COMPUTER SECURITY (CYBER SECURITY / IT SECURITY)

Introduction to Computer Security

Computer Security, also known as **Cyber Security** or **IT Security**, is the practice of protecting computers, networks, software, and data from unauthorized access, misuse, damage, theft, or cyber attacks.

Computer Security is the protection of computer systems, data, and networks from threats, attacks, and unauthorized access.

Example

If you protect your house with locks and security cameras, similarly computer security protects your computer using passwords, antivirus software, and security systems.

Exam Tip

Computer Security = Cyber Security = IT Security

Why is Computer Security Important?

Computer security is important because it helps to:

1. Protect personal information.
2. Prevent data theft.
3. Protect against viruses and malware.
4. Maintain privacy.
5. Ensure smooth operation of computer systems.
6. Prevent financial losses.

Example

Online banking systems use cybersecurity to protect customer accounts from hackers.

Exam Tip

Remember **CIA Triad**:

- **C** – Confidentiality
- **I** – Integrity
- **A** – Availability

These are the three main goals of cybersecurity.

CYBER ATTACK

A cyber attack is an attempt by hackers or malicious users to gain unauthorized access to a computer system, network, or data.

Simple Definition

Any harmful action performed through computers or networks to steal, damage, or misuse information is called a cyber attack.

Example

A hacker steals your social media password.

Exam Tip

Cyber Attack = Unauthorized attempt to access or damage a computer system.

COMPUTER VIRUS

A computer virus is a malicious software program that spreads from one computer to another and affects the normal functioning of the system.

A computer virus is a harmful program that can replicate itself and damage computer files and programs.

Example

A virus enters through an infected pen drive and corrupts important files.

Example

Just like a biological virus spreads from one person to another, a computer virus spreads from one computer to another.

Exam Tip

Virus = Self-replicating malicious software.

SOURCES OF CYBER ATTACK

The most common sources of cyber attacks are explained below.

1. Downloadable Programs

Downloadable files from the internet are one of the major sources of viruses.

These include:

- Games
- Screen savers
- Software installers
- Applications
- Free utilities

If downloaded from untrusted websites, they may contain malicious code.

Example

You download a free game from an unknown website and your computer becomes infected.

Prevention

- Download only from trusted websites.
- Scan files before installation.
- Use antivirus software.

Downloadable programs from untrusted sources may contain viruses and malware.

Exam Tip

"Free software from unknown websites" is a frequently asked example.

2. Cracked Software

Cracked software refers to illegal copies of paid software that have been modified to bypass licensing restrictions.

Why are they dangerous?

Hackers often insert:

- Viruses
- Trojans
- Spyware
- Ransomware

inside cracked software.

Example

Downloading a cracked version of Microsoft Office may infect the system with malware.

Prevention

- Use genuine software.
- Download only from official websites.

Cracked software is a modified illegal software that often contains viruses and security threats.

Exam Tip

Cracked Software = Illegal Software + High Security Risk.

3. E-mail Attachments

Email attachments are among the most common methods used to spread viruses.

Dangerous Attachments

Files such as:

- .exe
- .bat
- .scr
- .zip

may contain malware.

Example

An email claiming "You won a lottery" contains an attachment that installs malware.

Prevention

- Open attachments only from trusted senders.
- Scan attachments before opening.
- Avoid suspicious emails.

Malicious email attachments can install viruses and malware on a computer.

Exam Tip

Unknown Sender + Attachment = Possible Virus.

4. Booting from Unknown CD/DVD

If an infected CD/DVD remains inside the computer, the system may boot from it automatically.

This can introduce viruses during startup.

Example

A computer boots from an infected CD and the virus enters the operating system.

Prevention

- Remove CDs/DVDs when not in use.
- Change boot settings.
- Use trusted media only.

Booting from unknown CDs or DVDs can infect a computer with viruses.

Exam Tip

Always remove unused CDs/DVDs from the drive.

METHODS TO PROVIDE PROTECTION

There are four major methods used to protect computer systems.

1. System Access Control

System Access Control ensures that only authorized users can access a computer system.

System Access Control is the process of restricting system access to authorized users only.

How it Works

It uses:

- User IDs
- Passwords
- PINs
- Biometric authentication
- Smart cards

Example

Unlocking a smartphone using fingerprint authentication.

