To be secured, information needs to be hidden from:

- unauthorized access (confidentiality)
- protected from unauthorized change (integrity)
- available to an authorized entity when it is needed (availability).

Confidentiality

- Ensures that sensitive information is only accessible to authorized users and is protected from unauthorized access.
- Confidentiality not only applies to the storage of the information, it also applies to the transmission of information.
- When we send a piece of information to be stored in a remote computer or when we retrieve a piece of information from a remote computer, we need to conceal it during transmission.

Example:

an online banking system where users can access their account details, perform transactions, and check balances.

1.Encryption: The online banking system uses encryption to protect data transmitted between the user's device and the bank's servers.

2.User Authentication: Two-factor authentication (2FA) is implemented to verify that only authorized users can access accounts.

3. Access Control: The system blocks access attempts from unauthorized individuals, preventing them from accessing sensitive information.

4. Confidentiality Protection: These measures ensure that the user's financial data remains confidential and secure from unauthorized access.

In industry, hiding some information from competitors is crucial to the operation of the organization. In banking, customers’ accounts need to be kept secret.

Integrity

ensures that data is **accurate and complete and has not been tampered with or altered by unauthorized individuals.** Integrity means that changes need to be done only by authorized entities and through authorized mechanisms.

Example: Imagine a government website that publishes official documents and statistics. To ensure the integrity of these documents, the website uses digital signatures and hashing algorithms. When a user downloads a document, they can verify its integrity by checking the digital signature and comparing the hash value of the downloaded document with the one provided by the website. If the hash values match, the user can be confident that the document has not been tampered with. However, if an attacker tries to alter the document (e.g., changing statistics), the hash value will change, indicating a breach of integrity.

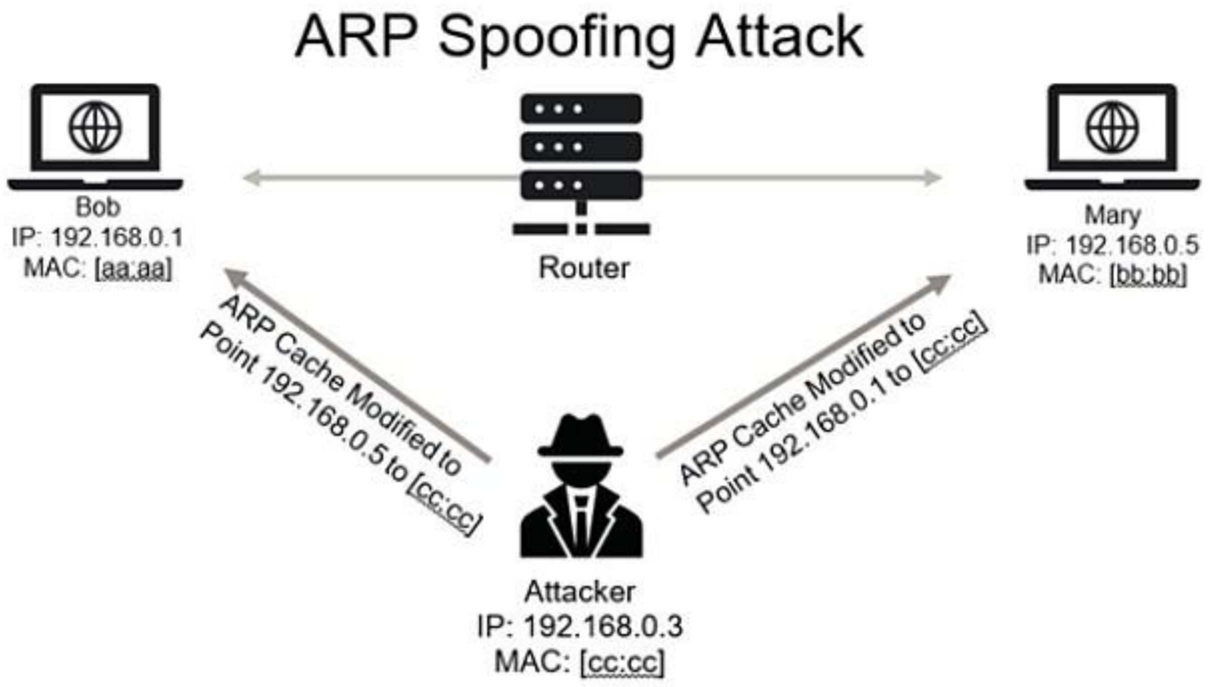
Availability

ensures that information and resources are available to authorized users when needed.

