Threats Vs. Attacks

- **Threats**
  - Potential for violation of security, which exists when there is a circumstance, capability, action or event that could breach the security and cause harm. Is a possible danger that might exploit Weakness.
    - Trojan, Worms etc.

Threats Vs Attacks: Cont....

- **Attacks**
  - An assault on system security that derives from threat. It is a deliberate attempt to escape from security services and violate the security policy of the system .
    - Hacking..

OSI Security Architecture

The OSI security architecture focuses on security attacks, mechanisms, and services. These can be defined briefly as:

- **Security Attack**
  - Any action that compromises the security of information owned by the organization.
- **Security Mechanism**
  - A Process that is designed to detect, prevent, or recover from security attack .

OSI Security Architecture: Cont..

- **Security Service**
  - A Processing or communication service that enhances the security of the data processing system and the information transfer of an organization

Security Attacks

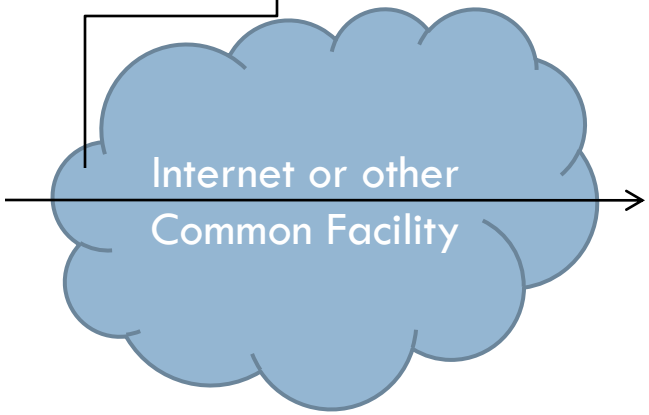
- Security Attack
- can be classified into, passive attacks and active attacks.
- A passive attack :attempts to learn or make use of information from the system but does not affect system resources.
- Eavesdrop, monitor transmission. Obtain information being transmitted.

- Release of message contents

is easily understood (Figure a). A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information .We would like to prevent an opponent from learning the contents of these transmissions.

Security Attacks: Cont..

C:
Reads contents of message from A to B



A **B**

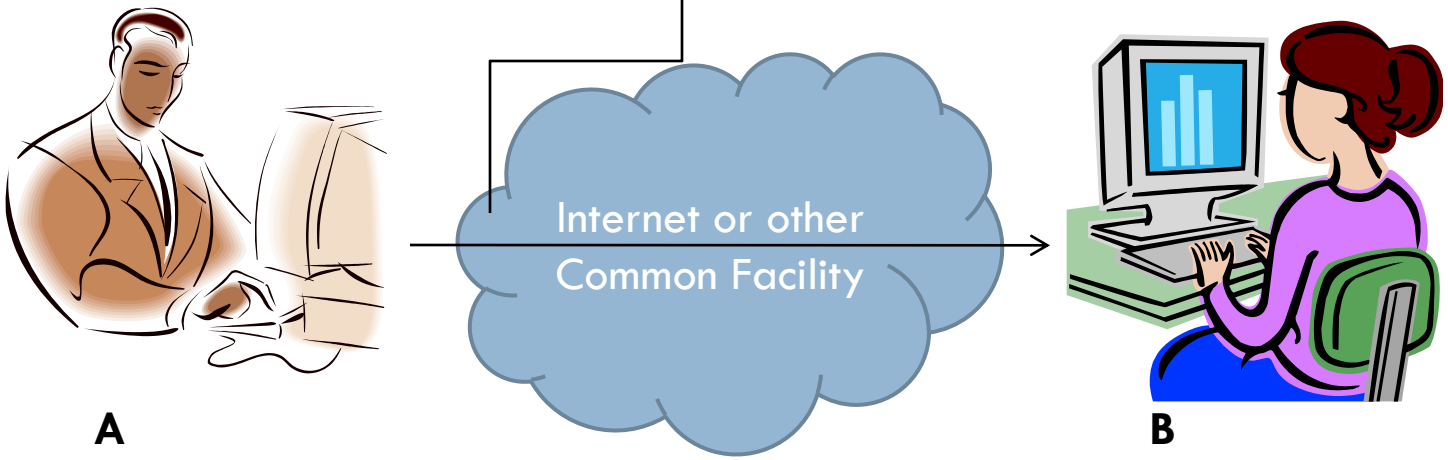
a) Release of Message Contents

Security Attacks: Cont..