Advantages

- Prevents unauthorized access.
- Protects sensitive information.
- Improves security.

Real-Life Example

An ATM allows access only after entering the correct PIN.

System Access Control restricts access to authorized users through authentication mechanisms.

Exam Tip

Keywords:

- Authentication
- Password
- Fingerprint
- User ID

2. Data Access Control

Data Access Control determines who can access data and what actions they can perform.

Data Access Control controls access to files and data based on user permissions.

Types of Permissions

- Read
- Write
- Modify
- Delete
- Execute

Example

A student can view examination results but cannot modify them.

Example

In a company:

- Employees can view documents.
- Managers can edit documents.
- Administrators can delete documents.

Advantages

- Prevents unauthorized modification.
- Protects confidential data.
- Maintains data integrity.

Data Access Control manages permissions for accessing and modifying data.

Exam Tip

Remember:
Who can access + What they can do = Data Access Control

3. System and Security Administration

System and Security Administration involves managing and maintaining computer security policies and procedures.

System and Security Administration refers to the management of security settings, users, backups, and updates.

Main Activities

- User management
- Password management
- Software updates
- Backup creation
- Security monitoring
- Antivirus management

Example

An administrator regularly updates antivirus software and changes security settings.

Example

A bank's IT department continuously monitors servers and applies security updates.

Advantages

- Reduces security vulnerabilities.
- Ensures system reliability.
- Detects threats early.

System and Security Administration manages security operations and policies of a computer system.

Exam Tip

Administrator = Security Manager of the computer system.

4. System Design

System Design incorporates security features during hardware and software development.

Simple Definition

System Design means building security into a system from the beginning.

Security Features in Design

- Secure hardware
- Secure operating systems
- Encryption
- Firewalls
- Authentication systems

Example

A banking application is designed with encryption and multi-factor authentication.

Example

Modern smartphones have built-in encryption and secure boot processes.

Advantages

- Stronger security.
- Reduced vulnerabilities.
- Better protection against attacks.

System Design integrates security features into hardware and software during development.

Exam Tip

Security built during development = Secure System Design.

COMPONENTS OF COMPUTER SECURITY

Computer Security is built upon several important components that work together to protect computer systems, networks, and information from unauthorized access, misuse, modification, and destruction.

These components ensure that information remains secure, accurate, available, and accessible only to authorized users.

Exam Tip

The most important components frequently asked in examinations are:

CIA + AANPSC

- **C** – Confidentiality
- **I** – Integrity
- **A** – Availability
- **A** – Authentication
- **A** – Access Control
- **N** – Non-Repudiation
- **P** – Privacy
- **S** – Steganography
- **C** – Cryptography

1. CONFIDENTIALITY

Confidentiality ensures that information is accessible only to authorized persons and remains protected from unauthorized access.

Definition

Confidentiality means keeping information secret from unauthorized users.

Example

A student's examination result can only be viewed by the student and authorized university officials.

Example

Your ATM PIN should be known only to you and your bank.

Methods Used to Maintain Confidentiality

- Passwords
- Encryption
- Biometrics
- Access permissions
- Smart cards

Advantages

- Protects sensitive information.
- Prevents data leakage.
- Maintains privacy.

Confidentiality ensures that data is not accessed by unauthorized persons.

Exam Tip

Confidentiality = Secrecy of Information

2. INTEGRITY

Integrity ensures that information remains accurate, complete, and unaltered unless modified by authorized users.

Definition

Integrity means ensuring that data remains correct and unchanged.

Example

A student's marks should not be changed by unauthorized persons.

Example

Bank account balances must remain accurate and cannot be altered by hackers.

Methods Used

- Hash functions
- Digital signatures
- Checksums
- Access control

Advantages

- Maintains data accuracy.
- Prevents unauthorized modifications.
- Builds trust in information systems.

Integrity ensures that information is not altered without authorization.

Exam Tip

Integrity = Accuracy of Data

3. AUTHENTICATION

Authentication is the process of verifying the identity of a user.

Definition

Authentication confirms that a user is who they claim to be.

Example

Entering a username and password to log in to an email account.

Example

Unlocking a smartphone using fingerprint recognition.

Types of Authentication

1. Something You Know

- Password
- PIN

2. Something You Have

- ATM card
- Smart card

3. Something You Are

- Fingerprint
- Face recognition
- Iris scan

One-Line Exam Definition

Authentication is the verification of a user's identity.

