INTRODUCTION TO CYBERSECURITY

The fundamental principles of cybersecurity revolve around safeguarding information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

Principles of protecting information (CIA Triad)

The CIA Triad is a foundational model in cybersecurity that outlines three core principles for securing information systems:

* Confidentiality
* Integrity
* Availability

Definitions of the CIA Triad

1. **Confidentiality:**

Confidentiality is ensuring that data is accessible only to authorized individuals or systems and is protected from unauthorized access or disclosure.

The purpose of confidentiality is to prevent sensitive information, such as personal data, financial records, or trade secrets, from being exposed to unintended parties.

Data confidentiality mechanism:

* Access control

This is a data security protocol that controls who and what can view or use resources in a computing environment.

* AAA (Authentication, Autorization, Accounting )

These three components form a framework for controlling access to systems, ensuring secure interactions, and tracking user activities.

*Authentication: verifies the identity of user or device trying to access a system or network.*

*Authorization: determines what a user or device is allowed to do after authentication.*

*Accounting: tracks the user activity like the login time, resources accessed and so on. The info gathered is used for security monitoring.*

* Encryption(*Symmetric and Asymmetric* )

This is the process of converting information into a coded format, making it unreadable without a decryption key.

*Symmetric Encryption uses the same key for both encryption and decryption.*

*Asymmetric Encryption uses a pair of keys, public key for encryption and private key for decryption.*

*Note: readable data can also be called plaintext and unreadable text is also known as ciphertext*

1. **Integrity:**

Integrity is ensuring that data is accurate, trustworthy and unaltered except by authorized processes or users. It protects against unauthorized modification or corruption of data.

The purpose is it maintains trust in the reliability of data and systems by preventing tampering or errors.

Data Integrity Mechanism:

* Hashing

*This is the process of converting data into a long string length of characters called hash-value.*

*In Cybersecurity, hashing is used to ensure data integrity and data authenticity & securely store sensitive information like passwords.*

* Digital signatures

*In cybersecurity, digital signature is used to verify the authenticity & integrity of digital documents and msgs.*

*This is achieved through the combination of asymmetric cryptography and hashing algorithms*

*How Digital Signatures Work*

* *Signing process: the sender creates a hash of the data. Encrypts the hash value with their private key(creating the digital signature)*
* *Verification process: the receiver decrypts the digital signature using the sender's public key and compares it to a newly calculated hash of the received data. If the hash matches, the signature is verified.*

1. **Availability:**

Availability ensures that data and systems are accessible and operational to authorized users when needed.

The purpose is it prevents disruptions, such as denial-of-service (DoS) attacks, that could render systems unusable.

Measures to ensure data availability:

Data backup

Data recovery

**VULNERABILITY:**

A vulnerability is a weakness or flaw in a system, software, hardware, or process that can be exploited by a threat actor to compromise the system's security. Vulnerabilities can arise from coding errors, misconfigurations, outdated software, or human error.

**EXPLOIT:**

An exploit is a piece of code, method, or technique used by attackers to take advantage of a vulnerability to gain unauthorized access, manipulate systems, or cause harm. Exploits are often developed to target specific vulnerabilities.

**IMPACT:**

Impact refers to the consequences or damage caused when a vulnerability is successfully exploited. This can include data breaches, financial losses, system downtime, reputational damage, or compromised user safety

**RISK:**

Risk is the potential for loss or damage when a vulnerability is exploited, calculated as a combination of the likelihood of an exploit occurring and the potential impact. Risk is often expressed as:

**Risk = Likelihood × Impact.**

**ATTACK:**

An attack is the actual act of a threat actor attempting to exploit a vulnerability using an exploit. Attacks can be targeted (aimed at a specific victim) or opportunistic (exploiting widespread vulnerabilities).