CHAPTER

14

COMPUTER SECURITY

Computer security is also known as **cyber security** or **IT security**. It is a branch of information technology known as **information security**, which is intended to protect computers.

Sources of Cyber Attack

The most potent and vulnerable threat to computer users is virus attacks. A computer virus is a small software program that spreads from one computer to another and that interferes with computer operation.

The sources of cyber attack can be as follows

1. **Downloadable Programs** Downloadable files are one of the best possible sources of virus. Any type of executable file like games, screen saver are one of the major sources.

   If you want to download programs from the Internet, then it is necessary to scan every program before downloading them.
2. **Cracked Software** These softwares are another source of virus attacks. Such cracked forms of illegal files contain virus and bugs that are difficult to detect as well as to remove. Hence, it is always a preferable option to download software from the appropriate source.
3. **E-mail Attachments** These attachments are the most common source of viruses. You must handle E-mail attachments with extreme care, especially if the E-mail comes from an unknown sender.
4. **Booting from Unknown CD** When the computer system is not working, it is a good practice to remove the CD. If you do not remove the CD, it may start to boot automatically from the disk which enhances the possibility of virus attacks.

Methods to Provide Protection

There are four primary methods to provide protection

1. **System Access Control** It ensures that unauthorised users do not get into the system by encouraging authorised users to be security conscious.
2. **Data Access Control** It monitors who can access the data, and for what purpose. The system determines access rules based on the security levels of the people, the files and the other objects in your system.

3. **System and Security Administration** It performs offline procedures that make or break secure system.
4. **System Design** It takes advantage of basic hardware and software security characteristics.

Components of Computer Security

Computer security is associated with many core areas.

Basic components of computer security system are as follows

1. **Confidentiality** It ensures that data is not accessed by any unauthorised person.
2. **Integrity** It ensures that information is not altered by any unauthorised person in such a way that it is not detectable by authorised users.
3. **Authentication** Verification of a login name and password is known as authentication. It ensures that users are the persons they claim to be.
4. **Access Control** It ensures that users access only those resources that they are allowed to access.
5. **Non-Repudiation** It ensures that originators of messages cannot deny that they are not sender of the message.
6. **Availability** It ensures that systems work promptly and service is not denied to authorised users.
7. **Privacy** It ensures that individual has the right to use the information and allows another to use that information.
8. **Stenography** It is an art of hiding the existence of a message. It aids confidentiality and integrity of the data.
9. **Cryptography** It is the science of writing information in a 'hidden' or 'secret' form and in an ancient art. It protects the data during transmission and also the data stored on the disk.

   Some terms commonly used in cryptography are as follows

   (i) **Plain text** is the original message that is an input.

   (ii) **Cipher** is a bit-by-bit or character-by-character transformation without regard to the meaning of the message.

   (iii) **Cipher text** is the coded message or the encrypted data.

   (iv) **Encryption** is the process of converting plain text to cipher text, using an encryption algorithm. The scrambling of code is known as encryption.

   (v) **Decryption** is the reverse of encryption, i.e. converting cipher text to plain text.

Malware

Malware stands for Malicious Software. It is a broad term that refers to a variety of malicious programs that are used to damage computer system, gather sensitive information or gain access to private computer systems.

It includes computer viruses, worms, trojan horses, rootkits, spyware, adware, etc.

Some of them are described below

VIRUS

VIRUS stands for Vital Information Resources Under Siege. Computer viruses or perverse softwares are small programs that can negatively affect the computer. It obtains control of a PC and directs it to perform unusual and often destructive actions.

Viruses are copied itself and attached itself to other programs which further spread the infection. The virus can affect or attack any part of the computer software such as the boot block, operating system, system areas, files and application programs.

Note • *The first computer virus, creeper was a self-replicating program written in 1971 by Bob Thomas at VBN Technologies.*

• *The first boot sector PC virus named Brain, which was identified in the year 1986.*

Effects of VIRUS

There are many different effects that viruses can have on your computer, depending on the types of virus. *Some viruses can*

(i) monitor what you are doing.
(ii) slow down your computer's performance.
(iii) destroy all data on your local disk.
(iv) affect on computer networks.
(v) increase or decrease memory size.
(vi) display different types of error messages.
(vii) decrease partition size.
(viii) alter PC settings.
(ix) display arrays of annoying advertising.
(x) extend boot times.
(xi) create more than one partition.

Worm

A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. Worms are hard to detect because they are invisible files.

For example, Bagle, I love you, Morris, Nimda, etc.

