Semester : VI Subject : CSS Academic Year: 2023-2024

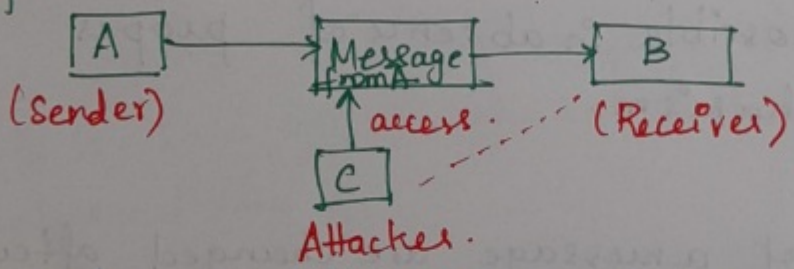
(1) PRINCIPLES / SERVICES / GOALS OF SECURITY:

* Confidentiality
* Authentication
* Integrity
* Non-Repudiation
* Access Control
* Availability.

Confidentiality :-

The principle of confidentiality specifies that only the sender and the intended recipients should be able to access the contents of message.

Example :-



Here sender A is sending a message to Receiver B. The attacker C tries to access the message and reads the message. Here the confidentiality is lost. This is known as interception. Interception causes loss of message confidentiality.

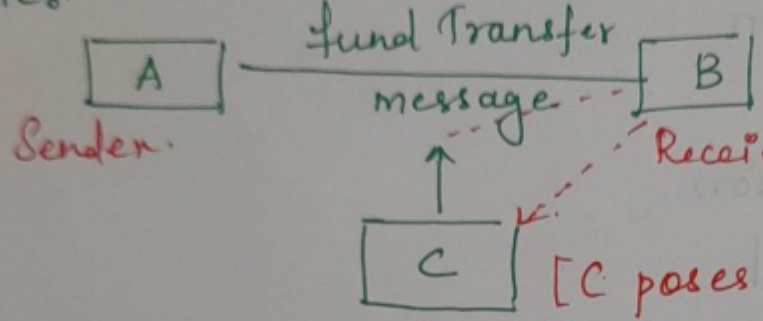
Authentication :-

This services helps to establish the proof of identities.

Semester: IV Subject: CSS Academic Year: 2023-2024

Authentication is a service where you prove urself to the system

Example:-

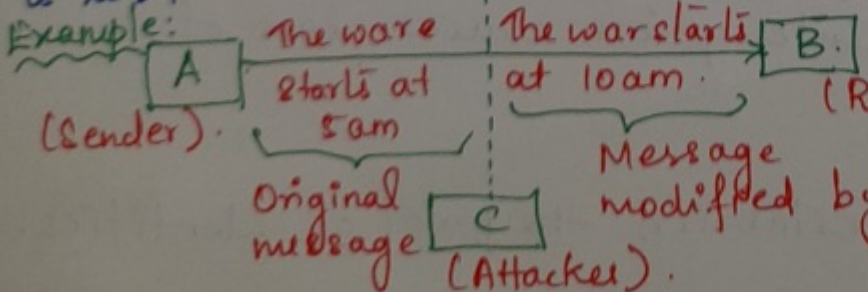


In this example sender sends a fund transfer message to B (Bank). The attacker C gets the access of A unethically and poses like A. The receiver bank B connects with the attacker instead of sender A. This condition is known as Fabrication. Fabrication is possible in absence of proper authentication mechanism.

Integrity :-

When the contents of a message are changed after the sender sends the data and before it reaches the intented receipt, we say that the integrity of the message is lost.

Example:

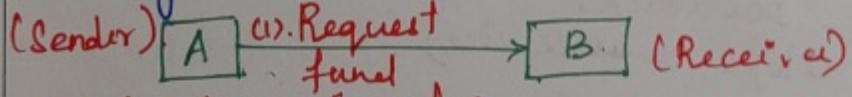


Semester : 4 Subject : CSS Academic Year: 2023-2024.

In this example, the sender A sends a message to the Receiver B as "the war starts at 5am". The attacker interupts the network and changes the message as "The war starts at 10am". The Receiver B actually beleives that the war starts at 10am. This condition is known as modification.

Non-Repudiation:-

There are situations where a user sends a message and later on refuses that he/she had not sent that message.



(2) A refuses Transfer. the msg not sent by he.

In this case, the send A requests fund transfer from seeiver B. Later on A refuses (or) denies that the message is not send by A.

Access Control:

The principle of access control determines who should be able to access what. There are two categories:

(1) Role management:
This defines the different roles of the users. It also specifies what that user can do. ~~(eg) (re~~

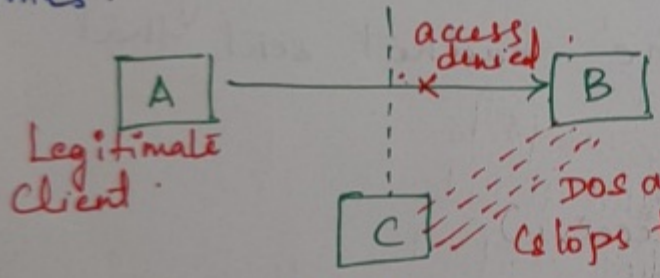
(2) Rule management:
This defines the access rule of a user on the resources.

Example:

The chmod is a best example in linux which helps to assign and change access of user on particular resources (file, folder etc).

Availability :-

The principle of availability states that resources should be available to the authorized parties at all times.



In the above example, the attackes floods the network with unwanted packets and floods the network. When a legitimate user tries to connect to the server, his access is denied. This condition is known as interuption.

Interaption stops the availability of resources.