


Course Contents
Unit-11:Computer Security (3 Hrs.) <ul style="list-style-type: none">• Introduction;• Security Threat and Security Attack;• Malicious Software;• Security Services;• Security Mechanisms (Cryptography, Digital Signature, Firewall, Users Identification and Authentication, Intrusion Detection Systems);• Security Awareness; Security Policy

Computer Security
Computer Security: <ul style="list-style-type: none">• Computer security: Security attacks, security mechanisms, security services• Security threat and security attack• Malicious software: Virus, worm, Trojan horse, Javascript, java applet, ActiveX control• Hacking: Packet sniffing, password cracking, e-mail hacking• Security services: Confidentiality, integrity, authentication, non-repudiation• Security mechanisms<ul style="list-style-type: none">• Cryptography—Secret key cryptography, public-key cryptography, hash function• Digital signature—Digital signature algorithms• Firewall—Functions of firewall, working principle, types of firewall (packet filter firewall, circuit filter firewall, proxy or application-level firewall)• Users identification and authentication—User name and password, smart card, biometrics• Other security measures—Intrusion detection systems, virus protection software, data and information backups, SSL, IPsec protocol• Security awareness, security policy (formulating a security policy)

Computer Security
Computer Security: Introduction <ul style="list-style-type: none">• Individual users, organizations, and enterprises who use to keep data in their computer and using internet for data sharing need to keep the computers and the network (Internet) secure.• We should be aware of from whom to secure your data, and also about the security mechanisms to ensure security.• Computer security includes security of, both, the computer and the Internet.• The purpose of this chapter is to introduce you to “Computer Security”.

Computer Security
Computer Security: <p>Computer security focuses on the security attacks, security mechanisms and security services.</p> <ul style="list-style-type: none">> Security attacks are the reasons for breach of security. Security attacks comprise of all actions that breaches the computer security.> Security mechanisms are the tools that include the algorithms, protocols or devices, that are designed to detect, prevent, or recover from a security attack.> Security services are the services that are provided by a system for a specific kind of protection to the system resources.

Computer Security
Security threat and Security attack : <p>A threat is a potential violation of security and causes harm. A threat can be a malicious program, a natural disaster or a thief. Vulnerability is a weakness of system that is left unprotected. Systems that are vulnerable are exposed to threats. Threat is a possible danger that might exploit vulnerability; the actions that cause it to occur are the security attacks.</p> <p>A security attack may be a passive attack or an active attack.</p> <p>The aim of a passive attack is to get information from the system but it does not affect the system resources. Passive attacks may analyze the traffic to find the nature of communication that is taking place, or, release the contents of the message to a person other than the intended receiver of the message. Passive attacks are difficult to detect because they do not involve any alteration of the data. Thus, the emphasis in dealing with passive attacks is on prevention rather than detection.</p>

Computer Security
Security threat and security attack : <p>An active attack tries to alter the system resources or affect its operations. Active attack may modify the data or create a false data. An active attack may be a masquerade (an entity pretends to be someone else), replay (capture events and replay them), modification of messages, and denial of service. Active attacks are difficult to prevent. However, an attempt is made to detect an active attack and recover from them.</p> <p>Security attacks can be on users, computer hardware and computer software.</p> 

Computer Security

Security threat and security attack :

Attacks on users could be to the identity of user and to the privacy of user. Identity attacks result in someone else acting on your behalf by using personal information like password, PIN number in an ATM, credit card number, social security number etc. Attacks on the privacy of user involve tracking of users habits and actions—the website user visits, the buying habit of the user etc. Cookies and spam mails are used for attacking the privacy of users.

Attacks on computer hardware could be due to a natural calamity like floods or earthquakes; due to power related problems like power fluctuations etc.; or by destructive actions of a burglar.

Software attacks harm the data stored in the computer. Software attacks may be due to malicious software, or, due to hacking. Malicious software or malware is a software code included into the system with a purpose to harm the system. Hacking is intruding(interfering) into another computer or network to perform an illegal act.

Computer Security

MALICIOUS SOFTWARE:

The software that is intentionally included into a system with the intention to harm the system is called malicious software. Viruses, Trojan horse, and Worms are examples of malicious programs. Java scripts and Java applets written with the purpose of attacking, are also malicious programs.

