Computer security

Section 1

Eng: Ahmed safar

Computer security

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

Objectives of computer security

1)Integrity

2)Availability

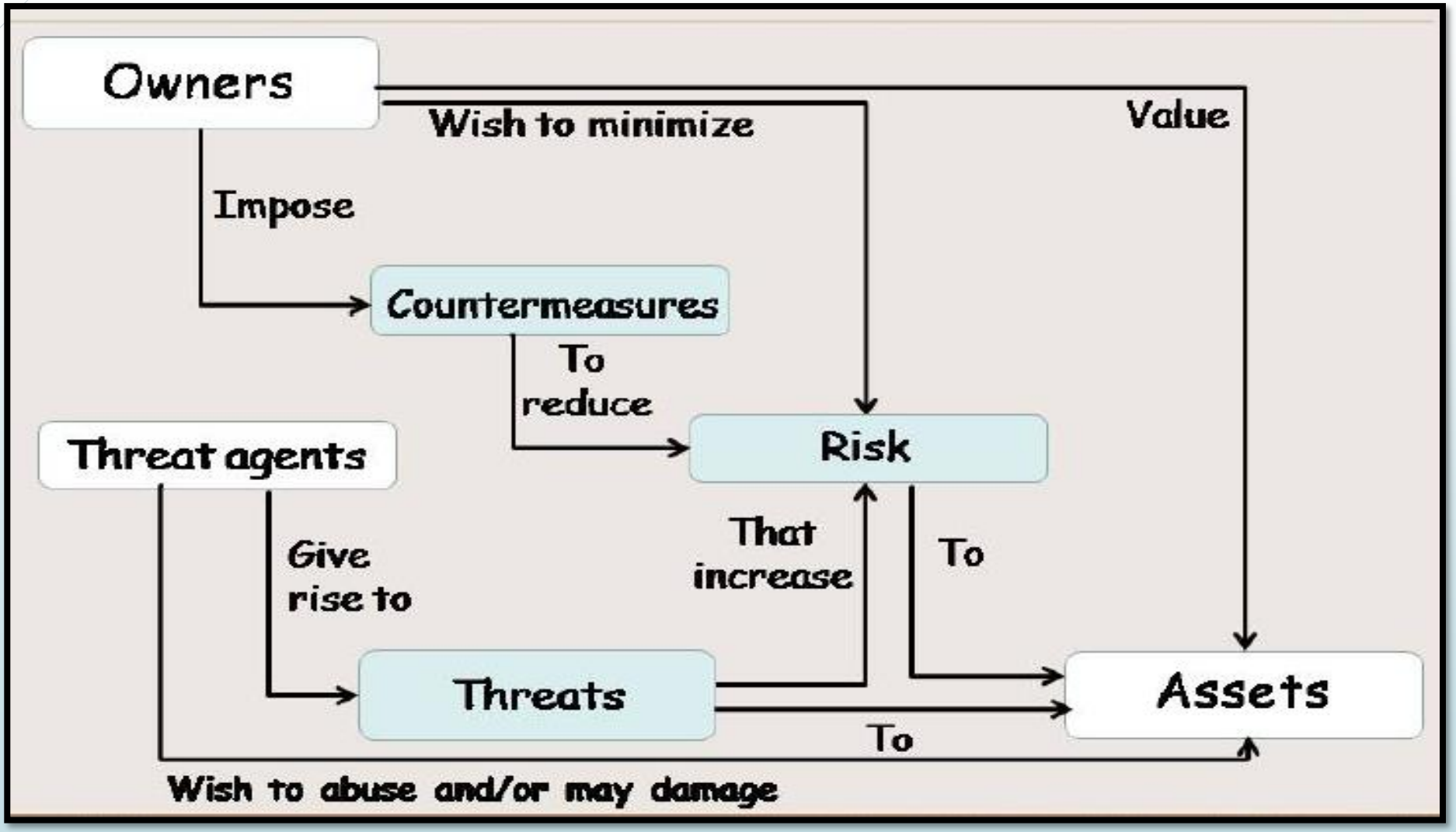
3)Confidentiality

Computer security terms :

- **Vulnerability :** A flow or weakness in a system that could be exploited to violate the systems security policy.
- **Threat**: A possible violation of security ,that could breach security and cause harm.
- **Attack**: Any action that compromises the security of information owned by organization.
- **Countermeasures** : An action,device,procedure ,or technique that reduces a threat , a vulnerability ,or an attack.

