CS & DF

Unit 2 : Cyber Crime Issues and Cyber attacks

contents

- Unauthorized access , Computer Intrusions

- Internet hacking and cracking
  - types of hackers
  - types of cracking methods

- Viruses , Worms ,Trojans
- Software piracy , Intellectual property
- Mail bombs
- Cybercrime prevention methods
- Backups , Archival storage , Disposal of data
- Firewall and Vpns
- Hardware protection mechanism
- OS security

Unauthorized access to Computers

- **Definition:** When someone uses a computer, network, or online account without the owner's permission, it is called unauthorized access. It means entering systems that you are not allowed to.

- **Key Idea:** This is illegal and can harm others. Hackers or intruders can steal data, change files, or misuse information for their benefit.

- **Examples:**
  - Logging into someone else's email or social media account without permission.
  - Hacking into a company's database to get secret information.
- **Impact:**
  Unauthorized access can cause serious problems like financial loss, leaking of personal or confidential information, damage to reputation, and legal punishment for the intruder.

Computer Intrusions

- **Definition:**
  Unauthorized access to a computer or network to steal, modify, or damage data.

- **How It Happens:**
  Through hacking, malware, phishing, or exploiting system weaknesses.

- **Examples:**
  Hacking emails, installing malware, or accessing private company data.

- **Impact:**

1. Data loss
2. financial damage
3. reduced trust
4. system problems.

Types of Computer Intrusions

- **Hacking:**

  Unauthorized access to a system to steal or alter data.

- **Malware Attack:**

  Using viruses, worms, or trojans to damage or spy on computers.

- **Phishing:**

  Tricking users into revealing passwords or sensitive information.

- **Denial of Service (DoS) Attack:**

  Making a system or network unavailable to users by overwhelming it with traffic.

Internet Hacking

- Hacking is the act of gaining unauthorized access to computer systems, networks, or digital devices by exploiting vulnerabilities, often with the intention of stealing, destroying sensitive information.
- It can cause serious consequences such as data theft, financial fraud, identity misuse, and large-scale security breaches that affect individuals, organizations, and even governments worldwide.
- **Types Of Hackers :**
- **White Hat Hacker:**

Ethical hackers who test systems to find security flaws and help protect companies or users.

Example: A security expert hired to find vulnerabilities before criminals exploit them.

- **Grey Hat Hacker:**

Hackers who sometimes hack systems legally and sometimes illegally. They may report flaws or sometimes exploit them.

Example: Someone who hacks a website without permission but informs the owner about the vulnerability.

- **Black Hat Hacker:**

Malicious hackers who illegally hack systems to steal data, cause damage, or commit financial fraud.

Example: A hacker breaking into bank accounts to steal money.

White, gray and black hat comparison

WHITE HAT

Considered the good guys because they follow the rules when it comes to hacking into systems without permission and obeying responsible disclosure laws

GRAY HAT

May have good intentions, but might not disclose flaws for immediate fixes

Prioritize their own perception of right versus wrong over what the law might say

BLACK HAT

Considered cybercriminals; they don't lose sleep over whether or not something is illegal or wrong

Exploit security flaws for personal or political gain—or for fun

Cracking

- Cracking means breaking into software or systems by removing security features like passwords, licenses, or encryption.
- It is usually done to use paid software for free, steal data, or bypass security protections, which is illegal.
- **Types Of Cracking :**
- **Password Cracking:**

  Breaking or guessing passwords using brute force or dictionary attacks.

  Example: Hacking a Facebook account by guessing or cracking its password.

- **Software Cracking:**

  Removing license keys or protections to use paid software for free.

  Example: Using a cracked version of Photoshop without buying it.

- **Network Cracking:**

  Breaking into secured networks like Wi-Fi to gain unauthorized access.

  Example: Cracking a neighbor’s Wi-Fi password to use the internet.

- **Email Cracking:**

  Hacking into email accounts to steal personal data or misuse identity.

  Example: Accessing someone’s Gmail account to send fake messages.

Virus , Worms , Trojans

VIRUS	WORMS	TROJANS
Requires a host program to spread	Self - Propagates through network	Disguises as legitimate Software
Damage or Disrupts System	Steal Data or Cause Harm	Create Backdoor Access
File Corruption or Deletion	Network Congestion	Data theft or Espionage
Cannot be controlled remotely.	Can be controlled remotely.	Can be controlled remotely.
Often detectable by antivirus software.	More difficult to detect as they exploit system vulnerabilities.	Often hidden in legitimate-looking software.
Spreading Rate is Moderate	Spreading Rate is Fast	Spreading Rate is Slow

Software Piracy

- Software piracy is the illegal use, copying, or distribution of software without a valid license.
- It commonly occurs through cracked software, fake license keys, or pirated downloads.
- Examples include using paid software like Microsoft Office or games without purchasing them.
- It leads to financial loss for companies, legal punishment for users, and risk of viruses or malware.
- Pirated software often lacks official updates and security patches, making systems more vulnerable.
- Many pirated copies come bundled with malware, spyware, or ransomware, risking user data.
- Software piracy hurts innovation, as companies lose revenue and may reduce new product development.