Example: A healthcare provider relies on electronic health records (EHR) systems to access patient information and manage healthcare operations. To ensure availability, the provider has redundant servers and network systems in different geographical locations. If the primary server goes down due to a hardware failure or a cyberattack like a Distributed Denial of Service (DDoS) attack, the backup servers immediately take over to maintain service availability. This redundancy ensures that healthcare professionals can continue to access patient records without disruption, providing uninterrupted patient care.

ATTACKKKKKKKKKKK…………

Spoofing Attack:



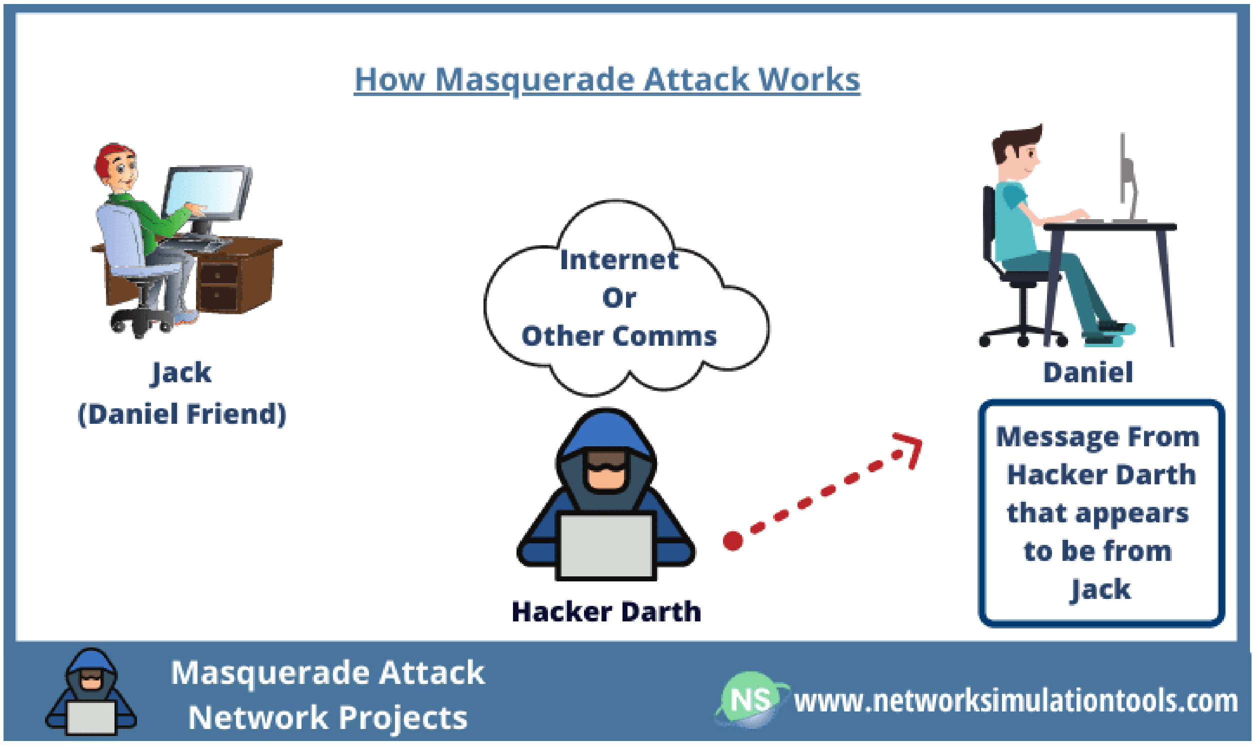
How Traffic Analysis Attack Works:

- ❖ **Network Monitoring:**
  - ✓ The attacker gains access to the network and sets up monitoring tools to capture the timing and volume of network packets being transmitted between endpoints.
- ❖ **Pattern Observation:**
  - ✓ The attacker observes the timing of the packets. For example, they notice that messages are exchanged between certain departments at regular intervals.
- ❖ **Traffic Correlation:**
  - ✓ By analyzing the intervals between packet transmissions and the volume of data, the attacker can deduce patterns. For instance, if a particular department sends a large amount of data every Monday morning, it could indicate a regular weekly report or meeting.
- ❖ **Inference of Communication:**
  - ✓ Even though the actual content of the messages is encrypted, the attacker can infer the nature of the communication. For instance, if the attacker notices a spike in traffic

corresponding to known meeting times, they might infer that these spikes are related to sensitive discussions or decision-making processes.

