POLITÉCNICO DE LEIRIA
ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO

Information Security

Computer Security Concepts - Background

Lecturer (Academic year 2016-2017):
Marisa Maximiano

Summary

- Computer Security Concepts
  - What is computer security ?
  - Objectives
  - Some examples
  - Requirements and mechanisms
  - Difficulties and barriers when handling security
  - Security attacks, mechanisms and services

Today, computers and software are pervasive…

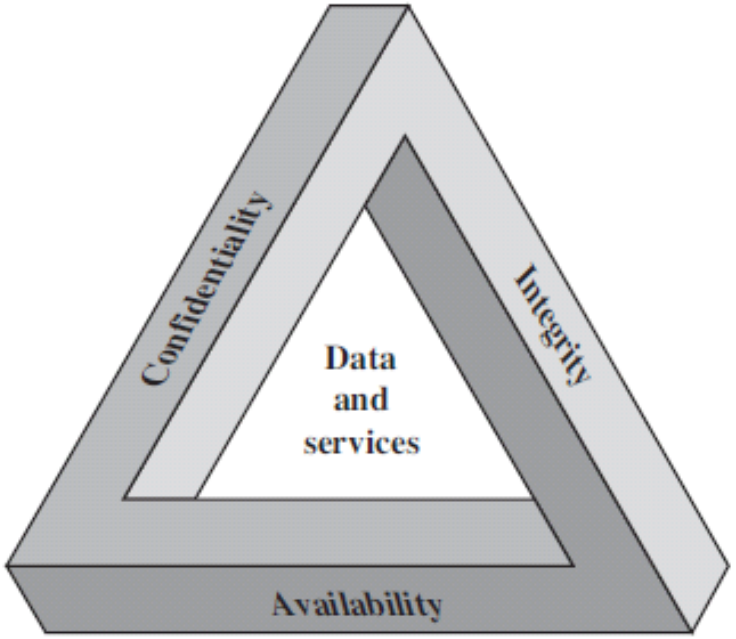
It’s embedded in nearly every aspect of our lives

What is computer security?

- The protection afforded to an automated information system
- Preserves the:
  - **Integrity**
  - **Availability** and
  - **Confidentiality** of information systems resources

    - (includes hardware, software, firmware, information/data and telecommunications)

What is computer security: 3 key objectives



[1]

The security requirements triad
(main security properties)

What is computer security: 3 key objectives

Confidentiality

- Not made available to unauthorized people (privacy)

Integrity

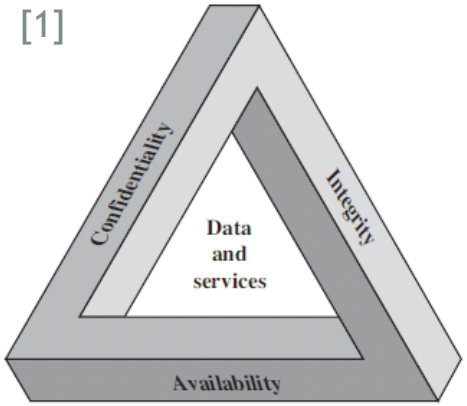
- Data and programs not changed by unauthorized people
- System not manipulated by unauthorized people

Availability

- System work promptly
- Services not denied to authorized people

What is computer security: loss of security in the key objectives

[1]



The security requirements triad

Confidentiality

- A loss of confidentiality is the unauthorized disclosure of information

Integrity

- A loss of integrity is the unauthorized modification and destruction of information

Availability

- A loss of availability is the disruption of access to or use of information or an information system

What is computer security: but there is more…

- **Authenticity**
  - Being genuine and being able to be verified (trusted)
  - Each input arriving at the system came from a trusted source

- **Non-repudiation**
  - "I did something and I could not say that was not me…"

- We must be able to trace a security breach to a responsible party
- Systems must keep records of their activities to permit later forensic analysis

What is computer security: some examples

- Let's define **levels of impact** on organizations or individuals if should there be a breach of security

Low	• Limited adverse effect on organization or individuals
Moderate	• Serious adverse effect…
High	• Severe or catastrophic adverse effect…

Source: FIPS PUB 199
Standards for Security Categorization of Federal Information and Information Systems

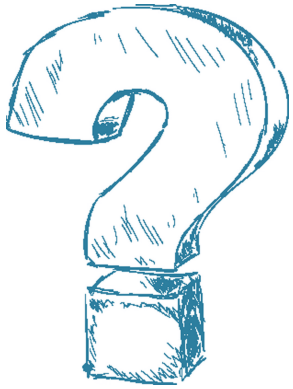
What is computer security?