Intellectual Property

- Intellectual Property (IP) means creations of the mind like inventions, designs, art, music, or software, which are legally protected.
- It gives the creator exclusive rights to use, sell, or license their work for a certain period.
- Types of IP include Patents (inventions), Copyrights (art, music, software), Trademarks (brand names, logos), and Trade Secrets (confidential business info).
- Protecting IP encourages innovation and creativity while preventing others from copying or misusing the work.
- Violation of IP rights, like piracy or counterfeiting, can lead to legal action, fines, or penalties.

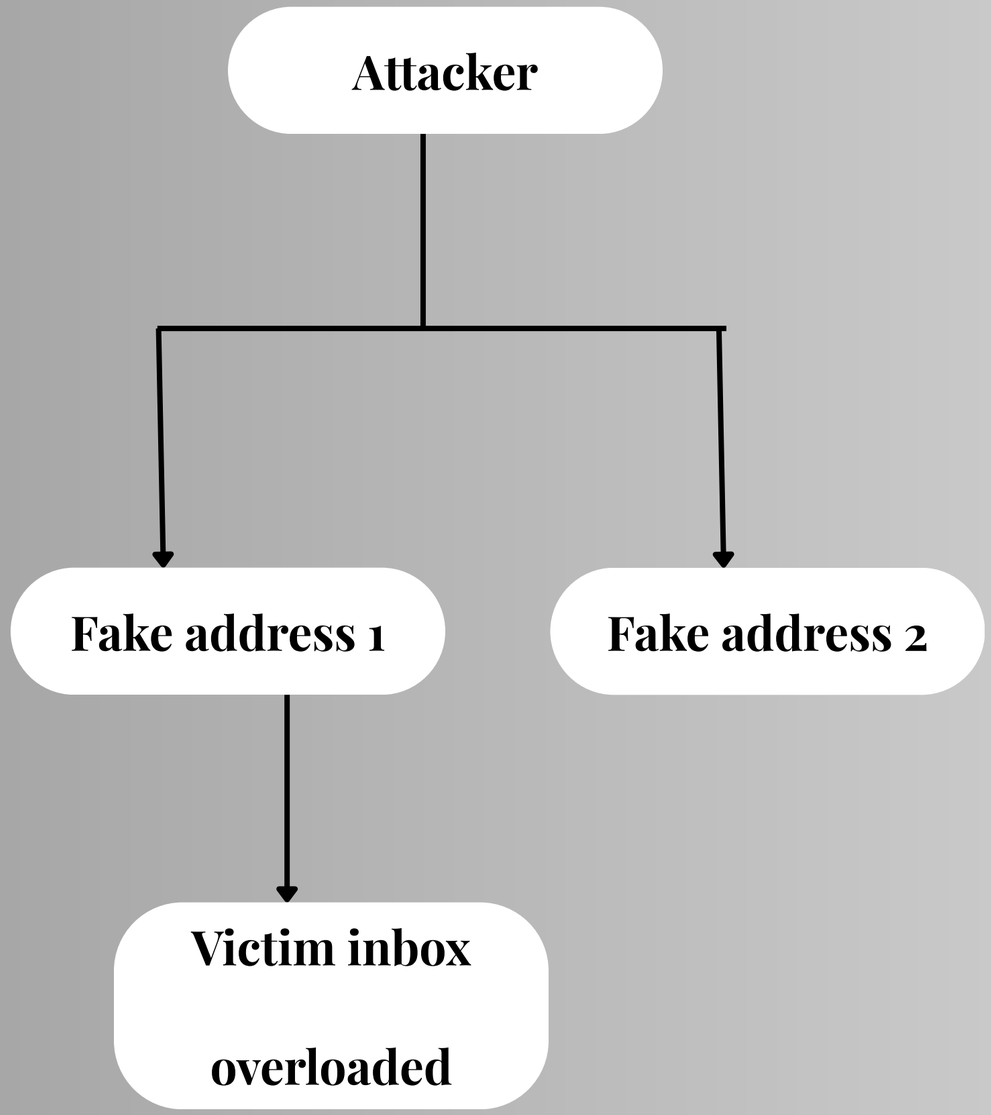
E mail Bombing

- Email bombing is when someone sends a huge number of emails to a target email account to overwhelm it.
- The goal is to flood the inbox, slow down the system, or make it unusable.
- It can cause loss of important emails, disruption of communication, and stress for the user.
- Prevention includes using spam filters, limiting incoming emails, and monitoring suspicious activity.

