Network Security (CSE 827)

A H M Sarowar Sattar

Department of Computer Science and Engineering
Rajshahi University of Engineering and Technology

sarowar@ruet.ac.bd ; *sarowar@gmail.com*

March 22, 2016

Overview

Goal of this course

- Comprehensive course on network security
- Includes both theory and practice
- Theory: Cryptography, Hashes, key exchange, Email Security, Web Security, Wireless security
- Practice (tools and/or programming) (individual work)
- Class tests (4)
- Writing survey papers (group work)

Writing survey papers

Topics

1. Security issues in social networks
2. Recent advance in network forensic
3. Cybercrime
4. Biometric security system
5. Security issues in mobile device
6. Cloud security issues and offering
7. Privacy issues in social networks
8. Security and privacy issues with GPS Tracking
9. Wireless security issues

Please note

Top three (or more) will be submitted to a conference/Journal.

Reminder

Zero tolerance for cheating

Standards Organizations

- National Institute of Standards & Technology (NIST) http://csrc.nist.gov/
- Internet Society (ISOC) Internet Engineering Task Force (IETF), ietf.org Internet Architecture Board (IAB)
- International Telecommunication Union Telecommunication Standardization Sector (ITU-T) http://www.itu.int
- International Organization for Standardization (ISO) http://www.iso.org

What is security?

Security

Security is keeping unauthorized entities from doing things you don't want them to do.....

This definition is to informal.....

What is security?

Security Components

- Confidentiality
- Integrity
- Availability

Confidentiality

"The property that information is not made available or disclosed to unauthorized individuals, entities, or processes [i.e., to any unauthorized system entity]." [Definitions from RFC 2828]

This is not privacy

Privacy

"The right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share information about itself with others."

"Privacy is a reason for confidentiality".

Integrity

- **Data integrity:** The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner.
- **System integrity:** The quality that a system has when it can perform its intended function in a unimpaired manner, free from deliberate or inadvertent unauthorized manipulation.

Availability

The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system; i.e., a system is available if it provides services according to the system design whenever users request them.

Example

Turning off a computer provides confidentiality and integrity, but hurts availability. . .

More definitions

- **vulnerability:** An error or weakness in the design, implementation, or operation of a system
- **attack:** A means of exploit some vulnerability in a system
- **threat** An adversary that is motivated and capable of exploiting a vulnerability

Few dot points

- The technical failing in a system is vulnerability
- If you can close the vulnerabilities, the threats don't matter. (Do they?)
- Different enemies have different abilities
- Teenage joy-hackers can't crack a modern cryptosystem
- You cant design a security system unless you know who the enemy is

OSI Security Architecture

The following concepts are used:

- **Security attack:** Any actions that compromises the security of information owned by an organization (or a person)
- **Security mechanism:** a mechanism that is designed to detect, prevent, or recover from a security attack
- **Security service:** a service that enhances the security of the data processing systems and the information transfers of an organization. The services make use of one or more security mechanisms to provide the service.

Security Attacks

Attack

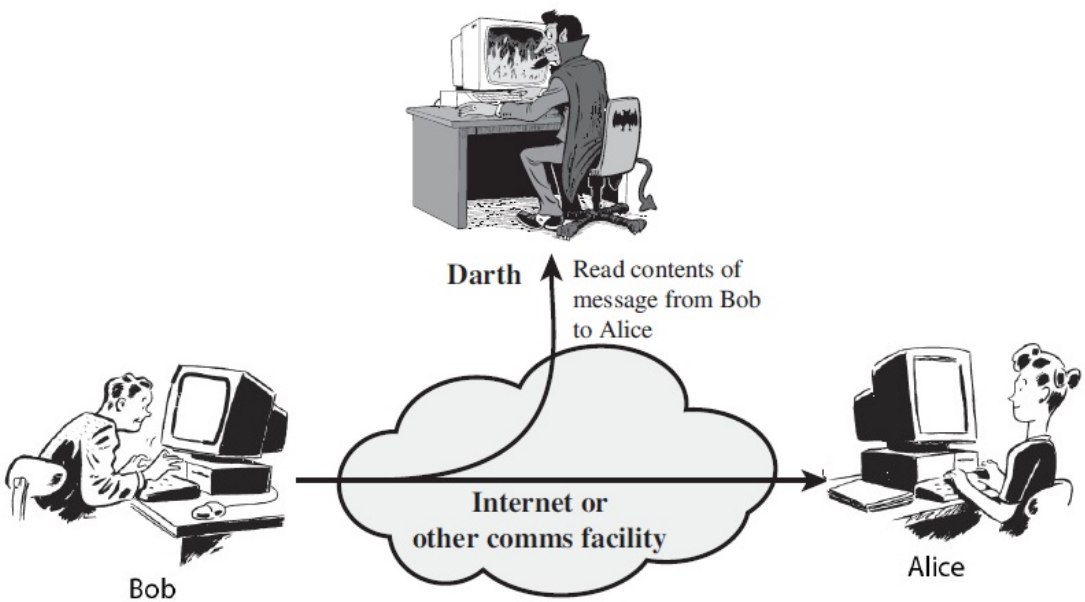
A means of exploit some vulnerability in a system

