19. Virtual Reality

81. Give differences between the following:

1. Mass media and Multimedia
2. Bitmap graphics and Vector graphics
3. Bitmap editor and Vector graphics editor
4. JPEG and GIF image compression
5. Streaming video and Surround video

14

COMPUTER SECURITY

Contents

- 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
    - 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)

Why this chapter

Individual users, organizations, and enterprises use the computers for keeping their data that is critical to their business and personal use. Also, they use the network (Internet) for the transmission of data. Since data is critical to the owner, there is a need to keep the computers storing the data and the network (Internet) over which the data is transmitted, secure. You 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”.

14.1 INTRODUCTION

We all like to be secure in our home, office, locality, city, country, and in this world. We use different mechanisms to ensure our security. Inside our homes, we keep our valuables safely locked in a cupboard that is accessible by the elders of the house; we keep the gates of our house bolted and even have an intrusion-detection system installed. We have high walls and gates surrounding our locality and also a watchman who guards the open gates. We have police for our security within a city and armed forces for the country. We take all these measures to make ourselves and our valuables, resources, possessions secure.

The widespread use of computers has resulted in the emergence of a new area for security—security of computer. Computer security is needed to protect the computing system and to protect the data that they store and access. Transmission of data using network (Internet) and communication links has necessitated the need to protect the data during transmission over the network. Here, we use the term computer security to refer to both the computer security and the network security.

Computer security focuses on the security attacks, security mechanisms and security services.

- *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.

The purpose of computer security is to provide reliable security services in the environments suffering security attacks, by using security mechanisms. The security services use one or more security mechanism(s).

This chapter discusses the different security threats and security attacks from malicious software and hackers. The chapter highlights the security services. The security mechanisms like cryptography, digital signatures, and firewalls are discussed in detail. The need for security awareness and the security policy in an organization is also emphasized.

14.2 SECURITY THREAT AND SECURITY ATTACK

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. For example, if we leave the house lock open—it is vulnerable to theft; an intruder in our locality (might exploit the open lock)is a security threat; the intruder comes to know of the open lock and gets inside the house—This is a security attack.

A security attack may be a passive attack or an active attack.

- The aim of a *passive attack* is to get information from the system but it does not affect the system resources. Passive attacks are similar to eavesdropping (Figure 14.1). 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.

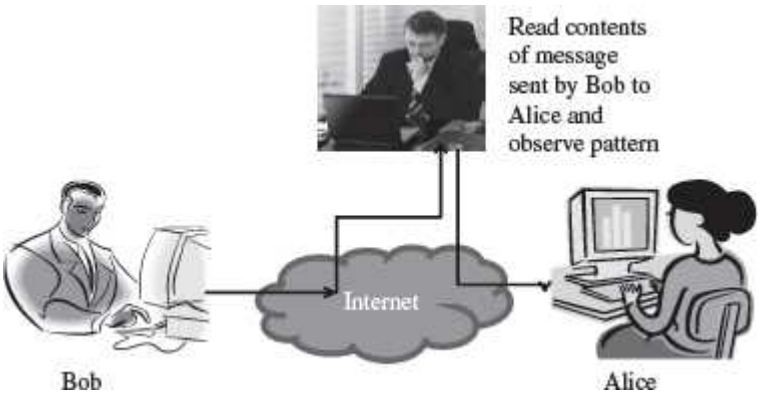

Figure 14.1 Passive attack

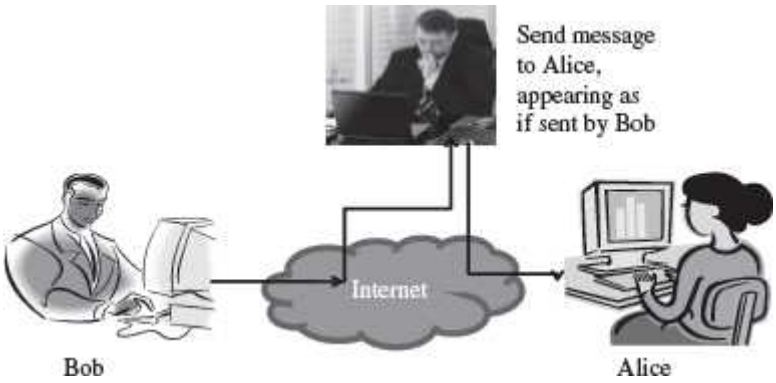

Figure 14.2 Active attack (masquerade)

- An *active attack* tries to alter the system resources or affect its operations. Active attack may modify the data or create a false data (Figure 14.2). 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.

