1. Malware (Malicious Software)

Definition:

Malware is *any software intentionally created to harm, exploit, or otherwise compromise a computer, network, or user's data.*

It operates silently and spreads through files, emails, downloads, or network vulnerabilities.

How It Works:

Malware can **infect** systems (like viruses), **spy** on users (spyware), **lock files for ransom** (ransomware), or **use your computer remotely** (botnets). It exploits **software flaws or human mistakes** (like downloading infected attachments).

Examples:

- **WannaCry (2017):** A ransomware that spread globally, encrypting files on Windows PCs and demanding Bitcoin payments. It affected hospitals, banks, and government offices.

- **Trojan: Zeus (2007):** Disguised as banking software to steal online banking credentials.

- **Spyware: Pegasus (2016):** Used to spy on journalists and politicians through mobile phones.

Key Point:

Malware targets *systems* — it's a **technical attack**.

---

2. Social Engineering

Definition:

Social engineering manipulates **people**, not machines. It uses *psychological tricks* to make victims share confidential data or perform unsafe actions.

How It Works:

Attackers pretend to be trusted individuals (like IT staff or bank agents) to gain passwords, financial data, or access. It relies on **trust, fear, urgency, or curiosity**.

Examples:

- **Phishing Emails:** "Your account is locked! Click here to reset your password." → Leads to a fake login page.

- **Vishing:** Fake calls pretending to be from "Microsoft support" asking for remote access.

- **Baiting:** USB drives left in offices labeled "Confidential Salary Data" — when plugged in, they install malware.

Key Point:

Social engineering targets *humans* — it's a **psychological attack**.

---

3. Insider Threats

Definition:

An insider threat arises from **individuals within the organization** (employees, contractors, or partners) who misuse their legitimate access, intentionally or accidentally, to harm the organization.

Types:

1. **Malicious Insider:** Intentionally leaks or sabotages data.

2. **Negligent Insider:** Carelessly causes breaches (e.g., weak passwords, clicking phishing links).

3. **Compromised Insider:** Accounts hijacked by outsiders.

Examples:

- **Edward Snowden (2013):** NSA contractor who leaked classified documents.
- **Capital One Breach (2019):** A former employee exploited internal access to steal customer data.
- **Employee Phishing:** Staff member accidentally clicking a fake HR email link.

Key Point:

Insider threats come from *within* — people who already have **authorized access**.

---

4. Nation-State Attacks

Definition:

These are **government-sponsored cyberattacks** aimed at another nation's digital infrastructure, economy, or military systems to gain **political, military, or strategic advantage.**

Characteristics:

- Highly **sophisticated**, **well-funded**, and **long-term**.
- Targets critical systems like **power grids, defense, finance, or communication**.
- Often linked with **cyber espionage** or **sabotage**.

Examples:

- **Stuxnet (2010):** Joint U.S.–Israel malware that damaged Iran's nuclear centrifuges.
- **SolarWinds Attack (2020):** Russian hackers infiltrated U.S. federal agencies via software updates.
- **Chinese APT Groups:** Conduct corporate espionage to steal trade secrets and military data.

Key Point:

Nation-state attacks are **politically motivated**, not profit-driven.

---

5. Organized Cybercrime

Definition:

Organized cybercrime involves **criminal groups or syndicates** using technology to conduct coordinated cyberattacks for **financial gain**.

Characteristics:

- Operates like a business (with hierarchy and roles).
- Sells hacking tools, ransomware kits, or stolen data.
- May collaborate with corrupt officials or other gangs.

Examples:

- **DarkSide Group (2021):** Carried out the Colonial Pipeline ransomware attack, causing fuel shortages in the U.S.

- **Conti Ransomware Group:** Used ransomware-as-a-service (RaaS) to attack hospitals and corporations.

- **FIN7 Group:** Targeted retail and hospitality companies to steal credit card data.

Key Point:

Organized cybercrime is **financially motivated**, functioning like **digital mafia operations**.

- **Malware** = a *tool or weapon* used in many types of attacks.

- **Social Engineering** = *method* of manipulation (often leads to malware infection).

- **Insider Threat** = *trusted user* misusing access.

- **Nation-State Attack** = *politically motivated*, large-scale cyberwarfare.

- **Organized Cybercrime** = *financially motivated*, structured like criminal businesses.

Types of system calls

- Process Control: These calls manage the lifecycle of a process.
    - Examples: fork() (create a child process),
    - exec() (replace the current process with a new program),
    - wait() (wait for a child process to finish)
    - exit() (terminate a process),
    - kill() (send a signal to a process).
- File Management: These calls handle operations on files.
    - Examples: open() (open a file), read() (read data from a file), write() (write data to a file), close() (close a file), seek()(move the file pointer).
- Device Management: These calls manage interactions with devices.
    - Examples: ioctl() (send an I/O control command to a device), read() and write() (for device buffers), requesting and

releasing devices, getting and setting device attributes.

- Information Maintenance: These calls manage system-level information.
    - Examples: getpid() (get the process ID), gettimeofday() (get the current time), setting system parameters, and getting system and process attributes.
- Communication: These calls enable processes to communicate with each other.
    - Examples: pipe() (create a communication pipe), shm_open()(shared memory open), mmap()(memory map), sending and receiving messages, creating and deleting connections.