Exam Tip

Authentication = Identity Verification

4. ACCESS CONTROL

Access Control determines what resources a user can access and what actions they can perform.

Definition

Access Control decides who can access what information.

Example

A teacher can modify student marks, but students can only view them.

Example

Employees may access office files, while visitors cannot.

Types of Permissions

- Read
- Write
- Modify
- Delete
- Execute

Advantages

- Prevents unauthorized access.
- Protects important resources.
- Improves security management.

One-Line Exam Definition

Access Control restricts users to authorized resources and actions.

Exam Tip

Authentication verifies identity; Access Control determines permissions.

5. NON-REPUDIATION

Definition

Non-Repudiation ensures that a sender cannot deny having sent a message and a receiver cannot deny having received it.

Definition

Non-Repudiation provides proof of sending and receiving information.

Example

An online transaction receipt proves that a payment was made.

Example

Digital signatures in online banking transactions.

Methods Used

- Digital signatures
- Electronic receipts
- Audit logs
- Certificates

Advantages

- Prevents denial of transactions.
- Provides legal proof.
- Increases trust.

Definition

Non-Repudiation prevents users from denying their actions or communications.

Exam Tip

Non-Repudiation = Proof of Action

6. AVAILABILITY

Definition

Availability ensures that systems, services, and data are accessible whenever authorized users need them.

Availability means information and services are available when required.

Example

A bank website should be available 24×7 for customers.

Real-Life Example

Online shopping websites remain operational during festivals and sales.

Methods Used

- Backups
- UPS systems
- Redundant servers
- Disaster recovery plans

Advantages

- Continuous service.
- Reduced downtime.
- Improved reliability.

Definition

Availability ensures that authorized users can access resources whenever needed.

Exam Tip

Availability = Ready to Use

7. PRIVACY

Definition

Privacy refers to an individual's right to control how personal information is collected, used, and shared.

Privacy means controlling personal information.

Example

Your mobile number should not be shared without your permission.

Real-Life Example

Social media privacy settings.

Advantages

- Protects personal information.
- Prevents misuse of data.
- Maintains user trust.

Definition

Privacy gives individuals control over their personal information.

Exam Tip

Privacy = Personal Information Protection.

8. STEGANOGRAPHY

Definition

Steganography is the art of hiding a secret message inside another file, image, audio, or video so that nobody knows the message exists.

Simple Definition

Steganography hides the existence of a message.

Example

A secret message hidden inside a photograph.

Example

Military organizations hiding confidential information in digital images.

How It Works

Original Image + Secret Message = Stego Image

Advantages

- Provides secrecy.
- Hides communication.
- Supports confidentiality.

Definition

Steganography is the technique of hiding information within another medium.

Exam Tip

Steganography = Hidden Message

9. CRYPTOGRAPHY

Definition

Cryptography is the science of protecting information by converting it into a secret form.

Simple Definition

Cryptography converts readable data into an unreadable form to protect it.

Example

WhatsApp messages are encrypted before transmission.

Real-Life Example

Online banking transactions use encryption.

Advantages

- Protects data.
- Secures communication.
- Prevents unauthorized access.

Definition

Cryptography is the science of securing information through encryption techniques.

Exam Tip

Cryptography = Secret Writing

IMPORTANT TERMS IN CRYPTOGRAPHY

1. Plain Text

Definition

The original readable message before encryption.

Example

HELLO

Definition

Plain Text is the original readable message.

Exam Tip

Plain Text = Input Message

2. Cipher

A mathematical algorithm used to convert plain text into cipher text.

Example

Caesar Cipher shifts letters by a fixed number.

Definition

A cipher is an algorithm used for encryption and decryption.

Exam Tip

Cipher = Rule of Encryption

3. Cipher Text

The encrypted form of the original message.

Example

HELLO → KHOOR

Definition

Cipher Text is the encrypted unreadable message.

Exam Tip

Cipher Text = Output of Encryption

4. Encryption

Encryption is the process of converting plain text into cipher text.

Example

HELLO → KHOOR

Definition

Encryption converts readable information into secret information.

Exam Tip

Encryption = Locking Data

5. Decryption

Decryption is the process of converting cipher text back into plain text.

Example

KHOOR → HELLO

Definition

Decryption converts encrypted data back into readable form.

