Practical-2

AIM: Explain Confidentiality, Integrity , Availability.

Confidentiality:

Ensures that sensitive information are accessed only by an authorized person and kept away from those not authorized to possess them. It is implemented using security mechanisms such as usernames, passwords, access control lists (ACLs), and encryption. It is also common for information to be categorized according to the extent of damage that could be done should it fall into unintended hands. Security measures can then be implemented accordingly.

Much of what laypeople think of as "cybersecurity" — essentially, anything that restricts access to data — falls under the rubric of confidentiality. This includes infosec's two big As:

- *Authentication*, which encompasses processes that allows systems to determine if a user is who they say they are. These include passwords and the panoply of techniques available for establishing identity: biometrics, security tokens, cryptographic keys, and the like.

- *Authorization*, which determines who has the right to access which data: Just because a system knows who you are, it doesn't necessarily open all its data for your perusal! One of the most important ways to enforce confidentiality is establishing need-to-know mechanisms for data access; that way, users whose accounts have been hacked or who have gone rogue can't compromise sensitive data. Most operating systems enforce confidentiality in this sense by having many files only accessible by their creators or an admin, for instance.

Integrity:

Ensures that information are in a format that is true and correct to its original purposes. The receiver of the information must have the information the creator intended him to have. The information can be edited by authorized persons only and remains in its original state when at rest. Integrity is implemented using security mechanism such as data encryption and hashing. Note that the changes in data might also occur as a result of non-human-caused events such as an electromagnetic pulse (EMP) or server crash, so it’s important to have the backup procedure and redundant systems in place to ensure data integrity.

The techniques for maintaining data integrity can span what many would consider disparate disciplines. For instance, many of the methods for protecting confidentiality also enforce data integrity: you can't maliciously alter data that you can't access, after all. We also mentioned the data access rules enforced by most operating systems: in some cases, files can be read by certain users but not edited, which can help maintain data integrity along with availability.

Availability:

Ensures that information and resources are available to those who need them. It is implemented using methods such as hardware maintenance, software patching and network optimization. Processes such as redundancy, failover, RAID and high-availability clusters are used to mitigate serious consequences when hardware issues do occur. Dedicated hardware devices can be used to guard against downtime and unreachable data due to malicious actions such as distributed denial of-service (DDoS) attacks.

Maintaining availability often falls on the shoulders of departments not strongly associated with cybersecurity. The best way to ensure that your data is available is to keep all your systems up and running, and make sure that they're able to handle expected network loads. This entails keeping hardware up-to-date, monitoring bandwidth usage, and providing failover and disaster recovery capacity if systems go down.

Example of Confidentiality , Integrity and Availablity :

To understand how the CIA triad works in practice, consider the example of a bank ATM, which can offer users access to bank balances and other information. An ATM has tools that cover all three principles of the triad:

- It provides **Confidentiality** by requiring two-factor authentication (both a physical card and a PIN code) before allowing access to data
- The ATM and bank software enforce data **Integrity** by ensuring that any transfers or withdrawals made via the machine are reflected in the accounting for the user's bank account
- The machine provides **Availability** because it's in a public place and is accessible even when the bank branch is closed