More clearly,
An assault on system security, a deliberate attempt to evade security services.

- **Passive attack**
- **Active attack**

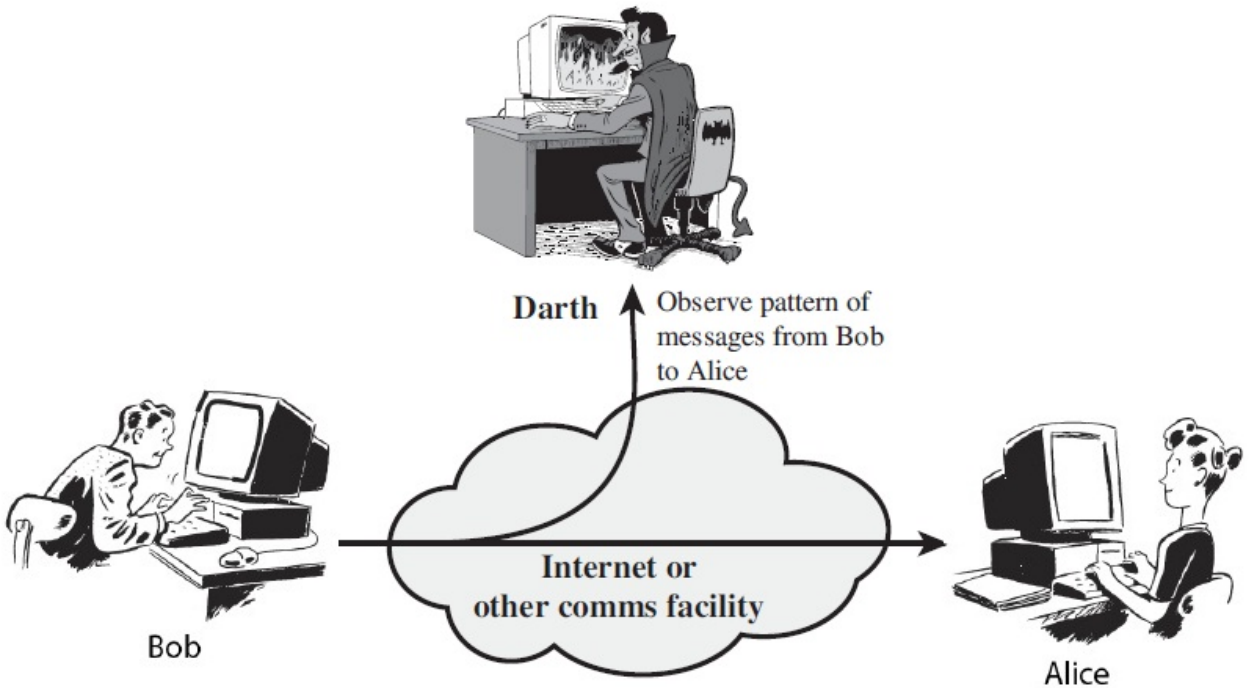
Passive Attack

The purpose is solely to gain information about the target and no data is changed on the target. Therefore, attempting to break the system solely based upon observed data