Viruses, worms and Trojan Horses are all malicious programs that can cause damage to computer, but there are differences among the three, and knowing those differences can help you better protect your computer from damaging effects.

Malicious software are:

1. Virus
2. Worms
3. Trojan Horse
4. Java scripts, Java Applets and ActiveX Controls

Computer Security

MALICIOUS SOFTWARE:

Malicious software are:

1. Virus
2. Worms
3. Trojan Horse
4. Java scripts, Java Applets and ActiveX Controls

Computer Security

MALICIOUS SOFTWARE:

1. Virus

Virus is a software program that is destructive in nature. Virus programs have the following properties:

- > It can attach itself to other healthy programs.
- > It can replicate itself and thus can spread across a network.
- > It is difficult to trace a virus after it has spread across a network.
- > Viruses harm the computer in many ways
 - corrupt or delete data or files on the computer,
 - change the functionality of software applications,
 - use e-mail program to spread itself to other computers,
 - erase everything on the hard disk, or,
 - degrade performance of the system by utilizing resources such as memory or disk space.
- > Virus infects an executable file or program. The virus executes when a program infected with virus is executed or you start a computer from a disk that has infected system files.

Computer Security

MALICIOUS SOFTWARE:

1. Virus

- > Virus infects an executable file or program. The virus executes when a program infected with virus is executed or you start a computer from a disk that has infected system files.
- > Once a virus is active, it loads into the computer's memory and may save itself to the hard drive or copies itself to applications or system files on the disk.
- > However, viruses cannot infect write protected disks or infect written documents. Viruses do not infect an already compressed file. Viruses also do not infect computer hardware; they only infect software.
- > Viruses are most easily spread by attachments in e-mail messages. Viruses also spread through download on the Internet.
- Some examples of viruses are—"Melissa" and "I Love You".

Computer Security

MALICIOUS SOFTWARE:

2. Worms

Worm is self-replicating software that uses network and security holes to replicate itself. A copy of the worm scans the network for another machine that has a specific security hole. It copies itself to the new machine using the security hole, and then starts replicating from there, as well. A worm is however different from a virus. A worm does not modify a program like a virus, however, it replicates so much that it consumes the resources of the computer and makes it slow.

Some examples of worms are—"Code Red" and "Nimda".

Computer Security

MALICIOUS SOFTWARE:

3. Trojan

Users install Trojan horses thinking that it will serve a useful purpose such as a game or provide entertainment. However, Trojan horses contain programs that corrupt the data or damage the files. Trojan horses can corrupt software applications. They can also damage files and can contain viruses that destroy and corrupt data and programs. Trojan horse does not replicate themselves like viruses.

Computer Security

MALICIOUS SOFTWARE:

4. Java scripts, Java Applets and ActiveX Controls

Javascript is a scripting language generally nested within HTML code. The client-side scripts on a HTML page execute inside the Web browser on the client computer. Javascript codes can be used to transfer files, send e-mails and write to local files. If used with a maligned intention, the scripts can be dangerous for the client machine.

Applets (Java programs), and ActiveX controls are used with Microsoft technology, which can be inserted in a Web page and are downloaded on the client browser for execution. Applets and ActiveX controls are generally used to provide added functionality such as sound and animation. However, these programs when designed with a malicious intention can be disastrous for the client machine.

Java Applets have strong security checks that define what an applet can do and what it cannot. ActiveX controls do not have such security checks. Normally, ActiveX controls must be kept disabled while working on the Internet.

Computer Security

HACKING :

Hacking is the act of intruding into someone else's computer or network. Hacking may result in a Denial of Service (DoS) attack or prevents authorized users from accessing the resources(email, web sites, online accounts banking, etc.) of the computer. It aims at making the computer resource unusable or unavailable to its intended users.

In a DoS attack, the services of the entire network, an Internet site or service, may be suppressed or disabled. The affected machine is flooded with spurious requests and messages so as to overload the network. As a result, the affected machine cannot process the valid requests. This is a denial of service to the valid users.

Generally, the targets of such attacks are the sites hosted on high-profile web servers such as banks and credit card payment gateways.

Packet sniffing, E-mail hacking and Password cracking are used to get the username and password of the system to gain unauthorized access to the system. These methods gather the information when the data is being transmitted over the network.