Security has guiding tenets, but **context** is everything

- It's all about:
  - Identify risk's
  - Understand were they come from
  - And somehow, designing systems an processes to mitigate them

What is computer security: some examples

- **Scenario 1:**
  - Student grade information should only be available to students and their parents



1. Which security requirement?
2. Level?

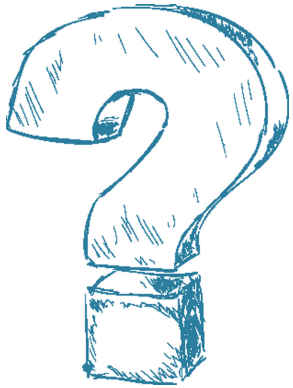
What is computer security: some examples

- **Scenario 1:**
  - Student grade information should only be available to students and their parents

1. Confidentiality
2. Low

What is computer security: some examples

- **Scenario 2:**
  - Hospital patient's allergy information stored in a database



1. Which security requirement?
2. Level?

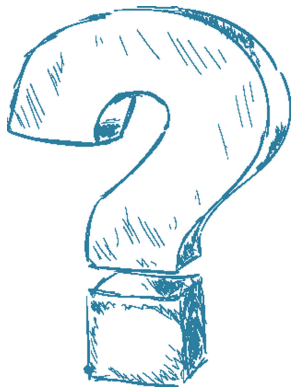
What is computer security: some examples

- **Scenario 2:**
  - Hospital patient's allergy information stored in a database

1. Integrity
2. High

What is computer security: some examples

- **Scenario 3:**
  - A Web site that offers a forum to registered users to discuss some specific topic
    - Either a registered user or a hacker could falsify some entries or deface the Web site



1. Which security requirement?
2. Level?

… in the web master perspective

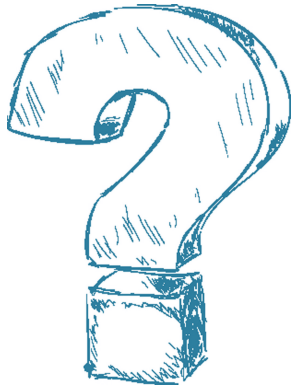
What is computer security: some examples

- **Scenario 3:**
  - A Web site that offers a forum to registered users to discuss some specific topic
    - Either a registered user or a hacker could falsify some entries or deface the Web site

1. Integrity
2. Moderate

What is computer security: some examples

- **Scenario 3 (other perspective):**
  - A Web site that offers a forum to registered users to discuss some specific topic
    - Either a registered user or a hacker could falsify some entries or deface the Web site



1. Which security requirement?
2. Level?

Suppose the topic is related top line research...

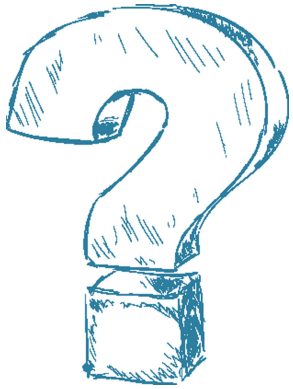
What is computer security: some examples

- **Scenario 3 (other perspective):**
  - A Web site that offers a forum to registered users to discuss some specific topic
    - Either a registered user or a hacker could falsify some entries or deface the Web site

1. Integrity
2. High

What is computer security: some examples

- **Scenario 4:**
  - An anonymous online poll in a newspaper web site



1. Which security requirement?
2. Level?

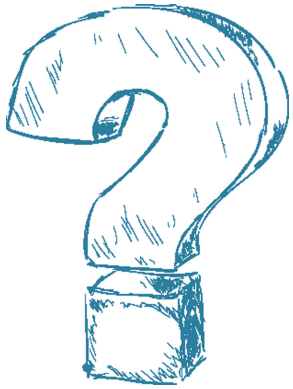
What is computer security: some examples