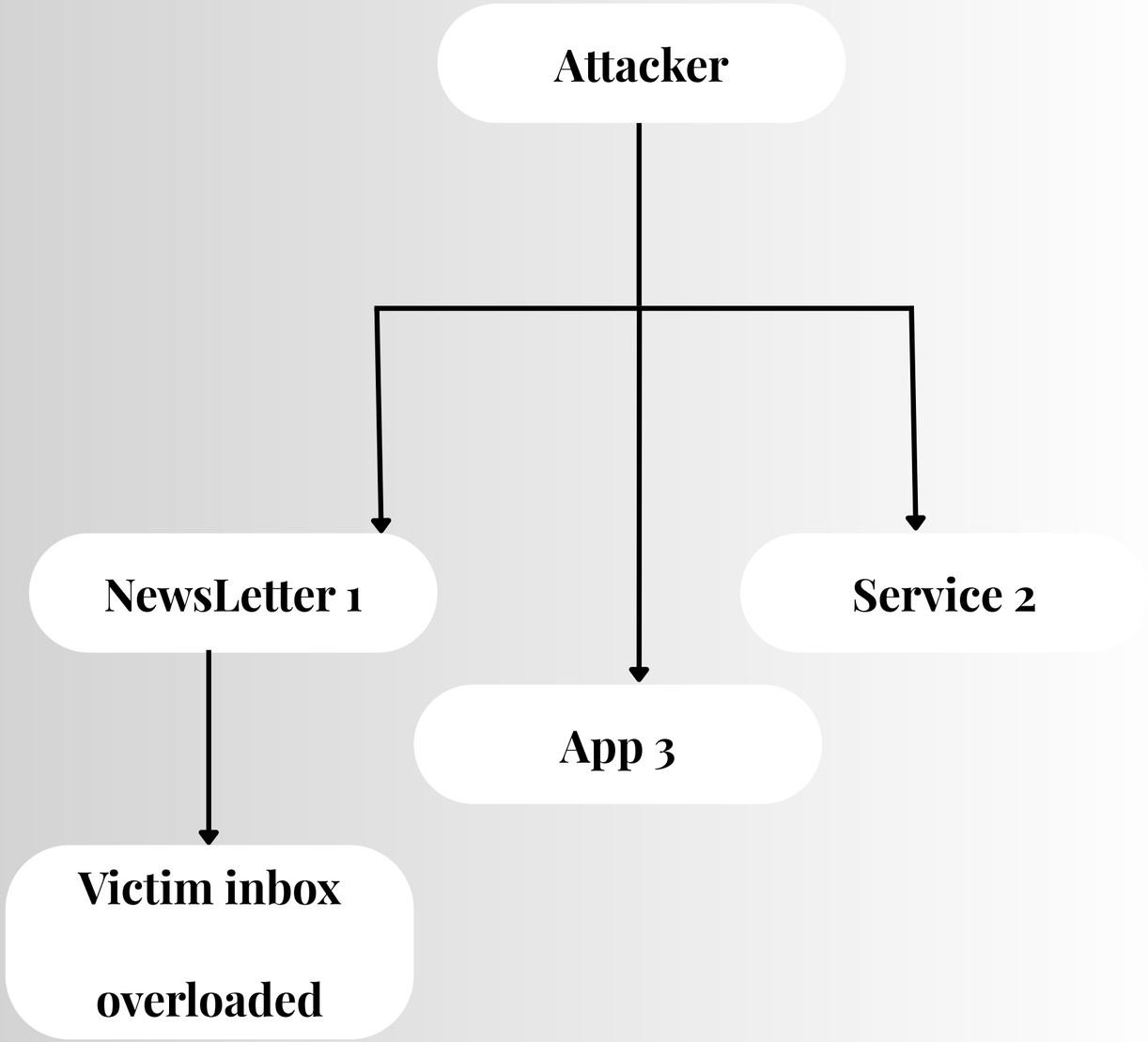
Types of Email Bombing :-

- **Mass Mailing:**
  Sending a huge number of emails to the target from one or multiple accounts.
- **Dictionary Attack:**
  Using automated tools to send emails to all possible combinations of addresses on a domain.

