# Information Systems Security

Lecture 1

## Introduction to Information System Security

**Dr. Eng. Bader Ahmad**

# Motivation

- When you store a private message on your HD or flash memory, how can you be sure that:
  - No one has read your message, or
  - No one has modified it during storage?

- When you receive a message from your colleague, how can you be sure that:
  - Your colleague is really the one who's sent the message, or
  - Your colleague would not deny sending it to you?

# Outline

1. What is Security?
2. What is Information Security?
3. Why Information System Security?
4. Vulnerability, Threat and Attack
5. Security Policies
6. Security Measures
7. Security Requirements
8. Security Services
9. Security Mechanisms
10. Conclusion

# 1. What is security?

- *Security:* protecting general assets
- Security can be realized through:
  1. ***Prevention***: take measures that prevent your assets from being damaged.
  2. ***Detection*****:** take measures so that you can detect when, how, and by whom an asset has been damaged.
  3. ***Reaction***: take measures so that you can recover your assets or to recover from a damage to your assets

- Examples: next slide

- There are many branches of Security: national security, economic security, *information security*, etc.

# Examples

- Ex. 1 - Private property
  - Prevention: locks at doors, window bars, walls around the property.
  - Detection: stolen items aren't there any more, burglar alarms, CCTV, …
  - Reaction: call the police,…

# Examples

- Ex. 2 - eCommerce
  - Prevention: encrypt your orders, rely on the merchant to perform checks on the caller,…
  - Detection: an unauthorized transaction appears on your credit card statement
  - Reaction: complain, ask for a new credit card number, …

# What is security?

- There are many branches of Security:
  - national security,
  - economic security,
  - *information security*
  - …

# 2. What is Information Security?

- ***Information security*: is concerned with protecting information and information resources such as: books, faxes, computer data, voice communications, etc.**

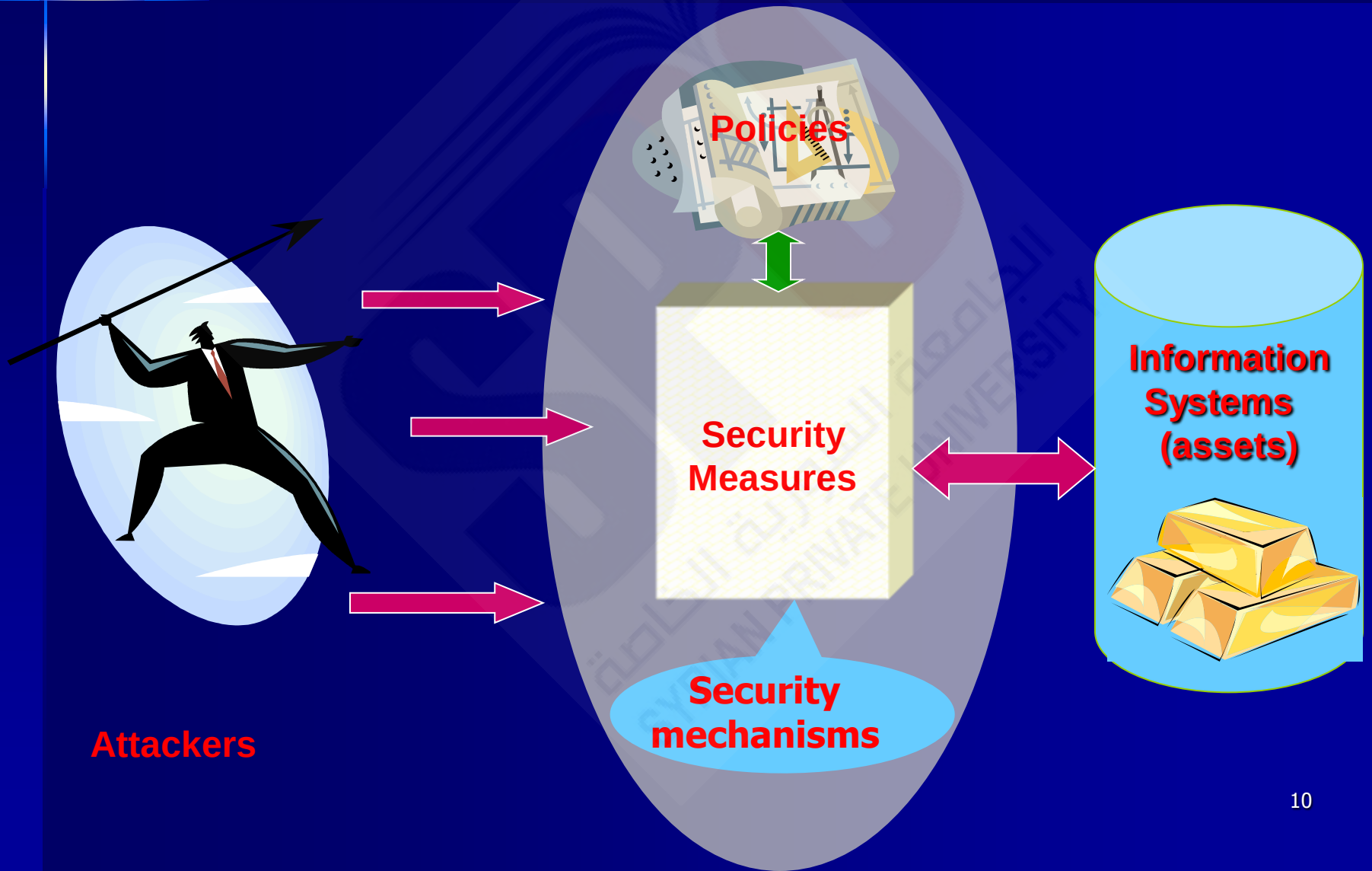
- **Information security is** determining:
  - what needs to be protected, *i.e.*, assets
  - why (Security requirements which include),
  - what needs to be protected from (*Threats*, *vulnerabilities*, *risks*),
  - and how (*Security measures*) to protect it for as long as it exists
    - Security measures which are implemented according to a **security policy**