Exam Tip

Decryption = Unlocking Data

MALWARE

Malware stands for **Malicious Software**.

It refers to harmful software designed to damage systems, steal information, spy on users, or gain unauthorized access.

Malware is any software intentionally designed to harm a computer system.

Examples of Malware

- Virus
- Worm
- Trojan Horse
- Spyware
- Adware
- Rootkit
- Ransomware

Definition

Malware is malicious software designed to damage or exploit computer systems.

Exam Tip

Malware = Malicious Software

VIRUS

Full Form

VIRUS = Vital Information Resources Under Siege

A computer virus is a malicious program that attaches itself to other files or programs and spreads from one computer to another.

Simple Definition

A virus is a harmful self-replicating program that infects computer systems.

Example

An infected pen drive transfers a virus to a computer.

How a Virus Spreads

1. Infected file
2. User opens file

3. Virus activates
4. Virus copies itself
5. Other files become infected

Areas Attacked by Virus

- Boot sector
- Operating system
- System files
- Application programs
- Hard disk

Definition

A virus is a malicious program that replicates itself and infects other programs.

HISTORY OF VIRUSES

Creeper Virus (1971)

- First computer virus-like self-replicating program.
- Created by **Bob Thomas**.
- Developed at BBN Technologies.

Brain Virus (1986)

- First PC boot sector virus.
- Originated in Pakistan.

Exam Tip

Virus	Year	Importance
Creeper	1971	First self-replicating program
Brain	1986	First PC boot sector virus

EFFECTS OF VIRUS

Different viruses can cause different types of damage.

1. Monitor User Activities

Example: Recording keyboard inputs.

2. Slow Down Computer Performance

Example: Computer takes longer to open programs.

3. Destroy Data

Example: Deleting important files.

4. Affect Computer Networks

Example: Spreading infection to connected computers.

5. Increase or Decrease Memory Usage

Example: Virus consumes RAM continuously.

6. Display Error Messages

Example: Frequent system warnings.

7. Alter Computer Settings

Example: Changing desktop settings automatically.

8. Show Annoying Advertisements

Example: Pop-up ads appearing repeatedly.

9. Increase Boot Time

Example: Computer takes several minutes to start.

10. Modify Disk Partitions

Example: Changing hard disk partition information.

A virus can slow down computers, corrupt files, alter settings, and spread infections.

WORM

A **computer worm** is a standalone malicious program that can copy itself and spread automatically from one computer to another through networks without requiring human action. Unlike viruses, worms do not need to attach themselves to another program to spread.

Worms usually exploit security weaknesses in operating systems or network services. Once they enter a system, they can rapidly infect multiple computers connected to the same network.

Characteristics of Worms

- Self-replicating malware.
- Spreads automatically through networks.
- Does not require a host program.
- Consumes system and network resources.
- Difficult to detect because they often run in the background.

Example

Morris Worm – One of the earliest and most famous computer worms.

Common Worms

- Bagle
- I Love You
- Morris Worm
- Nimda

Payload

A **Payload** is the harmful part of a worm that performs malicious activities such as deleting files, stealing data, or damaging the system after the worm successfully infects a computer.

Exam Tip

Virus needs a host file; Worm does not need a host file.

TROJAN HORSE

A **Trojan Horse** is a type of malware that appears to be useful or legitimate software but secretly performs harmful activities in the background.

The name comes from the famous Trojan Horse story of ancient Greece, where soldiers hid inside a wooden horse to enter the city of Troy.

Unlike viruses and worms, Trojans cannot replicate themselves.

Characteristics of Trojans

- Disguised as useful software.
- Creates backdoors for hackers.
- Steals personal information.
- Provides unauthorized access to attackers.
- Does not self-replicate.

Example

A fake antivirus program that appears to remove viruses but actually installs malware.

Common Trojans

- Beast
- Sub7
- Zeus
- ZeroAccess Rootkit

Exam Tip

Trojan = Looks useful outside, harmful inside.

SPYWARE

Spyware is software that secretly monitors user activities and collects information without the user's knowledge or consent.

It can track browsing habits, passwords, keystrokes, and personal information, then send the collected data to another person through the Internet.

Characteristics of Spyware

- Monitors user activities.
- Records browsing history.
- Steals passwords and personal data.
- Runs secretly in the background.
- Slows down system performance.

Example

A keylogger that records everything typed on the keyboard.

