

Name: Khadija Arefin Meem

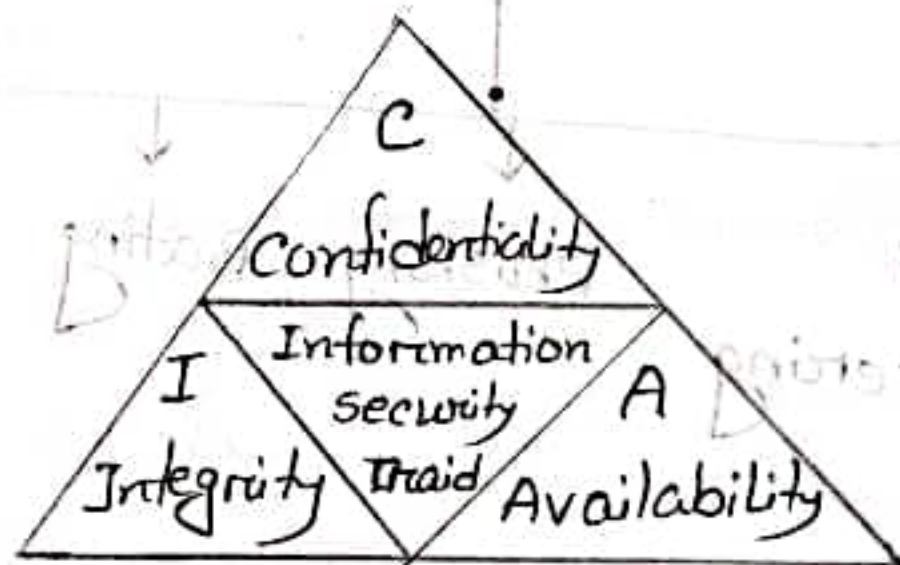
ID: IT21059

16-04-2025

### Assignment 01

Security triad CIA:

The CIA triad - Confidentiality, Integrity and Availability - is a guiding model in information security. A comprehensive information security strategy includes policies and security controls that minimize threats to these three crucial components.



Definition of cyber attack:

A cyberattack occurs when there is an unauthorized action against computer infrastructure that compromises the confidentiality, integrity or availability of its content.



## Types of cyber Attack:

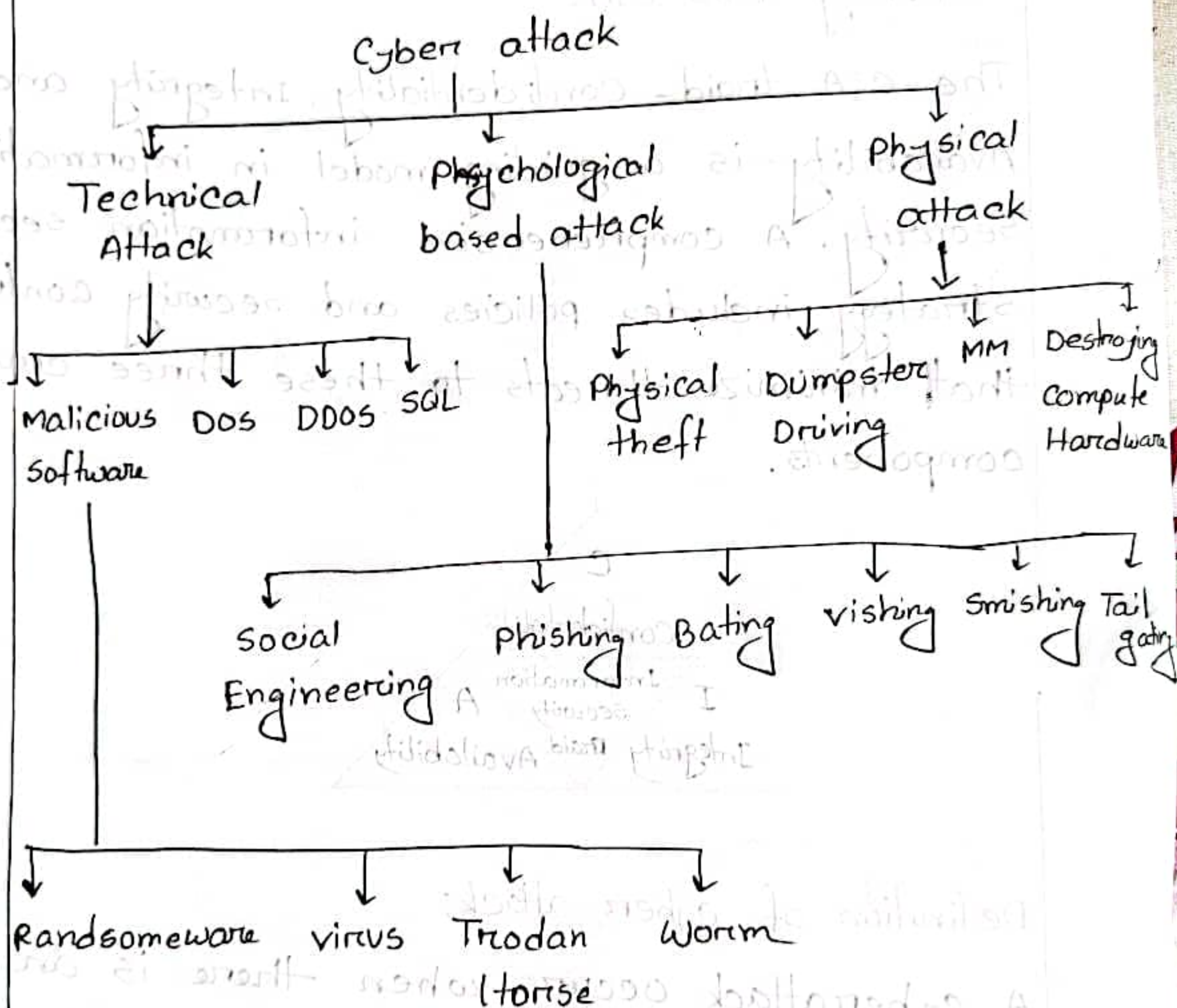


Fig: Types of cyber attack



Symmetric encryption:

Symmetric encryption is a type of cryptography where the same key is used for both encryption and decryption of data.

Key point:

- Single key is both encryption and decryption.
- Faster and less complex than asymmetric encryption.

- Suitable for large amount of data.

Challenge sector:

Securely sharing the key between parties.

Example:

AES, DES, 3DES, Blowfish and Twofish.



Asymmetric encryption:

Asymmetric encryption is a cryptographic method that uses two different keys - a public key and a private key for encryption and decryption.

- The public key is shared openly.
- The private key is kept secret.

How it work:

I) sender encrypts the plaintext using the receivers public key.

II) Only the receivers private key can decrypt the ciphertext.

Example:

RSA, ECC, DSA



Steganography:

Steganography is the practice of hiding secret information within an ordinary, non-secret file or message to avoid detection.

The goal is to conceal the existence of the information.

Key point:

- Unlike encryption, steganography hides the existence of the message itself.
- Commonly used with images, audio files, videos or text.
- If done properly, no one will even know there is a hidden message.

How it work -

- A secret message is embedded inside other file using special techniques.
- The file looks normal to a casual observer.