- **Scenario 4:**
  - An anonymous online pool in a newspaper web site

1. Integrity
2. Low

What is computer security: some examples

- **Scenario 5:**
  - Suppose a system that provides authentication services for critical systems, applications, and device goes down…



1. Which security requirement?
2. Level?

What is computer security: some examples

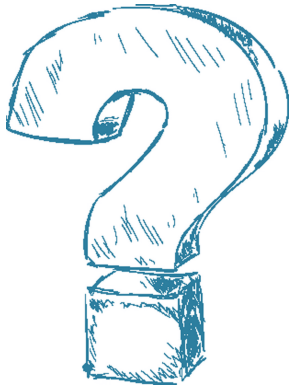
- **Scenario 5:**
  - Suppose a system that provides authentication services for critical systems, applications, and device goes down…

1. Availability
2. High

The more critical a component or service, the higher is the level of availability required

What is computer security: some examples

- **Scenario 6:**
  - An online telephone directory lookup application goes down



1. Which security requirement?
2. Level?

What is computer security: some examples

- **Scenario 6:**
  - An online telephone directory lookup application goes down

1. Availability
2. Low

Well, it seems to be very simple to ensure security…

- **Requirements** (they seem very simple!)
  - Confidentiality
  - Integrity
  - Availability

- Needed mechanisms
  - **Not so simple… and can be quite complex**
  - (We will study them during this course classes)

Difficulties and barriers when handling security

1) Security mechanisms typically involve more than a particular algorithm or protocol…

2) The battle between system/network administrator and the attack perpetrator…

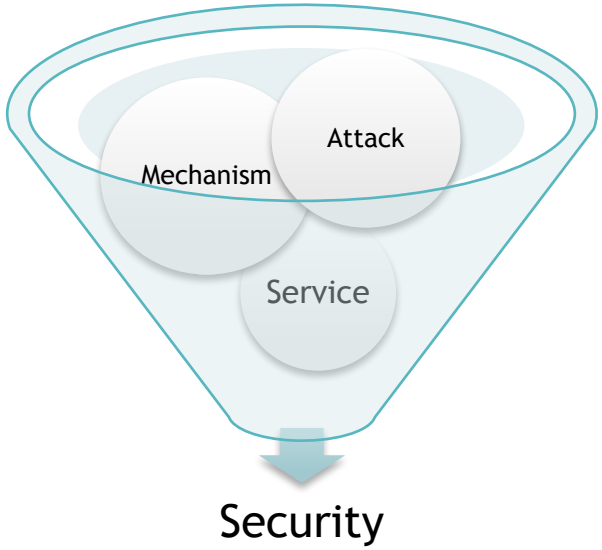
3) Until a security failure occurs, CEOs avoid enough security investment…

4) Users (and …) view strong security as an impediment of efficiency when working with an information system

5) etc..

Some definitions (they are related…)

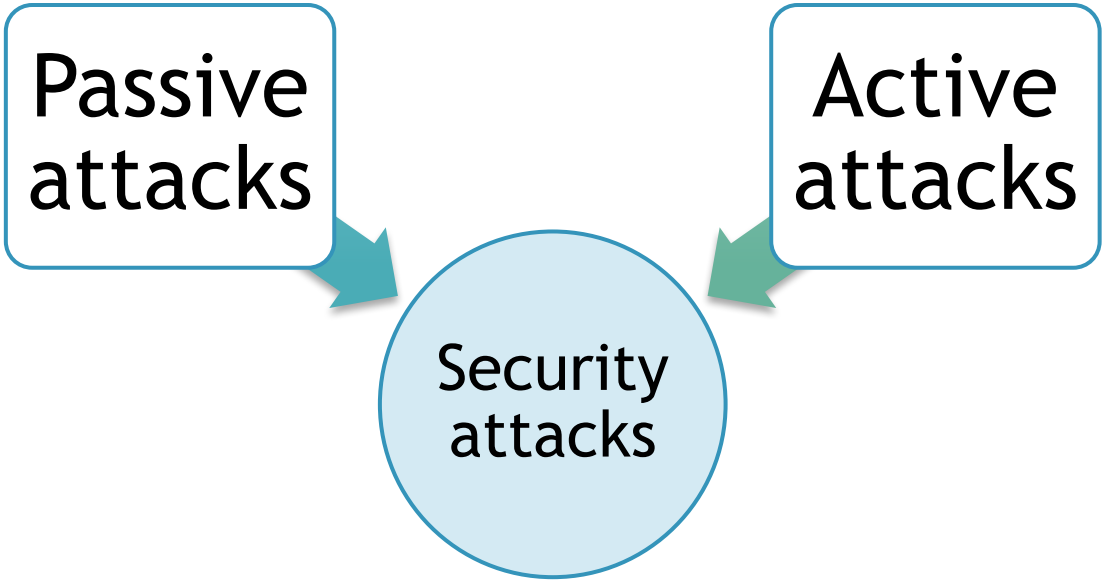
- Security **attack**
  - Action that compromises the security of information
- Security **mechanism**
  - A process design to **detect**, **prevent** or **recover** from a security attack
- Security **service**