Computer Security

1. Packet Sniffing

The data and the address information are sent as packets over the Internet. The packets may contain data like a user name and password, e-mail messages, files etc. Packet sniffing programs are used to intercept the packets while they are being transmitted from source to destination. Once intercepted, the data in the packets is captured and recorded. Generally, packet sniffers are interested in packets carrying the username and password. Packet sniffing attacks normally go undetected. Ethereal and Zx Sniffer are some freeware packet sniffers. Telnet, FTP, SMTP are some services that are commonly sniffed.

2. Password Cracking

Cracking of password is used by hackers to gain access to systems. The password is generally stored in the system in an encrypted form. Utilities like Password cracker is used to crack the encrypted passwords. Password cracker is an application that tries to obtain a password by repeatedly generating and comparing encrypted passwords or by authenticating multiple times to an authentication source.

Computer Security

3. E-mail Hacking

The e-mail transmitted over the network contains the e-mail header and the content. If this header and the content are sent without encryption, the hackers may read or alter the messages in transit. Hackers may also change the header to modify the sender's name or redirect the messages to some other user. Hackers use packet replay to retransmit message packets over a network. Packet replay may cause serious security threats to programs that require authentication sequences. A hacker may replay the packets containing authentication data to gain access to the resources of a computer.

Computer Security

SECURITY SERVICES:

The security services provide specific kind of protection to system resources. Security services ensure Confidentiality, Integrity, Authentication, and Non-Repudiation of data or message stored on the computer, or when transmitted over the network. Additionally, it provides assurance for access control and availability of resources to its authorized users.

Confidentiality: The confidentiality aspect specifies availability of information to only authorized users. In other words, it is the protection of data from unauthorized disclosure. It requires ensuring the privacy of data stored on a server or transmitted via a network, from being intercepted or stolen by unauthorized users. Data encryption stores or transmits data, in a form that unauthorized users cannot understand. Data encryption is used for ensuring confidentiality.

Computer Security

SECURITY SERVICES:

Integrity: It assures that the received data is exactly as sent by the sender, i.e. the data has not been modified, duplicated, reordered, inserted or deleted before reaching the intended recipient. The data received is the one actually sent and is not modified in transit.

Authentication: Authentication is the process of ensuring and confirming the identity of the user before revealing any information to the user. Authentication provides confidence in the identity of the user or the entity connected. It also assures that the source of the received data is as claimed. Authentication is facilitated by the use of username and password, smart cards, biometric methods like retina scanning and fingerprints.

Computer Security

SECURITY SERVICES:

Non-Repudiation prevents either sender or receiver from denying a transmitted message. For a message that is transmitted, proofs are available that the message was sent by the alleged sender and the message was received by the intended recipient. For example, if a sender places an order for a certain product to be purchased in a particular quantity, the receiver knows that it came from a specified sender. Non-repudiation deals with signatures.

Access Control: It is the prevention of unauthorized use of a resource. This specifies the users who can have access to the resource, and what are the users permitted to do once access is allowed.

Availability: It assures that the data and resources requested by authorized users are available to them when requested.

Computer Security

SECURITY MECHANISMS:

Security mechanisms deal with prevention, detection, and recovery from a security attack. Prevention involves mechanisms to prevent the computer from being damaged. Detection requires mechanisms that allow detection of when, how, and by whom an attack occurred. Recovery involves mechanism to stop the attack, assess the damage done, and then repair the damage.

Security mechanisms are built using personnel and technology.

- Personnel are used to frame security policy and procedures, and for training and awareness.
- Security mechanisms use technologies like cryptography, digital signature, firewall, user identification and authentication, and other measures like intrusion detection, virus protection, and, data and information backup, as countermeasures for security attack.

Computer Security

SECURITY MECHANISMS TECHNOLOGIES:

- **Cryptography:** Secret key cryptography, public-key cryptography, hash function
- **Digital signature:** Digital signature algorithms
- **Firewall:** Functions of firewall, working principle, types of firewall (packet filter firewall, circuit filter firewall, proxy or application-level firewall)
- **Users identification and authentication:** User name and password, smart card, biometrics
- **Other security measures:** Intrusion detection systems, virus protection software, data and information backups, SSL, IPsec protocol

Computer Security

SECURITY MECHANISMS TECHNOLOGIES:

Cryptography: Secret key cryptography, public-key cryptography, hash function

Cryptography is the science of writing information in a "hidden" or "secret" form. Cryptography is necessary when communicating data over any network, particularly the Internet. It protects the data in transit and also the data stored on the disk. Some terms commonly used in cryptography are:

- **Plaintext** is the original message that is an input, i.e. unencrypted data.
- **Cipher and Code** - Cipher is a bit-by-bit or character-by-character transformation without regard to the meaning of the message. Code replaces one word with another word or symbol. Codes are not used any more.
- **Cipher text** - It is the coded message or the encrypted data.
- **Encryption** - It is the process of converting plaintext to cipher text, using an encryption algorithm.
- **Decryption** - It is the reverse of encryption, i.e. converting cipher text to plaintext, using a decryption algorithm.