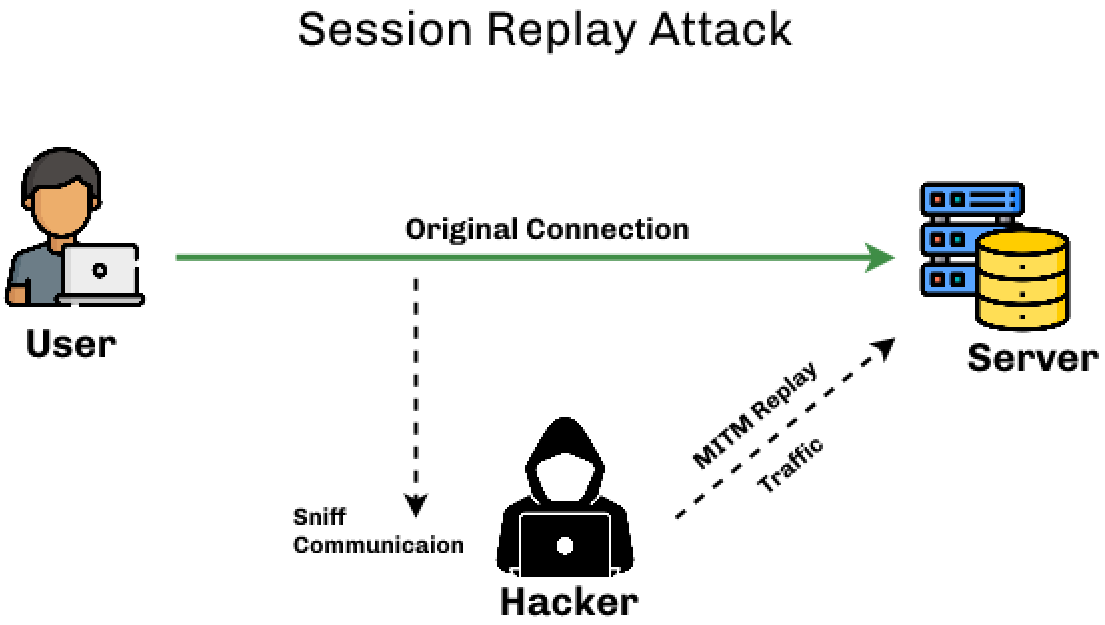
Masquerading Attack

An example of a **masquerading attack** is email phishing. An attacker sends an email that appears to be from a trusted company executive, asking employees to update their login credentials via a fake link. Unsuspecting employees enter their credentials, which are then captured by the attacker. This allows the attacker to gain unauthorized access to the company's systems. To prevent this, organizations should use email authentication methods and train employees to recognize suspicious emails.


How Masquerade Attack Works
Jack
(Daniel Friend)
Internet
Or
Other Comms
Daniel
Hacker Darth
Message From Hacker Darth that appears to be from Jack
Masquerade Attack
Network Projects
NS www.networksimulationtools.com

Replay Attack

An example of a **replay attack** is when an attacker intercepts a legitimate user's login request and reuses the captured authentication token to gain unauthorized access. For instance, the attacker records a valid login session's credentials or session cookies and then replays them to authenticate themselves as the user.



DDoS:

A DDoS attack works by overwhelming a target website, like an online store, with excessive traffic from many compromised computers (a botnet). For example, imagine thousands of computers suddenly flooding the store’s website with fake requests. This massive surge in traffic consumes the website's bandwidth and processing power, causing it to slow down or crash. As a result, legitimate customers can't access the site to make purchases. The attack disrupts normal operations, leading to potential loss of revenue and customer trust.