Security attacks can be on users, computer hardware and computer software (Figure 14.3).

- *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 into another computer or network to perform an illegal act.

This chapter will discuss the malicious software and hacking in detail.

Figure 14.3 Security attacks

14.3 MALICIOUS SOFTWARE

Malicious users use different methods to break into the systems. 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. Javascripts and Java applets written with the purpose of attacking, are also malicious programs.

14.3.1 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.
- 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".

14.3.2 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".

14.3.3 Trojan Horse

Trojan horse is destructive programs that masquerade as useful programs. The name "Trojan horse" is given because of the Greek soldiers who reached the city of Troy by hiding themselves inside a large wooden horse (Figure 14.4). The people of the city of Troy themselves pulled the horse inside their city, unaware of the fact that the Greek soldiers were hiding inside the horse. Similarly, 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.

Figure 14.4 Trojan horse

14.3.4 Javascripts, Java Applets and ActiveX Controls

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 (Figure 14.5).

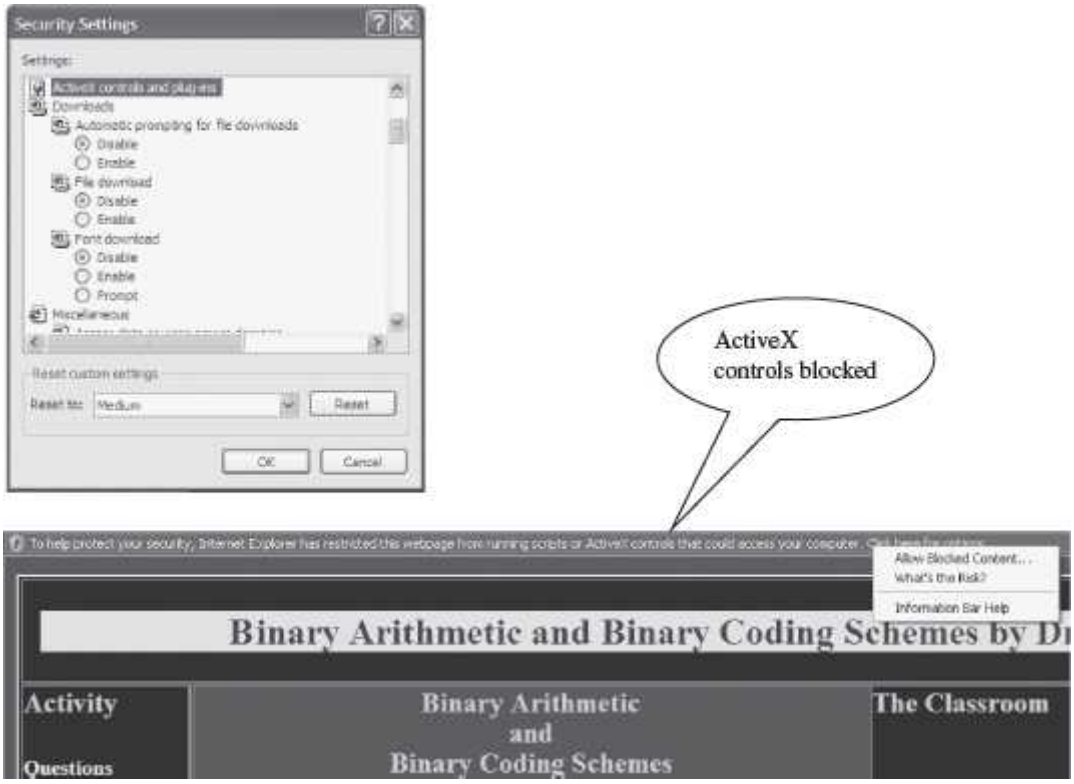

Figure 14.5 (a) Making security settings in Windows XP (b) ActiveX control popup in Internet

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.

14.4 HACKING

Hacking is the act of intruding into someone else's computer or network. A hacker is someone who does hacking. Hacking may result in a *Denial of Service (DoS) attack*. The DoS attack prevents authorized users from accessing the resources of the computer. It aims at making the

computer resource unusable or unavailable to its intended users. It targets the computer and its network connections, to prevent the user from accessing email, web sites, online accounts (banking, etc.), or other services that rely on the affected computer. 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.

14.4.1 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.

14.4.2 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.

14.4.3 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.

14.5 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.
- **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.
- **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.

14.6 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 attacked 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.

