SUB: Cyber Security

Unit 1: Introduction to cyber Crime & Cyber Security

Prof: Morade D.S.

Cybercrime

Definition:

- "Cybercrime is the criminal activity which is committed by hackers or cybercriminals, individuals or organizations."

OR

- "The crime that includes and makes use of electronic devices and internet is called cybercrime."
- Cybercrime is when someone uses a computer and the internet to do something **illegal**.
- It includes stealing data, spreading viruses, or hacking into systems.

Cybersecurity:

"Cybersecurity is the process of preventing and detecting unauthorized use of your computer and network."

- Cybersecurity refers to the body of technologies, process and practices designed to protect computing devices, networks, applications and data from unauthorized access, damage or attacks.

Key Features of Cybersecurity

1. Stops external threats **like hackers or viruses.**
2. Protects from inside threats**, like an employee stealing data.**
3. Follows rules **and legal standards.**
4. Uses cloud-based security**, which protects online services.**
5. Detects and responds **to threats.**
6. Combines security tools **for full protection.**
7. Analyzes threats **to improve security**.

Evolution and Historical Context of Cyber Security

1960s: Birth of Computer Security

- Computers were kept safe physically.
- Password protection started at MIT.
- U.S. government began making rules for security.

1970s: First Security Models

- New models were made for protecting confidential data. Ex. Bell-Lapdula
- First hacking attempt happened.
- Bob Thomas created First computer worm called **Creeper** .
- **Reaper** was created by Ray Tomlinson to remove it – first antivirus program.

1980s: Viruses and Hacking

- First antivirus software came.
- Hacker attacks increased.
- **McAfee** antivirus company was started.
- Ethical hacking and laws like **Computer Fraud and Abuse Act (1986)** began.

1990s: Internet and Global Threats

- People started putting personal data online.
- Attacks like **email viruses**, **phishing**, and **DDoS** started.
- **Firewalls and anti-virus software** became common.
- **SSL** started to secure online payments.

2000s: Corporate and Government Focus

- Dangerous malware like **ransomware** increased.
- Governments made new laws and task forces.
- Laws like **HIPAA** (health data) and **GDPR** (data protection) were created.

2010s–Present: AI and Advanced Threats

- **Cloud computing** and **IoT (Internet of Things)** opened new ways for attacks.
- **AI and machine learning** help detect and respond to attacks quickly.
- More focus on cybersecurity awareness and training.
- Cybersecurity became a **global issue**, not just technical.

Information Security:

➢ Information security is also referred to as infosecurity.

It means **protecting important information** from being:

- **Seen** by the wrong people (unauthorized access),
- **Changed** without permission (modification),
- **Stolen**, deleted, or misused.

Cybercriminals:

"Cybercriminals are nothing but Criminals who attempt a crime that involves a computer, network, or any digital appliance in the commission of a crime."

Cybercriminals are categorized into following three groups:

- **Type I: Cybercriminals – hungry for recognition**

Examples:

Hobby hackers

IT professionals

Politically motivated hackers

Terrorist Organizations

- **Type II: Cybercriminals – interested in recognition**

Examples:

Psychological corrupts

Financially motivated hackers

Sponsored hackers

Organized criminals

- **Type III: Cybercriminals – the insiders**

Examples:

Former employees seeking revenge

Companies using employees to gain economic advantages through damage and/or theft

Classifications of Cybercrimes/Types of cybercrime

Cybercrimes are classified into **5 categories**:

1. Cybercrime Against Individuals

Crimes that directly affect a person.

Examples:

- **Phishing** – Tricking people to get personal data.
- **Spamming** – Sending unwanted emails/messages.
- **Cyber defamation** – Posting false/harmful content online.
- **Cyberstalking & harassment** – Repeated online threats/annoyance.
- **Computer sabotage** – Destroying or corrupting data.
- **Pornographic offenses**
- **Password sniffing** – Stealing passwords secretly.

2. Cybercrime Against Property

Targets money or digital assets.

Examples:

- **Credit card frauds**
- **Intellectual property theft** – Stealing digital content (software, music, etc.)
- **Internet time theft**
- **Password sniffing**

3. Cybercrime Against Organization

Aimed at businesses or institutions.