Fights the security attacks using one or more security mechanism

Security attacks

- Two types:



Security attacks

Passive attacks

- Learn or use of information
- System resources remain “untouchable”
- Their nature
  - Eavesdropping on, or monitoring of transmission

✓ **Goal: Get information**

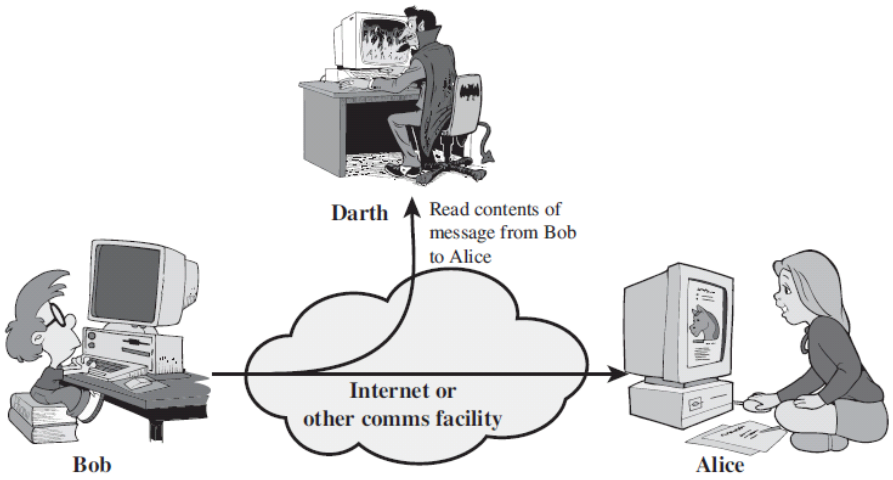
✓ **Two types:** unauthorized reading of message contents and traffic analysis

✓ **Difficult to detect!**
  ✓ Because they do not involve any alteration of data

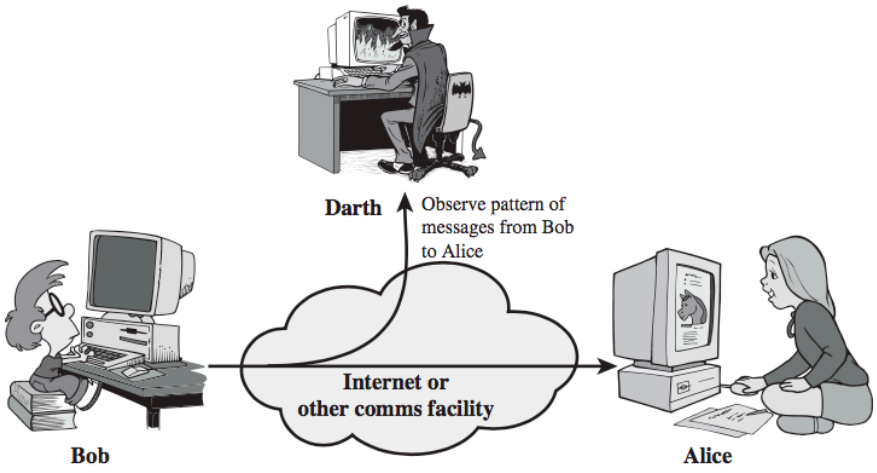
Security attacks

Passive attacks

- ✓ **Goal: Get information**
- ✓ **Two types:** unauthorized reading of message contents and traffic analysis