# 3. Information System Security

- **Information System Security** (ISS) is concerned with protecting Information system assets such as PCs, software, applications, etc.

- In order to ensure the security of Information Systems, we need to determine:
  1. Assets (i.e., Information systems) to be protected
  2. Security requirements;
  3. Threats, vulnerabilities, risks
  4. Security policies
  5. Security measures

# What is Information System Security (ISS)?



# 4. Vulnerability, Threat and Attack

- A ***vulnerability***: is a weakness in system design or implementation and can be in hardware or software.
  - Example: a software bug exists in the OS, or no password rules are set.

- A ***threat***:
  - is something that can potentially cause damage to the network or computer system.
  - is an indication of potential undesirable event
  - It refers to a situation in which
    - a person could do something undesirable (an attacker initiating a denial-of-service attack against an organization's email server), or
    - a natural occurrence could cause an undesirable outcome (a fire damaging an organization's information technology hardware).

# Vulnerability, Threat and Attack

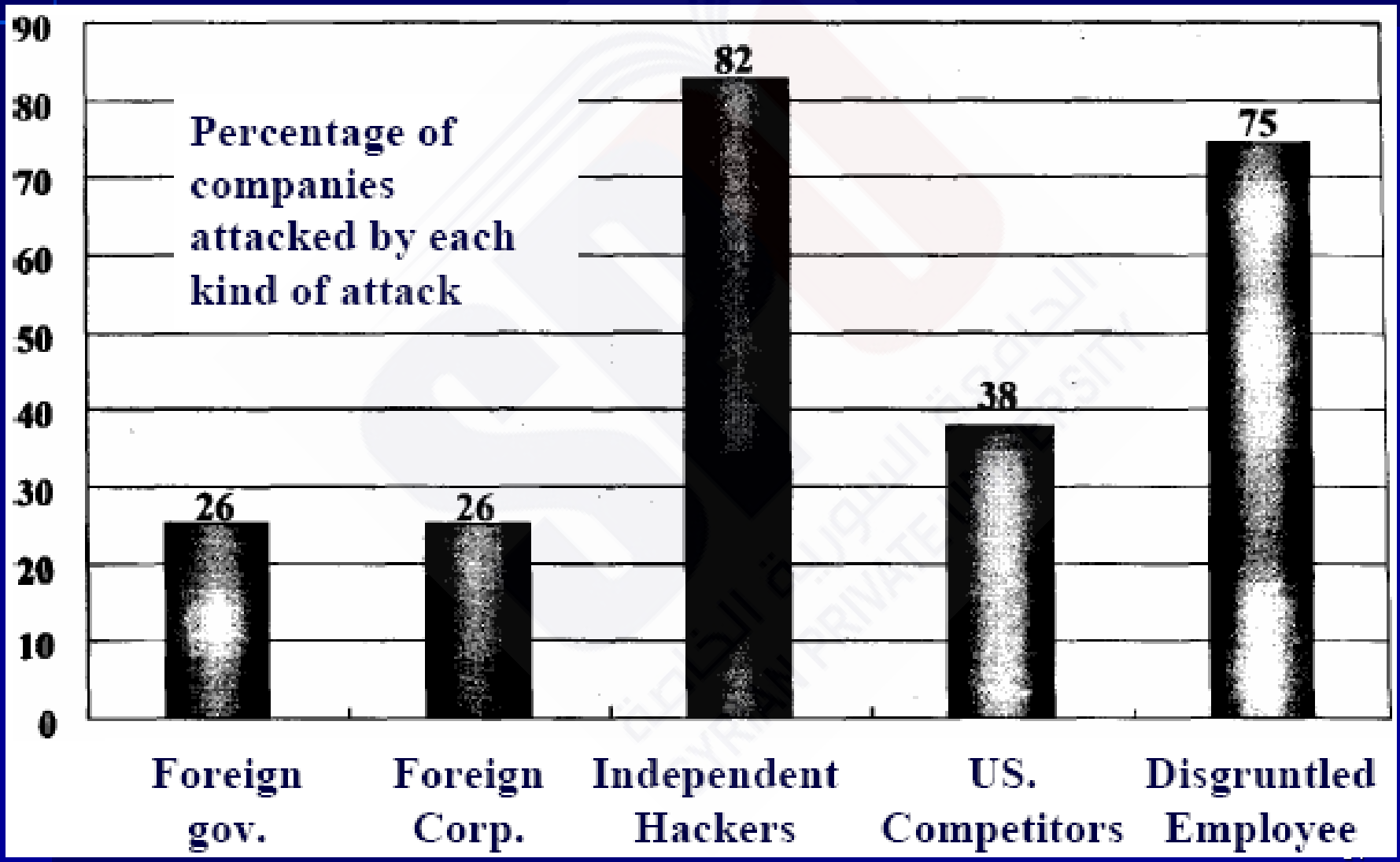
- A **vulnerability: Examples**
  - Unprotected data under transmission
  - Mistakes in firewall or router
  - Software bugs exist.
  - Passwords posted near the computer
  - There is no protection against computer viruses.
  - Security policy is not set.