(a) Release of message contents

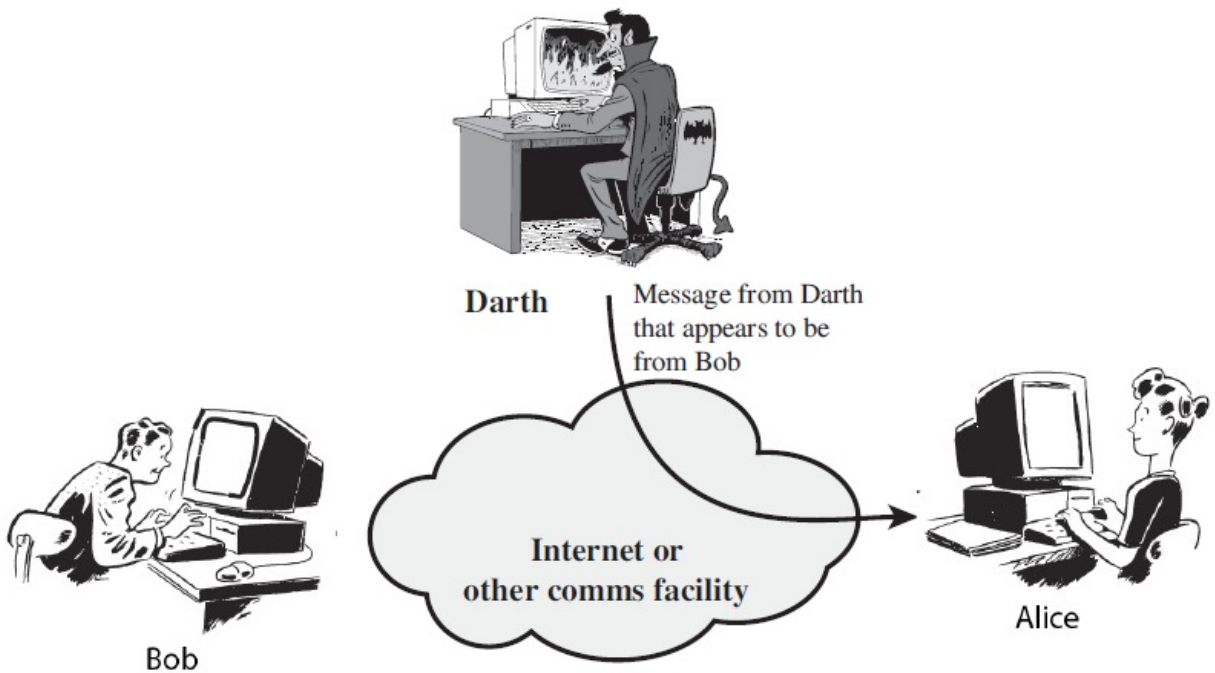
Passive Attack (Cont.)



