CHAPTER : COMPUTER SECURITY

INTRODUCTION

Computer security refers to the protection of computer systems, networks and data from unauthorised access. It is required to protect against cyber-attacks, maintain smooth functioning and protect important data. With the growing dependence on digital technologies, computer security has become essential. It involves measures such as firewalls, encryption and antivirus programs. It is also known as network security.

1. COMPONENTS OF COMPUTER SECURITY

The main components of computer security are:

1. Confidentiality It ensures that data is not accessed by any unauthorised person.

2. Integrity Integrity ensures that data has not been modified or accidentally altered by an unauthorised user.

3. Availability Availability ensures that data and resources are available or accessible by an authorised user whenever they are needed.

4. Authentication It is the process of verifying the identity of a user before granting access to resources. It ensures that users are the persons they claim to be.

5. Non-repudiation It ensures that originators of messages cannot deny that they are not sender of the message. It provides proof that the action really happened and who did it.

6. Access control It ensures that users access only those resources that they are allowed to access.

2. THREATS TO COMPUTER SECURITY

Computer security threats are activities that can steal information, make the system stop working properly or harm the devices. These threats can cause damage to the system or make it unsafe by affecting the way it works.

Security Threat	Description
Malware	Malicious software that harms or exploits a computer system
Phishing	Tricks people into revealing sensitive information such as usernames, passwords or credit card details
Denial-of-Service Attack	Makes a website or online service stop working by flooding it with too much traffic; causes the system to slow down or crash
Cyber Bullying	Using internet, social media or digital platforms to harass or threaten another person; includes sending mean messages, sharing hurtful posts or spreading rumours
Identity Theft	Stealing personal information like passwords or bank details to pretend to be someone and commit fraud
Salami Attack	A technique where an attacker steals small amounts of money from many bank transactions; also known as salami slicing
Cyber Stalking	Using the internet or digital platforms to monitor another person's activities; declared a crime under section 354 C and 354 D of the Indian Penal Code
Spoofing	When someone pretends to be a trusted person or system to trick others; can involve faking an email address, phone number or website
Piracy	Illegal copying, sharing or use of software, movies, music or other digital content without permission or paying for it
Hacking	Gaining unauthorised access to computer systems or networks to steal or manipulate sensitive data or information
Cracking	Breaking into a system or software to bypass its security, like unlocking a password or removing protection from a program; usually done to access something without permission
Data Diddling	Changing or tampering with data in a system to make it incorrect or fake

Security Threat	Description
SQL Injections	A type of attack where a hacker inserts harmful code into a website's database through things like search boxes or login forms; can allow the hacker to steal, change or delete important data
Eavesdropping	The act of secretly listening to or intercepting private communications like emails, phone calls or data being sent over a network, without permission
Cyber Pornography	Distribution, viewing, sharing or downloading of pornographic content in electronic form such as videos, images or text files
Cyber Warfare	Use of digital attacks by one country to damage or disrupt the computer systems of another country

3. MALWARE

Malware is short for malicious software, which refers to any software designed to harm, exploit or damage a computer or network. It can come in many forms such as viruses, worms, trojans, ransomware and spyware.

Type	Description
Virus	Full form is Vital Information Resource Under Siege; a malicious program that can corrupt, delete or steal data
Trojan Horse	A malware that looks like a legitimate program but once you open it, it secretly gives hackers access to your computer; also called hide malware program
Worm	A self-replicating program that spreads across networks without needing to attach to files; fills up the computer's memory and slows down its speed
Spyware	A malware program that is installed on a computer by hacker to monitor all activities of the user
Ransomware	A malware program that locks computer files and demands money or ransom in exchange for unlocking them
Keylogger	A type of spyware program that records your keystrokes to steal your passwords or credit card numbers
Adware	A malware program that displays unwanted advertisements on your computer, often in the form of pop-ups, banners or videos
Botnet	A network of computers that have been infected with malware and are controlled by a hacker; used to steal login IDs and passwords, to control computers and for DoS attacks
Scareware	Tricks users into downloading harmful software or visiting infected websites
Backdoor	A secret way for hackers to access your computer or network without your knowledge
Rootkits	Allows cyber criminals to access a computer without being detected

4. COMPUTER VIRUS

A computer virus is a type of malware that can infect your computer and cause harm. It attaches itself to files or programs and spreads when you open or share those files. The term virus was first used by a computer scientist, Fred Cohen in 1983.

Note: All viruses are malwares but not all malwares are viruses.