Threat Sources

Security concept



Quantitative Risk Analysis

Example

- Value of breach, $10,000 per month (SLE)
- Annual Rate of Occurrence, 12 (ARO)
- Countermeasure cost, $30,000

ALE = 10,000 * 12

Based on Quantitative Risk Analysis, is the countermeasure a cost effective solution to the issue?

Some basic terminology

- Plaintext: original message .
- Cipher text: coded message .
- key: info used in cipher known only to sender/receiver .
- Encryption : converting plaintext to cipher text .
- Decryption : recovering plaintext from cipher text.

Security Attacks

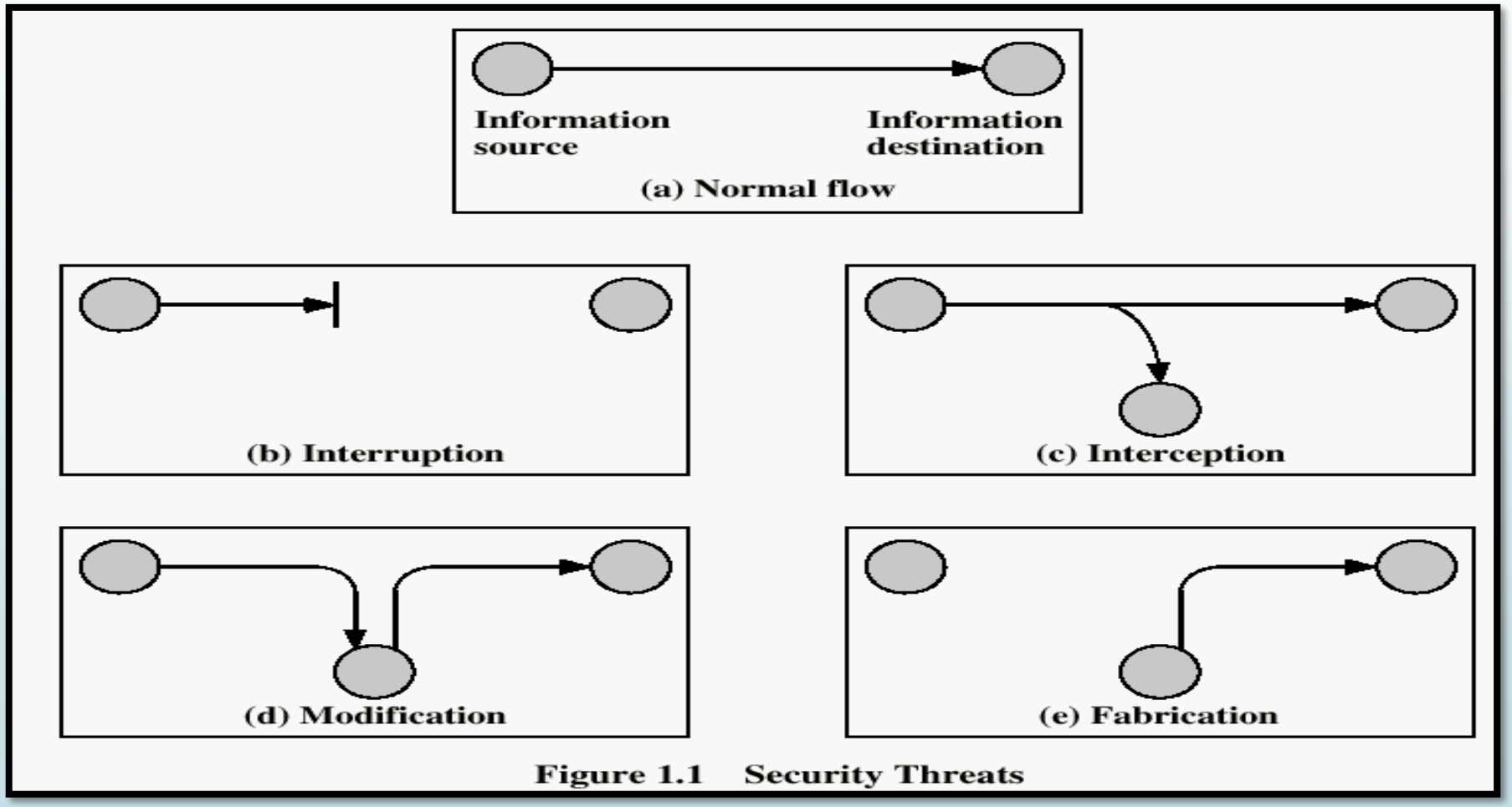
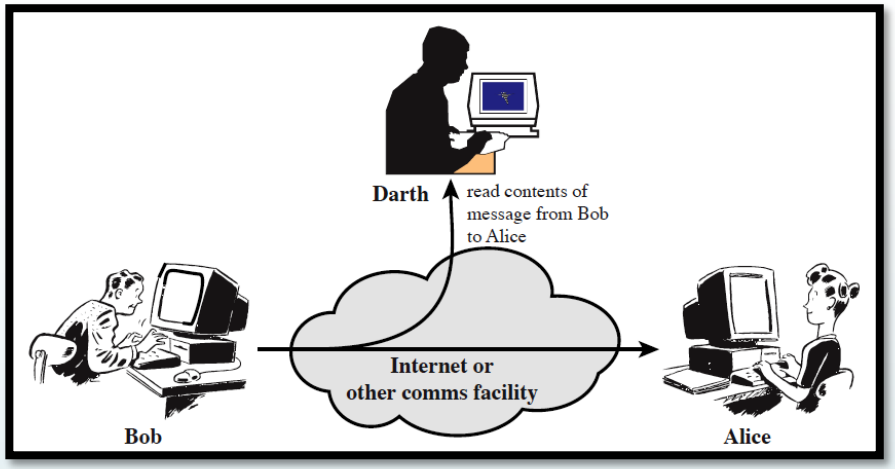