Note *Payload is a code designed in the form of a worm and for the purpose of expanding on a larger scale than the worm.*

Trojan

A Trojan, or Trojan Horse, is a non-self-replicating type of malware which appears to perform a desirable function but instead facilitates unauthorised access to the user's computer system.

Trojans do not attempt to inject themselves into other files like a computer virus. Trojan horses may steal information, or harm their host computer systems.

Trojans may use drive by downloads or install *via* online games or Internet driven applications in order to reach target computers. Unlike viruses, Trojan Horses do not replicate themselves.

For example, Beast, Sub7.Zeus, ZeroAccess Rootkit, etc.

Spyware

It is a program which is installed on a computer system to spy on the system owner's activity and collects all the information which is misused afterwards. It tracks the user's behaviour and reports back to a central source.

These are used for either legal or illegal purpose. Spyware can transmit personal information to another person's computer over the Internet.

For example, CoolWeb Search, FinFisher, Zango, Zlob Trojan, Keyloggers, etc.

Symptoms of Malware Attack

There is a list of symptoms of malware attack which indicates that your system is infected with a computer malware.

Some primary symptoms of malware attack are as follows

(i) Odd messages are displaying on the screen.
(ii) Some files are missing.
(iii) System runs slower.
(iv) PC crashes and restarts again and again.
(v) Drives are not accessible.
(vi) Anti-virus software will not run or installed.
(vii) Unexpected sound or music plays.
(viii) The mouse pointer changes its graphic.
(ix) System receives strange E-mails containing odd attachments or viruses.
(x) PC starts performing functions like opening or closing window, running programs on its own.

Some Other Threats to Computer Security

There are some other threats to computer security, which are described below

1. **Spoofing** It is the technique to access the unauthorised data without concerning to the authorised user. It accesses the resources over the network. It is also known as **Masquerade**.

   IP spoofing is a process or technique to enter in another computer by accessing its IP address.
2. **Salami Technique** It diverts small amounts of money from a large number of accounts maintained by the system.

3. **Hacking** It is the act of intruding into someone else's computer or network. Hacking may result in a Denial of Service (DoS) attack.

   It prevents authorised users from accessing the resources of the computer. A hacker is someone, who does hacking process.

4. **Cracking** It is the act of breaking into computers. It is a popular, growing subject on Internet.

   Cracking tools are widely distributed on the Internet. They include password crackers, trojans, viruses, war-dialers, etc.

Note *Cyber cracker is a person called who uses a computer to cause harm to people or destroy critical systems.*

5. **Phishing** It is characterised by attempting to fraudulently acquire sensitive information such as passwords, credit cards details, etc., by masquerading as a trustworthy person.
6. **Spam** It is the abuse of messaging systems to send unsolicited bulk messages in the form of E-mails. It is a subset of electronic spam involving nearly identical messages sent to numerous recipients by E-mails.
7. **Adware** It is any software package which automatically renders advertisements in order to generate revenue for its author. The term is sometimes used to refer the software that displays unwanted advertisements.
8. **Rootkit** It is a type of malware that is designed to gain administrative level control over a computer system without being detected.

Solutions to Computer Security Threats

Some safeguards (or solutions) to protect a computer system from accidental access are described below

Anti-virus Software

It is an application software that is designed to prevent, search for, detect and remove viruses and other malicious softwares like worms, trojans, adware and more.

It consists of computer programs that attempt to identify threats and eliminate computer viruses and other malware.

Some popular anti-viruses are

(i) Avast
(ii) Avg
(iii) K7
(iv) Kaspersky
(v) Trend Micro
(vi) Quick Heal
(vii) Symantec
(viii) Norton
(ix) McAfee

Digital Certificate

It is the attachment to an electronic message used for security purposes. The common use of a digital certificate is to verify that a user sending a message is who he or she claims to be, and to provide the receiver with the means to encode a reply.

Digital Signature

It is an electronic form of a signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and also ensure that the original content of the message or document that has been sent is unchanged.

Firewall

It can either be software based or hardware based and is used to help in keeping a network secure. Its primary objective is to control the incoming and outgoing network traffic by analysing the data packets and determining whether it should be allowed through or not, based on a pre-determined rule set.

A network's firewall builds a bridge between an internal network that is assumed to be secure and trusted, and another network, usually an external (inter) network, such as the Internet, that is not assumed to be secure and trusted. A firewall also includes or works with a proxy server that makes network requests on behalf of work station users.

Password

It is a secret word or a string of characters used for user authentication to prove identity or approval to gain access to a resource.

