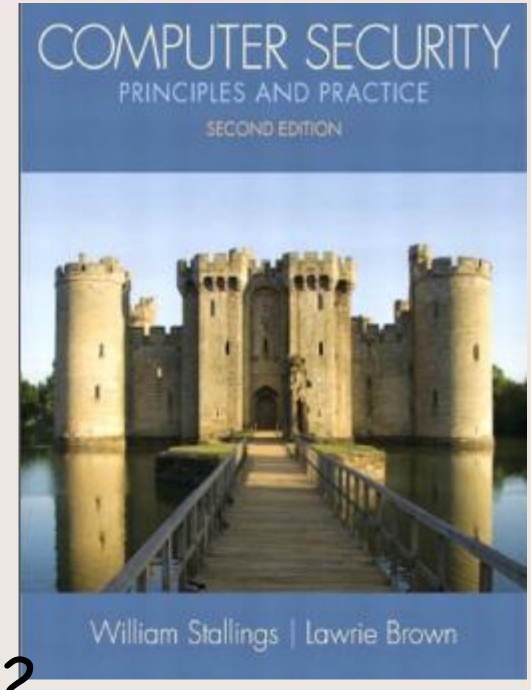
# 4104 - Computer Security



Dr. : Tarek Salah Sobh

E-mail : tarekbox2000@gmail.com

Book Title: Computer Security, 2nd Ed.

Publisher: Pearson Education, Inc., 2012

Author: William Stallings

Course Link :

https://drive.google.com/open?id=0B7ZV2yiUM34mdVdmemZBbGJkUlk

# LEARNING OUTCOMES

On completion of this course we will be able to:

- ❑ Survey the developments of IT security.
- ❑ Identify security problems that confront security designers & administrators
- ❑ Define the threats to IT systems, evaluating the relative risks of these threats and countermeasures
- ❑ Understand the principle aspects of a comprehensive security strategy.
- ❑ Overview different aspects of defense mainly authentication, access control
- ❑ Be aware of various cryptosystems.
- ❑ Computer security technology and principles

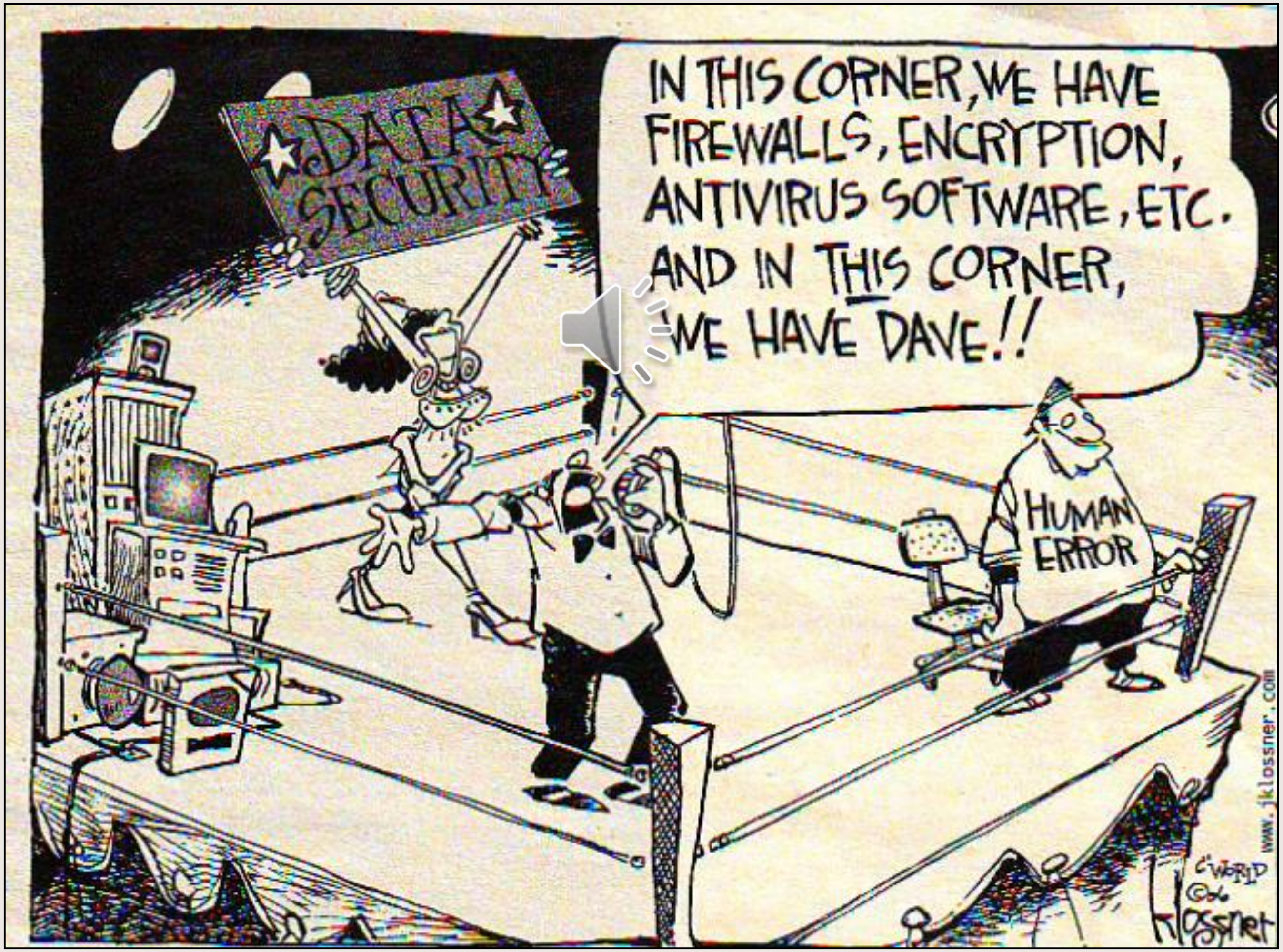
# TENTATIVE COURSE SCHEDULE & OUTLINE

| WEEK | LECTURE TOPIC |
|---|---|
| 1,2,3 | Computer Security Overview |
| 4,5,6 | Technology and Principles :<br>Cryptographic Tools |
| 7 | Public Key Infrastructure |
| 8 | Mid-Term Exam |
| 9 | User Authentication |
| 10 | Access Control |
| 11 | Firewalls |
| 12 | Software Security : OS & DB Security |
| 13 | Final Revision |

# Grading Criterion

| Activity | Grade |
|---|---|
| Midterm Exam | 10% |
| Assignments & Student participations | 10% |
| Final Exam | 80% |

# Computer Security


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com
C WORLD ©06
Klossner

# Computer security fact

*"Never has information system security been better than it is today; and never have information system been more vulnerable than they are today"*

# Computer security fact

“The average user is not, does not want to be, and should not need to be a computer security expert any more than an airplane passenger wants to or should need to be an expert in aerodynamics or piloting. This very lack of sophisticated end users renders our society at risk to a threat that is becoming more prevalent and more sophisticated”.