Examples:

- **Unauthorized access**
- **DoS attacks** – Crashing systems by overwhelming traffic.
- **Virus attacks**
- **Email bombing**
- **Salami attacks** – Stealing small amounts over time.
- **Logic bomb**
- **Trojan horse**
- **Data diddling**
- **Industrial spying**
- **Software piracy**

4. Cybercrime Against Society

Affects larger communities or the entire society.

Examples:

- **Forgery**
- **Cyberterrorism**
- **Web jacking** – Taking over websites.

5. Crime from Usenet Newsgroups

Crimes on public forums.

Examples:

- **Posting offensive or illegal content**

1] E-Mail Spoofing:

The E-Mail Spoofing technique is used to create a fake sender email address to deceive the recipient about the origin of the message Because of a change in the header information of the email, the original source is not able to identify and the recipient open or possibly responds to a message.

- There are various reasons for spoofing sender addresses such as:

A] Hide true identity of sender.

B] Avoid spam block lists.

Example - You worked at a small company and you received an mail that appear to come from your CEO you the CEO asks for some money you don't suspect anything because the display name reads as CEO and email address looks exactly like her company

2] Spamming:

Spamming is nothing but sending unwanted and profit-making bulk messages to a large number of users of the internet.

- **E-mails are categorized into spam if they are meeting the following criteria:**

A] *Mass Mailing*: Emails are targeted to multiple recipients(receiver) at the same time.

B] Anonymity: The identity of the sender is hidden.

Example – You get lots of identical emails from unknown senders offering something you never ask for

3] Cyber Defamation:

Cyber defamation happens when someone says or writes something **bad or false** about another person **online**, which can **damage their reputation**.

Two types of defamation:

A] Libel: It is also called written defamation. An offensive statement was published in paper form. Example - Someone writes a **false post** on Instagram saying a teacher is a thief. People see it and believe it, harming the teacher's image.

B] Slander: It is also called verbal defamation. An offensive statement made in a vocal form.

Example - Someone spreads **a false voice note** on WhatsApp saying a shop owner sells fake products. It harms the owner's business.

4] Internet Time Theft:

Internet Time Theft means to use the internet of another person at his cost by stealing the username and password without knowledge of that person.

Wi-Fi Theft:

- A neighbor secretly connects to your Wi-Fi using your password.
- You're paying the bill, but they're using your internet.

5] Salami Attack/Salami Technique:

It is a chain of small-small attacks, which results in bigger attacks. In other words, it is a practice to steal money a bit at a time with the intention that there is no noticeable variation in overall size.

Example - A programmer writes a code in a bank's system to **steal 1 paise (₹0.01)** from every customer's account.One customer won't notice 1 paise missing. But if there are **1 crore customers**, the attacker gets ₹10 lakh!

6] Data Diddling:

It is a technique of unauthorized change or alters the data as entered into the computer system by a clerk of data entry or computer virus.

7] Forgery:

Forgery means the creation of false documents, signatures with false intention. An example of forgery is when a person signs in using another's name to deceive(cheat).

Example - A person finds someone else's cheque book and **signs that person's name** on a cheque to **withdraw money from their bank account**. Even though it looks like the original person signed it, it's actually **a fake signature** done with the **intention to cheat** and get money.

8] Web Jacking:

Web Jacking is a hacker who blocks an organization's website after gaining access to it. For example, one of the Indian hackers got access to the website of Pakistani railways and flicked the Indian flag on the homepage for some hours in 2014 at the time of Independence Day of India.

9 . Newsgroup, Spam/Crimes Emanating from Usenet Newsgroup:

Newsgroup spam means sending **unwanted or junk messages** in these discussion groups — like ads or fake messages — to trick or scam people.

Example - Someone posts a fake message in a health discussion group claiming a "miracle cure" and adds a link. When users click the link, it installs a virus or steals their information.

10 spying/industrial Espionage:

is a crime conducted illegally to steal business secrets. An employee of the company may gain company employment for spying purposes or collecting business data unethically

Example:
A person gets a job in a mobile company and secretly sends the designs of a new phone model to a competitor before it is launched. The competitor uses that idea to build a similar phone faster

11. Hacking:

Hacking is a practice used to gain unauthorized access to data of computers or systems.