Computer Security

SECURITY MECHANISMS TECHNOLOGIES:

Cryptography: Secret key cryptography, public-key cryptography, hash function
Cryptography uses different schemes for the encryption of data. These schemes constitute a pair of algorithms which creates the encryption and decryption, and a key.

Key is a secret parameter (string of bits) for a specific message exchange context. Keys are important, as algorithms without keys are not useful. The encrypted data cannot be accessed without the appropriate key. The size of key is also important. The larger the key, the harder it is to crack a block of encrypted data. The algorithms differ based on the number of keys that are used for encryption and decryption. The three cryptographic schemes are as follows:

- **Secret Key Cryptography (SKC):** Uses a single key for both encryption and decryption,
- **Public Key Cryptography (PKC):** Public-key cryptography uses two keys—one public key and one private key. Uses one key for encryption and another for decryption,
- **Hash Functions:** Hash functions are one-way encryption algorithms and doesn't use key. This scheme computes a fixed-length hash value based upon the plaintext. Once a hash function is used, it is difficult to recover the contents or length of the plaintext. Uses a mathematical transformation to irreversibly encrypt information.

In all these schemes, algorithms encrypt the plaintext into cipher text, which in turn is decrypted into plaintext.

Computer Security

SECURITY MECHANISMS TECHNOLOGIES:

Cryptography: Secret key cryptography, public-key cryptography, hash function

The different cryptographic schemes are often used in combination for a secure transmission. Cryptography is used in applications like, security of ATM cards, computer passwords, and electronic commerce. Cryptography is used to protect data from theft or alteration, and also for user authentication.

Certification Authorities (CA) are necessary for widespread use of cryptography for e-commerce applications. CAs are trusted third parties that issue digital certificates for use by other parties. A CA issues digital certificates which contains a public key, a name, an expiration date, the name of authority that issued the certificate, a serial number, any policies describing how the certificate was issued, how the certificate may be used, the digital signature of the certificate issuer, and any other information.

Computer Security

SECURITY MECHANISMS TECHNOLOGIES:

> Digital signature: Digital signature algorithms

A signature on a legal, financial or any other document authenticates the document. A photocopy of that document does not count. For computerized documents, the conditions that a signed document must hold are—(1) The receiver is able to verify the sender (as claimed), (2) The sender cannot later repudiate the contents of the message, (3) The receiver cannot concoct the message himself. A digital signature is used to sign a computerized document. The properties of a digital signature are same as that of ordinary signature on a paper. Digital signatures are easy for a user to produce, but difficult for anyone else to forge. Digital signatures can be permanently tied to the content of the message being signed and then cannot be moved from one document to another, as such an attempt will be detectable.

Digital signature scheme is a type of asymmetric cryptography. Digital signatures use the public key cryptography, which employs two keys—private key and public key. The digital signature scheme typically consists of three algorithms:

Computer Security

SECURITY MECHANISMS TECHNOLOGIES:

> Digital signature: Digital signature algorithms

Digital signature scheme is a type of asymmetric cryptography. Digital signatures use the public key cryptography, which employs two keys—private key and public key. The digital signature scheme typically consists of three algorithms:

- Key generation algorithm - The algorithm outputs private key and a corresponding public key.
- Signing algorithm - It takes, message + private key, as input, and, outputs a digital signature.
- Signature verifying algorithm - It takes, message + public key + digital signature, as input, and, accepts or rejects digital signature.

The use of digital signatures typically consists of two processes—Digital signature creation and Digital signature verification. Two methods are commonly used for creation and verification of the digital signatures.