# Computer Security “KISS” mantra

*“Keep It Simple, Stupid !”*

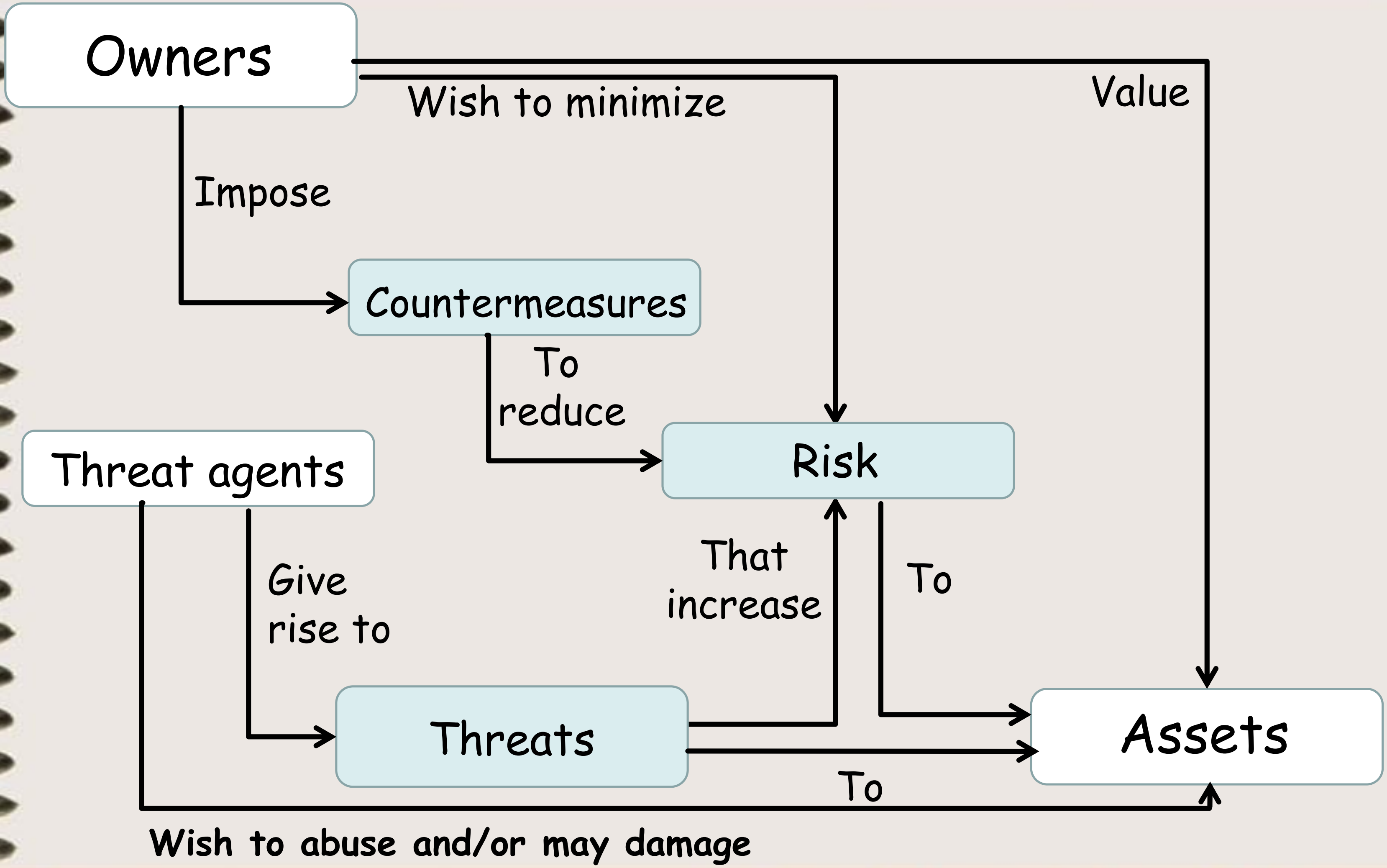
- ❑ Complexity increases the risk of problems.
- ❑ Avoid complexity and avoid problems.

# Good security practices

The "90/10" rule:

- ❑ 10% of security safeguards are technical
- ❑ 90% of security safeguards rely on us - the user - to adhere to good computing practices

# Security Concepts and Relationships



Owners

Wish to minimize

Value

Impose

Countermeasures

To reduce

Risk

Threat agents

Give rise to

That increase

To

Threats

Assets

To

Wish to abuse and/or may damage

# Computer security

The study of computer security will answer the three fundamental questions:

- ❖ What assets do we need to protect?

  Assets include:

**Hardware**

- ▪ Computer components.
- ▪ Networks & comm. channels.
- ▪ Mobile devices.

**Data**

- ▪ Files
- ▪ Databases

**Software**

- ▪ Operating systems
- ▪ Off-the-shelf programs and apps
- ▪ Custom or customized programs and apps

- ❖ How are those assets threatened?
- ❖ What can we do to counter those threats?

# What is Computer security ?

"Measures to deter, prevent, detect, and correct security violation on computer system"

Source : William Stallings, Computer Security

"The protection afforded to an automated IT resources (hardware, software, data, and networks) in order to attain its applicable objectives of preserving the integrity, availability, and confidentiality".

Source : NIST (National Institute of Standards and Technology) Computer security Handbook

# International organizations

ITU: The International Telecommunication Union (ITU) is an international organization within the United Nations System in which governments and the private sector coordinate global telecom networks and services

NIST: National Institute of Standards and Technology: (former NBS National Bureau of Standards) is a U.S. federal agency that deals with measurement science, standards, and technology related to U.S. government.

IEEE: Institute of Electrical and Electronics Engineers. a leading standards development organization for the development of standards including information technology, information assurance, telecommunications, aerospace, and nanotechnology, …

ISO: International Organization for Standardization, is a worldwide federation of national standards bodies from more than 140 countries. ISO is a nongovernmental organization that promotes the development of standardization and related activities

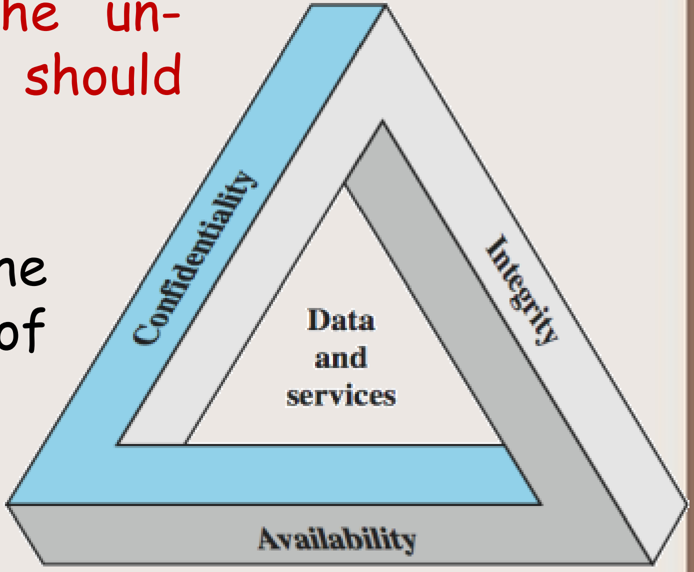
# Objectives of Computer Security

Main objectives (CIA):

❑ Confidentiality

- ❖ Ensuring that information is only accessible to authorized users ( keep the information secret)
- ❖ Information is exchanged over the un-trusted network. while exchange, should remain secret.
- ❖ Confidentiality related to both the storage as well as transmission of information

Cryptography is used to enforce confidentiality.