14.7 CRYPTOGRAPHY

Cryptography is the science of writing information in a “hidden” or “secret” form and is an ancient art. 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.

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): Uses one key for encryption and another for decryption,
- Hash Functions: 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.

14.7.1 Secret Key Cryptography

- Secret key cryptography uses a single key for both encryption and decryption. The sender uses the key to encrypt the plaintext and sends the cipher text to the receiver. The receiver applies the same key to decrypt the message and recover the plaintext (Figure 14.6). Since a single key is used for encryption and decryption, secret key cryptography is also called *symmetric encryption*.

Figure 14.6 Secret key cryptography (uses a single key for both encryption and decryption)

- Secret key cryptography scheme are generally categorized as *stream ciphers or block ciphers*.
- *Stream ciphers* operate on a single bit (byte or computer word) at a time and implement some form of feedback mechanism so that the key is constantly changing.

- *Block cipher* encrypts one block of data at a time using the same key on each block. In general, the same plaintext block will always encrypt to the same cipher text when using a same key in a block cipher.
- Secret key cryptography requires that the key must be known to both the sender and the receiver. The drawback of using this approach is the distribution of the key. Any person who has the key can use it to decrypt a message. So, the key must be sent securely to the receiver, which is a problem if the receiver and the sender are at different physical locations.
- Data Encryption Standard (DES) and Advanced Encryption Standard (AES) are some of the secret key cryptography algorithms that are in use nowadays.

14.7.2 Public-Key Cryptography

- Public-key cryptography facilitates secure communication over a non-secure communication channel without having to share a secret key.
- Public-key cryptography uses two keys—one public key and one private key.
- The public key can be shared freely and may be known publicly.
- The private key is never revealed to anyone and is kept secret.
- The two keys are mathematically related although knowledge of one key does not allow someone to easily determine the other key.

Figure 14.7 Public key cryptography (uses two keys—one for encryption and other for decryption)

- The plaintext can be encrypted using the public key and decrypted with the private key and conversely the plaintext can be encrypted with the private key and decrypted with the public key. Both keys are required for the process to work (Figure 14.7). Because a pair of keys is required for encryption and decryption; public-key cryptography is also called *asymmetric encryption*.
- Rivest, Shamir, Adleman (RSA) is the first and the most common public-key cryptography algorithm in use today. It is used in several software products for key exchange, digital signatures, or encryption of small blocks of data. The Digital Signature Algorithm (DSA) is used to provide digital signature capability for the authentication of messages.

14.7.3 Hash Functions

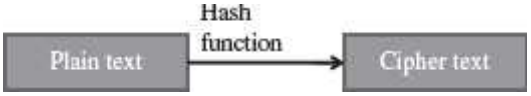

Figure 14.8 Hash function (have no key since plain text is not recoverable from cipher text)

- Hash functions are one-way encryption algorithms that, in some sense, use no 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 (Figure 14.8).

- Hash functions are generally used to ensure that the file has not been altered by an intruder or virus. Any change made to the contents of a message will result in the receiver calculating a different hash value than the one placed in the transmission by the sender.
- Hash functions are commonly employed by many operating systems to encrypt passwords. Message Digest (MD) algorithm and Secure Hash Algorithm (SHA) are some of the common used hash algorithms.

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.

14.8 DIGITAL SIGNATURE

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:

- *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 (Figure 14.9). Two methods are commonly used for creation and verification of the digital signatures.