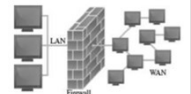
Computer Security

SECURITY MECHANISMS TECHNOLOGIES:

Firewall:

A firewall is a security mechanism to protect a local network from the threats it may face while interacting with other networks (Internet). A firewall can be a hardware component, a software component, or a combination of both. It prevents computers in one network domain from communicating directly with other network domains. All communication takes place through the firewall, which examines all incoming data before allowing it to enter the local network.

1. Functions of firewall,
2. Working principle,
3. Types of firewall
 - a) packet filter firewall,
 - b) circuit filter firewall,
 - c) proxy or application-level firewall)



Computer Security

SECURITY MECHANISMS TECHNOLOGIES:

Firewall:

Functions of Firewall: The main purpose of firewall is to protect computers of an organization (local network) from unauthorized access. Some of the basic functions of firewall are:

- Firewalls provide security by examining the incoming data packets and allowing them to enter the local network only if the conditions are met.
- Firewalls provide user authentication by verifying the username and password. This ensures that only authorized users have access to the local network.
- Firewalls can be used for hiding the structure and contents of a local network from external users. Network Address Translation (NAT) conceals the internal network addresses and replaces all the IP addresses of the local network with one or more public IP addresses.

Computer Security

SECURITY MECHANISMS TECHNOLOGIES:

Firewall: Working of Firewall

The working of firewall is based on a filtering mechanism. The filtering mechanism keeps track of source address of data, destination address of data and contents of data. The filtering mechanism allows information to be passed to the Internet from a local network without any authentication. It makes sure that the downloading of information from the Internet to a local network happens based only on a request by an authorized user.

Computer Security

SECURITY MECHANISMS TECHNOLOGIES:

Firewall: Firewall Related Terminology:

- **Gateway:** The computer that helps to establish a connection between two networks is called gateway. A firewall gateway is used for exchanging information between a local network and the Internet.
- **Proxy Server:** A proxy server masks the local network's IP address with the proxy server IP address, thus concealing the identity of local network from the external network. Web proxy and application-level gateway are some examples of proxy servers. A firewall can be deployed with the proxy for protecting the local network from external network.
- **Screening Routers:** They are special types of router with filters, which are used along with the various firewalls. Screening routers check the incoming and outgoing traffic based on the IP address, and ports.

Computer Security

SECURITY MECHANISMS TECHNOLOGIES:

Firewall: Types of Firewall

All the data that enter a local network must come through a firewall. The type of firewall used varies from network to network. The following are the various types of firewalls generally used:

- Packet filter Firewall
- Circuit Filter Firewall
- Proxy server or Application-level Gateway

Computer Security

SECURITY MECHANISMS TECHNOLOGIES:

Firewall: Types of Firewall: 1. Packet filter Firewall

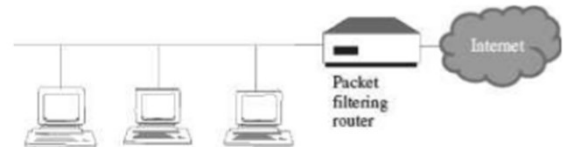
Packet Filter Firewall is usually deployed on the routers. It is the simplest kind of mechanism used in firewall protection.

- It is implemented at the network level to check incoming and outgoing packets.
- The IP packet header is checked for the source and the destination IP addresses and the port combinations.
- After checking, the filtering rules are applied to the data packets for filtering. The filtering rules are set by an organization based on its security policies.
- If the packet is found valid, then it is allowed to enter or exit the local network.
- Packet filtering is fast, easy to use, simple and cost effective.
- A majority of routers in the market provide packet filtering capability. It is used in small and medium businesses.
- Packet filter firewall does not provide a complete solution.

Computer Security

SECURITY MECHANISMS TECHNOLOGIES:

Firewall: Types of Firewall: 1. Packet filter Firewall



Computer Security

SECURITY MECHANISMS TECHNOLOGIES:

Firewall: Types of Firewall: 2. Circuit Filter Firewall

Circuit filter firewalls provide more protection than packet filter firewalls. Circuit filter firewall is also known as a "stateful inspection" firewall.