A password is typically somewhere between 4 to 16 characters, depending on how the computer system is setup. When a password is entered, the computer system is careful not to display the characters on the display screen, in case others might see it.

There are two common modes of password as follows

(i) **Weak Password** Easily remember just like names, birth dates, phone number, etc.

(ii) **Strong Password** Difficult to break and a combination of alphabets and symbols.

File Access Permission

Most current file systems have methods of assigning permissions or access rights to specific user and group of users. These systems control the ability of the users to view or make changes to the contents of the file system.

File access permission refers to privileges that allow a user to read, write or execute a file.

There are three specific file access permissions as follows

(i) Read permission (ii) Write permission

(iii) Execute permission

Terms Related to Security

1. **Eavesdropping** The unauthorised real time interception of a private communication such as a phone call, instant message is known as eavesdropping.
2. **Masquerading** The attacker impersonates an authorised user and thereby gain certain unauthorised privilege.
3. **Patches** It is a piece of software designed to fix problems with a computer program or its supporting data.

   This includes fixing security vulnerabilities and other bugs and improving the usability and performance.

Note *Vendor created program modifications are called patches.*

4. **Logic Bomb** It is a piece of code intentionally inserted into a computer's memory that will set off a malicious function when specified conditions are met. They are also called **slag code** and does not replicate itself.
5. **Application Gateway** This applies security mechanisms to specific applications such as File Transfer Protocol (FTP) and Telnet services.
6. **Proxy Server** It can act as a firewall by responding to input packets in the manner of an application while blocking other packets.

   It hides the true network addresses and used to intercept all messages entering and leaving the network.

Tit-Bits

- The legal right to use software based on specific restrictions is granted *via* **Software License**.
- **Software Piracy** means copying of data or computer software without the owner's permission.

QUESTION BANK

1. .... is a branch of information technology known as information security.
(1) Computer security (2) Cyber security
(3) IT security (4) All of these

2. It takes advantages of basic hardware and software security characteristics.
(1) System design
(2) Data access control
(3) System access control
(4) None of the above

3. Verification of a login name and password is known as **[IBPS Clerk 2014]**
(1) configuration (2) accessibility
(3) authentication (4) logging in
(5) Other than those given as options

4. If you are allowing a person on the network based on the credentials to maintain the security of your network, then this act refers to the process of **[IBPS PO 2016]**
(1) authentication (2) automation
(3) firewall (4) encryption
(5) None of these

5. The scrambling of code is known as
(1) encryption (2) firewalling
(3) scrambling (4) deception

6. The main reason to encrypt a file is to
(1) reduce its size
(2) secure it for transmission
(3) prepare it for backup
(4) include it in the start-up sequence

7. Cracked softwares are another source of
(1) e-mail attack (2) virus attack
(3) trojan horse (4) All of these

8. A malware is a
(1) program (2) hardware
(3) person (4) None of these

9. Softwares such as viruses, worms and trojan horses that have a malicious content, is known as **[IBPS Clerk 2014]**
(1) malicious software (malware)
(2) adware (3) scareware
(4) spyware (5) firewall

10. Viruses, trojan horses and worms are **[IBPS Clerk 2012]**
(1) able to harm computer system
(2) unable to detect if present on computer
(3) user-friendly applications
(4) harmless applications resident on computer
(5) None of the above

11. It is a self-replicating program that infects computer and spreads by inserting copies of itself into other executable code or documents.
(1) Keylogger (2) Worm
(3) Virus (4) Cracker

12. A computer virus is
(1) deliberately created
(2) created accidently
(3) produced as a result of some program error
(4) All of the above

13. ...... are often delivered to a PC through a mail attachment and are often designed to do harm. **[IBPS PO 2015]**
(1) Portals
(2) Spam
(3) Viruses
(4) Other than those given as options
(5) E-mail messages

14. Which of the following refers to dangerous programs that can be 'caught' of opening E-mail attachments and downloading software from the Internet? **[SBI PO 2014]**
(1) Utility (2) Virus (3) Honey Pot
(4) Spam (5) App

15. A program designed to destroy data on your computer which can travel to 'infect' other computers is called a **[RBI Grade B 2012]]**
(1) disease (2) torpedo
(3) hurricane (4) virus
(5) infector

16. If your computer rebooting itself, then it is likely that **[SBI Clerk 2012]**
(1) it has a virus
(2) it does not have enough memory
(3) there is no printer
(4) there has been a power surge
(5) it needs a CD-ROM