Some types of hackers are:

a. **Script Kiddies**: Script kiddies are one of the types of hackers who don't have much idea about hacking but want to learn more.
b. **White Hat:** White hat hackers are the professionals. who are specialized in hack the system. White hat hackers work for an organization ethically.
c. **Black Hat**: Black hat hackers are professionals. who maliciously break into a computer system or network system with the wrong intention.
d. **Grey Hat:** Grey hat hackers are professionals, who sometimes violate laws but without wrong intention like black hat hackers.
e. **State Sponsored /Nations Sponsored hackers**: State Sponsored / Nation's Sponsored hackers are the professional who works for the nation.

12. Online Frauds:

Online Frauds is the deceptive activity which includes identity theft, identity spoofing, spam, online scams etc.,

13. Computer Sabotage:

Computer Sabotage is defined as purposeful damage the information or equipments of an organization or business.

14. Email Bombing/Mail Bombs:

Email bombing/Mail bombs is the misuse of an internet to send large number of mails to a single recipient with the aim to overflow the inbox.

15. Computer Network Intrusions:

Computer network intrusion is any unlawful activity of the network to steal valuable resources of network, which always put at risk the security of network and its data.

Example - A hacker breaks into a school's computer system and deletes students' exam records.

16. Password Sniffing:

Password sniffing technique is used to steal sensitive information of user, such as username and password. Database can be breached even it is having strong password.

Example: You use Wi-Fi at a café. A hacker on the same Wi-Fi uses a tool to "sniff" your login details when you access your email or bank account

17. **Credit Card Frauds:**

Credit card frauds are the scammer fraud committed through a payment card (debit/credit card) from your bank account without your knowledge.

Example:You enter your card number on a fake shopping website. The scammer uses it to buy expensive items using your money.

18. Identity Theft:

It is the crime which gains personal/financial information of someone and use their identity to commit fraud.

Example: A fraudster uses your PAN and photo to apply for a loan. Later, you get a notice that you didn't pay the loan — even though you never took it

Vulnerability, Threats, and Harmful Acts

Vulnerability

Meaning:
A **vulnerability** is a weakness in a system that can be used by hackers or attackers to harm it.

Example:
Using an old password like "123456" is a vulnerability.

Types of Vulnerabilities:

1. **Hardware**
   - Sensitive to humidity/dust
   - Old storage devices
   - Overheating issues
2. **Software**
   - Bugs in programs
   - Weak or insecure code
   - No proper audit system
3. **Network**
   - No data encryption (e.g., messages sent in plain text)
   - Poor network design
4. **Personnel (People)**
   - Poor hiring process
   - Employees with no cybersecurity knowledge
   - Insider threats
5. **Physical Site**
   - Natural disasters like floods
   - Power cuts
6. **Organizational**
   - No regular checking/audits

Reasons for Vulnerabilities

1. **Complexity** – Big systems = More chances of mistakes
2. **Familiarity** – Common software is easier for hackers to attack
3. **Connectivity** – More connections = More entry points
4. **Password Flaws** – Weak/repeated passwords
5. **OS Design Flaws** – Bad system design
6. **Unsafe Internet Use** – Clicking unknown links
7. **Software Bugs** – Errors in the code
8. **Unchecked User Input** – No validation = Hackers can insert harmful commands
9. **Repeating Mistakes** – Not fixing old errors

➢ Threats

Meaning:
A **threat** is anything that can harm or disrupt a system. It can be done by people (hackers) or by mistake (like not updating software).

Example:
A hacker trying to steal your data is a threat.

Types of Cyber Security Threats:

- **Malware**: Harmful software like spyware, ransomware, worms
- **Hacking**
- **Viruses & Worms**
- **Trojan Horse**
- **Spoofing, Sniffing**
- **Denial of Service (DoS)**

➢ Harmful Attacks

Meaning:
Attacks that use threats to damage a system.