- It prevents transfer of suspected packets by checking them at the network layer.
- It checks for all the connections made to the local network, in contrast, to the packet filter firewall which makes a filtering decision based on individual packets.
- It takes its decision by checking all the packets that are passed through the network layer and using this information to generate a decision table. The circuit level filter uses these decisions tables to keep track of the connections that go through the firewall.
- For example, when an application that uses TCP creates a session with the remote host, the TCP port number for the remote application is less than 1024 and the TCP port number for the local client is between 1024 and 65535. A packet filter firewall will allow any packet which has a port number within the range 1024 and 65535. However, the circuit filter firewall creates a directory of all outbound TCP connections. An incoming packet is allowed if its profile matches with an entry in the directory for the TCP port numbers.

Computer Security

SECURITY MECHANISMS TECHNOLOGIES:

Firewall: Types of Firewall: 3. Proxy server or Application-level Gateway

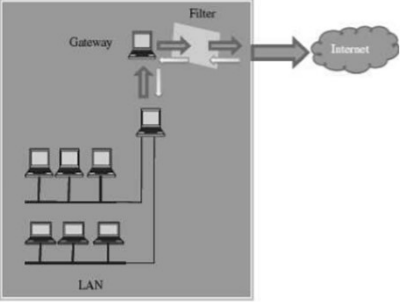
An application-level gateway or a proxy server protects all the client applications running on a local network from the Internet by using the firewall itself as the gateway

- A proxy server creates a virtual connection between the source and the destination hosts.
- A proxy firewall operates on the application layer. The proxy ensures that a direct connection from an external computer to local network never takes place.
- The proxy automatically segregates all the packets depending upon the protocols used for them. A proxy server must support various protocols. It checks each application or service, like Telnet or e-mail, when they are passed through it.
- A proxy server is easy to implement on a local network.
- Application level gateways or proxy server tend to be more secure than packet filters. Instead of checking the TCP and IP combinations that are to be allowed, it checks the allowable applications.

Computer Security

SECURITY MECHANISMS TECHNOLOGIES:

Firewall: Types of Firewall: 3. Proxy server or Application-level Gateway



The diagram illustrates a network architecture where a Local Area Network (LAN) containing several desktop computers is connected to a Gateway. This Gateway is linked to a Filter, which in turn connects to the Internet. This setup represents a Proxy server or Application-level Gateway, which acts as an intermediary between the LAN and the Internet.

Computer Security

SECURITY MECHANISMS TECHNOLOGIES:

Users identification and authentication:

1. User name and password,
2. Smart card
3. Biometrics

Identification is the process whereby a system recognizes a valid user's identity. Authentication is the process of verifying the claimed identity of a user. For example, a system uses user password for identification. The user enters his password for identification. Authentication is the system which verifies that the password is correct, and thus the user is a valid user. Before granting access to a system, the user's identity needs to be authenticated. If users are not properly authenticated then the system is potentially vulnerable to access by unauthorized users. If strong identification and authentication mechanisms are used, then the risk that unauthorized users will gain access to a system is significantly decreased. Authentication is done using one or more combinations of - what you have (like smartcards), what you know (Password), and what you are (Biometrics like Fingerprints, retina scans).

Computer Security

SECURITY MECHANISMS TECHNOLOGIES:

Users identification and authentication:

Authentication mechanisms are:

1. User name and password
2. Smart Card
3. Biometrics—Fingerprints, Iris/retina scan

Once the user is authenticated, the access controls for the user are also defined. Access controls is what the user can access once he is authenticated.

Computer Security

SECURITY MECHANISMS TECHNOLOGIES:

Other security measures:

In addition to the above discussed security techniques, several other security techniques are used for security purposes. Some of these are listed below:

1. Intrusion detection systems,
2. virus protection software,
3. data and information backups,
4. SSL,
5. IPsec protocol

Computer Security

SECURITY MECHANISMS TECHNOLOGIES:

Other security measures: Intrusion detection systems, virus protection software, data and information backups, SSL, IPsec protocol

In addition to the above discussed security techniques, several other security techniques are used for security purposes. Some of these are listed below:

Intrusion Detection Systems : They complement firewalls to detect if internal assets are being hacked or exploited. A Network-based Intrusion Detection monitors real-time network traffic for malicious activity and sends alarms for network traffic that meets certain attack patterns or signatures. A Host-based Intrusion Detection monitors computer or server files for anomalies and sends alarms for network traffic that meets a predetermined attack signature.

Virus Protection Software: They should be installed on all network servers, as well as computers. They screen all software coming into your computer or network system (files, attachments, programs, etc.) preventing a virus from entering into the system.