(b) Traffic analysis

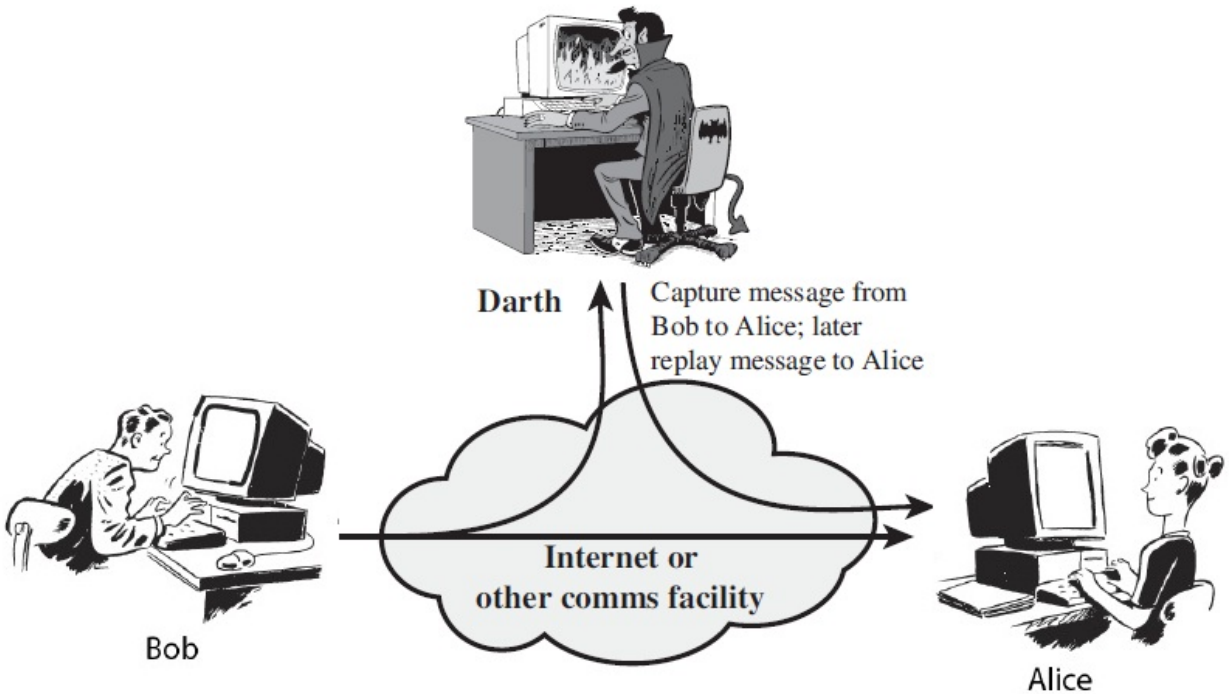
Active Attack

An active attack is a network exploit in which a hacker attempts to make changes to data on the target or data en route to the target.



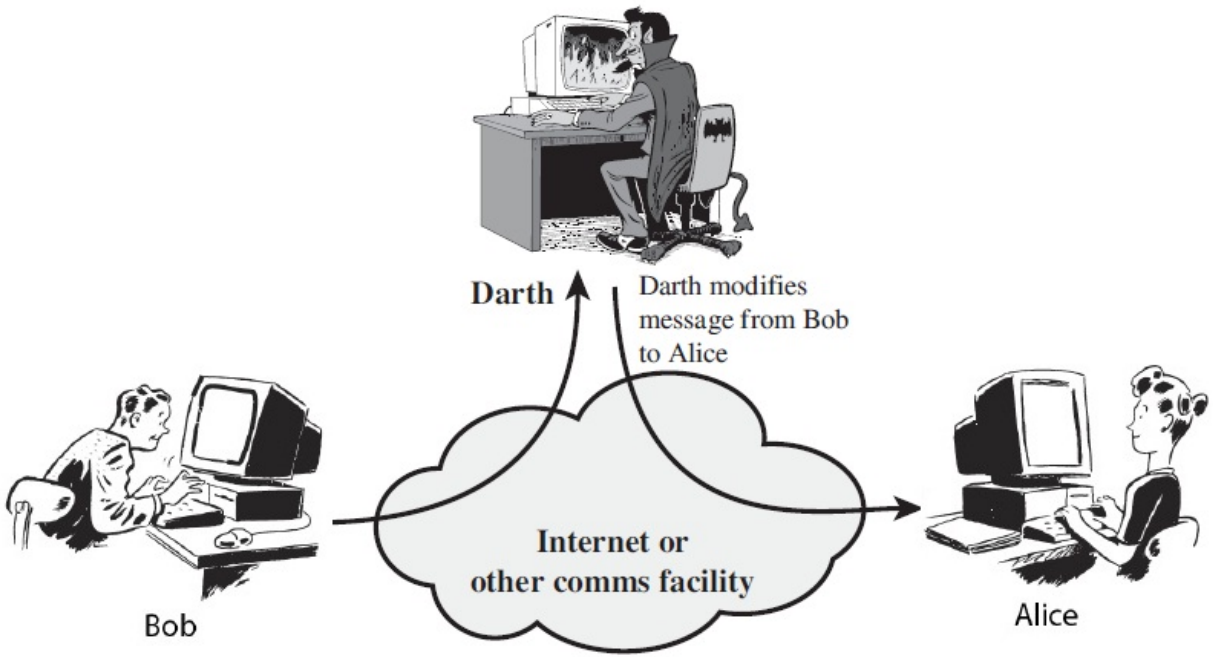
(a) Masquerade

Active Attack (Cont.)