Common Spyware

- CoolWeb Search
- FinFisher
- Zango
- Zlob Trojan
- Keyloggers

Exam Tip

Spyware = Spy + Software = Secret Monitoring Program.

SYMPTOMS OF MALWARE ATTACK

When malware infects a computer, several warning signs may appear.

Common Symptoms

1. Strange Messages on Screen

Unexpected pop-ups and warning messages start appearing.

Example: Random error messages appear repeatedly.

2. Missing Files

Important files disappear without any action from the user.

Example: Documents stored yesterday are missing today.

3. Slow System Performance

Programs take longer than usual to open and execute.

Example: Computer takes several minutes to start.

4. Frequent Crashes

The system hangs, freezes, or restarts unexpectedly.

Example: PC restarts automatically every few minutes.

5. Inaccessible Drives

Hard disk partitions or drives become inaccessible.

Example: Drive D: cannot be opened.

6. Antivirus Stops Working

Antivirus software fails to run or cannot be installed.

Example: Antivirus closes automatically after opening.

7. Unexpected Sounds

Unknown sounds or music play without user action.

Example: Music starts playing while no media player is running.

8. Mouse Pointer Behaves Abnormally

Mouse pointer changes shape or moves unexpectedly.

Example: Cursor moves on its own.

9. Strange Emails Sent Automatically

The system sends emails without user knowledge.

Example: Friends receive suspicious emails from your account.

10. Automatic Program Execution

Programs open and close automatically.

Example: Browser windows open repeatedly.

Exam Tip

Remember **"SLOW CRASH"**

- **S** = Strange messages
- **L** = Loss of files
- **O** = Odd sounds
- **W** = Working slowly
- **C** = Crashes
- **R** = Restricted drives
- **A** = Antivirus failure
- **S** = Strange emails
- **H** = Hardware/Mouse abnormal behavior

OTHER THREATS TO COMPUTER SECURITY

SPOOFING

Spoofing is a technique in which an attacker pretends to be a trusted user, computer, or website in order to gain unauthorized access to information.

It is also known as **Masquerading**.

Types

- IP Spoofing
- Email Spoofing
- Website Spoofing

IP Spoofing

In IP Spoofing, an attacker uses another computer's IP address to hide their identity.

Example

A hacker uses a fake IP address to access a network.

Exam Tip

Spoofing = Pretending to be someone else.

SALAMI TECHNIQUE

The **Salami Technique** is a cybercrime in which very small amounts of money are stolen from many accounts so that individual victims do not notice the loss.

The total stolen amount becomes large when collected from thousands of accounts.

Example

₹1 is deducted from one lakh bank accounts.

Exam Tip

Salami Attack = Small Loss × Many Victims = Huge Profit

HACKING

Hacking is the act of gaining unauthorized access to a computer system, network, or data.

Hackers identify weaknesses and exploit them to enter systems.

Hacking may sometimes lead to a **Denial of Service (DoS)** attack, which prevents legitimate users from accessing resources.

Example

A person breaks into a company's server without permission.

Exam Tip

Hacker = Unauthorized Intruder

CRACKING

Cracking is the act of illegally breaking security protections of software, systems, or networks.

Crackers often use malicious tools to damage systems or steal information.

Common Cracking Tools

- Password Crackers
- Trojans
- Viruses
- War Dialers

Example

Breaking a software license key to use paid software for free.

Cyber Cracker

A **Cyber Cracker** is a person who uses computers to cause harm, steal information, or destroy systems.

Exam Tip

Hacking = Accessing System; Cracking = Breaking Security.

PHISHING

Phishing is a fraudulent technique used to obtain sensitive information such as usernames, passwords, ATM PINs, OTPs, and credit card details by pretending to be a trusted source.

Example

A fake bank website asks users to enter their login credentials.

Exam Tip

Phishing = Fake Website + Stolen Information

SPAM

Spam refers to unwanted or unsolicited bulk electronic messages sent to a large number of users.

Spam is most commonly associated with email.

Characteristics

- Unwanted messages.
- Sent in bulk.
- Often contains advertisements or scams.

Example

Hundreds of promotional emails arriving daily.

Exam Tip

Spam = Unwanted Bulk Messages

ADWARE

Adware is software that automatically displays advertisements to generate revenue for its developer.

Some adware is legitimate, while others display unwanted advertisements excessively.