(a) Release of message contents



(b) Traffic analysis

Security attacks

Passive attacks

- Learn or use of information
- System resources remain “untouchable”
- Their nature
  - Eavesdropping on, or monitoring, of transmission

✓ **Prevention instead of detection!**

✓ **How?**

✓ **Cryptography !**

Security attacks

Active attacks

- System resources are altered or their operation is affected
- Four categories:

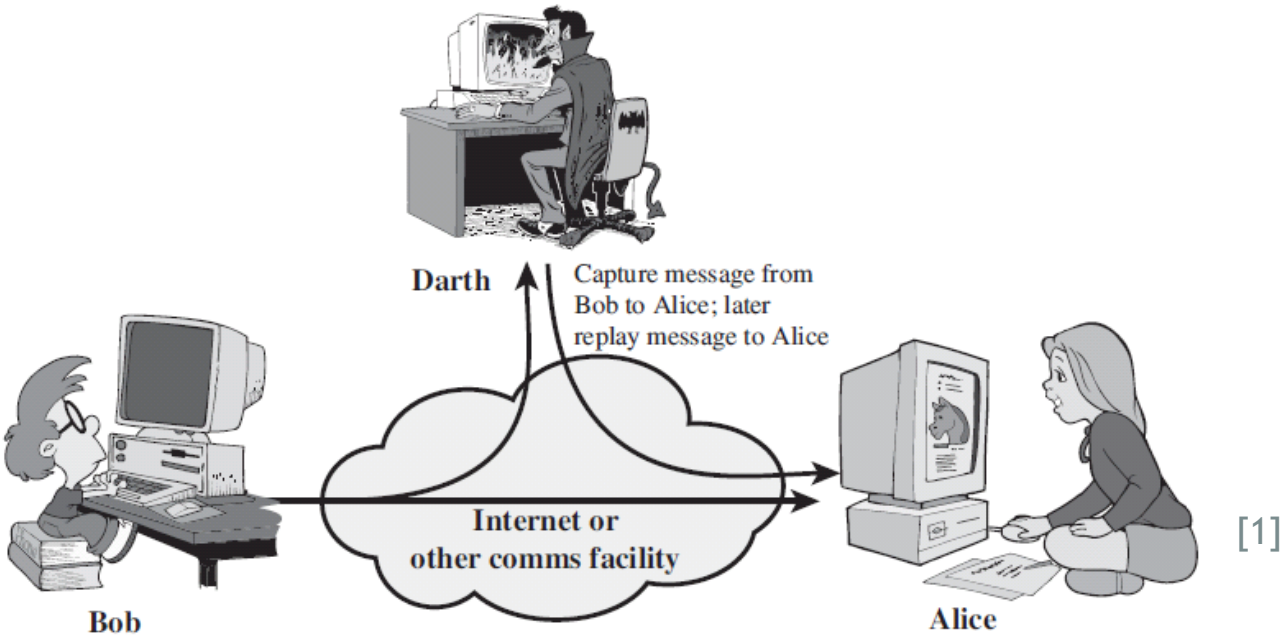
1. **Replay**
2. **Message modification**
3. **Denial of service (DoS)**
4. **Impersonation**

Security attacks

Active attacks

- **1. Replay** (to produce an unauthorized effect)

