INTRODUCTION

COMPUTER SECURITY

Computer Security refers to the protection afforded to an automated information system.

This process happens in order to attain the applicable objectives of:

- Preserving the integrity availability and confidentiality of integrity
- Availability and confidentiality of information system resources

KEY SECURITY CONCEPTS

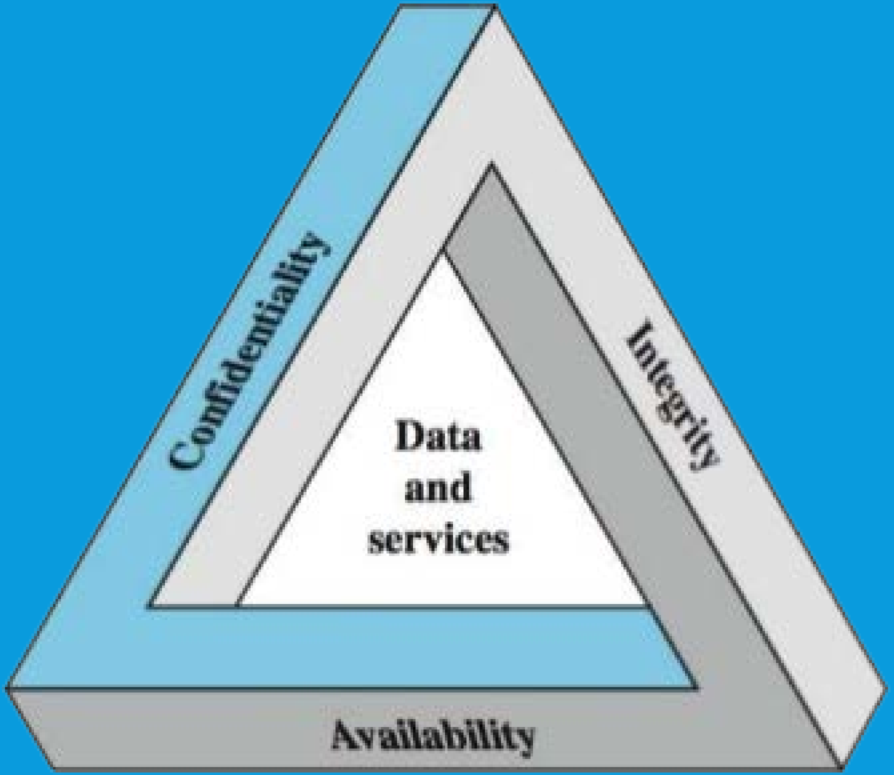

Image Source: http://image.slidesharecdn.com/presentation1-141119103935-conversion-gate01/95/overview-on-cryptography-and-network-security-2-638.jpg

LEVEL OF IMPACT

Three levels of impact can be defined for a security breach:

- Low
- Moderate
- High

EXAMPLES OF SECURITY REQUIREMENTS

- Confidentiality
- Integrity
- Availability

COMPUTER SECURITY CHALLENGES

- Not simple
- Must consider potential attacks
- Procedures used counter-intuitive
- Involve algorithms and secret info
- Must decide where to deploy mechanisms
- Battle of wits between attacker/admin
- Not perceived on benefit until fails
- Requires regular monitoring
- Too often an after-thought
- Regarded as impediment to using system

ASPECTS OF SECURITY

Consider 3 aspects of information security:

- Security attack
- Security mechanism
- Security services

Note the terms:

- **Threat:** a potential for violation of security
- **Attack:** an assault on system security, a deliberate attempt to evade/exploit security services