Characteristics

- Displays advertisements.
- May slow down computers.
- Can redirect browsers.

Example

A free application continuously showing pop-up advertisements.

Exam Tip

Adware = Advertisement + Software

ROOTKIT

A **Rootkit** is a special type of malware designed to gain administrator-level access to a computer while remaining hidden from users and security software.

Rootkits are among the most dangerous malware because they are difficult to detect and remove.

Characteristics

- Hides its presence.
- Gains administrative privileges.
- Allows attackers complete control.
- Evades antivirus detection.

Example

A hidden malware that secretly gives hackers full control over a computer.

Exam Tip

Rootkit = Hidden Administrator Malware

QUICK REVISION TABLE

Threat	Main Purpose
Worm	Self-spreading malware
Trojan	Fake useful software
Spyware	Secretly collects information
Spoofing	Pretending to be someone else
Salami Technique	Stealing tiny amounts from many accounts
Hacking	Unauthorized access
Cracking	Breaking security protections
Phishing	Stealing information through deception
Spam	Unwanted bulk messages
Adware	Displays advertisements
Rootkit	Hidden administrator-level malware

SOLUTIONS TO COMPUTER SECURITY THREATS

Computer security threats can be reduced or prevented by using various security tools and techniques. These safeguards protect computers, networks, and data from unauthorized access, viruses, malware, and cyber attacks.

ANTI-VIRUS SOFTWARE

Anti-virus software is a security application designed to detect, prevent, block, and remove viruses, worms, trojans, spyware, adware, and other malicious programs from a computer system.

It continuously monitors files, programs, and system activities to identify suspicious behavior and eliminate threats before they can damage the computer.

Functions of Anti-Virus Software

- Detects viruses and malware.
- Scans files and folders.
- Removes infected files.
- Provides real-time protection.
- Protects internet browsing.
- Blocks malicious downloads.

Popular Anti-Virus Software

- Avast
- AVG
- K7
- Kaspersky
- Trend Micro
- Quick Heal
- Symantec
- Norton
- McAfee

Example

Quick Heal detects and removes an infected file from a computer.

Exam Tip

Anti-virus = Detect + Prevent + Remove Malware

DIGITAL CERTIFICATE

A Digital Certificate is an electronic document used to verify the identity of a person, organization, website, or device communicating over a network.

It acts like a digital identity card and helps users confirm that a sender is genuine.

Digital certificates are issued by trusted organizations called Certificate Authorities (CA).

Functions of Digital Certificate

- Verifies identity.
- Secures online communication.
- Supports encryption.
- Prevents impersonation.

Example

A secure banking website uses a digital certificate to prove that the website is genuine.

Exam Tip

Digital Certificate = Electronic Identity Card

DIGITAL SIGNATURE

A Digital Signature is an electronic signature used to verify the authenticity and integrity of a digital document or message.

It confirms:

- Who sent the document.
- That the document has not been modified.

Advantages

- Authentication.
- Integrity.
- Non-repudiation.
- Security.

Example

Signing an online income tax return using a Digital Signature Certificate (DSC).

Exam Tip

Digital Signature = Verify Sender + Verify Content

FIREWALL

A Firewall is a hardware or software security system that monitors and controls incoming and outgoing network traffic based on predefined security rules.

It acts as a security barrier between a trusted internal network and an untrusted external network such as the Internet.

Functions of Firewall

- Blocks unauthorized access.
- Filters network traffic.
- Protects against hackers.
- Monitors data packets.
- Prevents network attacks.

Types of Firewall

1. Hardware Firewall

Installed as a physical device between the network and the Internet.

2. Software Firewall

Installed as a program on a computer.

Example

Windows Firewall blocks suspicious internet connections.

Exam Tip

Firewall = Security Guard of Network

PASSWORD

A Password is a secret combination of characters used to verify a user's identity and grant access to a system or resource.

Passwords protect accounts, files, applications, and devices from unauthorized access.

Characteristics of Good Passwords

- Long length.
- Combination of letters.
- Numbers included.
- Special symbols included.
- Difficult to guess.

WEAK PASSWORD

A weak password is easy to guess and can be cracked quickly.

Common Weak Passwords

- Name
- Birth date
- Mobile number
- 123456
- Password123

Example

Rahul123

Exam Tip

Weak Password = Easy to Guess

STRONG PASSWORD

A strong password contains uppercase letters, lowercase letters, numbers, and special symbols.