- Traffic Analysis
  - Observe message pattern if encrypted
  - Determine location and identity of parties
  - Very difficult to detect

Security Attacks: Cont..

C:
Observe the pattern of message from A to B



a) Traffic Analysis

Security Attacks: Cont..

- **Important …**
  - They are very difficult to detect because they do not involve any alteration of data
  - Typically a message is sent and received in a normal fashion and neither the sender nor receiver is aware that third party has read the message or observed the traffic pattern .

Security Attacks: Cont..

- **Solution**
  - Can be prevented by means of encryption
- **Recommendation**
  - The emphasis in dealing with passive attack is on prevention rather than detection

Security Attacks: Cont..

- **Active Attack**
- An active attack attempts to alter system resources or affect their operation.
  - Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into three categories:
    - Masquerade
    - Modification of Message
    - Denial of Service (DOS)

Security Attacks: Cont..

Masquerade

takes place when one entity pretends to be a different entity (Figure a).

For example:

- getting a specific account and behaving like account's owner .
- hacking a specific webpage and behaving like a webpage's admin .

Security Attacks: Cont..

C:
Message from C, that appears to be from 'A' to B

Internet or other Common Facility

A **B**

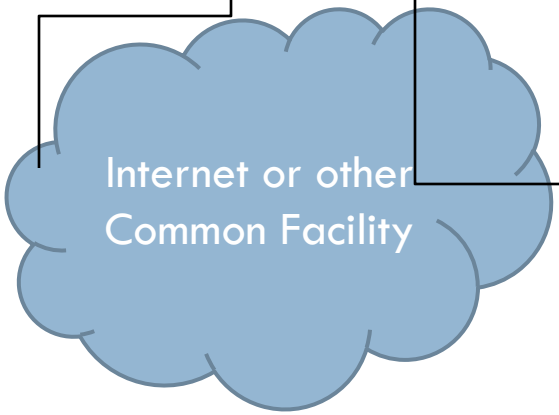
a)Masquerade

Security Attacks: Cont..

- **Modification of Message**
- Modification of message simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect (Figure c).
- Example:
  - A message meaning
    - "Allow John Smith to read confidential file accounts",
  - is modified as
    - "Allow Fred Brown to read confidential file accounts"

Security Attacks: Cont..

C:
Modification of Message from A to B



A **B**

c) Modification of Message

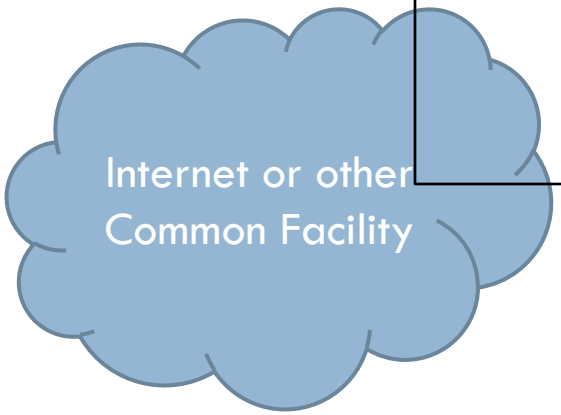
Security Attacks: Cont..

- **Denial of Service**
  - Prevents a normal use of management of communication facilities(Figure d).
    - Example:
      - Disruption of an entire network, either by disabling entire network or by overloading it with a message so as to degrade performance of communication system
      - Disruption of a particular client from a server .

Security Attacks: Cont..

C:
Disrupts service provided by serve

A



Server

d)Denial of Service

Thank You