17. Computer virus is **[IBPS Clerk 2011]**

(1) a hardware (2) a windows tool
(3) a computer program (4) a system software
(5) None of the above

18. Which among the following is related to the internet and mail?

(1) Boot-Up
(2) Magnetic Tapes
(3) Applications Software
(4) Virus

19. The first PC virus was developed in

(1) 1980 (2) 1984 (3) 1986 (4) 1988

20. Which was the first PC boot sector virus?

(1) Creeper (2) Payload
(3) Bomb (4) Brain

21. The first computer virus is

(1) Creeper (2) PARAM
(3) The Famous (4) HARLIE

22. The .... of a threat measures its potential impact on a system. **[IBPS Clerk 2011]**

(1) vulnerabilities (2) counter measures
(3) degree of harm (4) susceptibility
(5) None of these

23. Which of the following is the type of software that has self-replicating software that causes damage to files and system?

(1) Viruses (2) Trojan horses
(3) Bots (4) Worms

24. Like a virus, it is also a self-replicating program. The difference between a virus and it is that it does not create copies of itself on one system it propagates through computer networks.

(1) Keylogger (2) Worm
(3) Cracker (4) None of these

25. A worm

(1) can automatically move in network
(2) can only be transferred with human intervention
(3) worms are harmless
(4) None of the above

26. Worm is a program that infects computer and spreads by inserting copies of itself into other executable code or documents.

(1) Self- attach (2) Self-replicating
(3) Non-self-replicating (4) Hacking

27. A computer virus normally attaches itself to another computer program known as a **[IBPS PO 2015]**

(1) host program (2) target program
(3) backdoor program (4) bluetooth
(5) trojan horse

28. These are program designed as to seem to being or be doing one thing, but actually being or doing another.

(1) Trojan horses (2) Keyloggers
(3) Worms (4) Crackers

29. Viruses that fool a user into downloading and/or executing them by pretending to be useful applications are also sometimes called

(1) trojan horses (2) keyloggers
(3) worms (4) crackers

30. A .... is a small program embedded inside of a GIF image.

(1) web bug (2) cookie
(3) spyware application (4) spam

31. Hackers often gain entry to a network be pretending to be at a legitimate computer.

(1) Spoofing (2) Forging
(3) IP spoofing (4) All of these

32. Attempt to gain unauthorised access to a user's system or information by pretending to be the user. **[IBPS RRB PO 2018]**

(1) Spoofing (2) Hacker
(3) Cracker (4) Phishing
(5) None of these

33. Which of the following enables to determine how often a user visited a website? **[IBPS Clerk 2014]**

(1) Hacker (2) Spammer
(3) Phish (4) Identify theft
(5) Cookie

34. A person who uses his or her expertise to gain access to other people computers to get information illegally or do damage is a **[Allahabad Bank PO 2011]**

Or

A person who uses his expertise for software. **[IBPS RRB PO 2018]**

(1) Spammer (2) Hacker
(3) Instant messenger (4) All of these
(5) None of these

35. Hackers
(1) have the same motive
(2) is another name of users
(3) many legally break into computer as long as they do not do any damage
(4) break into other people's computer

36. What is a person called who uses a computer to cause harm to people or destroy critical systems? **[IBPS Clerk 2014]**
(1) Cyber Terrorist
(2) Black-Hat-Hacker
(3) Cyber Cracker
(4) Hacktivist
(5) Other than those given as options

37. .... are attempts by individuals to obtain confidential information from you by falsifying their identity. **[IBPS Clerk 2013]**
(1) Phishing trips (2) Computer viruses
(3) Spyware scams (4) Viruses
(5) Phishing scams

38. Which of the following is a criminal activity attempting to acquire sensitive information such as passwords, credit cards, debits by masquerading as a trustworthy person or business in an electronic communication? **[IBPS Clerk 2010]**
(1) Spoofing (2) Phishing
(3) Stalking (4) Hacking
(5) None of these

39. All of the following are examples of real-security and privacy risks except **[IBPS Clerk 2014]**
(1) hackers (2) spam
(3) viruses (4) identify theft
(5) None of these

40. Junk E-mail is also called **[Union Bank of India 2011]**
(1) spam (2) spoof
(3) sniffer script (4) spool
(5) None of these

41. .... is a type of electronic spam where unsolicited messages are sent by e-mail.
(1) Trash mail (2) Cram mail
(3) Draft mail (4) Spam mail

42. Adware is something
(1) which is added to your computers
(2) by adding this performance of your computer increases
(3) software that gets different advertisement
(4) None of the above