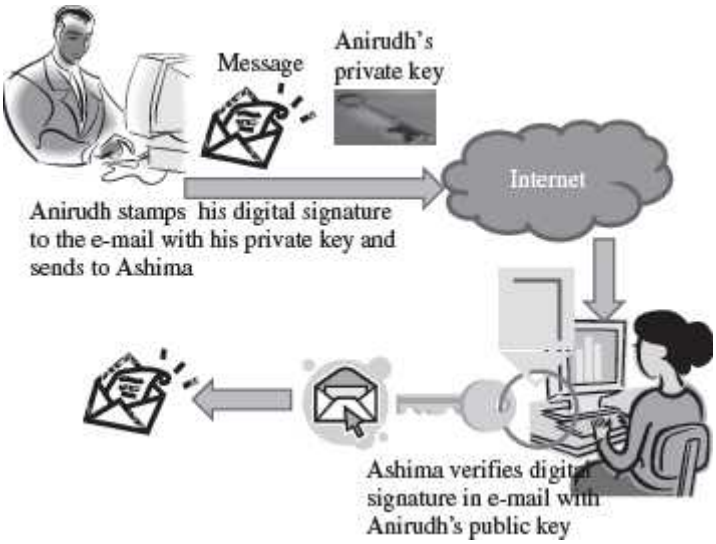

Figure 14.9 Digital signature

- In the First Method, the signer has a private key and a public key. For a message to be sent, the signer generates the digital signature by using the private key to encrypt the message. The digital signature along with the message is sent to the receiver. The receiver uses the public key (known to the receiver) to verify the digital signature. This method is used to verify the digital signature. Even if many people may know the public key of a given signer and use it to verify that signer's signature, they cannot generate the signer's private key and use it to forge digital signatures.
- In the Second Method, a hash function is used for digital signature. It works as follows:
    - Digital signature creation
        - The signer has a private key and a public key.
        - For a message to be sent, a hash function in the signer's software computes an "original hash result" unique to the "original message".
        - The signer uses signing algorithm to generate a unique digital signature. "original hash result" + signer's private key = digital signature.
    - The generated digital signature is attached to its "original message" and transmitted with it.
    - *Digital signature verification* uses digital signature, "received message" and signer's public key.
        - A "new hash result" of the "received message" is computed using the same hash function used for the creation of the digital signature.
        - The verification software verifies two things—whether the digital signature was created using the signer's private key and, whether the "received message" is unaltered. For this, the signer's public key verifies the digital signature (signer's public key can only verify a digital signature created with the signer's private key). Once the key is verified, the "original hash result" of the digital signature is available. It compares "original hash result" with the "new hash result". When the verification software verifies both the steps as "true"; it verifies the received message.

The digital signature accomplish the effects desired of a signature for many legal purposes:

- ***Signer Authentication:*** The digital signature cannot be forged, unless the signer loses control of the private key.
- ***Message Authentication:*** The digital signature verification reveals any tampering, since the comparison of the hash results shows whether the message is the same as when signed.
- ***Efficiency***. The digital signatures yield a high degree of assurance (as compared to paper methods like checking specimen signatures) without adding much to the resources required for processing.

The likelihood of malfunction or a security problem in a digital signature cryptosystem, designed and implemented as prescribed in the industry standards, is extremely remote. Digital signatures have been accepted in several national and international standards developed in cooperation with and accepted by many corporations, banks, and government agencies. In India "Information Technology Act 2000" provides legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involves the use of alternatives to paper based methods of communication and storage of information, to facilitate electronic filing of documents with the government agencies.

14.9 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 (Figure 14.10).

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 (Figure 14.11).
- 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.

Figure 14.10 (a) Windows firewall icon in control panel (b) Windows firewall setting (c) Security center

The local network uses a single network interface to interact with the server. Local network clients use IP addresses that are not attached to any computer. When a client sends a packet to the Internet, the masquerading server replaces the IP address of the packet with its own IP address. When a packet is received by local network, the server replaces the IP address of the packet with the masqueraded address and sends the packet to the respective client.

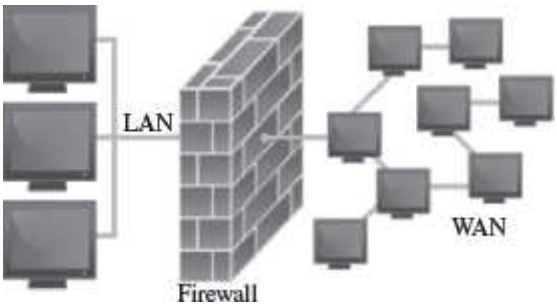

Figure 14.11 Firewall

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.

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.

14.9.1 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

14.9.1.1 Packet Filter Firewall

Packet Filter Firewall is usually deployed on the routers (Figure 14.12). It is the simplest kind of mechanism used in firewall protection.

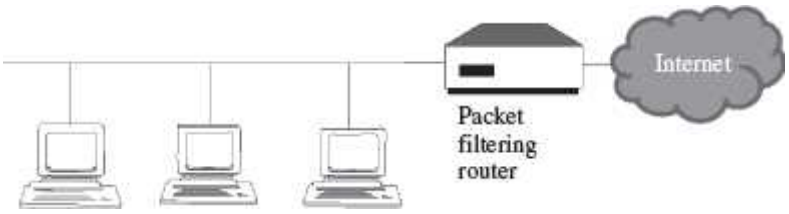

Figure 14.12 Packet fi Itering

- 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.

14.9.1.2 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.

14.9.1.3 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 (Figure 14.13).

- 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.