- Threats: **Examples**
  - Virus
  - Illegal Passwords  use
  - Illegal access to the internet

# Vulnerability, Threat and Attack

- A ***Risk*** is the possibility of suffering harm or loss.
- An ***attack***: is a realization of a threat
- An ***attacker***: is a person who exploit a vulnerability
- An attacker must have means, opportunity, and motive
  - Synonyms: enemy, adversary, opponent, eavesdropper, intruder

# Likely sources of Attacks (US Statistics)



# Threats from hackers

**hackers** are computer or network expert

They Conduct illegal access only to satisfy their interest, or try out their technology (no damage to other people)

They cause damage by stealing information from networks/servers they accessed illegally, or by forcing services to shutdown

**Crackers**

Examples of threats :

- Illegally use IDs or passwords that they stole
- Illegally access servers and steal personal information, etc.

# Common security attacks

- Interruption, delay, denial of receipt or denial of service
  - System assets or information become unavailable or are rendered unavailable
- Interception or snooping
  - Unauthorized party gains access to information by browsing through files or reading communications.
- Modification or alteration
  - Unauthorized party changes information in transit or information stored for subsequent access.
- Masquerade or spoofing
  - Spurious information is inserted into the system or network by making it appears as if it is from a legitimate entity.
- Repudiation of origin
  - False denial that an entity created something.

# 5. Security Policy

- A ***security policy*** states what is, and is not, allowed
- Is a document describing a company's security controls and activities.
- Does not specify technologies.
- Examples:
  - **Policy: Password construction** Account names must not be used in passwords.
  - **Policy: Confidentiality of Personal information** all personal information must be treated as confidential.
- A **security Policy** is a guideline for implementing security measures.

# 6. Security measures

- ***Security measures*** include techniques for ensuring:
  - Prevention: such as **encryption**, **user authentication**, **one time password**, **anti-virus**, **firewall**, etc.
  - Detection: such as **IDS (Intrusion Detection Systems)**, Monitoring tools, Firewall log, **digital signature**, etc.
  - Reaction (or recovery): Such as Backup systems, OS's recovery points, etc.

# 7. Security Requirements

- Most important security requirements are:
  - ***Confidentiality***: keeping information secret from all but those who are authorized to see it.
    - Also called secrecy or privacy
  - ***Integrity***: ensuring information has not been altered by unauthorized or unknown means.
  - ***Availability:*** keeping information accessible by authorized users when required

# Security Requirements

- Other requirements:
  - ***Entity authentication:*** corroboration of the identity of an entity (e.g., a person, a credit card, etc.)
    - Identification, identity verification
  - ***Message authentication***: corroborating the source of information; also known as *data origin authentication*.
    - Message authentication implicitly provides data integrity
  - ***Non-repudiation:*** preventing the denial of previous commitments or actions

# Security Requirements

- ***Authorization***: conveyance, to another party, of official sanction to do or to be something.
- ***Access control***: restricting access to resources to privileged entities.
- ***Validation***: a means to provide timeliness of authorization to use or manipulate information or resources.

- These Requirements are referred to as ***ISS objectives*** (another definition of ISS).

# 8. Security services

- An ***information security service*** is a method to provide some specific aspects of security
  - Examples
    - Confidentiality is a security objective (requirement), encryption is an information security service
    - Integrity is another security objective (requirement), a method to ensure integrity is a security service.
- ***Breaking*** a security service implies defeating the objective of the intended service.

# 9. Security mechanisms

- A ***security mechanism*** encompasses Protocols, algorithms, to achieve specific security objectives (confidentiality, integrity, …).
  - Digital signature
  - Encryption
  - ..

# 10. Conclusion

- Security terms
  - ISS
  - Security Requirements (Objectives)
  - Security Policy
  - Vulnerabilities and Threats,
  - Security measures

- Next lectures:
  - Studying those terms in detail


Questions?