43. It is a toolkit for hiding the fact that a computer's security has been compromised, is a general description of a set of programs which work to subvert control of an operating system from its legitimate (in accordance with established rules) operators.
(1) Rootkit (2) Keylogger
(3) Worm (4) Cracker

44. An anti-virus is a(n)
(1) program code
(2) computer
(3) company name
(4) application software

45. Anti-virus software is an example of
(1) business software
(2) an operating system
(3) a security
(4) an office suite

46. A digital signature is a/an **[SBI Clerk 2011]**
(1) scanned signature
(2) signature in binary form
(3) encrypting information
(4) handwritten signature
(5) None of the above

47. To protect yourself from computer hacker intrusions, you should install a **[RBI Grade B 2012]**
(1) firewall (2) mailer
(3) macro (4) script
(5) None of these

48. Which one of the following is a key function of firewall? **[SBI PO 2010]**
(1) Monitoring (2) Deleting
(3) Copying (4) Moving
(5) None of these

49. Mechanism to protect network from outside attack is
(1) firewall (2) anti-virus
(3) digital signature (4) formatting

50. A firewall operated by **[SBI Clerk 2010]**

(1) the pre-purchase phase
(2) isolating intranet from extranet
(3) screening packets to/from the network and provide controllable filtering of network traffic
(4) All of the above
(5) None of the above

51. Coded entries which are used to gain access to a computer system are called

(1) Entry codes
(2) Passwords
(3) Security commands
(4) Codewords

52. Password enables users to

(1) get into the system quickly
(2) make efficient use of time
(3) retain confidentiality of files
(4) simplify file structure

53. Which of the following is the combination of numbers, alphabets along with username used to get access to user account?

(1) Password (2) Username
(3) Titlename (4) Host-Id

54. ……… refers to privileges that allow a user to read, write or execute a file.

(1) Authentication
(2) File access permission
(3) Password
(4) Firewall

55. The unauthorised real-time interception of a private communication such as a phone call, instant message is known as

(1) replay
(2) eavesdropping
(3) patches
(4) payloads

56. Vendor created program modifications are called **[Allahabad Bank PO 2011]**

(1) patches (2) anti-viruses
(3) hales (4) fixes
(5) overlaps

57. Which of the following is a computer's memory, but unlike a virus, it does not replicate itself ? **[SBI PO 2011]**

(1) Trojan Horse (2) Logic Bomb
(3) Cracker (4) Firewall
(5) None of these

58. They are also called slag code and does not replicate itself.

(1) Time (2) Anti-virus
(3) Logic bomb (4) All of these

59. It hides the true network addresses and used to intercept all messages entering and leaving the network.

(1) Logic bomb (2) Firewall
(3) Patches (4) Proxy server

60. The legal right to use software based on specific restrictions is granted *via* a **[RBI Grade B 2012]**

(1) software privacy policy
(2) software license
(3) software password manager
(4) software log
(5) None of the above

61. …….. refers to the unauthorised copying and distribution of software. **[IBPS Clerk 2014]**

Or

Illegal copying and distribution of software is **[IBPS RRB PO 2018]**

(1) hacking (2) software piracy
(3) software literacy (4) cracking
(5) copyright

ANSWERS

1. *(4)*	2. *(1)*	3. *(3)*	4. *(1)*	5. *(1)*	6. *(2)*	7. *(2)*	8. *(1)*	9. *(1)*	10. *(1)*
11. *(3)*	12. *(1)*	13. *(3)*	14. *(2)*	15. *(4)*	16. *(1)*	17. *(3)*	18. *(4)*	19. *(3)*	20. *(4)*
21. *(1)*	22. *(3)*	23. *(4)*	24. *(2)*	25. *(1)*	26. *(2)*	27. *(5)*	28. *(1)*	29. *(1)*	30. *(3)*
31. *(3)*	32. *(1)*	33. *(1)*	34. *(2)*	35. *(4)*	36. *(3)*	37. *(1)*	38. *(2)*	39. *(2)*	40. *(1)*
41. *(4)*	42. *(3)*	43. *(1)*	44. *(4)*	45. *(3)*	46. *(3)*	47. *(1)*	48. *(1)*	49. *(1)*	50. *(3)*
51. *(2)*	52. *(3)*	53. *(1)*	54. *(2)*	55. *(2)*	56. *(1)*	57. *(2)*	58. *(3)*	59. *(4)*	60. *(2)*
61. *(2)*									