discuss some of tools that are available to the planner.

Secure Transport Stacks:

- The internet was the transport control protocol TCP/IP as the primary network protocol.
- The IP packet consists of a 32 bit source and destination address.
- Most users access the internet via a graphical interface.
- Web browser such or Netscape Navigator spyglass enhance mosaic (or) Microsoft explore communicate with a web server by means of HTTP.

Two most prominent

Secure sockets layer

Secure HTTP (S-HTTPS)

Kerberos

- Kerberos provides an authentication means in an open (Un protected) network.
- Service by using conventional (Shared secret key) Cryptography
- It is developed as a part of the Institute of technology project. A distributed system service running on the running on the computer network.

Design principles of Kerberos:

1. Both one way and two way authentication supported.
2. Transmitting when encrypted password (clear text) over a Network.
3. No Unencrypted password should be stared in the data's.

4. Memory for the shared time possible the length of the users current login session.

Kerberos Authentication Process

Client sends a request to the authentication server requesting Credentials for a given server.

The credentials consists of the following.

A ticket for the server

A temporary encryption key (often called a session key).

Secure transaction user the internet:

It is a need for worked secure transaction mechanism for transaction processing access the internet.

Use public key encryption well as RSA cryptography techniques.

Unix Security

Unix provides various built in security features. Such as user password file access directory access, file encryption and security on password files.

Web support (or) more generally for FTP (or) related support.

Eight character passwords for user. User password are generally encrypted using the DES algorithm.

Password Security

Password and password information's files are often the target for many attackers.

Login attempts should be limited to their as less tires.

Password security is only as good as the password itself.

One time password

This is accomplished via an authentication scheme.

There are several ways to implement one time password.

Smart Cards:

A smart card is a portable device that contains some non-volatile memory & a micro processor.

Some smart cards allow users to enter personal identification number (PIN) code 45.

Electronic mail

E-mail is one of most widely used forms of communication over to the internet.

It is a simple mail transfer protocol(SMTP).

Provides inter-machine e-mail transfer services

The content of the message itself is usually in plain text format

There is a multi of encryption system available.

It is privacy enhanced electronic mail (PEM).

Anonyms remailers provide a service that forwards a user's mail message onto the destination address but without disclosing the return address of the sender.

Example

hh@pmaintis.berkely.edu

nc@mailes@rehma.mn.org

Privacy Enhanced Mail:

Used to send e-mail and how it automatically encrypted.

PEM supports confidentiality original authentication, message integrity and non repudiation of origins

MIC-Message Integrity Code

MIC only.

Pretty Good Privacy (PGP).

PGP is an actual program that has become the de facts standard on the internet for electronic mail.

Multipurpose Internet mail Extensions

Textual massager exchanged on the internet.

Many types of recognizable non ASCII data.

MIME – enclosed messages.

There is a potential for the download object to be distributed to a users PC once executed.

Server security:

Many of the web browser allow user to save the HTML source code used to create the web pages that are viewed.

File name of respective graphics, video programs and hyperlinks that would be executed clicking on the web page items.

Trusting Binaries:

Security does not end with the various files well and browser security products available.

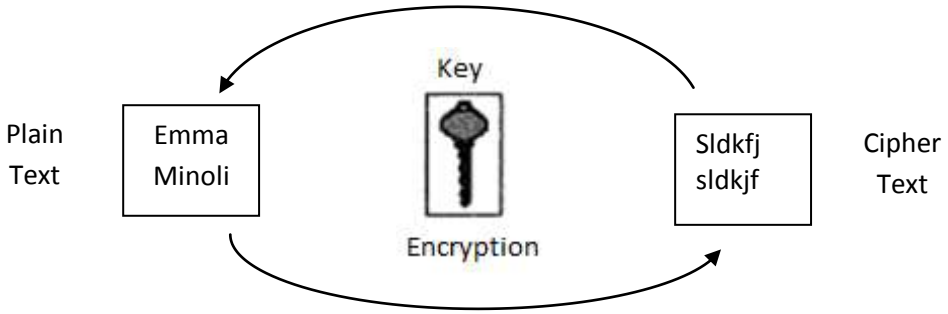
Account the issue of trusting executable.

Binaries at both ends must be secure as well.

3.5 Encryption

Encryption involves the scrambling of data by use of the mathematical algorithm. The term cryptography comes from the two creak words. Krupto and graph, that mean secret and writing.

There are three kinds of cryptography functions:



- Hash functions (involves the use of no keys)
- Secret key functions (involves the use of one key)
- Public key function (involves the use of two keys)

Conventional Environment:

A original message, referred to as plain text, is converted into apparently random nonsense referred to as cipher text.

Public key encryption:

Public key encryption, first proposed in 1976, does not require key distribution.

Public key encryption solves the distribution problem because there are no key distributed.

A public key cryptography is sometimes called in asymmetric cryptography.

Application of Encryption: Private key encryption to function the two communicating partics must have same key, and that key must be protected from access by others.

Session Key: When two end system want to communicate, they establish a logical connection for they duration of that logical connection, all user data in encrypted with a one time session key. At they conclusion of the session (or) connection, the session key is destroyed.

Permanent Key: A permanent key is used between entities two distributed session keys. Access Control centre: A Access control centre determines which system can communicate with each other.

Key distribution centre: The network interface centre unit performs end-to-end encryption and obtains session key on behalf of its host terminals.

Breaking an encryption scheme:

For every measure there is a countermeasure, and the counter measure for cryptography is crypto analysis, which is the art of undoing what the cryptography did.