Involves the passive capture of a data unit and its subsequent retransmission



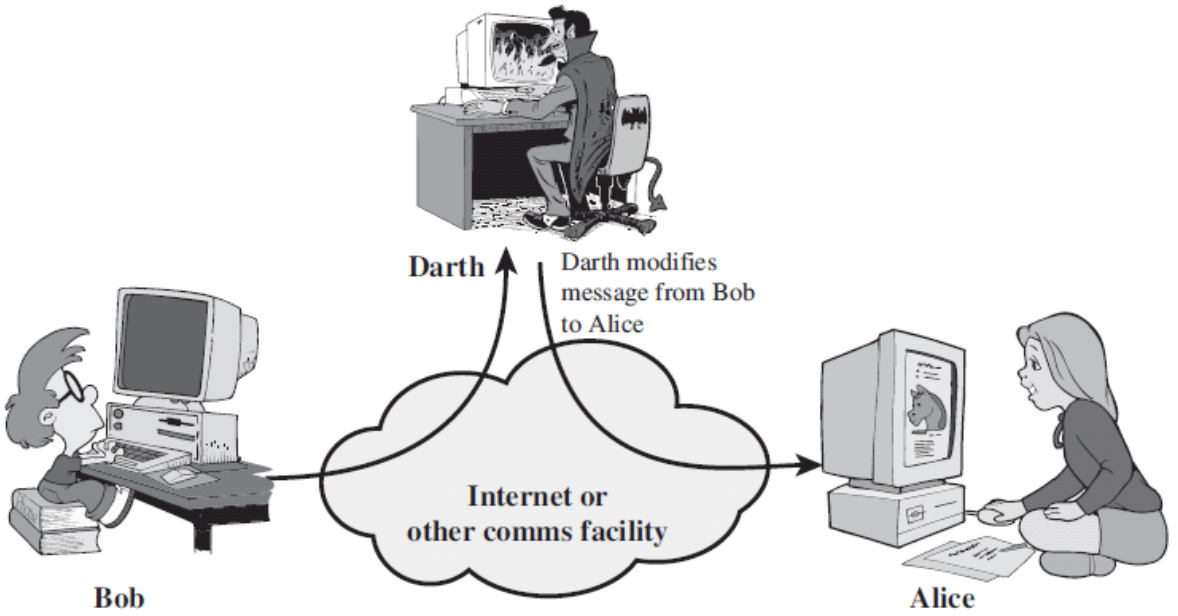
[1]

Security attacks

Active attacks

- **2. Message modification:** (to produce an unauthorized effect)

  - some portion of a legitimate message is **altered**,
  - or that messages are **delayed** or **reordered**



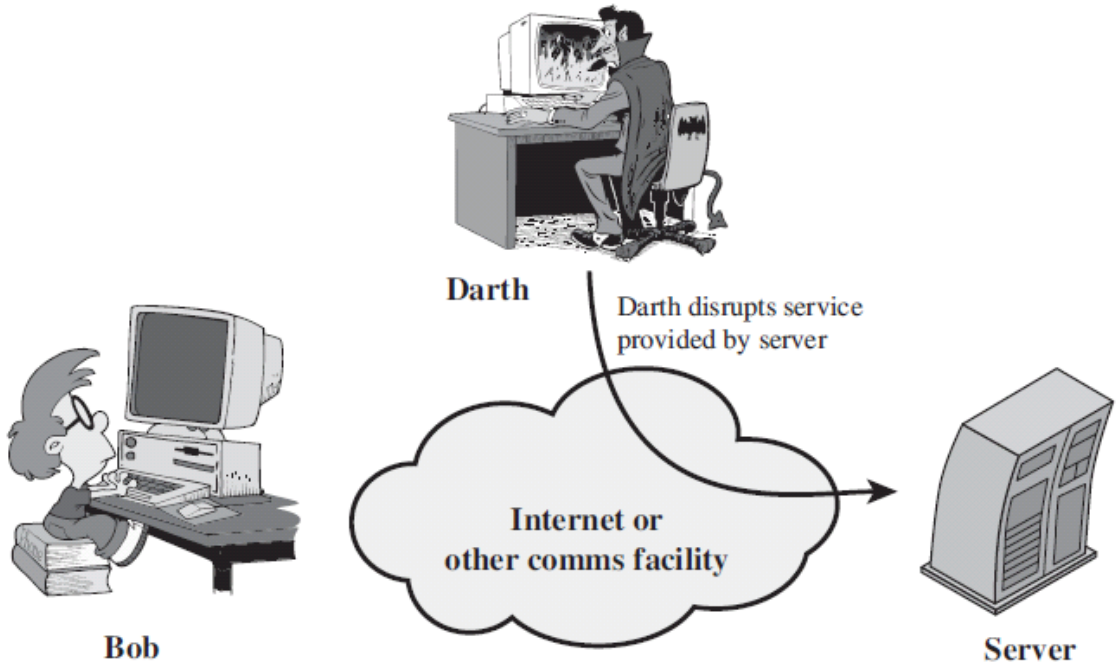
[1]