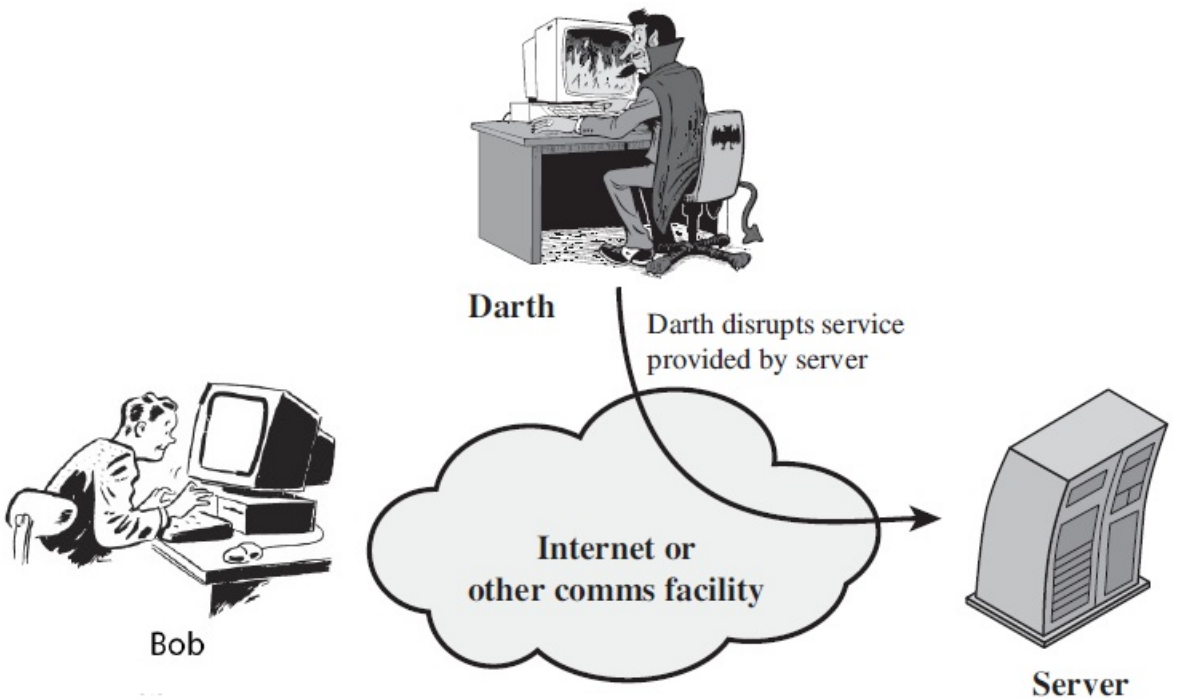
(b) Replay

Active Attack (Cont.)



(c) Modification of messages

Active Attack (Cont.)



(d) Denial of service

Security Services

Security service is a service which ensures adequate security of the systems or of data transfers.

X.800 Recommendation divides security services into these categories:

- Authentication
- Access control
- Data confidentiality
- Data integrity
- Non-repudiation
- Availability service

Authentication

Assurance that communicating entity is the one claimed

Example: Consider a person, using online banking service. Both the user and the bank should be assured in identities of each other

Access Control

Prevention of the unauthorized use of a resource

Example: In online banking a user may be allowed to see his balance, but not allowed to make any transactions for some of his accounts.

Data confidentiality

Protection of data from unauthorized disclosure

Example: In online banking a user may be allowed to see his balance, but not allowed to see others' balance.

Data integrity

The assurance that data received are exactly as sent by an authorized entity,

i.e. contain

- no modification
- no insertion
- no deletion
- no replay

Nonrepudiation

Protection against denial by one of the entities involved in a communication of having participated in the communication.

Example: Imagine a user of online banking who has made a transaction, but later denied that. How the bank can protect itself in a such situation?

Availability service

Protects a system to ensure its availability

We already have enough discussion regarding this.

Security Mechanism

Feature designed to detect, prevent, or recover from a security attack.

Security mechanisms are used to implement security services.

They include (X.800):

- Encipherment
- Digital signature
- Access Control mechanisms
- Data Integrity mechanisms
- Authentication Exchange
- Traffic Padding
- Routing Control
- more.....

Few dot points about security mechanism

- no single mechanism that will support all services required
- however one particular element underlies many of the security mechanisms in use
- cryptographic techniques hence our focus on this topic

Summary

- Some organizations develop standards for network security
- CIA represents the 3 key components of security
- ISO X.800 security architecture specifies security attacks, services, mechanisms
- Active attacks may modify the transmitted information.
- Security services include authentication, access control,....
- Security mechanisms are used to implement security services.

Acknowledgement

- Lawrie Browns slides supplied with William Stallings book Cryptography and Network Security: Principles and Practice, 5th Ed, 2011
- Network Security course at Department of Computer Science & Engineering, Washington University in Saint Louis.
- Network Security course at Department of Computer Science, Columbia University, New York.