The Security Objectives Triad

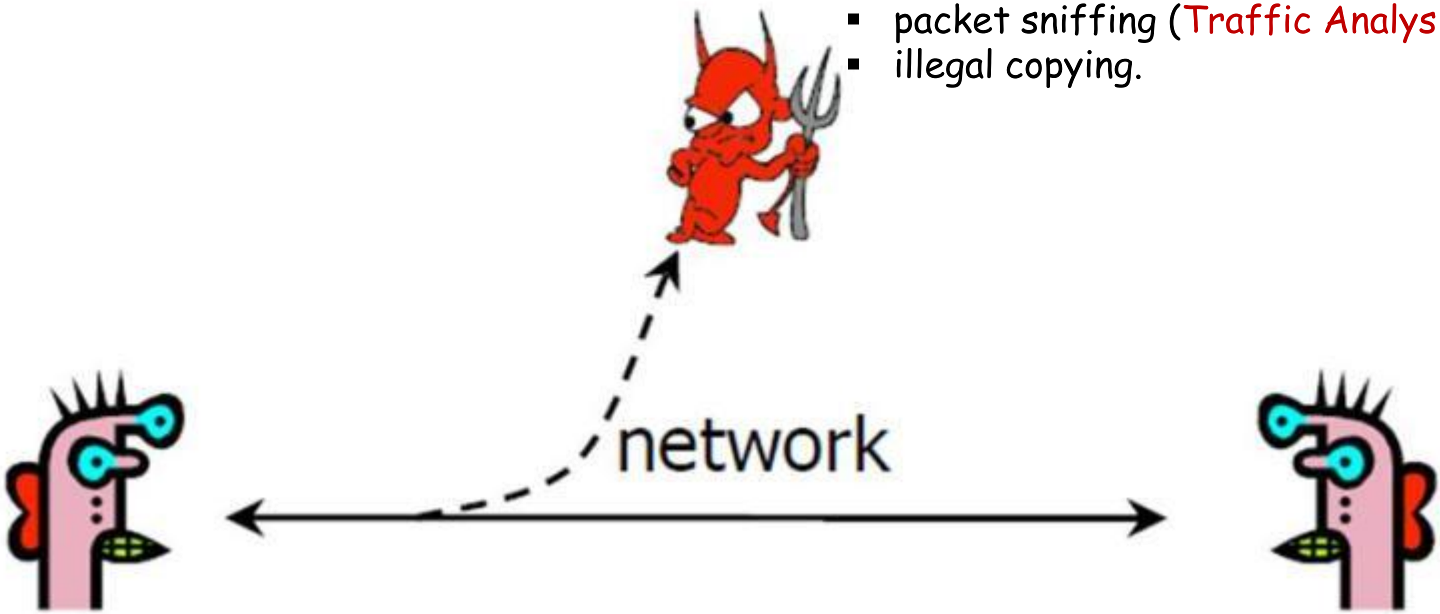
# Objectives of Computer Security

Main objectives (CIA):

❑ Confidentiality

Confidentiality is concealment of information

- Eavesdropping (Snooping ),
- packet sniffing (Traffic Analysis),
- illegal copying.



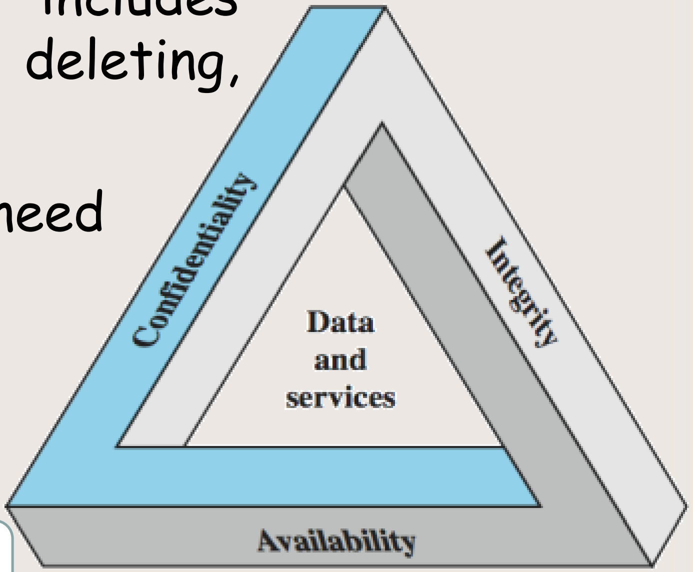
# Objectives of Computer Security

## Main objectives (CIA):

### ❑ Integrity

- ❖ Integrity means that assets can be modified only by authorized parties or only in authorized ways.
- ❖ In this context, modification includes writing, changing, changing status, deleting, and creating.
- ❖ To ensure the integrity of data we need techniques to:
  - ▪ Prevent the modification.
  - ▪ Detect any modification made.

Cryptography can be used to force integrity.



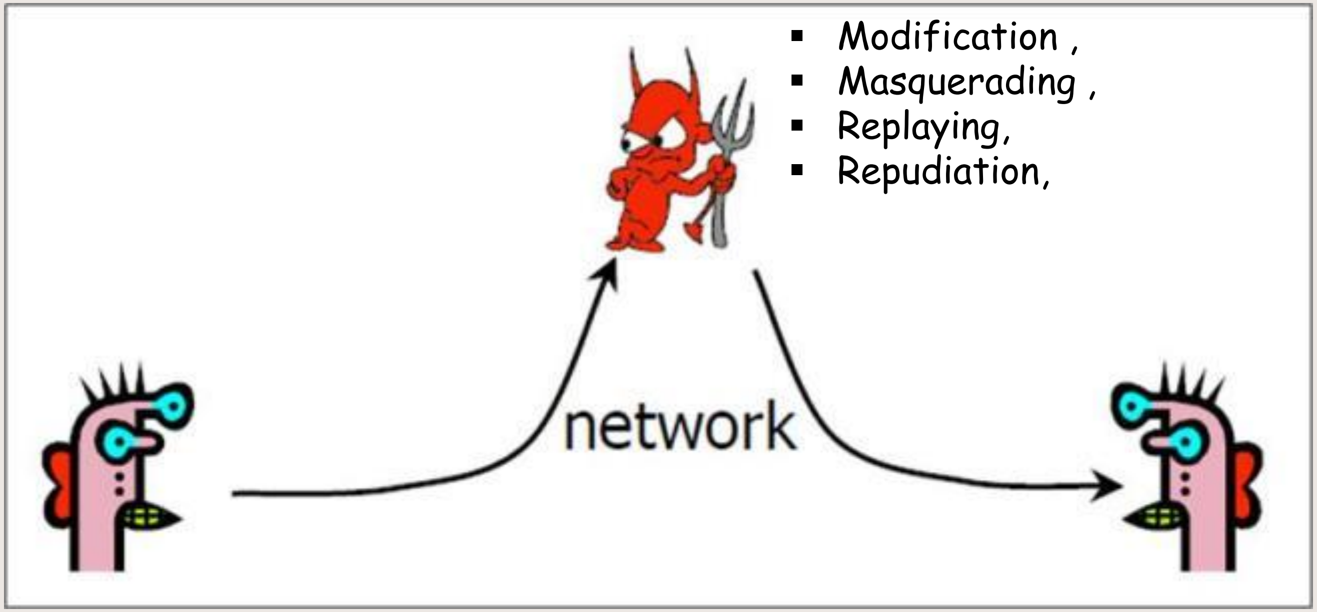
The Security Objectives Triad

# Objectives of Computer Security

Main objectives (CIA):

- Integrity

  Integrity is prevention of unauthorized changes



- Modification ,
- Masquerading ,
- Replaying,
- Repudiation,

# Objectives of Computer Security

## Main objectives (CIA):

### ❑ Threat to Integrity

- ❖ Modification: An attacker can modify the transmitted information, without needing to know the actual content.

  It could delay or change the content to foil the objective of a transaction
- ❖ Masquerading: An attacker can modify the communication data to pretend (spoof) as a legal sender or receiver to obtain the information to which it does not have access
- ❖ Replaying: An attacker copies a message sent by a different users and replays later.
- ❖ Repudiation: Sender of a message may later deny that it has sent it. A receiver of a data may also deny that it has

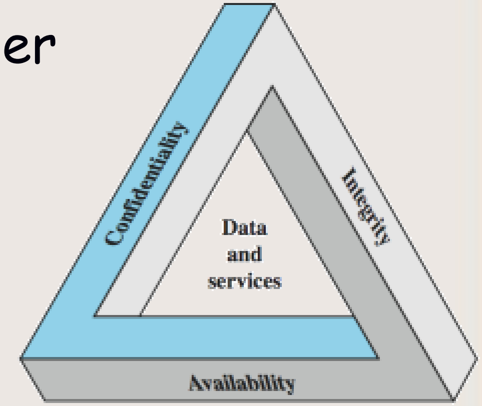
Cryptography should guarantee non repudiation in these application.