Security attacks

Active attacks

- **3. Denial of service (DoS)**

Prevents or inhibits the normal use or management of communications facilities



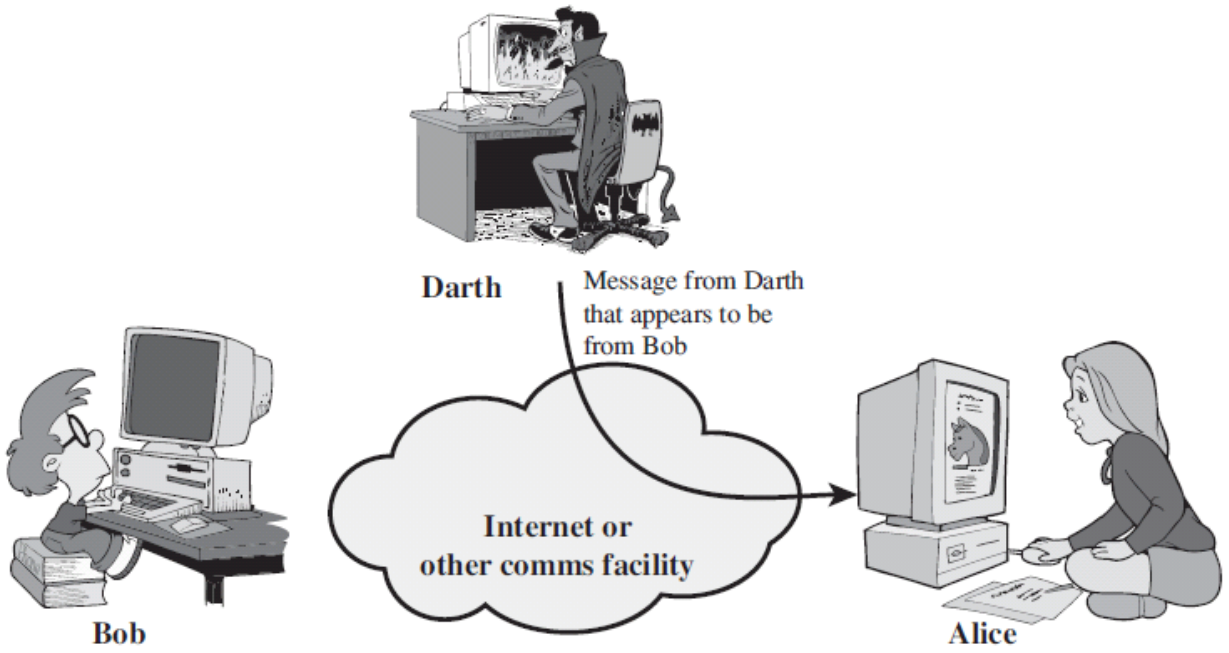
[1]

Security attacks

Active attacks

- **4. Impersonation** (to produce an unauthorized effect)

  Takes place when one entity pretends to be a different entity



[1]

Security attacks

Active attacks

- **Four categories**
  - **Replay, Msg modification, DoS and Impersonation**

Can we focus on prevention?

It is difficult... (lots of possibilities)

Detect early and recover from them!

[1]

Security services

X.800 categories

- **Authentication**
  - Entity is the one that it claims to be
- **Access control**
  - Prevention of unauthorized use of resources
    - Who can access to a resource, under what conditions, what those accessing the resource are allowed to do
- **Data confidentiality**
  - Data ("plain text") protection
- **Data integrity**
  - Ensure that received data is exactly as sent by an authorized entity
- **Non repudiation**
  - Some authorized entity did participated in a process
  - It can not say (later) that it did not participate in the process

Security mechanisms

- We will study them, in detail, in the next class…

Examples of mechanisms are encryption algorithms, digital signatures, and authentication protocols

Software's complexity will always introduce vulnerabilities

There will always be attackers

⇨ Defensive behavior

Bibliography

[1] W. Stallings, Cryptography and Network Security: Principles and Practice, 5th Edition, Prentice Hall, 2010 (Chapter 1).

Additional reading:

[2] M. Andrews and J. Whittaker, "Computer Security." IEEE Security and Privacy, September/October 2004.

Note: This presentation is (almost entirely) based on the first book (reference [1]).

Also, some adaptations from Prof. Nuno Costa and Vitor Fernandes from previous academic years were made.