Computer Network Security

Dr. Nadine ZBIB
Assistant Professor
College of Science and Information Systems

Aim of Course

- our focus is on **Internet Security**
- which consists of measures to deter, prevent, detect, and correct security violations that involve the transmission & storage of information

Chapter I: Introduction

1. What is Security
2. The OSI Security Architecture
3. Security Attacks
4. Security Services
5. Security Mechanisms

Background

- Information Security requirements have changed in recent times
- traditionally provided by physical and administrative mechanisms
- computer use requires automated tools to protect files and other stored information
- use of networks and communications links requires measures to protect data during transmission

Definitions

- **Computer Security** - generic name for the collection of tools designed to protect data and to thwart hackers
- **Network Security** - measures to protect data during their transmission
- **Internet Security** - measures to protect data during their transmission over a collection of interconnected networks

What is network security?

Confidentiality: only sender, intended receiver should "understand" message contents

- **sender encrypts message**
- **receiver decrypts message**

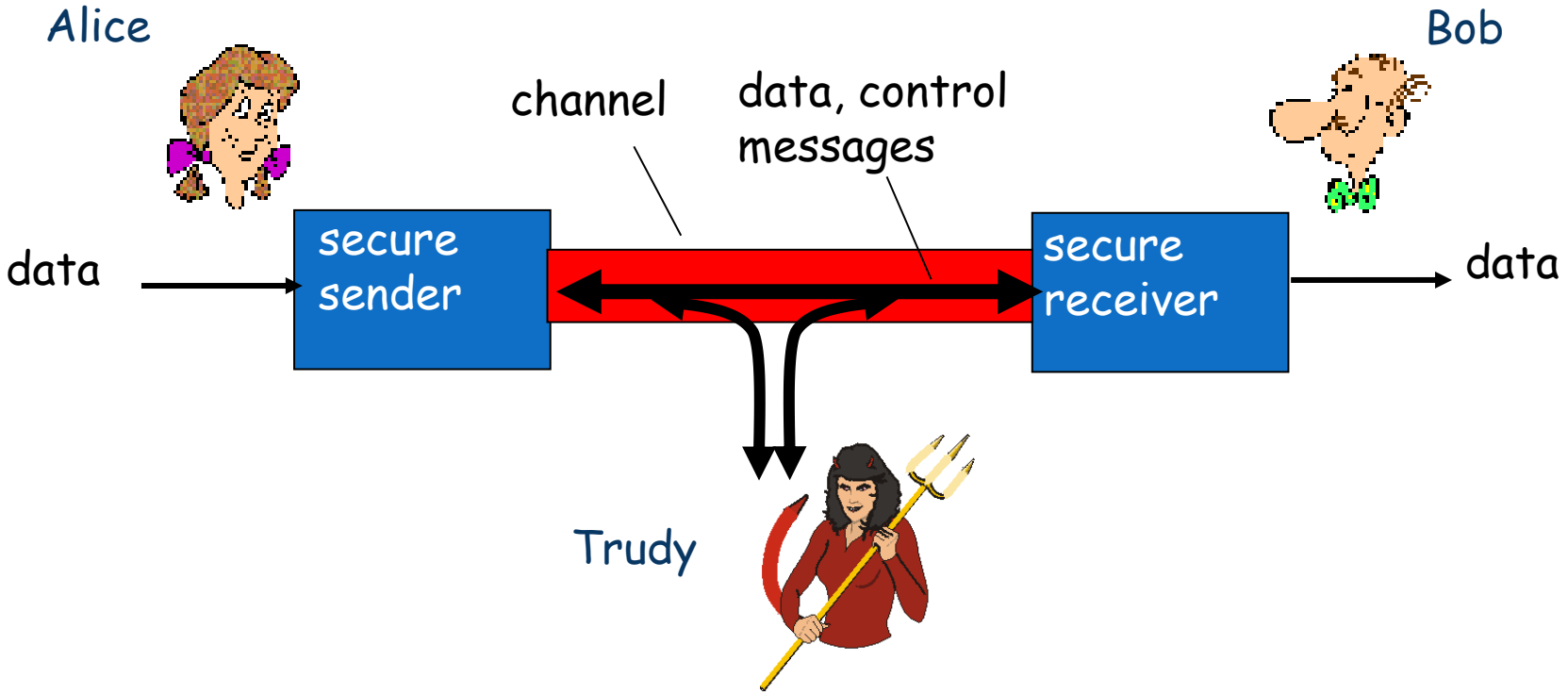
Authentication: sender, receiver want to confirm identity of each other