TYPES OF VIRUS

1. Boot Sector Virus It is a type of virus that infects the boot sector of a computer's hard drive. When the computer starts up, this virus can load itself into memory, allows itself to spread and infect other systems. This virus overwrites and changes the boot record program. Examples: Brain, Disk Killer, Stoned Virus

2. File/Program Infector Virus This virus infects executable program files with extensions such as .exe, .bin, .txt etc. It makes its own copies and becomes active in memory by infecting the executable files. Examples: Sunday, Cascade

3. Browser Hijacker This virus takes control of your web browser settings without your permission. It changes things like your homepage, search engine or new tab page and redirects you to unwanted websites. Examples: Ask Toolbar, Sweet Page

4. Macro Virus This virus infects files created by software programs that use macros, like Microsoft Word or Excel. Macros are small programs used to automate tasks and a macro virus exploits these to spread and execute harmful commands. Examples: DMW, Concept

5. Encrypted Virus This type of virus hides itself by encrypting its code. These viruses are harder to detect by antivirus programs.

6. Polymorphic Virus It is a type of virus that changes its code or structure each time it infects a new file or system. This makes it harder for antivirus programs to detect because it appears different every time. Examples: Storm Worm, VirLock, Ursnif

7. Network Virus It is a type of virus that spreads through computer networks. They are designed to move quickly between systems, causing disruptions and spreading infections across the network. Examples: SQL Slammer, Nimda

8. Directory Virus This virus changes the path of the file. It tricks the system into running the virus instead of the intended program. Example: Dir-2 Virus

9. Multipartite Virus It is a type of virus that can infect both the boot sector and executable files. It can spread through storage devices, email attachments or file downloads. Example: Tequila

10. Logic Bomb/Time Bomb This type of viruses are programmed to activate under specific conditions, like a certain date or action. They remain hidden in the system until triggered.

COMMON REASONS FOR THE SPREAD OF VIRUSES

- Opening infected email attachments
- Downloading files from unsafe websites
- Using infected USB drives or external media
- Clicking on phishing links or fake ads
- Sharing files over insecure networks

SOME COMMON EFFECTS OF VIRUSES

- Data loss or corruption
- Slows down system performance
- Causes crashes or freezes
- Allows unauthorised access
- Displays unwanted ads
- Disables security features

FAMOUS VIRUSES AND THEIR INVENTION YEARS

Virus	Year	Description
Creeper	1971	The first computer virus; spreads on networks
Brain	1986	First boot sector virus; designed as copy protection, made in Pakistan
Jerusalem	1987	A virus that activated on Friday the 13th, causing file corruption
Melissa Virus	1999	Spread through email and caused widespread email traffic
I Love You	2000	Spread via email attachments and caused damage worldwide
Code Red	2001	Targeted Microsoft IIS servers and caused website crashes
My Doom	2004	Affected email systems and caused denial-of-service attacks
Conficker	2008	A worm that spread across Windows systems and created a botnet
Petya Ransomware	2016	A ransomware virus that encrypted files and demanded payment to restore access
Stuxnet	2010	Targeted industrial systems, specifically Iranian nuclear plants

---

5. COMPUTER SECURITY MEASURES

1. Antivirus Antivirus is a type of utility software. It is designed to detect, prevent and remove viruses on computers or networks. It blocks viruses from entering your system.
Examples of popular antivirus software: Norton, McAfee, Kaspersky, Avast, Bitdefender, AVG, Windows Defender (built into Windows), PANDA, Quick Heal, Trend Micro
2. Password Passwords are used to secure a computer and network. It is basically a secret word or phrase used to authenticate a user's identity and grant access to a system. Passwords are of two types — weak and strong passwords. Strong passwords are long, complex and unique; they include combination of alphabets, numbers or special characters. Weak passwords are more vulnerable to attacks.
3. Firewall It is a security system that monitors and controls incoming and outgoing network traffic based on predefined security rules. It acts as a barrier between a trusted internal network and untrusted external networks. It can be both hardware and software. It prevents unauthorised access to the computer system.
4. Biometric It is a security measure that uses unique physical characteristics (like fingerprints, face recognition or iris scans) to verify identity.
5. CAPTCHA It stands for Completely Automated Public Turing Test to Tell Computers and Humans Apart. It is used to protect website from spammers. It is a challenge-response test used to determine if the user is human or a robot.
6. Encryption It is the process of converting original message into a secret code to prevent unauthorised access. The original message is called normal text and the secret code is called cipher text. Encryption happens on the sender's side.
7. Decryption The process of converting encrypted code back into its original form is called decryption. This happens on the receiver's side.
8. Cryptography Cryptography is the process of securing communication and information by converting it into a secret code. It uses algorithms and keys to protect data from unauthorised access. Encryption and decryption both are used together in cryptography.
9. Patch It refers to the small software updates, released time to time by software companies to fix bugs, vulnerabilities or security issues in a software. Regular patching ensures systems are protected from known threats.
10. Digital Signature It is a cryptographic technique used to verify the authenticity and integrity of digital documents. It is similar to hand signature but it is digital. This ensures that the document is original.