Types:

1. **Active Attack** – Change or damage data
    - *Example:* Hacker modifies your files
2. **Passive Attack** – Steal info secretly
    - *Example:* Reading your emails without changing anything
3. **Insider Attack** – Done by someone from inside (employee)
4. **Outsider Attack** – Done by someone from outside (hacker)

➢ Risk

Meaning:
Risk is the chance that a threat will use a vulnerability to harm a system.

Example:
If you use a weak password:

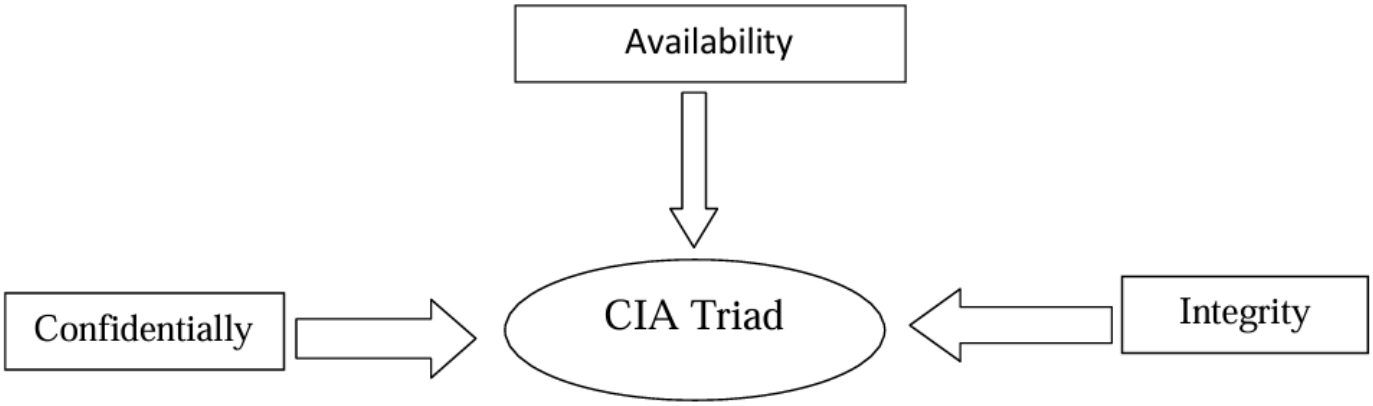
- **Vulnerability**: Weak password
- **Threat**: Hacker tries to guess the password
- **Risk**: Hacker enters your system and steals data

CIA Triad:

- The CIA triad is a security model that represents core objectives of data security
- CIA triad is a representation to show policies for security of information within an organization.
- The three key principles, confidentiality, integrity and availability, are guaranteed available in any secure system.
- The CIA Triad is a model used in cybersecurity to protect information. It stands for:

C – Confidentiality
I – Integrity
A – Availability

These are the three main goals of keeping data safe.



1. **Confidentiality:**
    - Confidentiality is the ability to ensure that information is accessible only to those who are authorized to access. it hides information from unauthorized people
    - Confidentiality of data means protecting the information from disclosure to unauthorized parties.
    - It is ensured that the information, either in transit or stored, is accessible only to entities which are authorized to access those resources
    - Information such as ATM pin, bank account details and personal information should be kept private and confidential. Protecting this information is a major part of information security.

2. **Integrity:**
    - Integrity is the ability to ensure that unauthorized person should not modify data without owner's permission
    - Integrity means making sure the information is correct and not changed by anyone who is not allowed.

3. **Availability:**
    - Availability is the ability of infrastructure to function according to business expectations.
    - Availability of data should be available 24 × 7.
    - Data availability has two dimensions for their access, the first dimension is about to make data available publically without any restrictions (e.g., annual turnover and list of their products are commonly available at authenticated websites of the company). The second dimension of data availability is non-availability of the data to the public at large because of critical nature or its secrecy. Since privacy of the information is a major concern then such data should make available to special and authorized users only. E.g., Income tax- related information is not allowed to publish in public.

Questions:

What is cybersecurity? [2M]

What is cybercrime? [2M]

What is cybercrime?

What is cybercriminal? [2M]

Explain History of cybersecurity.

Explain **categories of Cybercriminals.**

Explain categories of cybercrime and different types of cybercrime.

Explain CIA traid