Forged/Bot Email Bombing



Subscription Bombing



Cybercrime Prevention Methods

- **Strong Passwords & Authentication**
  - Use complex and unique passwords.
  - Enable Multi-Factor Authentication (MFA).

- **Use Updated Security Software**
  - Install antivirus and anti-malware software.
  - Keep the firewall active.

- **Safe Browsing & Email Practices**
  - Do not click on unknown links or attachments.
  - Learn to identify phishing emails.

- **Secure Wi-Fi & Networks**
  - Protect Wi-Fi with a strong password.
  - Use a VPN (Virtual Private Network).

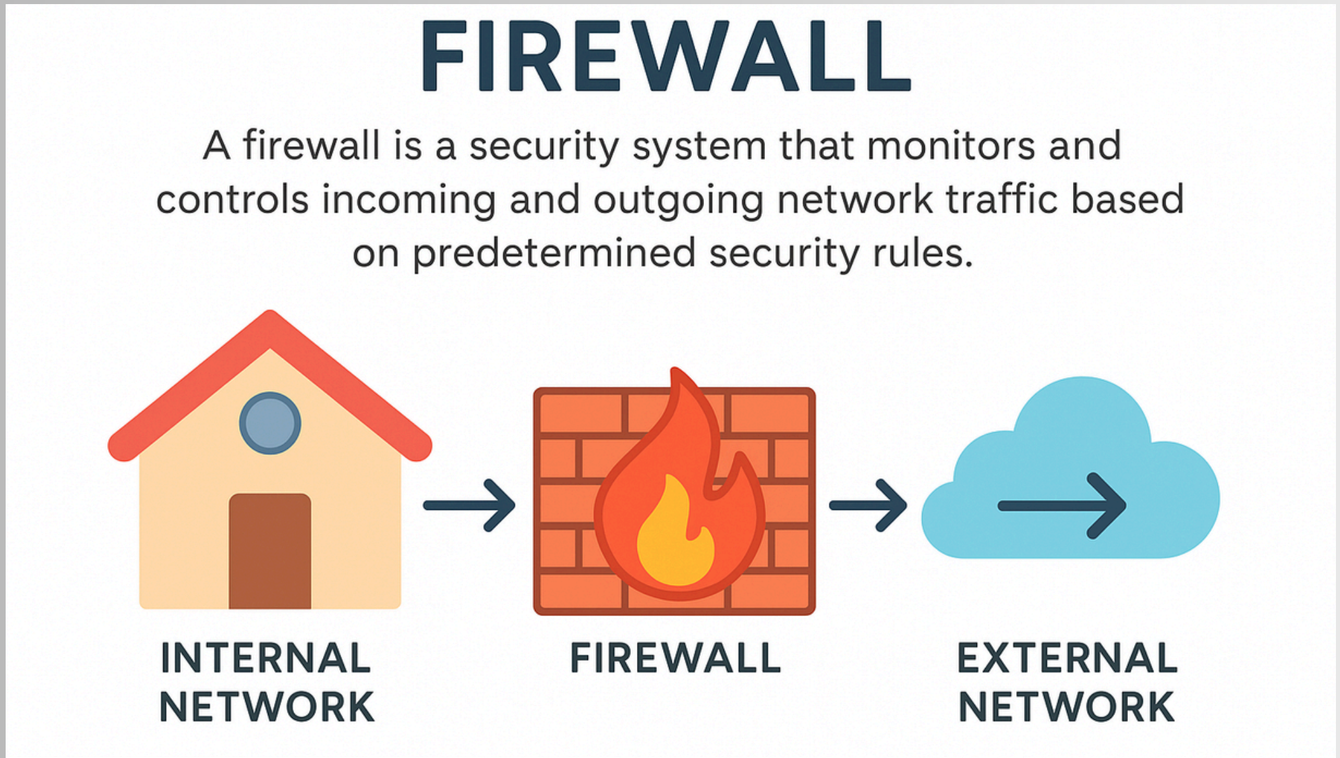
Backup , Archival Storage and Disposal of data

BACKUP	ARCHIVAL STORAGE	DISPOSAL OF DATA
Data recovery in case of loss or corruption	Long-term preservation of data for future reference or compliance	Permanent removal of data when no longer needed
Frequent (daily, weekly, or real-time)	Infrequent (monthly, yearly, or as needed)	One-time when data retention period ends
Quick and easy access for recovery	Slower access, mainly for reference or audits	Data becomes inaccessible permanently
Short to medium term	Long-term (years)	Not applicable (data deleted)

Firewall and VPNs

- **Definition:**

A firewall is a security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It acts like a barrier between your internal network and external networks (like the internet) to block unauthorized access



- **Types of Firewall:**

1. **Hardware Firewall** – Physical device that protects the entire network.
2. **Software Firewall** – Program installed on a computer to protect that device.
3. **Cloud Firewall** – Firewall deployed in cloud environments to secure cloud networks.