Figure 1.1 Security Threats

Types of Attacks:

- Passive attack
- Active attack

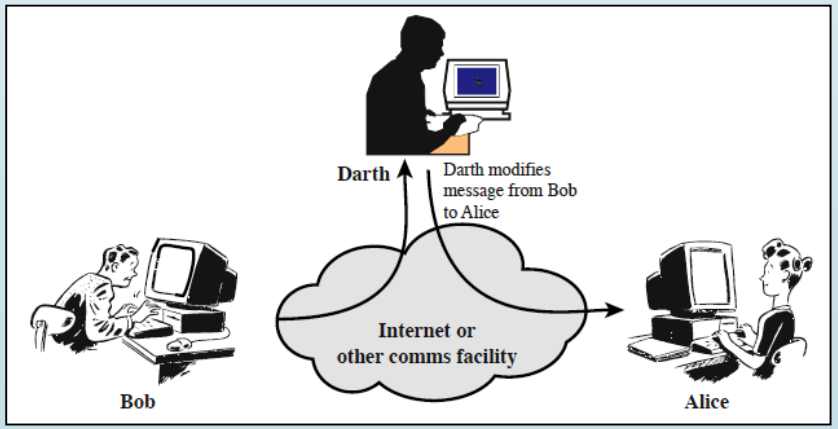
Passive attack:



- 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

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.



Caesar Cipher

- Plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with cipher text bit patterns.
- For Encryption using: $(p + k) \bmod (26)$
- For Decryption using : $(c - k) \bmod (26)$

Example 1

Plain text :meet me after the ali party

K = 3

Answer

a b c d e f g h i j k l m n o p q r s t u v w x y z

Plain text :meet me after the ali party
Cipher text :PHHW PH DIWHU WKH DOL SDUWB

Example 2

Plain text :I love coffee

K = 7

Answer

a b c d e f g h i j k l m n o p q r s t u v w x y z

Plain text :I love coffee
Cipher text :P SVCL JVMMLL