

# BANKURA UNNAYANI INSTITUTE OF ENGINEERING



**STUDENT NAME:** SACHIN MANDAL

**DEPARTMENT NAME:** COMPUTER SCIENCE AND ENGINEERING

**UNIVERSITY ROLL NO:** 10500119021

**CLASS ROLL NO:** 17

**SUBJECT NAME:** CRYPTOGRAPHY AND NETWORK SECURITY

**SUBJECT CODE:** PEC-CS801B

**SEMESTER:** 8<sup>TH</sup>


**YEAR:** 4<sup>TH</sup>



**SESSION:** 2022-2023



# PRINCIPLES OF SECURITY

- 
1. **CONFIDELITY**
  2. **INTEGRITY**
  3. **AUTHENTICATION**
  4. **AUTHORIZATION**
  5. **AVAILABILITY**
  6. **NON-REPUDIATION**

- 
- **Confidentiality** :- This is equivalent to privacy, and it has a set of rules which limits access to information. It protects against disclosure of information to unintended recipients, and is designed to prevent sensitive information from reaching the wrong people. It ensures that only the designated person gets the information and access will be restricted to those authorized to view the data in question.
  - **Integrity** :- It involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle, and allows transferring accurate and desired information from senders to intended receivers. It ensures that data cannot be altered by unauthorized people (for example, in a breach of confidentiality).
  - **Authentication** :- This confirms the identity of a user and allows a user to have confidence that the information he receives originated from specific known sources.



- 
- 
- **Authorization** :- It specifies access rights to the users, based on the user role.
  - **Availability** :- Ensures the readiness of the information on requirement. To simplify, information must be available to authorized person(s) when they require it. Availability is best ensured by rigorously maintaining all hardware, performing hardware repairs immediately when needed and maintaining a correctly functioning operating system environment that is free of software conflicts.
  - **Non-repudiation** :- This ensures there is no denial from the sender or the receiver for sent/received messages. It exchanges authentication information with provable time stamp, for example, 'session id' and so forth.

# TYPES OF ATTACKS

## 1. ACTIVE ATTACK

## 2. PASSIVE ATTACK

- **Active Attack** :- An active attack could be a network exploit during which the attackers will modify or alter the content and impact the system resource. It'll cause damages to the victims. The attackers can perform passive attacks to gather info before they begin playacting a vigorous attack. The attackers attempt to disrupt and forced the lock of the system. The victims can get informed concerning the active attack. This sort of attack can threaten their integrity and accessibility. A vigorous attack is tougher to perform compared to a passive attack.
- **Denial-of-Service** attacks (DoS) are one in each of the samples of active attack. A denial-of-Service attack happens once the attackers take action to close up a tool or network. This may cause the first user to be unable to access the actual device or network. The attackers can flood the target device or network with traffic till it's not responding or flaming. The services that are affected are emails, websites, or on-line banking accounts. Dos attacks may be performed merely from any location.

- 
- 
- **Passive Attack:-**The first type of attack is passive attack. A passive attack can monitor, observe or build use of the system's data for sure functions. However, it doesn't have any impact on the system resources, and also, the data can stay unchanged. The victim is difficult to note passive attacks as this sort of attack is conducted in secret. Passive attack aims to achieve data or scan open ports and vulnerabilities of the network.
  - An **eavesdropping attack** is taken into account as a kind of passive attack. An eavesdropping attack is to steal data transmitted among two devices that are unit connected to the net. Traffic analysis is enclosed in eavesdropping. An eavesdropping attack happens once the attackers insert a software package within the network path to capture future study network traffic. The attackers have to be compelled to get into the network path between the end point and the UC system to capture the network traffic. If their area unit additional network methods and also the network methods area unit longer, it'll be more comfortable for the offender to insert a software package within the network path.



THAN YOU