Computer/Network Security:

Preserving the integrity, availability and confidentiality of information of the system resources.

Confidentiality:

Confidentiality ensures that sensitive information is accessible only to authorized individuals or systems and prevents unauthorized access. The goal is to protect private data from being viewed, accessed, or used by unauthorized persons.

**Risks to Confidentiality**

* **Unauthorized Access**: This occurs when an unauthorized individual gains access to sensitive data, either by bypassing security measures or exploiting weaknesses.
* **Weak Encryption: Description**: If encryption standards are not robust enough, encrypted data may be easily decrypted by attackers.
* **Insider Threats: Description**: Employees or other trusted individuals within the organization intentionally or unintentionally leak sensitive information.

**Integrity:**

Integrity ensures that data remains unaltered during transmission or storage. If the data is modified in any way, its integrity is compromised. When data is corrupted, it means the integrity is lost, leading to potential errors or malicious changes.

**Risks to Integrity**

* **Data Tampering**: Attackers or unauthorized users may intentionally alter, corrupt, or destroy data to manipulate information for malicious purposes or personal gain.
* **Malware and Ransomware**: Malicious software can infect systems, altering or encrypting data, and rendering it unusable until a ransom is paid or it is repaired.

**How Hash Functions Work For data Integrity:**

* **Host A Sends Data**: Suppose Host 'A' wants to send data to Host 'B'. To maintain integrity, Host 'A' generates a hash value (H1) by running a hash function over the data.
* **Attaching the Hash**: The generated hash value (H1) is attached to the data before transmission.
* **Host B Verifies Integrity**: When Host 'B' receives the data, it runs the same hash function over the received data to generate a new hash value (H2).
* **Comparison**: If the two hash values, H1 and H2, are equal (H1 = H2), this confirms that the data has not been modified, and its integrity has been maintained.

**Availability:**

Availability ensures that the network, systems, and data are accessible and operational for users when needed. A network that is unavailable can disrupt business operations, causing significant issues for companies and users relying on it.

**Risks to Availability:**

* **DoS and DDoS Attacks**: Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks can overwhelm network resources, making the network unavailable to legitimate users.
* **Impact**: These attacks can severely disrupt services, causing downtime and losses for companies.

**Security Services:**

**1.Authentication:**

**1.Peer Entity Authentication**

**In a network an bogus or unwanted node**

**Joins then the detection of that**

**peer/node.**

**2.Data Origin Authentication**

**If Alice receiving data from Bob, Alice**

**should confirm that the source is**

**Bob only, there is on other third party(attacker) is sending the data.**

**2.Access Control:**

**Controls access of the system resources,**

**Everyone could not access everything there**

**has to be access control based on their**

**roles.**

**3.Data Confidentiality:**

**Data should be accessed only by sender and receiver, one third person should not access the data. Need encryption.**

**4.Data Integrity:**

**The data sender sends the exact same data**

**should be received by the receiver any alteration or modification of data breaks the integrity. (Alteration attack, replay attack).**

**5. Non Repudiation:**

**When sender sends the data, the sender can not deny that he/she has not send the data the system should prove that and vice verse when the receiver already received the data he/she cannot deny that. Very import in transactions based systems.**

**Security Mechanisms:**

* **Encipherment**
* **Digital Signature**
* **Access Control**
* **Data Integrity**
* **Authentication Exchange**
* **Traffic Padding**
* **Routing Control**
* **Notarization**