Information Protection & Computer Security

Rajendra Kachhwaha
Email: rajendra1983@gmail.com

June 3, 2015

- Lecture 1.

  Topic Covered:

  Security Architecture

  Security Attacks

  Security Services

- **Security Architecture:**

  Security Attack: Any action that compromises the security of information owned by an organization.

  Security Mechanism: A process (or a device incorporating such a process) that is designed to detect, prevent or recover from a security attack.

  Security Services: A processing or communication service that enhance the security of the data processing systems and the information transfers of an organization.

  Threat: A potential for violation of security, which exists when there is a action or event that could breach security and cause harm.
  A threat is a possible danger that might exploit a vulnerability.

  Attack: An intelligent act that is a deliberate attempt to violate the security policy of a system/network.

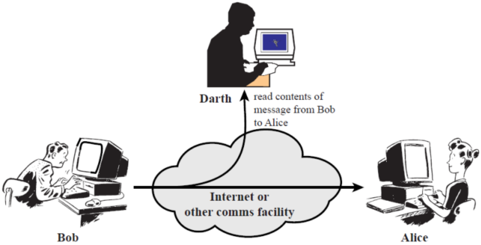
- **Security Attacks:**

Passive Attacks: It is the eavesdropping on or monitoring of, transmission. A Passive attack attempts to learn or make use of information from the system but does not affect system resources. Very difficult to detect but prevention is easy.(By encryption)
Types:
Release of message contents,
Traffic analysis.

Active Attacks: It involves modification of data stream or creation of false stream or It attempts to alter system resources or affect their operation.
Very easy to detect but difficult to prevent.
Types:
Masquerade,
Replay,
Modification of Messages,
Denial of service.

- **Security Attacks:**

Passive Attacks: Release of message contents:
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.

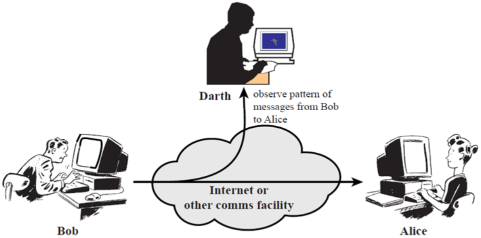

Darth
read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

(a) Release of message contents

- **Security Attacks:**

Passive Attacks: Traffic analysis:

Suppose that we had a way of masking (encryption) the contents of messages or other information traffic so that opponents, even if they captured the message, could not extract the information from the message. An opponent might still be able to observe the pattern of the message.


Darth
observe pattern of messages from Bob to Alice
Internet or other comms facility
Bob
Alice

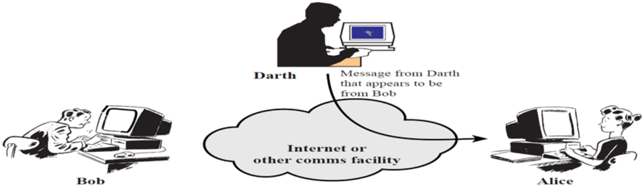
(b) Traffic analysis

- **Security Attacks:**

Active Attacks: Masquerade:

Takes place when one entity pretend (act as if) to be a different entity. It includes one of the other forms of active attack.

Ex: Authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating (imitating) an entity that has those privileges.

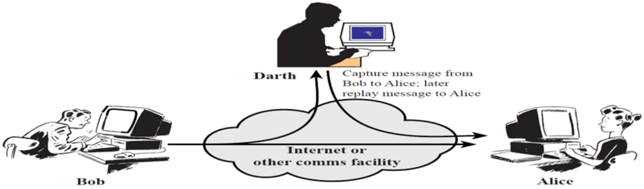

Darth
Message from Darth that appears to be from Bob
Internet or other comms facility
Bob
Alice

(a) Masquerade

- **Security Attacks:**

Active Attacks: Replay:

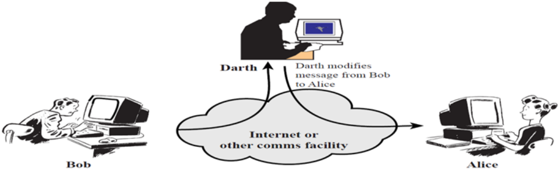
Involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.


Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice

(b) Replay

Security Attacks:

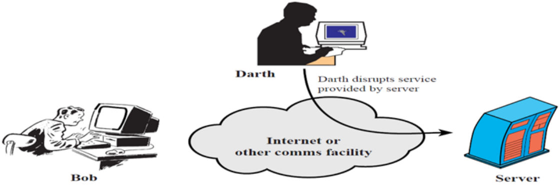
Active Attacks: Modification of Messages:
Simply means that some portion of a legitimate (genuine) message is altered, or that messages are delayed or recorded, to produce an unauthorized effect.
Ex: A message meaning "Allow John Smith to read confidential file accounts" is modified to mean "Allow Fred Brown to read confidential file accounts."


Darth
Darth modifies message from Bob to Alice
Internet or other comms facility
Bob
Alice

(c) Modification of messages

- **Security Attacks:**

Active Attacks: Denial of Service:
Prevents or inhibits the normal use or management of communications facilities. This attack may have a specific target.
Ex: an entity may suppress all messages directed to a particular destination


Darth
Darth disrupts service provided by server
Internet or other comms facility
Bob
Server

(d) Denial of service

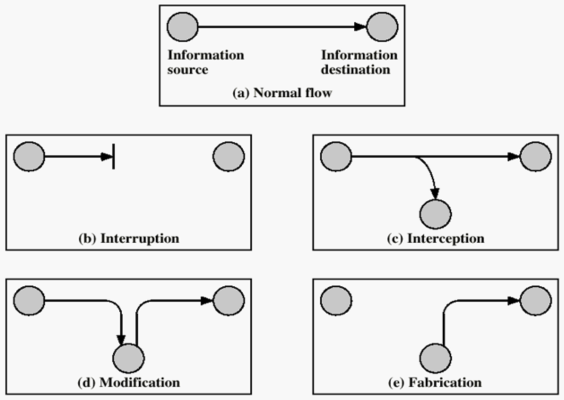
- **Security Attacks:**Summery:

Interruption: This is an attack on availability

Interception: This is an attack on confidentiality

Modification: This is an attack on integrity

Fabrication: This is an attack on authenticity



- **Security Services:**

  Authentication: The assurance that the communicating entity is the one that it claims to be. (Communication is authentic)

  Access Control: The Prevention of unauthorized use of a resource OR Ability to limit and control the access to host systems and applications. It includes:
  Authentication (Who can login)
  Authorization (What authorized users can do)
  Accountability (Identifies what a user did)

  Data Confidentiality: The protection of data from unauthorized disclosure.

  Data Integrity: The assurance that data received are exactly as sent by an authorized entity.

  Non-repudiation: Neither sender nor receiver denies that they have not send, not receive the data.

  Availability: Property of a system/resource being accessible and usable upon demand by an authorized system entity. (Authorized users have reliable and timely access to information.