---

6. HACKERS

The act of gaining unauthorised access to computer systems, networks or data is called hacking. The person or professional who does hacking is called a hacker. They gain access to systems by detecting security vulnerabilities in computer and network systems. Hackers are mostly programmers.

TYPES OF HACKERS

Hackers are classified into the following categories:
1. White Hat Hacker They are also known as ethical hackers. They work to improve security. They find vulnerabilities in systems or networks and inform the owners to fix them. Hackers falling into this category do hacking for good work.
2. Black Hat Hacker These are also called crackers. They perform illegal activities. They exploit security weaknesses for personal gain, such as stealing data, spreading malware or causing damage.
3. Grey Hat Hacker Hackers of this category are a mixture of black and white hat hackers. They may break into systems without permission but usually don't cause harm. They might report the vulnerabilities they find, often without authorisation.
4. Blue Hat Hacker Hackers who expose and correct the flaws of the software before it is launched are called blue hat hackers.
5. Green Hat Hacker Hackers who are still learning hacking come under this category. They are eager to learn and develop their skills. These are also known as pre-hacker.
6. Red Hat Hacker Their objective is same as that of white hat hackers. They go after black hat hackers with the intention to destroy or block their activities.

FACTS DRIVE (Additional Important Points)

- Steganography is an art of hiding the existence of a message.

- The legal right to use software based on specific restrictions is granted via software license.
- A proxy server also called application gateway, acts as an intermediary between user's device and the internet.
- SSL (Secure Sockets Layer) and TLS (Transport Layer Security) both are cryptographic protocols used to secure communication over the internet.
- Masquerading in computer security refers to an attack where an unauthorized entity impersonates a legitimate user or system to gain access to sensitive data.
- A hacktivist is a person who uses hacking techniques to promote political, social or environmental causes.

IMPORTANT ABBREVIATIONS

- DDoS — Distributed Denial of Service
- OTP — One-Time Password
- CAPTCHA — Completely Automated Public Turing Test to Tell Computers and Humans Apart
- CIA — Confidentiality, Integrity and Availability
- VIRUS — Vital Information Resource Under Siege
- SSL — Secure Sockets Layer
- TLS — Transport Layer Security
- MBR — Master Boot Record

PYQs ONELINER (Key Exam Facts)

1. The hashing method is commonly used to verify the integrity of data. *(SSC CGL T-II 20.01.2025)*
2. The process of verifying a user's identity is called authentication. *(DSSSB TGT 2023)*
3. The information transformed during encryption is plain text. *(DSSSB TGT 2023)*
4. Trojans appear to perform one function but in fact perform another malicious function. *(DSSSB Patwari 2022)*
5. Resident viruses are embedded in a system's memory so it can be reactivated if the original virus is deleted. *(SSC CGL 2023)*
6. Keyloggers can be either hardware or software to record the keys pressed by a user on the keyboard. *(SSC CGL 2023)*
7. Worm is a type of malware that appears useful but in reality, damages the files. *(CPCT 2024)*
8. Macro virus spreads through application software. *(IBPS RRB 2022)*