PASSIVE ATTACKS

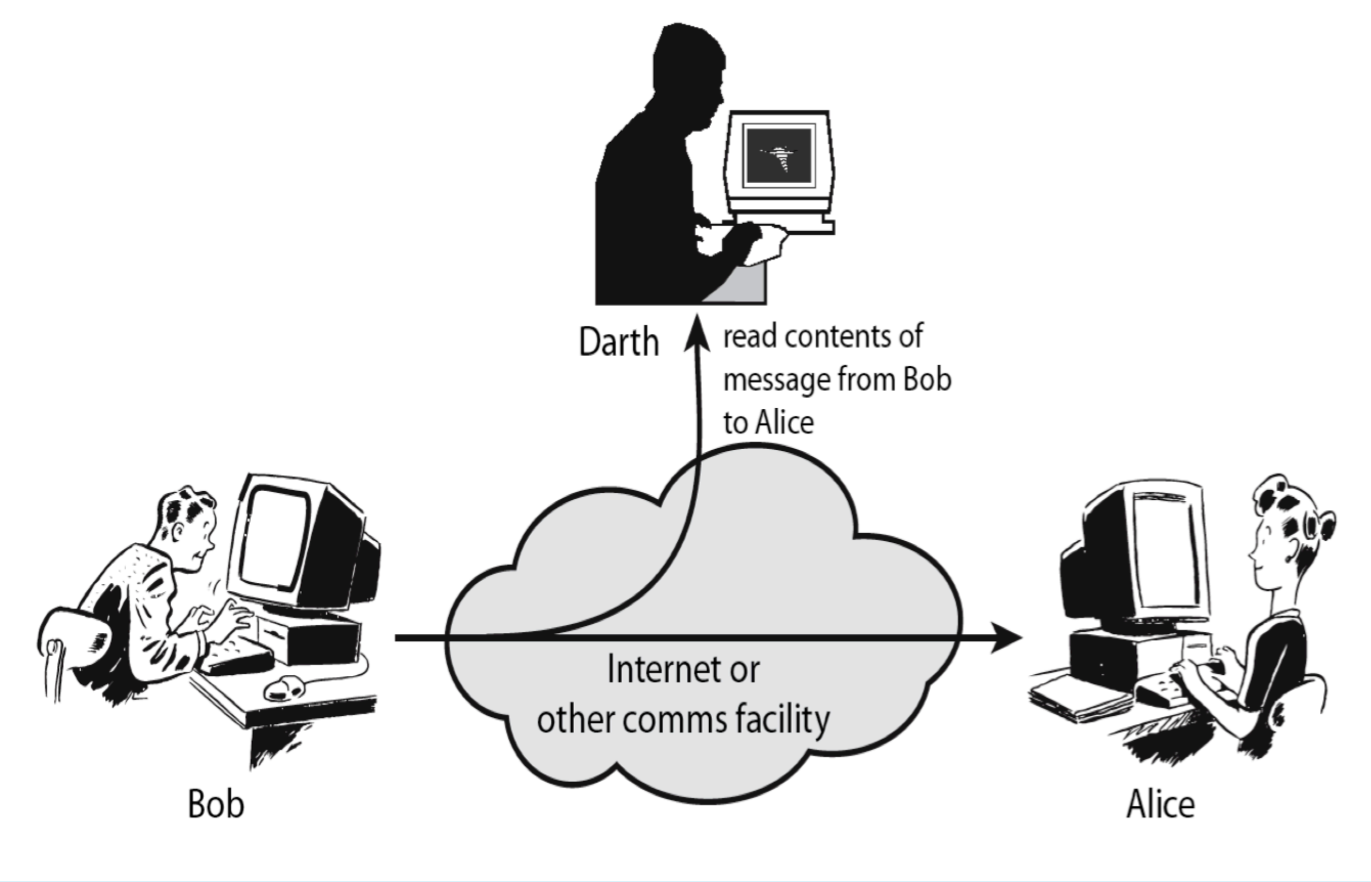
Darth
read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

Image Source: http://madeinkwt.com/blog/wp-content/uploads/2013/03/passive_attacks_1.png