# Objectives of Computer Security

Main objectives (CIA):

❑ Availability

- ❖ Ensuring that authorized users have access to information and associated assets when needed
- ❖ Data must be available to authorized users.
- ❖ Note that:
  - Any security mechanism used should have a small overhead
  - Confidentiality and integrity should not hinder the availability of data
  - Availability differs in kind from the other two components of IT security its dedicated to both information and resources, while the other two components dedicated to information only



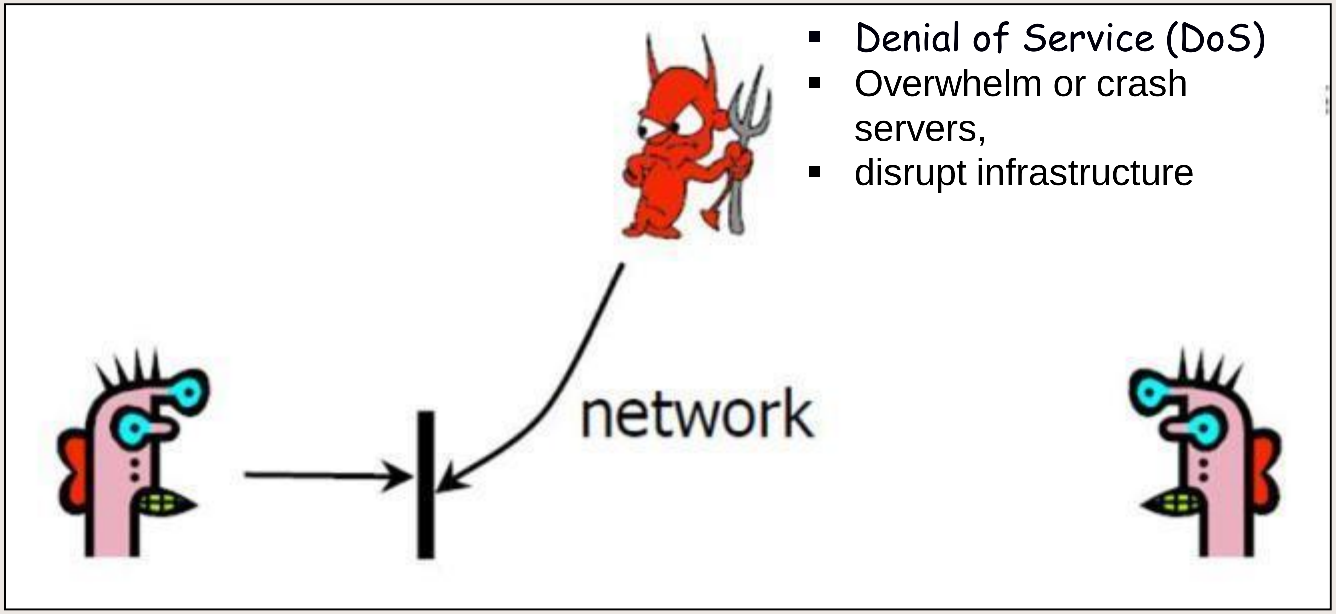
The Security Objectives Triad

# Objectives of Computer Security

Main objectives (CIA):

❑ Integrity

Integrity is prevention of unauthorized changes



- Denial of Service (DoS)
- Overwhelm or crash servers,
- disrupt infrastructure

# Objectives of Computer Security

Main objectives (CIA):

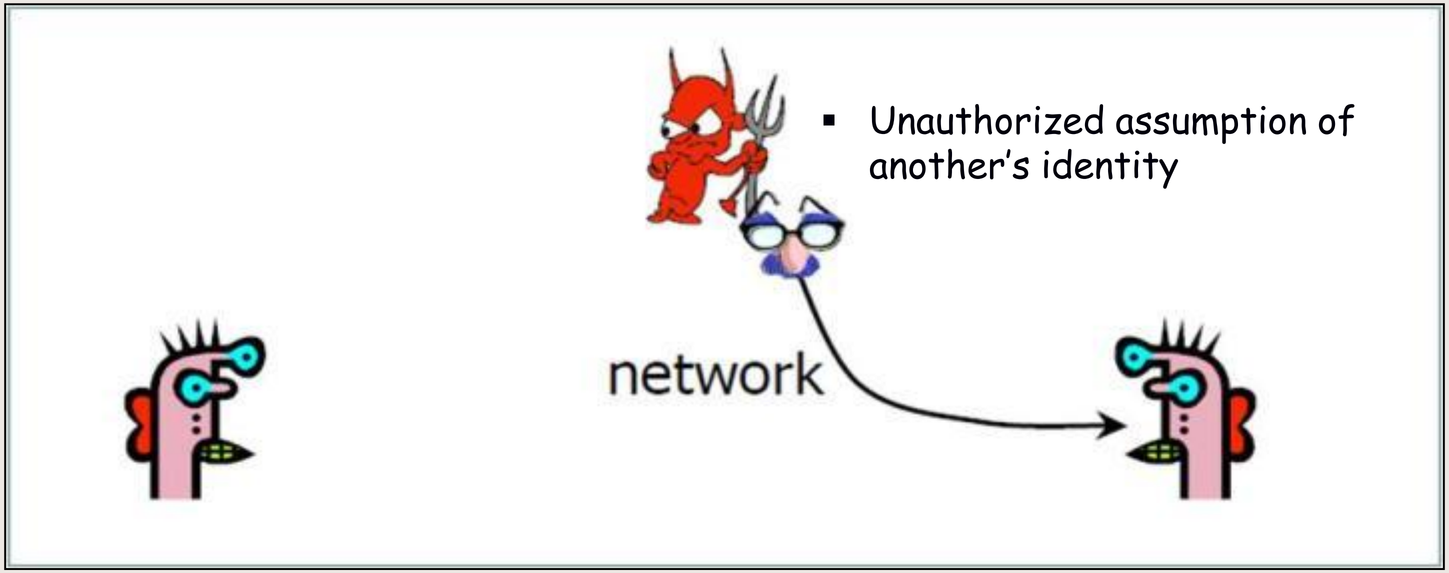
- ❑ Threat to Availability
  - ❖ Denial of Service (DoS): Slow down or totally disable the system. Examples:
    - ▪ Slow down the system with multiple requests
    - ▪ Delete the acknowledgments from the server

# Objectives of Computer Security

CIAAAAN (Security objectives added to CIA):

❑ Authentication:

- The ability of a system to confirm the identity of a sender.
- Authenticity is identification and assurance of origin of information
- Variant of integrity



- Unauthorized assumption of another's identity

# Objectives of Computer Security

CIAAAAN (Security objectives added to CIA):

- □ Authorization:

  Security mechanism to determine access levels or user/client privileges to system resources

- □ Auditability:

  The ability of a system to trace all actions related to a given asset

- □ Non-repudiation:

  The ability of a system to confirm that a sender cannot deny having sent a message.

# Objectives of Computer Security

## Impact of Security Breaches (violation)

How do security breaches impact organization?

- ❑ Effectiveness of primary operations are reduced
- ❑ Financial loss
- ❑ Damage to assets
- ❑ Harm to individuals

Different levels of impact (Risk) :

- ❑ Low/Minor,
- ❑ Moderate/Significant,
- ❑ High/Severe

# Objectives of Computer Security

## Levels of impact due to breach of security

Low/Minor: The loss could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

I. cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced.
II. result in minor damage to organizational assets.
III.result in minor financial loss.
IV. result in minor harm to individuals.

# Objectives of Computer Security

## Levels of impact due to breach of security

Moderate/Significant: The loss could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

I. cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly Reduced.
II. result in significant damage to organizational assets.
III. result in significant financial loss.
IV. result in significant harm to individuals that does not involve loss of life or serious, life-threatening injuries.

# Objectives of Computer Security

## Levels of impact due to breach of security

High/Severe: The loss could be expected to have a severe or catastrophic adverse effect on organizational operations, assets, or individuals.

I. cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions.

II. result in major damage to organizational assets.

III. result in major financial loss.

IV. result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.

# Objectives of Computer Security

Quiz: Assign security objective and Level of security impact for each of the following assets:

| Asset | Objective (C/I/A) | Level (L/M/H) |
|---|---|---|
| Student grade information | | |
| Student enrollment information | | |
| lists of students or departmental lists | | |
| Patient allergy information | | |
| A Web site that offers a forum to registered users to discuss some specific topic. | | |
| Online telephone directory lookup application | | |
| Anonymous online poll | | |
| A system that provides authentication services | | |
| Public Web site for a university | | |

SH. A

# Objectives/Assets Threats Matrix

| | Availability | Confidentiality | Integrity |
|---|---|---|---|
| Hardware | Equipment is stolen or disabled, thus denying service. | | |
| Software | Programs are deleted, denying access to users. | An unauthorized copy of software is made. | A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task. |
| Data | Files are deleted, denying access to users. | An unauthorized read of data is performed. An analysis of statistical data reveals underlying data. | Existing files are modified or new files are fabricated. |
| Network | Messages are destroyed or deleted. Communication lines or networks are rendered unavailable. | Messages are read. The traffic pattern of messages is observed. | Messages are modified, delayed, reordered, or duplicated. False messages are fabricated. |

# Computer Security Terms

Vulnerabilities: A flaw or weakness in a system that could be exploited to violate the system's security policy.