There are three basic attacks; there are known as cipher text only, known plain text and chosen plain text.

The Data encryption standard:

DIS is the result of the request for proposal for a national cipher standard.

DES has flourished in recent years and its widely used, especially in financial applications.

Commercial communications Security endorsement Program:

The most likely replacement is a family algorithm developed under the NSA commercial COMSEC (Communications Security Endorsement Program) CCEP is the joint NSA and industry effort is produce a new generation of encryption devices that are more secure then DES algorithm.

Government Security Events:

The US department of defense has defined seven levels of computer operating system security in a document known as the trusted computer standard Evaluations Criteria. The feature has capabilities of a secure operating system secure significant amount of processing power and disk space.

The clipper ship:

In 1993 and 1994, the FBI proposed the clipped chip, the clipped chip uses key escrow which is a type of private key encryption that allows of two parties to hold the secret key. The encryption algorithm is based on the NSA's skipjack algorithm.

Commercial Outlook on encryption:-

Security experts recommend layering security because no single layer of encryption is sufficient. So many early users of encryption have deployed the technology at multiple layers, such as at the fire wall and web server.

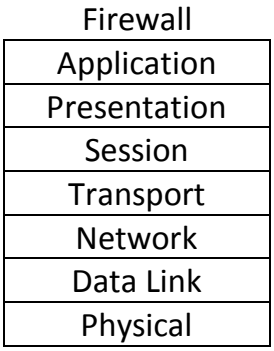
3.6 Enterprise Networking & Access to the Internet

Access to the internet is accomplished in a number of ways, Access can be attained via(1) a companies LAN – resident internet gateway (or) 2. By using a modem corrections.

Approaches for enterprise level security:

A firewall is a security device that allows limited access out of end into one's network from the internet.

So a firewall is a price of hardware that is connected to a network to protect it from agents reaching resource on the network via public open networks.



A firewalls are classified into three main categories:

- Packet filters
- Applications level gateways
- Proxy Servers

Packet filtering

A packet filtering at the network layer can be used a first defense.

Application level gateways: An Application level gateway provides a mechanism for filtering traffic far various applications.

Proxy Server: A proxy server terminals a users connections (by Applications) and set up a new connections to the ultimate destination on behalf of the user proxying for the users.

Variations and Combinations: This sections describes some variants of the basic firewalls categories described in the previous sections.

Dual Homed Host: In TCP/IP networks, the term multihomed host describes a host that has multiple network Interface connections.

Dual homed gateways: The dual homed gateways in an alternative to packet filtering routers.

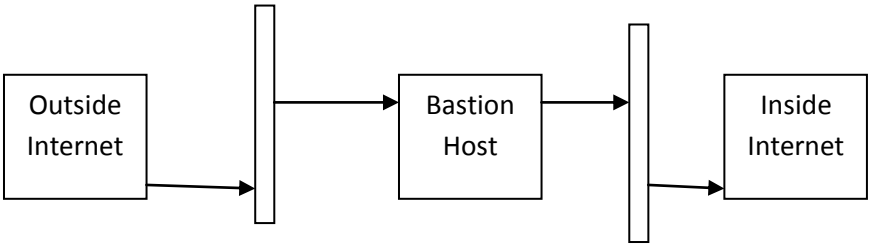
Screened Host firewall

The screened host firewall is more flexible the dual home gateway however the flexibility is achieved with same cost to security.

Screened Subnet firewall: It is a variations of the dual – homed gateway and the screened host firewall.

Bastion Host: A bastion host is any host subject to critical security requirements.

Design Considerations : Deployment approach, Packet filtering can be used to implement a variety of network security policies.



The consequence of restricted access for clients

A blanket prohibition on protocol data units arriving for an unknown protocol port seems to solves many potential security problems by preventing outside from accessing server in a organizations.

Bastion deployment Approach:

The implementation of the firewall concept is straight forward.

Monitoring and logging:

Monitoring is one of the most implement aspects of firewall designs.

Antivirus Programs:

Virus : A virus is a program that can effect other programs by modifying them the modified program includes a copy of virus program, which can then go on to infect other programs.

Worms : A Worm is a program that make use of networking software to replicate itself and move from system to system.

The nature of viruses: A virus can do anything that other programs do; the only difference is that it attaches itself to another program & executes secretly every time the host program is run.

A simple virus that does anything more then infect programs might work some thing like this.

- Find to the first program instructions.
- Replace it with a jump to the memory locations following the last instruction in the program.
- Insert a copy of the virus code at the locations.
- Have to the virus simulate the instruction replaced by the jump.
- Jump back to the 2nd instructions of the host programs.
- Finishing the executing the host programs.

Countering the threat of virus: The best solution for the threat of viruses in prevention do not allow a virus to get into the system in the first place.

The next best approach is do the following.

Detection: After the infection has occurred, determine that it has occurred and locate the virus.

Purging: Remove the virus from all infect system so, that the discuss cannot secured further.

Recovery: Recover any lost data (or) program

Security teams

The issue of network and internet security have become increasingly more important as more and more business and people go on line a term of people have been formed to assist in solving hacker attacks and do disseminate information on security attacks and how to prevent then two such teams are

- Computer emergency response team
- Forum of incident response & security team (FIRST)

Computer emergency response team (CERT)

The computer emergency response team(CERT) exists as a point of contact for suspected security problems related to the internet.

A CERT can help determine the secope of the threat and recommend an appropriate response.

Forum of incident response and security teems: (FIRST)

Security threats are a problems that effect computers and networks around the world.

FIRST is made up of a variety of computer emergency response teams including teams from government, business and academic sectors.