Example

R@hul#2026!

Characteristics

- Difficult to guess.
- Hard to crack.
- Better security.

Exam Tip

Strong Password = Letters + Numbers + Symbols

FILE ACCESS PERMISSION

File Access Permission refers to the rights granted to users for accessing and managing files.

Modern operating systems allow administrators to control who can view, modify, or execute files.

Benefits

- Protects files.
- Controls user actions.
- Prevents unauthorized modifications.

Example

An employee can read a document but cannot edit it.

READ PERMISSION

Allows a user to open and view a file.

Example

A student can view examination results.

Exam Tip

Read = View Only

WRITE PERMISSION

Allows a user to modify or edit a file.

Example

A teacher updates student marks.

Exam Tip

Write = Modify Data

EXECUTE PERMISSION

Allows a user to run a program or script.

Example

Running a calculator application.

Exam Tip

Execute = Run Program

TERMS RELATED TO SECURITY

EAVESDROPPING

Eavesdropping is the unauthorized interception of private communication while it is taking place.

The attacker secretly listens to or captures communication between users.

Example

A hacker intercepts a conversation on a public Wi-Fi network.

Exam Tip

Eavesdropping = Secret Listening

MASQUERADING

Masquerading occurs when an attacker pretends to be an authorized user in order to gain unauthorized privileges.

It is closely related to spoofing.

Example

A hacker logs in using another user's credentials.

Exam Tip

Masquerading = Fake Identity

PATCHES

A Patch is a small software update released by developers to fix bugs, vulnerabilities, and performance issues.

Patches improve security and functionality.

Functions

- Fix security holes.
- Remove bugs.
- Improve performance.
- Add stability.

Example

Microsoft releases a security patch for Windows.

Exam Tip

Patch = Software Repair Tool

Important Fact

Vendor-created program modifications are called Patches.

LOGIC BOMB

A Logic Bomb is malicious code intentionally inserted into a system that activates only when specific conditions are met.

Unlike viruses and worms, logic bombs do not replicate themselves.

Characteristics

- Hidden inside software.
- Activates on a specific date or event.
- Causes damage after activation.

Example

A program automatically deletes files on a particular date.

Exam Tip

Logic Bomb = Time-Based or Event-Based Attack

APPLICATION GATEWAY

An Application Gateway is a security mechanism that controls traffic for specific applications such as FTP, HTTP, and Telnet.

It examines application-level data before allowing communication.

Functions

- Filters application traffic.
- Provides additional security.
- Monitors user requests.

Example

An FTP gateway checks file transfer requests before allowing them.

Exam Tip

Application Gateway = Application-Level Firewall

PROXY SERVER

A Proxy Server is an intermediary server that receives requests from users and forwards them to the destination server.

It hides the user's actual IP address and improves security.

Functions

- Hides network identity.
- Filters traffic.
- Improves privacy.
- Controls internet access.
- Acts as a firewall.

Example

A company uses a proxy server to monitor employee internet usage.

Exam Tip

Proxy Server = Middleman Between User and Internet

SOFTWARE LICENSE

A Software License is a legal permission granted by the software owner that specifies how software can be used.

It defines the rights and restrictions associated with software usage.

Example

Purchasing a Microsoft Office license.

Exam Tip

Software License = Legal Permission to Use Software

SOFTWARE PIRACY

Software Piracy refers to copying, distributing, installing, or using software without the permission of the copyright owner.

It is illegal and punishable under law.

Types of Software Piracy

- Illegal copying
- Unauthorized distribution
- Using cracked software
- Sharing license keys

Example

Installing one licensed software on multiple computers without permission.

Exam Tip

Software Piracy = Unauthorized Copying of Software

QUICK REVISION TABLE

Term	Remember As
Anti-virus	Malware remover
Digital Certificate	Electronic identity card
Digital Signature	Electronic signature
Firewall	Network security guard
Password	Secret access key
Read Permission	View file
Write Permission	Modify file
Execute Permission	Run file
Eavesdropping	Secret listening
Masquerading	Fake identity
Patch	Software fix
Logic Bomb	Condition-based attack
Application Gateway	Application-level security
Proxy Server	Internet middleman
Software License	Legal software permission
Software Piracy	Illegal software copying