System resource (assets) vulnerabilities may:

- ❖ Be corrupted (loss of integrity)
- ❖ Become leaky (loss of confidentiality)
- ❖ Become unavailable (loss of availability)

# Computer Security Terms

Threat : A possible violation of security, that could breach security and cause harm

Attack: (threat turn into action).

- □ Any action that compromises the security of information owned by an organization
- □ Often threat & attack used to mean same thing
- □ Attacks may be:
  - ❖ Passive attack
  - ❖ Active attack

# Computer Security Terms

Security Breaches: It is the unauthorized access of information on networks, servers, or devices, getting around security on those systems, ultimately resulting in data leakage.

Secrecy: is to hide information that can be observed and analyzed by others.

Privacy: attempts to keep communications between people from being intercepted. Security technologies of privacy — including access control and encryption.

# Computer Security Terms

## Countermeasures:

- ❑ An action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack
- ❑ Means used to achieve security objectives (to deal with security attacks)
  - ❖ Prevent (firewalls, encryption, access control)
  - ❖ Detect (IDS, auditing, monitoring)
  - ❖ Recover (backup, logging, restore points)
- ❑ No single mechanism that will support all services required.
- ❑ May result in new vulnerabilities
- ❑ Will have residual vulnerability

# Computer Security Challenges

1. Not simple.
2. Must always consider potential attacks.
3. Procedures used counter-intuitive.
4. It is necessary to decide where to deploy various security mechanisms.
5. Battle of wits between attacker / admin.
6. Not perceived on benefit until fails.
7. Requires regular monitoring.
8. Too often an after thought - incorporated after the design is complete. .
9. Regarded as impediment to using system.

# Computer Security Strategy

The overall strategy for providing computer security involves three aspects:

- ❑ Specification/Policy
- ❑ Implementation/Mechanisms
- ❑ Correctness/Assurance

# Computer Security Strategy

## ❑ Specification /Policy

- Security policy is a document that states in writing how a company plans to protect its (IT) assets.
- Security policy may be:
  - An acceptable use policy,
  - A description of how the company plans to educate its employees about protecting the company's assets,
  - An explanation of how security measurements will be carried out and enforced.
  - Procedures for evaluating the effectiveness of the security policy to ensure that necessary corrections will be made.

# Computer Security Strategy

## ❑ Specification /Policy

- Security policy never finished, but is continuously updated as technology and employee requirements change.
- To develop a security policy we should consider:
  - ❖ The value of the assets being protected
  - ❖ The vulnerabilities of the system
  - ❖ Potential threats and the likelihood of attacks
  - ❖ Ease of use versus security
  - ❖ Performance versus security
  - ❖ Cost of security versus cost of failure and recovery

# Computer Security Strategy

## ❑ Implementation/Mechanisms

Security implementation involves 4 courses of action:

- ❖ Prevention: An ideal security scheme is one in which no attack is successful.
- ❖ Detection: In a number of cases, absolute protection is not feasible, but it is practical to detect security attacks.
- ❖ Response: If security mechanisms detect an ongoing attack, the system may be able to respond in such a way as to halt the attack and prevent further damage.
- ❖ Recovery: An example of recovery is the use of backup systems, so that if data integrity is compromised, a prior, correct copy of the data can be reloaded.

# Computer Security Strategy

## ❑ Correctness/Assurance

Does the security system really work

- ❖ Assurance: is defined as the degree of confidence one has that the security measures, work as intended to protect the system and the information it processes. Assurance deals with the questions:
  - ○ "Does the security system design meet its requirements?"
  - ○ "Does the security system implementation meet its specifications?"
- ❖ Evaluation: is the process of examining a computer product or system with respect to certain criteria.

# Security Architecture (X.800)

- ❑ Recommended by ITU (International Telecom Union) for open systems interconnection (OSI) as a way of organizing the task of providing security
- ❑ Systematic approach to define requirements for security and approaches to satisfying those requirements
- ❑ Focuses on security in the context of networks and communications, the concepts apply also to computer security.
- ❑ Focuses on security attacks, mechanisms, and services.

## Security Architecture (X.800)

Attacks:

- ❑ Types of Attacks:
  - ❖ Passive attack
  - ❖ Active attack
- ❑ Attacks can be classified based on the origin of the attack:
  - ❖ Inside attack.
  - ❖ Outside attack.

# Security Architecture for (X.800)

## Attacks:

❑ Passive attack:

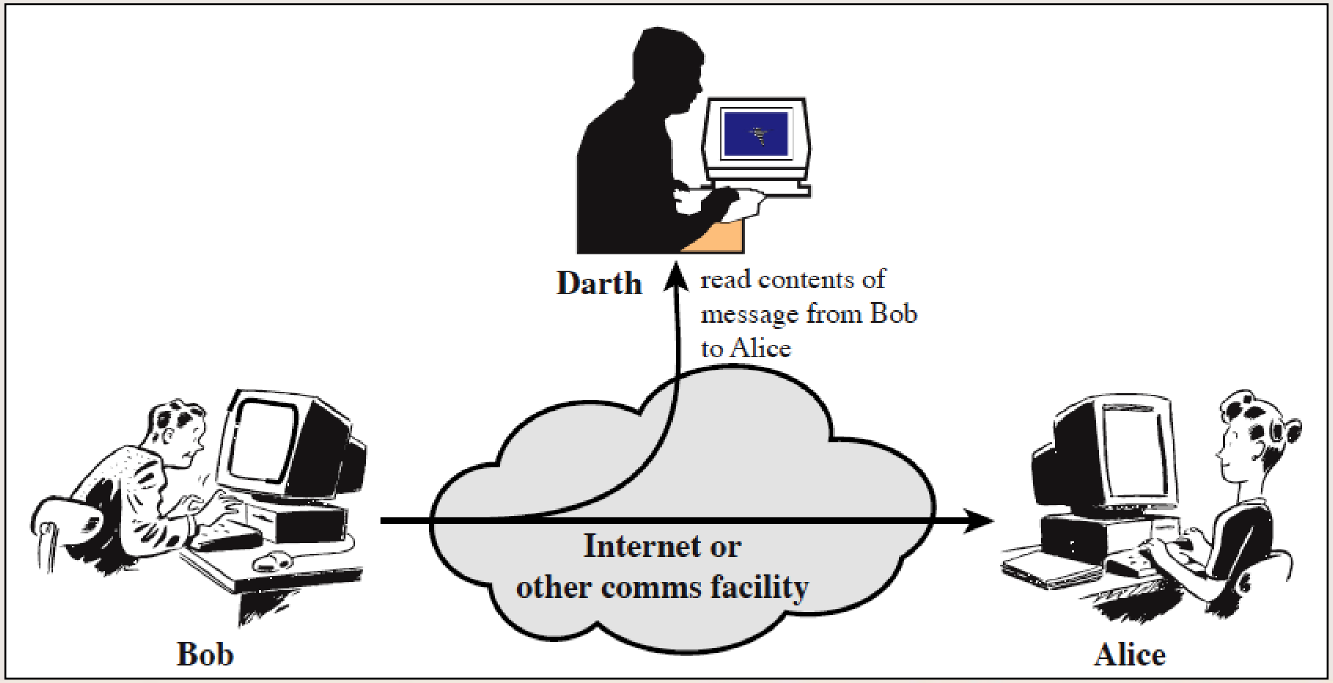
- ❖ Do not affect system resources
- ❖ Very difficult to detect
- ❖ The goal is to prevent.
- ❖ Message transmission apparently normal
- ❖ No alteration of the data
- ❖ Two types of passive attacks:
  A- Unauthorized reading of messages.
  B- Traffic analysis

# Security Architecture (X.800)

## Attacks:

❑ Passive attack:

A- Unauthorized reading of messages.