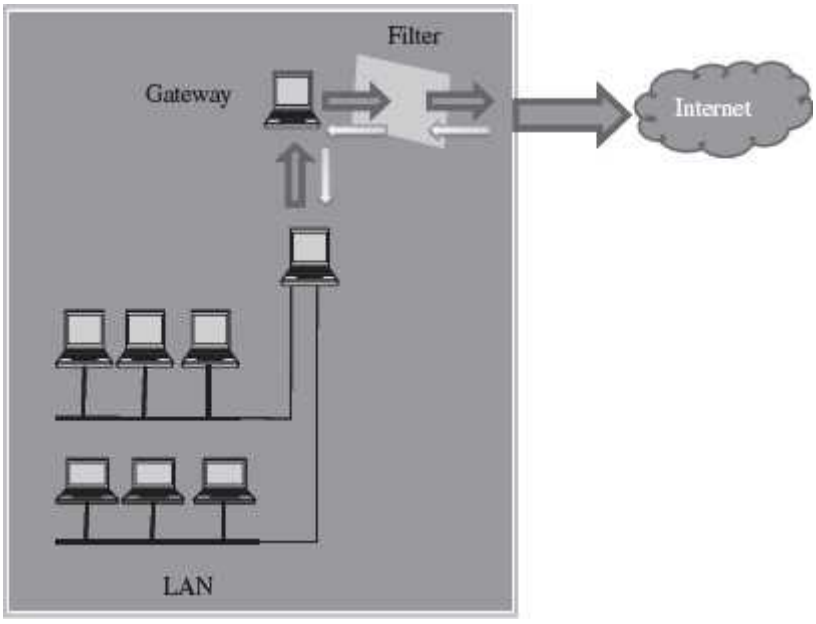

Figure 14.13 Application-level gateway

14.10 USERS IDENTIFICATION AND AUTHENTICATION

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).

We will now briefly discuss the following authentication mechanisms:

- User name and password
- Smart Card
- 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.

14.10.1 User Name and Password

The combination of username and password is the most common method of user identification and authentication. The systems that use password authentication first require the user to have a username and a password. Next time, when the user uses the system, user enters their username and password. The system checks the username and password by comparing it to the stored password for that username. If it matches, the user is authenticated and is granted access to the system (Figure 14.14).

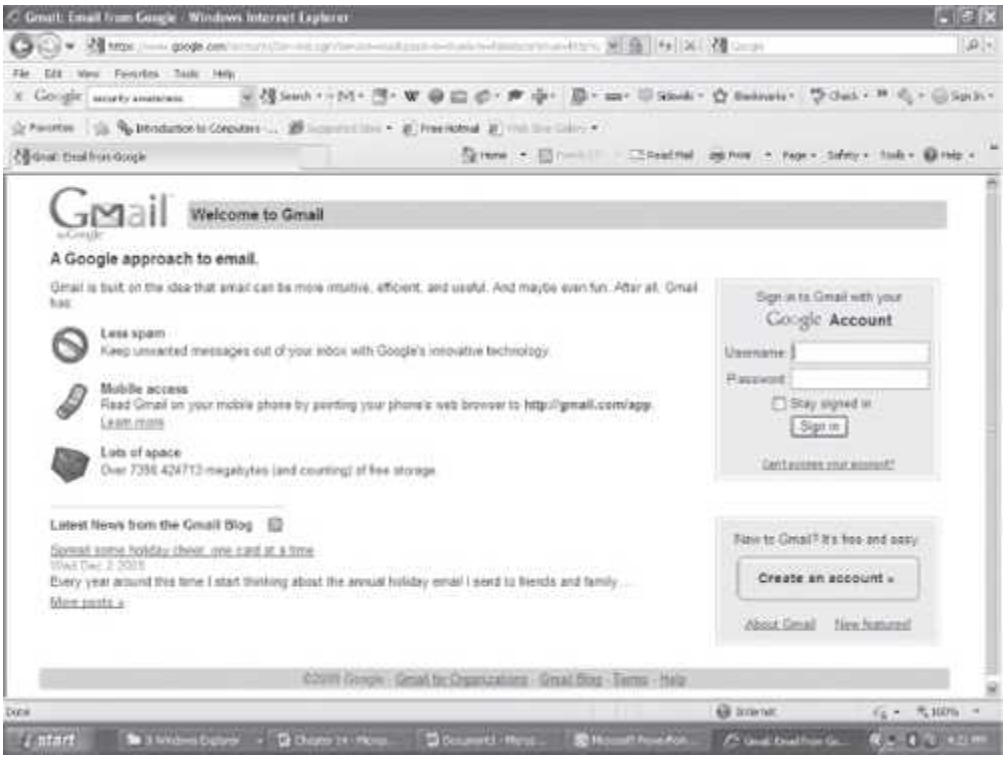

Figure 14.14 User authentication page

However, there are several security issues with the use of password, like, any invalid user if gets to know of a valid password can get access to the system, a simple password can be easily cracked etc. According to CERT, approximately 80% of all network security issues are caused by bad passwords. Some actions that can be taken to make the passwords safer are as follows:

- It is good to change passwords periodically. This decreases chances of cracking passwords.
- Make a password complex, like mix case, use numbers and special characters. This decreases ability of automated attacks by increasing possible character combinations.
- Use longer passwords so as to create exponentially higher number of permutations and combinations of characters used, making them difficult to break.
- Be cautious not to leave passwords lying around and don't share them with friends.
- Do not use your or your families' name, age, address, city etc., as part of the passwords.

Nearly all modern multiuser computer and network operating systems, at the very least, employ passwords to protect and authenticate users accessing computer and network resources. The passwords are not kept in plaintext, but are generally encrypted using some sort of hash scheme. For example, In Unix/ Linux, all passwords are hashed and stored as a 13-byte string. In Windows NT, all passwords are hashed resulting in a 16-byte hash value.

14.10.2 Smart Card

A smart card is in a pocket-sized card with embedded integrated circuits which can process data. With an embedded microcontroller, smart cards have the unique ability to store large amounts of

data, carry out their own on-card functions (e.g. encryption and mutual authentication) and interact intelligently with a smart card reader. A smart card inserted into a smart card reader makes a direct connection to a conductive contact plate on the surface of the card (typically gold plated). Transmission of commands, data, and card status takes place over these physical contact points.

The smart card is made of plastic, generally PVC. The card may embed a hologram. Using smart cards is a strong security authentication for single sign-on within large companies and organizations. Smart cards are used in secure identity applications like employee-ID badges, citizen-ID documents, electronic passports, driver license and online authentication devices.

14.10.3 Biometric Techniques

Biometrics is the science and technology of measuring and statistically analyzing biological data. In information technology, biometrics refers to technologies that measures and analyzes human traits for authentication. This can include fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements, for authentication purposes. Figure 14.15 shows a fingerprint biometric device.

Biometrics is still not widely used, though it may play a critical role in future computers. For example, many PCs nowadays include a fingerprint scanner where you could place your index finger. The computer analyzes the fingerprint to determine your identity and authenticate you. Biometric systems are relatively costly and are used in environments requiring high-level security.

In the Hindi movie *Krissh*, the computer identified and authenticated the heartbeat (Biometric) of *Hrithik Roshan* to start working.

Figure 14.15 Biometric device (fingerprint)

14.11 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:

- **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.
- **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
- **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.

14.12 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. For example, not disclosing your password to unauthorized users is a security practice, but if the users are not aware of the possible consequences of disclosing the password, they may disclose their password to other users, unintentionally, thus making their systems prone to security attack. In order to make the users and people in an organization aware of the security practices to be followed, regular training programs are conducted in organizations. Awareness is also promoted by regular security awareness sessions, videotapes, newsletters, posters, and flyers. Figure 14.16 shows a poster for security awareness.

Figure 14.16 Security awareness (A poster)

14.13 SECURITY POLICY

- A *securitypolicy* 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.
- 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.

14.13.1 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:

- *Analyzing Current Security Policies*—The vulnerabilities and the current security policies must be analyzed by the security administrators before defining an effective security policy. The security administrator is required to study the existing documents containing details of the physical security policies, network security policies, data security policies, disaster recovery plans, and contingency plans.
- *Identifying IT Assets that Need to be Secure*—The security administrator must identify the IT resources of an organization that need to be secure. It may include the following:
    - Physical resources like computers, servers like database servers and web servers, local networks that are used to share the local computer with the remote computer, private networks shared by two or more organizations, corporate network permanently connected to the Internet, laptop, manuals, backup media, communication equipment, network cables, and CDs.
    - Information resources like password, data, or applications. The data of an organization can be classified for security purposes based upon the sensitivity and the integrity of data. For example, public information, internal information, confidential information, and secret information
- *Identifying Security Threats and Likely Security Attacks*—After identifying the IT assets and classifying them, a security administrator must identify the various security threats to the assets. For example, in a bank the security threat to the database storing the account details of the customers may be—unauthorized access to information, attacks of viruses, worms and Trojan horses, natural disasters like earthquake, fire etc.
- *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.

