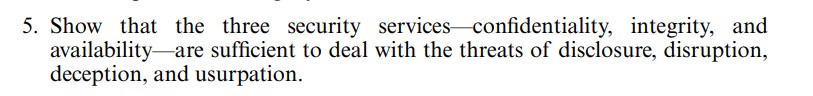
1. **John copies Mary's homework**: This is primarily a violation of **integrity**, as the authenticity of the homework is compromised by copying.
2. **Paul crashes Linda's system**: This act affects **availability**, as Linda can no longer access her system.
3. **Carol changes the amount of Angelo’s check from $100 to $1,000**: This is a violation of **integrity**, since the information on the check has been altered.
4. **Gina forges Roger’s signature on a deed**: This is a violation of **integrity**, as the deed's data (in this case, the signature) is not accurate.
5. **Rhonda registers the domain name “Pearson.com” and refuses to let the publishing house buy or use that domain name**: This is a violation of **availability**, because the publishing house cannot use the domain name they desire.
6. **Jonah obtains Peter’s credit card number and has the credit card company cancel the card and replace it with another card bearing a different account number**: This could be seen as a violation of **confidentiality** (since personal information was accessed) and **availability** (since Peter can no longer use his credit card).
7. **Henry spoofs Julie’s IP address to gain access to her computer**: This is a violation of **confidentiality**, as Henry is accessing information he is not authorized to see, and could also impact **integrity** if he changes data.



Disclosure – unauthorized access to information

Disruption – Prevention of correct operation

Deception – acceptance of false information

Usurpation – Unauthorized access to systems

The text from your image pertains to the three core principles of cybersecurity, often referred to as the CIA triad: confidentiality, integrity, and availability. These principles are fundamental for protecting information against various threats. Here's how they address the mentioned threats:

1. **Disclosure**: The principle of confidentiality is aimed at preventing unauthorized disclosure of information. Techniques such as encryption, access controls, and secure authentication methods ensure that sensitive information is only accessible to those with the proper authorization.
2. **Disruption**: Availability ensures that systems and data are accessible to authorized users when needed, thereby dealing with threats that cause disruption. This includes implementing redundancies, backups, and disaster recovery plans to maintain service continuity in the face of attacks such as Denial-of-Service (DoS).
3. **Deception**: Integrity is the principle that protects against deception by ensuring that information is trustworthy and has not been tampered with. This includes using checksums, digital signatures, and audit trails to detect and prevent unauthorized changes to data.
4. **Usurpation**: This involves unauthorized control or use of system resources. Integrity and availability combined help to prevent and respond to such incidents. Integrity checks can detect unauthorized changes, while availability controls can prevent the unauthorized use of resources.

By maintaining the confidentiality, integrity, and availability of information and systems, organizations can address these threats effectively. Each principle plays a unique role in thwarting security breaches and mitigating the damage they can cause.

Q)what is replay attack

A replay attack is a type of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is done by capturing a data transmission and retransmitting it to produce an unauthorized effect. Here's how it generally works:

1. **Capture**: The attacker intercepts a legitimate message or data packet that is part of a communication between two parties. This message could be anything from a request for access to a network to a transfer of funds in a financial transaction.
2. **Replay**: The attacker then resends this intercepted message or data packet to the original recipient. The recipient, believing that the message is a new, legitimate request, processes it accordingly.
3. **Unauthorized Effect**: This can result in various unauthorized actions. For example, in a financial transaction, it might mean duplicate transfers of funds. In a network security context, it could result in unauthorized access.

Replay attacks are a significant concern in various areas, including financial services, secure communication, and network protocols. To prevent them, various methods are used, such as:

* **Timestamps**: Including a timestamp in a message so that if the same message is received outside a specific time window, it is discarded.
* **Nonce Values**: Using a unique number or value (nonce) that is used only once, so any repeated message with the same nonce can be detected as a replay.
* **Session Tokens**: Implementing session-specific tokens that change with each communication, making replayed messages invalid.
* **Encryption Techniques**: Using advanced encryption techniques that incorporate elements like time or session-specific data to make captured data less useful if replayed.