ACTIVE ATTACKS

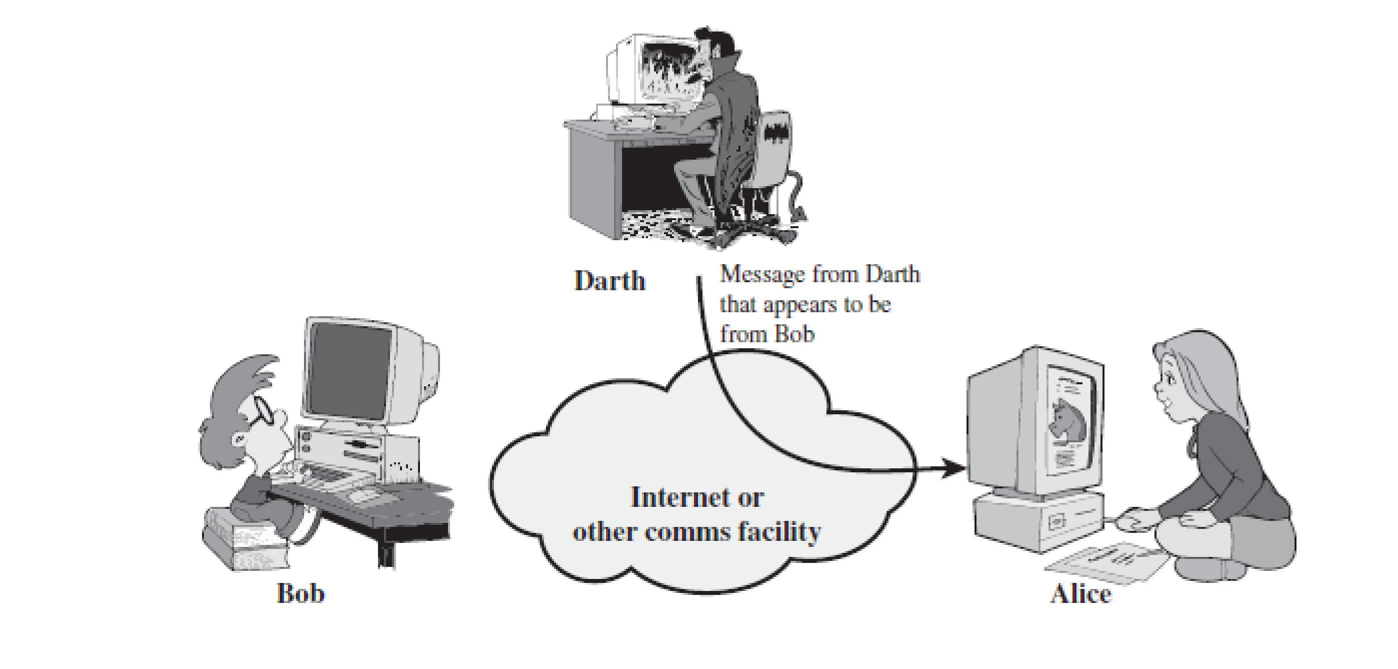
Darth
Message from Darth that appears to be from Bob
Bob
Internet or other comms facility
Alice

Image Source: http://3.bp.blogspot.com/-aQfr3xYYP8A/UEDSsHY01NI/AAAAAAAAAnI/Nw-YVswPJ_w/s1600/MAS.png

SECURITY SERVICE

Security Service enhances the security of data processing systems and information transfers of an organization.

- It is intended to counter security attacks
  - By using one or more security attacks
  - Often replicates functions normally associated with physical documents

SECURITY SERVICES

Authentication is a process to assurance that the communicating entity is the one claimed

  - authentication occurs for both peer-entity & data origin

- **Access Control:** prevention of the unauthorized use of a resource
- **Data Confidentiality** : the protection of data from unauthorized access
- **Data Integrity:** the assurance that data received is as sent by an authorized entity
- **Non-Repudiation:** the protection against the denial by one of the parties in a communication
- **Availability:** resource accessibility/usability

SECURITY MECHANISM

Security Mechanisms are features designed to detect, prevent, or recover the system from a security attack

- There is no single mechanism that will support everything
- Security Services are required
- Many of the security mechanisms use **cryptographic techniques**

SECURITY MECHANISMS

- • specific security mechanisms:
- – encipherment, digital signatures, access controls,
- data integrity, authentication exchange, traffic
- padding, routing control, notarization
- • pervasive security mechanisms:
- – trusted functionality, security labels, event
- detection, security audit trails, security recovery

SUMMARY