SUMMARY

- *Computer security* protects the data stored on the computing system and the data transmitted over a network. It focuses on security attacks, security mechanisms and security services.
- A *security threat* is a potential violation of security and causes harm.
- *Vulnerability* is a weakness of system that is left unprotected and is exposed to threats.
- *Security attacks* are the reasons for breach of security.
- *Malicious software or malware* is a software code intentionally included into a system with the intention to harm the system. Viruses, Trojan horses, Worms, and, Javascripts, Java applets, and activeX controls written with the purpose of attacking are malicious programs.
- *Hacking* is intruding into another computer or network to perform an illegal act.
- *DoS attack* makes the computer resource unusable or unavailable to its intended users thus preventing authorized users from accessing the resources on the computer.
- 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*.
- *Security service* provides specific kind of protection to system resources. Security service ensures confidentiality, integrity, authentication, and non-repudiation of data. It provides assurance for access control and availability of the resources to its authorized users.
- *Security mechanisms* are tools that include algorithms, protocols or devices, that are designed to detect, prevent or recover from a security attack. They use cryptography, digital signature, firewall, user identification and authentication as countermeasures for security attack.
- *Cryptography* encrypts the data to protect the data in transit over a network. Cryptography schemes use a pair of algorithms for encryption and decryption, and a key. Secret key cryptography, Public-key cryptography, and hash functions are some cryptographic schemes.
- *Secret key cryptography or symmetric encryption* uses a single key for both encryption and decryption. It is difficult to distribute the key securely to the receiver if the receiver and the sender are at different physical locations.
- *Public-key cryptography or asymmetric encryption* uses a pair of keys—public key and private key, for encryption and decryption. The public key is shared freely, but private key is kept secret.
- *Digital signatures* are used to sign a computerized document. The digital signature scheme consists of key generation algorithm, signing algorithm and signature verifying algorithm.
- A *firewall* protects a local network from the threats it may face while interacting with other networks (Internet). Gateway, proxy server and screening routers are used as firewall.
- In *username and password authentication*, the system checks the username and password by comparing it to the stored password for that username.
- A *smart card* is a pocket-sized card with strong security authentication for single sign-on.
- *Biometrics* measures and analyzes human traits like fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements, for authentication.
- Intrusion Detection Systems, Virus Protection software, Data and Information Backups, SSL, and IPsec protocol are *other security techniques* used for security purposes.
- The aim of *security awareness* is to enhance security of the organization's resources by improving the awareness of the need to secure system resources.
- *Security policy* states the management's overall security expectations, goals and objectives with regard to the organization's technology, system, and information.
- A *securityplan* specifies how the rules put forward by security policy will be implemented.

KEYWORDS

Active attack
ActiveX controls
Application-level Gateway
Asymmetric encryption
Authentication
Biometrics
Block ciphers
Certification Authorities (CA)
Cipher
Cipher text
Circuit Filter Firewall
Code
Computer security
Confidentiality
Cryptography
Decryption
Denial of Service (DoS)
Digital signature
Digital Signature Algorithm (DSA)
E-mail hacking
Encryption
Firewall
Gateway
Hacking
Hash Function
HTTP Secure (HTTPS)
Integrity
Intrusion Detection System
IP Security (IPsec) Protocol
Java applets
Javascripts
Key
Malicious software
Malware
Network Address Translation (NAT)
Non-Repudiation
Packet filter Firewall
Packet replay
Packet sniffing
Passive attack
Password
Password cracking
Plaintext
Private key
Proxy Server
Public key
Public Key Cryptography (PKC)
RSA
Screening routers
Secret Key Cryptography (SKC)
Secure Socket Layer (SSL)
Security attacks
Security awareness
Security mechanisms
Security plan
Security policy
Security services
Security threat
Smart card
Stream ciphers
Symmetric encryption
Trojan horse
User identification
User name
Viruses
Virus Protection software
Vulnerability
Worms

QUESTIONS

Section 14.2

1. What do you understand by the term Computer security?

2. Define: (i) Security attack, (ii) Security mechanism, and (iii) Security service.

3. Define: (i) Security threat, (ii) Vulnerability, (iii) Passive attack, and (iv) Active attack.

4. A security attack may be a _____ attack or a _____attack.

5. What are the targets of the security attack?

6. List some security attacks that can be made on the users of the computer.

7. List some security attacks that can be made on the computer hardware.

8. What kind of attacks can be made on the computer software?

Section 14.3

9. What is malicious software?

10. Give three examples of malicious programs.

11. List some properties of virus.

12. How can virus harm the computer?

13. Give an example of virus program.

14. Define a worm.

15. Give an example of a worm program.

16. What are Trojan horses?

17. Why is it advisable to keep the active control disabled on your computer?

Section 14.4

18. Define hacking.

19. What is a Denial of Service attack?

20. _____, _____and_____are the methods used to get the username and password of the system to gain unauthorized access to the system.