- **Functions / Uses:**

- Blocks unauthorized access from hackers.
- Filters harmful or suspicious data packets.

- **VPN(Virtual Private Network)**

- VPN creates a secure, encrypted tunnel for your internet traffic.
- Hides your real IP address and shows the VPN server's IP.
- Protects your online activity from hackers, ISPs, and government tracking.

- **Types of VPN**

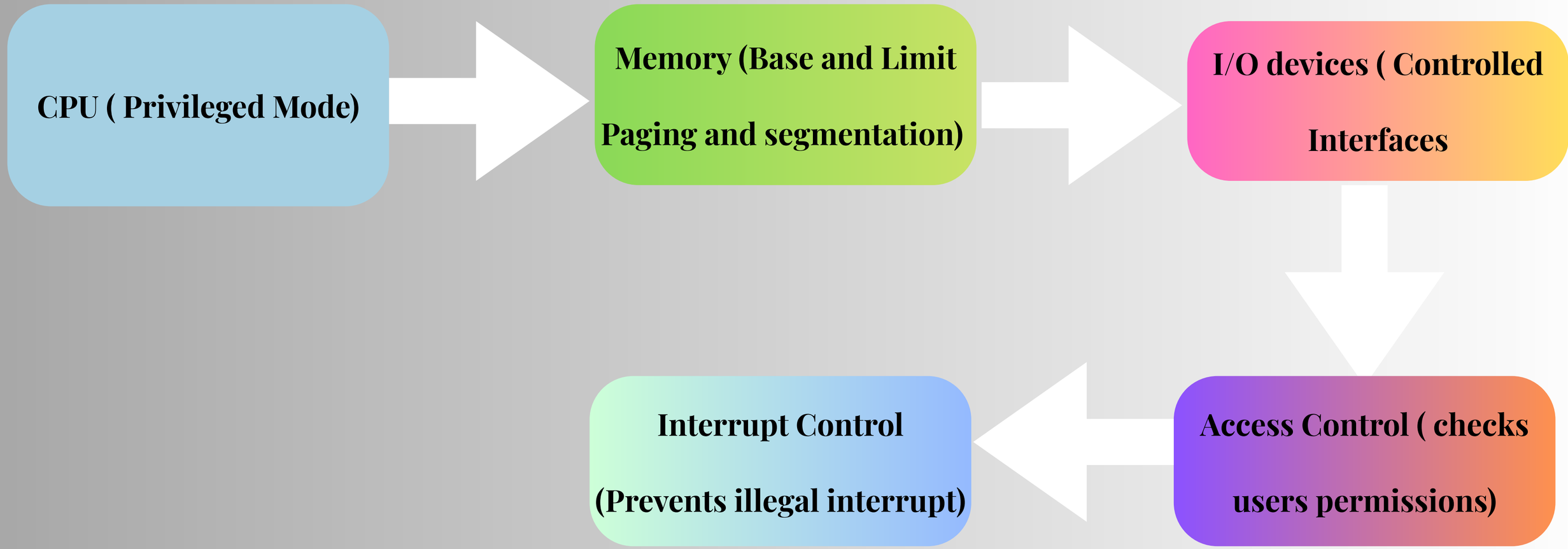
- **Remote Access VPN** – Connects individual users securely to a network.
- **Site-to-Site VPN** – Connects two networks securely, commonly used by businesses.
- **Benefits**

1. **Privacy & Anonymity** – Keeps your identity hidden online.
2. **Security** – Safe browsing, especially on public Wi-Fi.

- **Popular VPNs**

- ExpressVPN
- NordVPN
- Surfshark

Hardware Protection Mechanism



OS Security

- **User Authentication**
  - Allows only authorized users to access the system.
  - Methods: Passwords, Biometrics, Security Tokens.

- **Access Control**
  - Restricts who can access files, memory, and devices.
  - Uses permissions: Read, Write, Execute.

- **Audit & Logging**
  - Records user activities and system events.
  - Helps in tracking unauthorized access or breaches.

- **Malware & Threat Protection**
  - Protects against viruses, worms, and malware.
  - Uses antivirus software, firewalls, and system updates.

THANK YOU