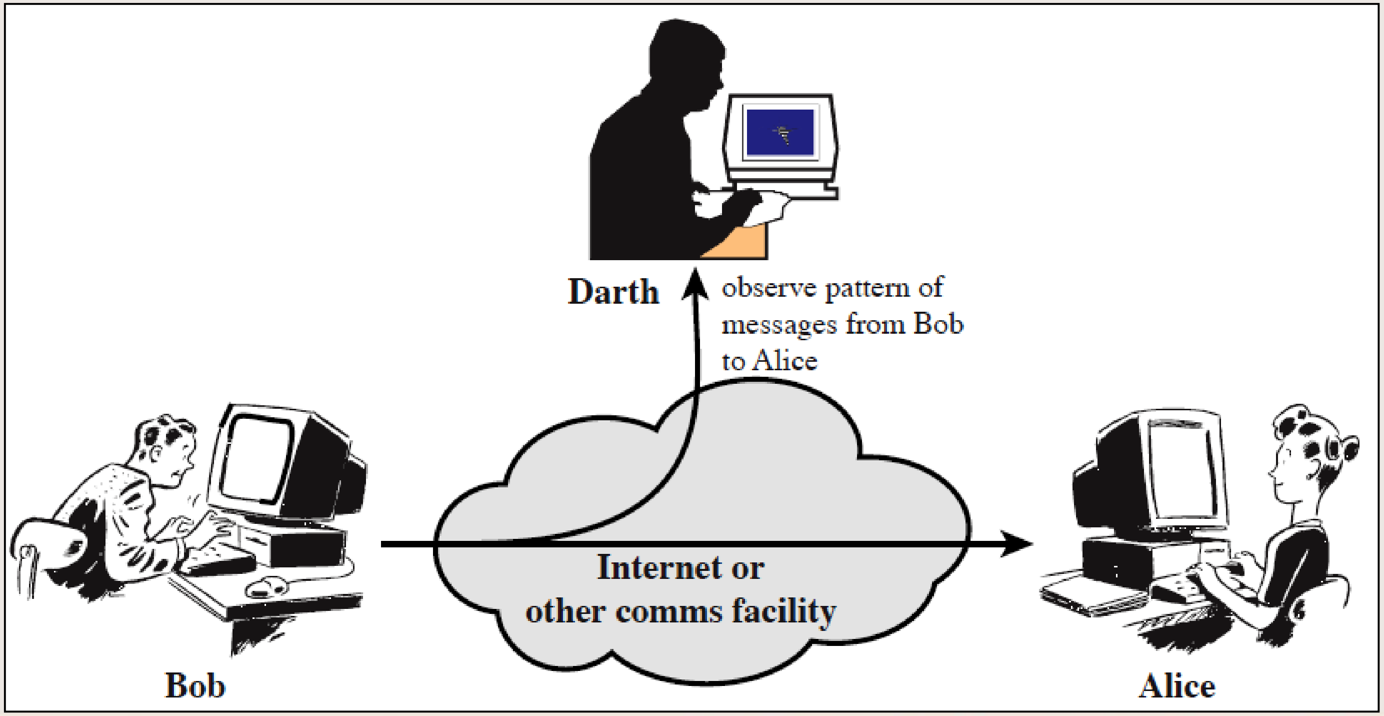

Darth
read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

# Security Architecture (X.800)

## Attacks:

- ❑ Passive attack:

  B- Traffic analysis


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

# Security Architecture (X.800)

## Attacks:

### ❑ Active attack:

- ❖ Active attacks try to alter system resources or affect their operation.
- ❖ Modification of data, or creation of false data.
- ❖ Difficult to prevent
- ❖ The goal is to detect and recover.
- ❖ Four categories:

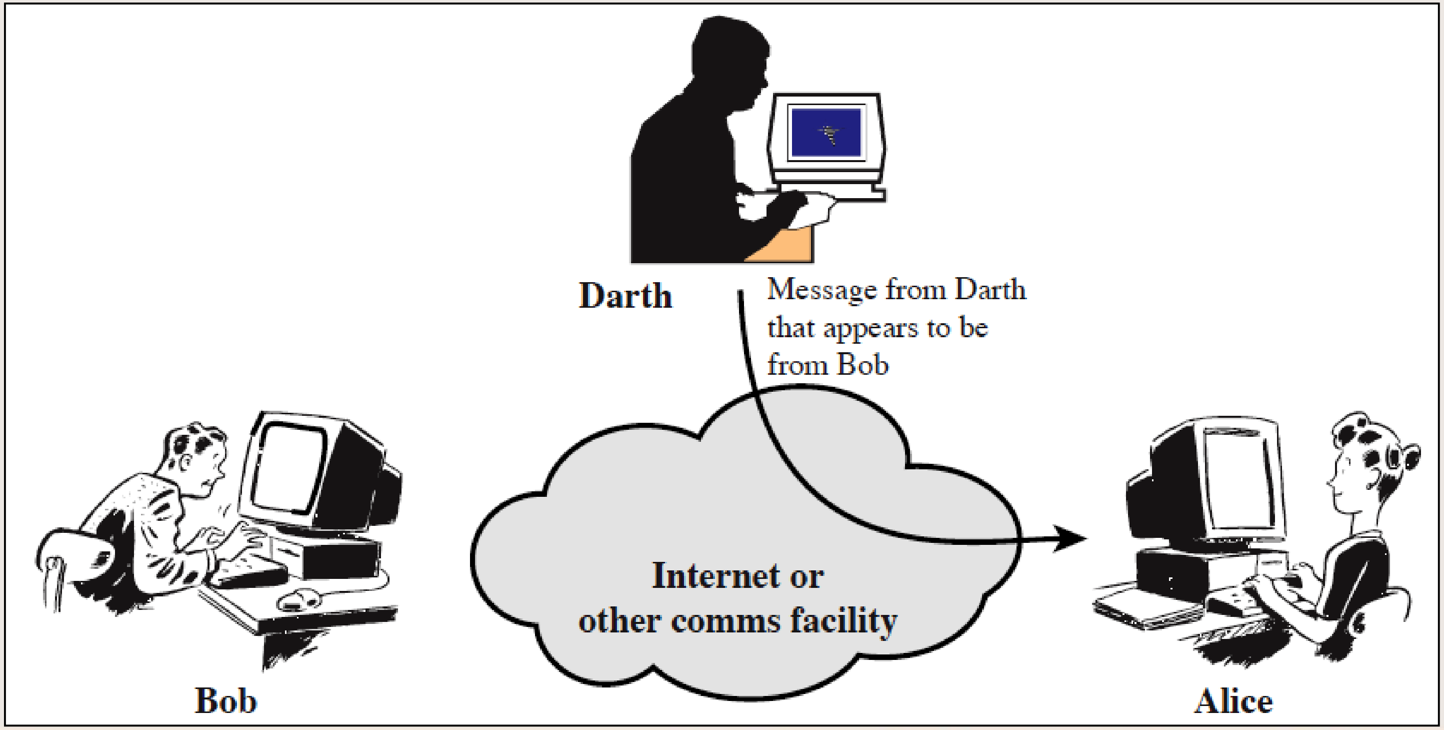
  A- Masquerade
  B- Replay
  C- Modification of messages.
  D- Denial of service: preventing normal use

# Security Architecture (X.800)

## Attacks:

- ❑ Active attack:

A- Masquerade

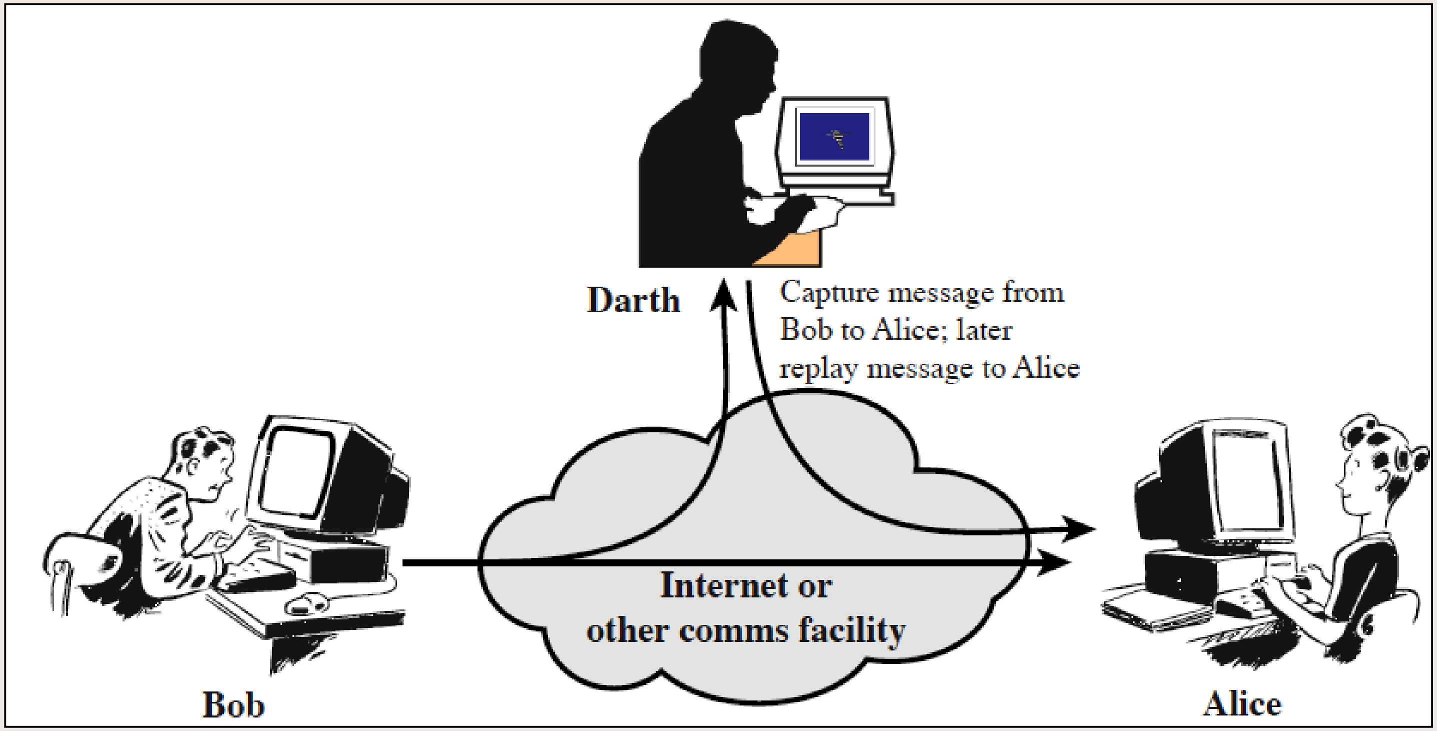

Darth
Message from Darth that appears to be from Bob
Internet or other comms facility
Bob
Alice

# Security Architecture (X.800)

## Attacks:

❑ Active attack:

B- Replay

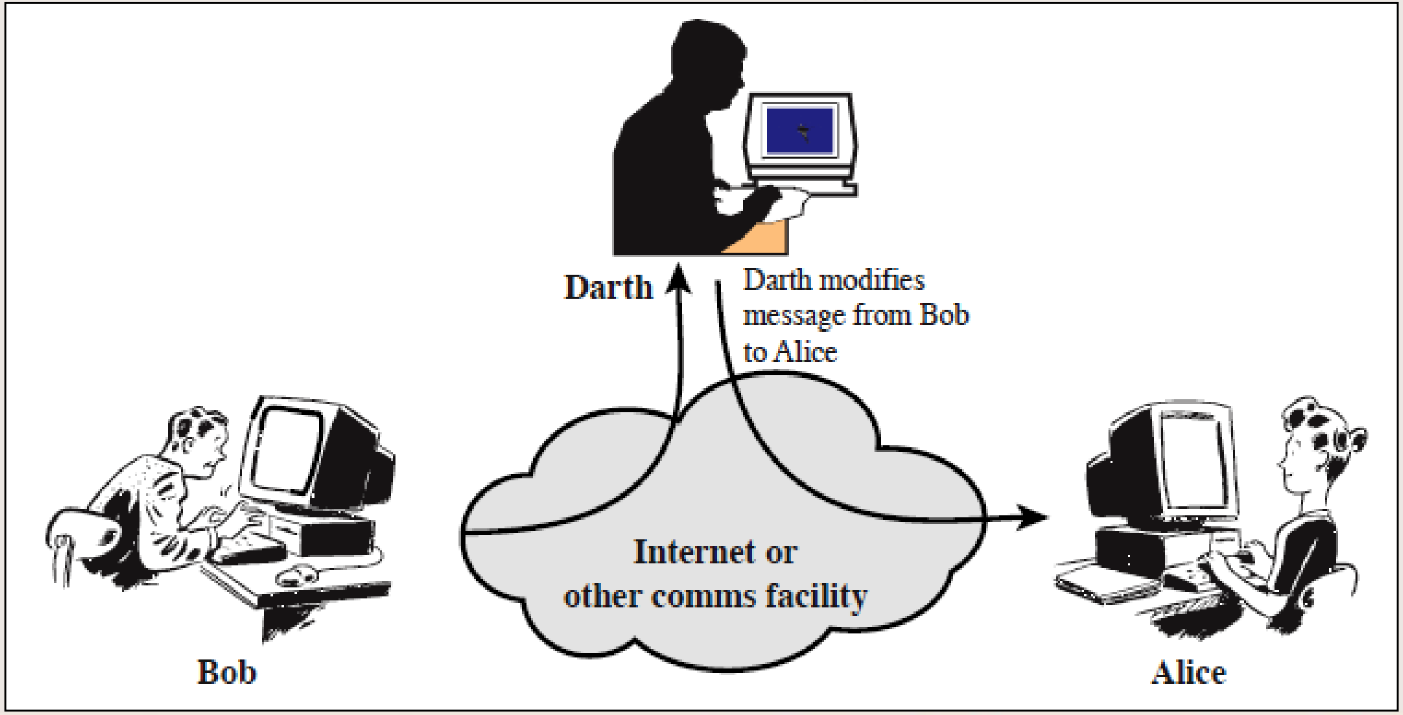

Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice

# Security Architecture (X.800)

## Attacks:

❑ Active attack:

C- Modification of messages


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

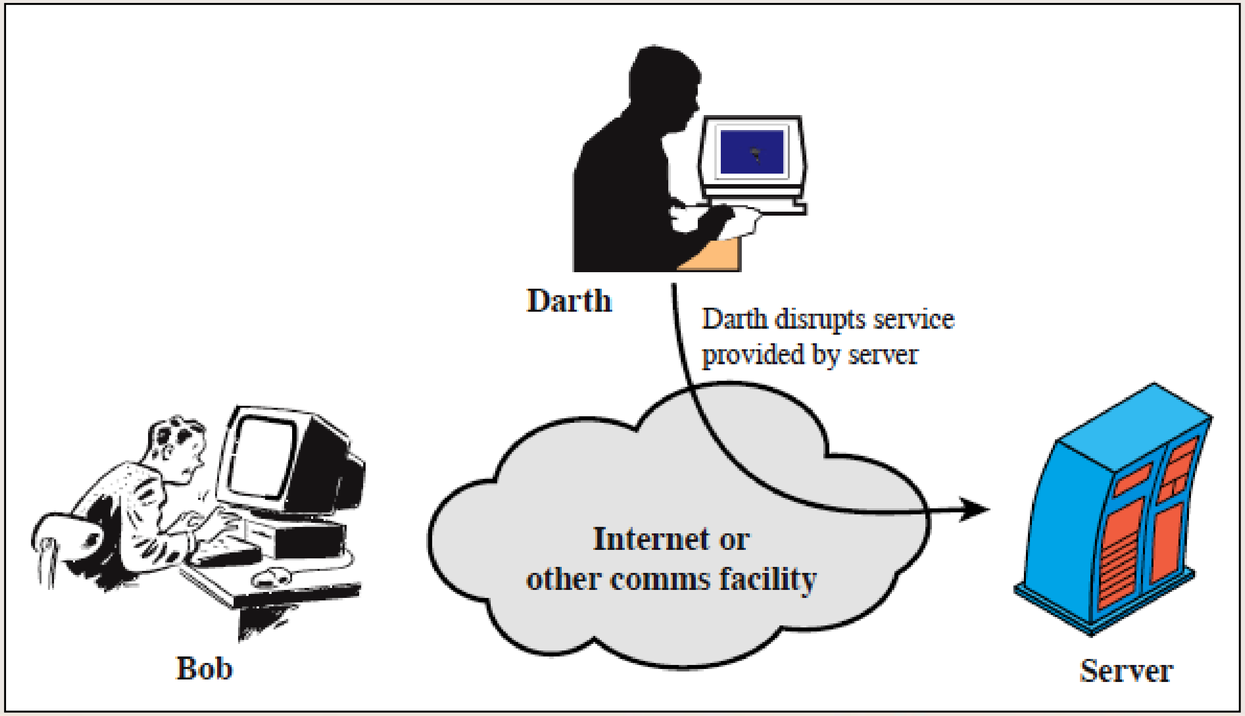
SH. A

# Security Architecture (X.800)

## Attacks:

❑ Active attack:

D- Denial of service


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

# Security Architecture (X.800)

## Security services:

- ❑ A service that enhance the security of the systems and the information transfers of an organization in order to counter and stop attacks.
- ❑ They make use of one or more security mechanisms to provide the service.

# Security Architecture (X.800)

## Security services:

- ❑ Authentication (who created or sent the data): identification and assurance of origin of information
- ❑ Access Control (prevent misuse of resources): Prevent unauthorized use of a resource.
- ❑ Data Confidentiality(privacy): Protect data from unauthorized disclosure (concealment of data).
- ❑ Data Integrity (has not been altered): Assure data received are exactly as sent by authorized entity (prevention of unauthorized changes.
- ❑ Non-repudiation (the order is final): Protect against denial of one entity involved in communications of having participated in communications.
- ❑ Availability (performance, non-erasure): System is accessible and usable on demand by authorized users according to intended goal (ability to use information or resources desired

## Security Architecture (X.800)

Security mechanism:

- ❑ Defined by "A Technique that is designed to prevent, detect or recover from security attack".
- ❑ No single mechanism can provide all services
- ❑ Security mechanisms should be as simple as possible.
- ❑ Common in most mechanisms : Cryptographic techniques

# Security Architecture (X.800)

- ❑ Security Mechanisms for X.800:
  - ❖ Encipherment
  - ❖ Data integrity
  - ❖ Digital signature
  - ❖ Authentication exchange
  - ❖ Access control
  - ❖ Traffic padding
  - ❖ Routing control
  - ❖ Notarization.

# Security Architecture (X.800)

## Security mechanism:

- ❑ Encipherment:

  Hiding information by encryption, stenography. It may be used for other services also along with other mechanisms, like for authentication, non-repudiation etc.

- ❑ Data Integrity:

  A small checksum (hash) value for a message is appended and sent. The receiver checks for the validity of the checksum.

# Security Architecture for OSI (X.800)

## Security mechanism:

- ❑ Digital Signature:

  Sender can electronically sign an information and a receiver can verify it.

- ❑ Authentication:

  Two parties can exchange information to prove to each other that they are communicate, and not being masqueraded

- ❑ Access control:

  Uses methods to prove that users have access to information, via password or PIN

# Security Architecture for OSI (X.800)

## Security mechanism:

- ❑ Traffic Padding:

  Insert bogus data to prevent traffic analysis

- ❑ Routing Control:

  To select and change available channels of communication to make the attacker's job harder.

- ❑ Notarization:

  To have a trusted third party to control the communication.

# Security Architecture for OSI (X.800)

## Relationship Between Security Services and Mechanisms

### Mechanisms

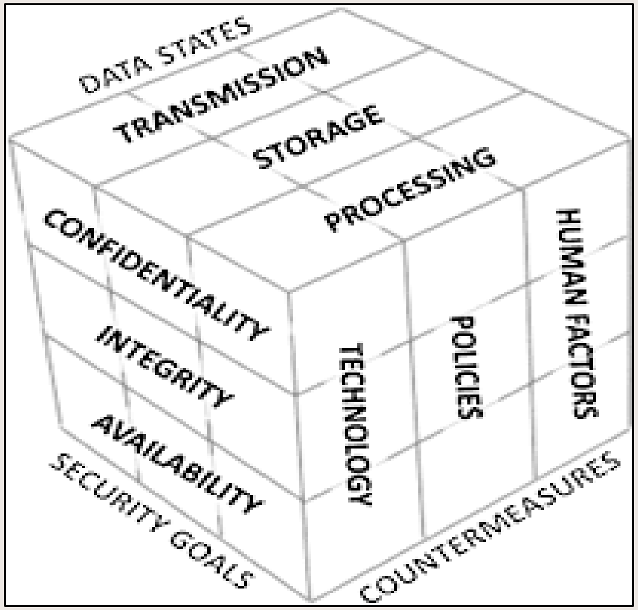
| Services | Encripherment | Digital Signature | Access Control | Data Integrity | Authentication Exchange | Traffic Padding | Routing Control | Notarization |
|---|---|---|---|---|---|---|---|---|
| Peer entity authentication | y | y |  |  | y |  |  |  |
| Data origin authentication | y | y |  |  |  |  |  |  |
| Access control |  |  | y |  |  |  |  |  |
| Confidentiality | y |  |  |  |  |  | y |  |
| Traffic flow confidentiality | y |  |  |  | y | y | y |  |
| Data integrity | y | y |  | y |  |  |  |  |
| Non-repudiation |  | y |  | y |  |  |  | y |
| Availability |  |  |  | y | y |  |  |  |

# Assignment

1) You are a member of the computer and data security team in shorouk academy:
   a. Make a list of all possible threats that can have an impact on the security of data and internal and external IT services.
   (Hint : Nature, People, Malware, Infrastructure or service problems, Human errors they are all possible risks).
   a. Make a list of recommendation to lower the risks.
2) Write short report defines the different between security risks and vulnerabilities.
3) Define the type of security attack:
   a. A student steals the question paper.
   b. I buy a book through credit card for 2000$ but find in my bank account that 4000$ has been paid.
   c. One receives hundreds of emails from a colleagues from an anonymous email account
4) Think of possible security mechanism to prevent attacks in question 3.

# McCumber cube

- ❑ It looks at security as a three-dimensional cube.
- ❑ The dimensions are
  - ❖ goals
  - ❖ information states
  - ❖ safeguards

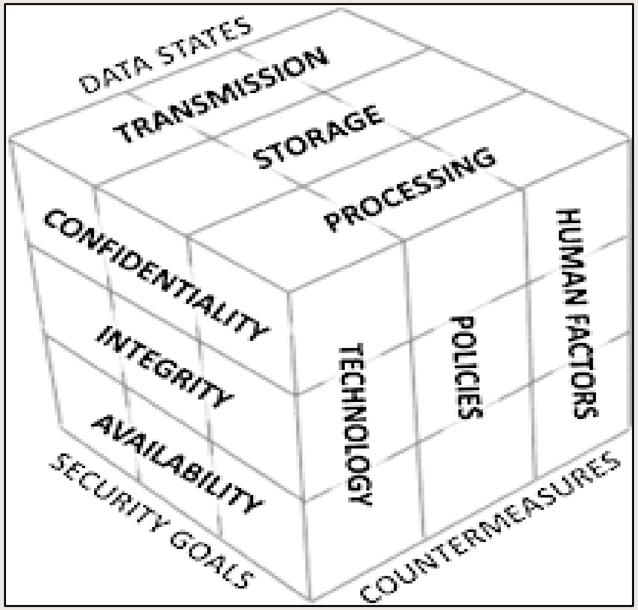


- ❑ The McCumber cube has the advantage of being a natural expansion of the CIA triangle into three dimensions.

# McCumber cube

- It looks at security as a three-dimensional cube.

- The dimensions are
  - goals
  - information states
  - safeguards



- The McCumber cube has the advantage of being a natural expansion of the CIA triangle into three dimensions.