Computer Security

SECURITY MECHANISMS TECHNOLOGIES:

Other security measures: Intrusion detection systems, virus protection software, data and information backups, SSL, IPsec protocol

Data and Information Backups: It is required for disaster recovery and business continuity. Back-ups should be taken daily and periodically (weekly) and should be kept for at least 30 days while rotating stockpile.

Secure Socket Layer (SSL): is an algorithm developed by Netscape Communications to provide application-independent security and privacy over the Internet. SSL is designed so that protocols such as HTTP, FTP, and Telnet can operate over it transparently. SSL allows both server authentication (mandatory) and client authentication (optional). It uses public-key cryptography (RSA algorithm). HTTP Secure(HTTPS) is an extension to HTTP to provide secure exchange of documents over the WWW

Computer Security

SECURITY MECHANISMS TECHNOLOGIES:

- Other security measures: Intrusion detection systems, virus protection software, data and information backups, SSL, IPsec protocol

IP Security (IPsec) Protocol: The IPsec protocol suite is used to provide privacy and authentication services at the Internet layer. IPv4 is currently the dominant Internet Protocol version. IPv6 is the next-generation Internet Layer protocol for the Internet. IPv6 protocol stacks include IPsec, which allows authentication, encryption, and compression of IP traffic. IPsec can be used to protect any application traffic across the Internet. Applications need not be specifically designed to use IPsec, unlike SSL where the use of SSL must be incorporated into the design of application.

Computer Security

Security Awareness:

The aim of the security awareness is to enhance the security of the organization's resources by improving the awareness of the need to secure the system resources.

Staff members play a critical role in protecting the integrity, confidentiality, and availability of IT systems and networks. It is necessary for an organization to train their staff for security awareness and accepted computer practices.

Security of resources can be ensured when the people using it are aware of the need to secure their resources.

Security awareness of staff includes the knowledge of practices that must be adhered to, for ensuring the security and the possible consequences of not using those security practices.

Computer Security

Security Policy:

- A security policy is a formal statement that embodies the organization's overall security expectations, goals, and objectives with regard to the organization's technology, system and information.
- To be practical and implementable, policies must be defined by standards, guidelines, and procedures. Standards, guidelines, and procedures provide specific interpretation of policies and instruct users, customers, technicians, management, and others on how to implement the policies.
- The security policy states what is, and what is not allowed. A security policy must be comprehensive, up-to-date, complete, delivered effectively, and available to all staff. A security policy must also be enforceable. To accomplish this, the security policy can mention that strict action will be taken against employees who violate it, like disclosing a password.

Computer Security

Security Policy:

- Generally, security policies are included within a security plan. A security plan details how the rules put forward by the security policy will be implemented. The statements within a security
- plan can ensure that each employee knows the boundaries and the penalties of overstepping those boundaries. For example, some rules could be included in the security policy of an organization, such as, to log off the system before leaving the workstation, or not to share the password with other users.
- The security policy also includes physical security of the computers. Some of the measures taken to ensure the physical security of a computer are - taking regular backups to prevent data loss from natural calamity, virus attack or theft, securing the backup media, keeping valuable hardware resources in locked room (like servers), to avoid theft of systems and storage media.

Computer Security

Formulating a Security Policy:

Security policies are defined based on an organization's needs. A security policy includes approaches and techniques that an organization is going to apply or include in order to secure its resources. The steps followed while formulating the security policy are:

1. Analyzing Current Security Policies
2. Identifying IT Assets that Need to be Secure
3. Identifying Security Threats and Likely Security Attacks
4. Defining the Proactive and Reactive Security Strategies

Computer Security

Formulating a Security Policy:

Defining the Proactive and Reactive Security Strategies:

A proactive strategy is a pre-attack strategy. It involves identifying possible damage from each type of attack, determining the vulnerabilities that each type of attack can exploit, minimizing those vulnerabilities and making a contingency plan. A contingency plan specifies the actions to be taken in case an attack penetrates into a system and damages the IT assets of the organization. A contingency plan aims at keeping the computer functional and ensuring the availability, integrity, and confidentiality of data. However, it is not possible for the security administrator to prepare a computer against all attacks. A reactive strategy is implemented on the failure of the proactive strategy. It defines the steps to be taken after the attack. It aims at identifying the cause of attack, vulnerabilities used to attack the system, damage caused by the attack, and repairing of the damage caused by the attack.