21. What do you mean by packet sniffing?

22. Name one packet sniffer software.

23. How does a password cracker work?

24. How is e-mail hacked?

Section 14.6

25. Security services ensure_____, _____ _____and _____of the data.

26. Define (i) Confidentiality, (ii) Integrity, (iii) Authentication, and (iv) Non-Repudiation.

27. _____is used for ensuring confidentiality.

28. Name any two methods that are used for authentication.

29. Non-repudiation deals with_____.

30. List three technologies used for implementing the security mechanisms.

Section 14.7

31. Define cryptography.

32. Define (i) Plain text, (ii) Cipher, (iii) Cipher text, (iv) Encryption, and (v) Decryption.

33. Define a key.

34. What is the significance of key in cryptography?

35. Name the three cryptographic schemes.

36. Why secret key cryptography is also called symmetric encryption?

37. Explain the working of Secret key cryptography.

38. What is the difference between a stream cipher and block cipher?

39. Name a secret key cryptography algorithm.

40. In public key cryptography, how is the public key different from the private key?

41. Why public key cryptography is also called asymmetric encryption?

42. Name a public key cryptography algorithm.

43. _____algorithm is used to provide digital signature.

44. What is the purpose of hash function?

45. Name a hash algorithm.

46. What is the function of Certification Authorities (CA)?

Section 14.8

47. What is the use of digital signature?

48. Is digital signature scheme a symmetric cryptography or asymmetric cryptography?

49. Name the three algorithms included in a digital signature scheme.

50. Explain the digital signature creation and verification using hash function.

51. Signer authentication, Message authentication, and Efficiency are three effects accomplished by digital signature. Explain.

Section 14.9

52. What is the purpose of firewall?

53. List the functions of firewall.

54. Explain the working of firewall.

55. Define: (i) Gateway, (ii) Proxy Server, and (iii) Screening Routers.

56. Name the three types of firewall.

57. How does the Packet filter Firewall work?

58. How does the Circuit Filter Firewall work?

59. How does the Application-level Gateway work?

Section 14.10—14.11

60. What is the difference between user identification and user authentication?

61. Name three authentication mechanisms.

62. Explain user identification and authentication.

63. What is the need of user authentication?

64. List some steps to make the password safe.

65. What is a smart card?

66. Name three areas where smart card is commonly used.

67. How does biometric technique help in user authentication?

68. What is the purpose of intrusion detection system?

69. What is the need of installing virus protection software on your computer?

70. What is the need of taking regular data and information backups?

71. How is HTTPS different from HTTP?

72. IPv6 protocol includes network security. Explain.

Section 14.12

73. What is the need of spreading security awareness?

74. What is a security policy?

75. What is the need of a security plan?

76. List the steps followed in formulating the security policy.

77. Explain in detail the formulation of security policy.

78. What IT resources need to be made secure in an organization?

79. What is the purpose of proactive security strategy?

80. What is the purpose of reactive security strategy?

Extra Questions

81. Give full form of the following abbreviations:

1. DoS
2. SKC
3. PKC
4. DES
5. AES
6. DSA
7. sha
8. ca
9. nat
10. SSL
11. IPsec

82. Write short notes on:

1. Security attack
2. Malicious software
3. Viruses
4. Trojan horse
5. Worms
6. Hacking
7. Security services
8. Cryptography
9. Secret key cryptography
10. Public-key cryptography
11. Digital signature
12. Firewall
13. Types of firewall
14. User identification and authentication
15. User authentication mechanisms
16. User name and Password
17. Security awareness
18. Security Policy
19. Formulating a security policy

83. Give differences between the following:

1. Passive security attack and Active security attack
2. Viruses and Worms
3. Malicious software and Hacking
4. Secret Key Cryptography and Public-Key Cryptography
5. Packet filter firewall and Circuit Filter firewall
6. Users identification and User authentication
7. Proactive Security Strategy and Reactive Security Strategy

Unit IV

COMPUTER PRACTICALS

15

WINDOWS XP

Contents