1. Computer security is also known as:
(1)Data security (2)Network security (3)Hardware security (4)Digital security
2. Which component of computer security ensures that data is not accessed by any unauthorised person?
(1)Integrity (2)Availability (3)Confidentiality (4)Authentication
3. The process of verifying the identity of a user before granting access to resources is called:
(1)Authorisation (2)Non-repudiation (3)Access control (4)Authentication
4. Which component ensures that data has not been modified or accidentally altered by an unauthorised user?
(1)Confidentiality (2)Availability (3)Non-repudiation (4)Integrity
5. Non-repudiation ensures that:
(1)Data is encrypted during transfer (2)Senders cannot deny sending a message (3)Users can access all resources (4)Systems remain available 24/7
6. CIA in computer security stands for:
(1)Computer Intelligence Agency (2)Central Information Access (3)Confidentiality, Integrity and Availability (4)Cyber Integrity Architecture
7. A technique where an attacker steals small amounts of money from many bank transactions is called:
(1)Phishing (2)Data diddling (3)Salami attack (4)SQL injection
8. Which of the following involves inserting harmful code into a website's database through input forms?
(1)Phishing (2)SQL injection (3)Eavesdropping (4)Spoofing
9. When someone pretends to be a trusted person or system to trick others, it is called:
(1)Hacking (2)Cracking (3)Spoofing (4)Cyber stalking
10. Cyber stalking has been declared a crime in India under sections:

(1)120 A and 120 B of IPC (2)354 C and 354 D of IPC (3)420 A and 420 B of IPC (4)66 A and 66 B of IT Act

11. A DoS attack makes a website unavailable by:
(1)Encrypting all its data (2)Flooding it with too much traffic (3)Stealing its database (4)Changing its homepage
12. Which threat involves secretly listening to private communications without permission?
(1)Piracy (2)Data diddling (3)Eavesdropping (4)Cyber warfare
13. VIRUS stands for:
(1)Virtual Information Resource Under System (2)Vital Information Resource Under Siege (3)Viral Integrated Resource Under Security (4)Vital Internet Resource Under Surveillance
14. Which malware is a self-replicating program that spreads across networks without needing to attach to files?
(1)Trojan horse (2)Spyware (3)Worm (4)Adware
15. A malware that looks like a legitimate program but secretly gives hackers access to your computer is called:
(1)Worm (2)Trojan horse (3)Keylogger (4)Rootkit
16. Which malware records your keystrokes to steal passwords or credit card numbers?
(1)Adware (2)Spyware (3)Keylogger (4)Botnet
17. A malware that locks your computer files and demands money to unlock them is called:
(1)Adware (2)Scareware (3)Backdoor (4)Ransomware
18. Which malware creates a network of infected computers controlled remotely by a hacker?
(1)Rootkit (2)Botnet (3)Backdoor (4)Scareware
19. The term 'computer virus' was first used by which computer scientist?
(1)Alan Turing (2)Bill Gates (3)Fred Cohen (4)John von Neumann
20. Which type of virus infects the boot sector of a computer's hard drive?
(1)Macro virus (2)Boot sector virus (3)Network virus (4)Directory virus
21. Which virus changes its code or structure each time it infects a new file to avoid detection?
(1)Encrypted virus (2)Multipartite virus (3)Directory virus (4)Polymorphic virus
22. The first computer virus, Creeper, was created in:
(1)1965 (2)1971 (3)1983 (4)1986
23. A virus that can infect both the boot sector and executable files is called:
(1)Macro virus (2)Polymorphic virus (3)Multipartite virus (4)Network virus
24. Which virus infects files created by software programs that use macros like Microsoft Word or Excel?
(1)Directory virus (2)Browser hijacker (3)Macro virus (4)Logic bomb
25. CAPTCHA stands for:
(1)Completely Automated Public Turing Test to Tell Computers and Humans Apart (2)Central Automated Protocol for Testing Computer and Human Agents (3)Computer Automated Public Test for Controlling Human Access (4)Completely Authorised Public Turing Test for Cyber and Hacker Attacks
26. Antivirus software is classified as which type of software?
(1)Application software (2)System software (3)Utility software (4)Programming software
27. The process of converting plain text into cipher text is called:
(1)Decryption (2)Hashing (3)Cryptography (4)Encryption
28. Decryption happens on which side of communication?
(1)Sender's side (2)Network's side (3)Receiver's side (4)Server's side
29. White hat hackers are also known as:
(1)Crackers (2)Pre-hackers (3)Ethical hackers (4)Hacktivists
30. Black hat hackers are also called:
(1)Ethical hackers (2)Crackers (3)Pre-hackers (4)Blue hats

ANSWER KEY (Quick Reference)

Q1-b | Q2-c | Q3-d | Q4-d | Q5-b | Q6-c | Q7-c | Q8-b | Q9-c | Q10-b | Q11-b | Q12-c | Q13-b | Q14-c | Q15-b | Q16-c | Q17-d | Q18-b | Q19-c | Q20-b | Q21-d | Q22-b | Q23-c | Q24-c | Q25-a | Q26-c | Q27-d | Q28-c | Q29-c | Q30-b