Message integrity: sender, receiver want to ensure message not altered (in transit, or afterwards) without detection

Access and availability: services must be accessible and available to users

Friends and enemies: Alice, Bob, Trudy

- well-known in network security world
- Bob, Alice (lovers!) want to communicate “securely”
- Trudy (intruder) may intercept, delete, add messages



Who might Bob, Alice be?

- … well, *real-life* Bobs and Alices!
- Web browser/server for electronic transactions (e.g., on-line purchases)
- on-line banking client/server
- DNS servers
- routers exchanging routing table updates
- other examples?

There are bad guys (and girls) out there!

Q: What can a "bad guy" do?

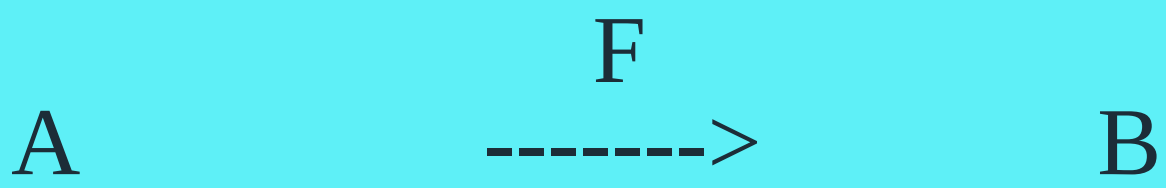
A: a lot!

- *eavesdrop:* intercept messages (ecouter)
- actively *insert* messages into connection
- *impersonation:* can fake (spoof) source address in packet (or any field in packet)
- *hijacking:* "take over" ongoing connection by removing sender or receiver, inserting himself in place
- *denial of service*: prevent service from being used by others (e.g., by overloading resources)

Security Violations

1. Capture

File F is SENSITIVE



C CAPTURES F

Security Violations

2. Intercept - Update

Authorisation File F is SENSITIVE

A sends message to B: ”Update F with names”

A(m) →m B(F)

C INTERCEPTS m and adds name of C

A(m) →m C(m) →m B(F)

Security Violations

3. Substitute

Authorisation File F is SENSITIVE

C PRETENDS to be A

C sends message to B: ”Update F with name of C”

$$\{C\}_A(m) \quad \rightarrow_m \quad B(F)$$

Security Violations

4. Intercept - Preempt

A sends message to B: ”STOP C’s r/w access”

A(m0) →m0 B(m1)

B(m1) →m1 STOP(C)

C INTERCEPTS m0:

A(m0) →m0 C →m0 B(m1)

C(r/w ACCESS)

B(m1) →m1 STOP(C)

Security Violations

5. Denial

C sends message to B

C(m) →m B

Later,

B QUERIES C about message

B →m,? C

C DENIES sending message

C(m,?) →NO B

The OSI Security Architecture

Security architecture for OSI, define such a systematic approach. The OSI security architecture is useful to managers, as a way of organizing the task of providing security.

- It was developed as an international standard.
- The OSI security architecture focus on security attack, mechanism, and services. These can be defined briefly as fallows:

- **Security Attack:** Any action that compromise the security of information owned by an organization.

- **Security Mechanism:** A process that is designed to detect, prevent or recover from a security attack. And security mechanism is a method which is used to protect your message from unauthorized entity.

- **Security Services:** Security Services is the services to implement security policies and implemented by security mechanism.

OSI Security Architecture

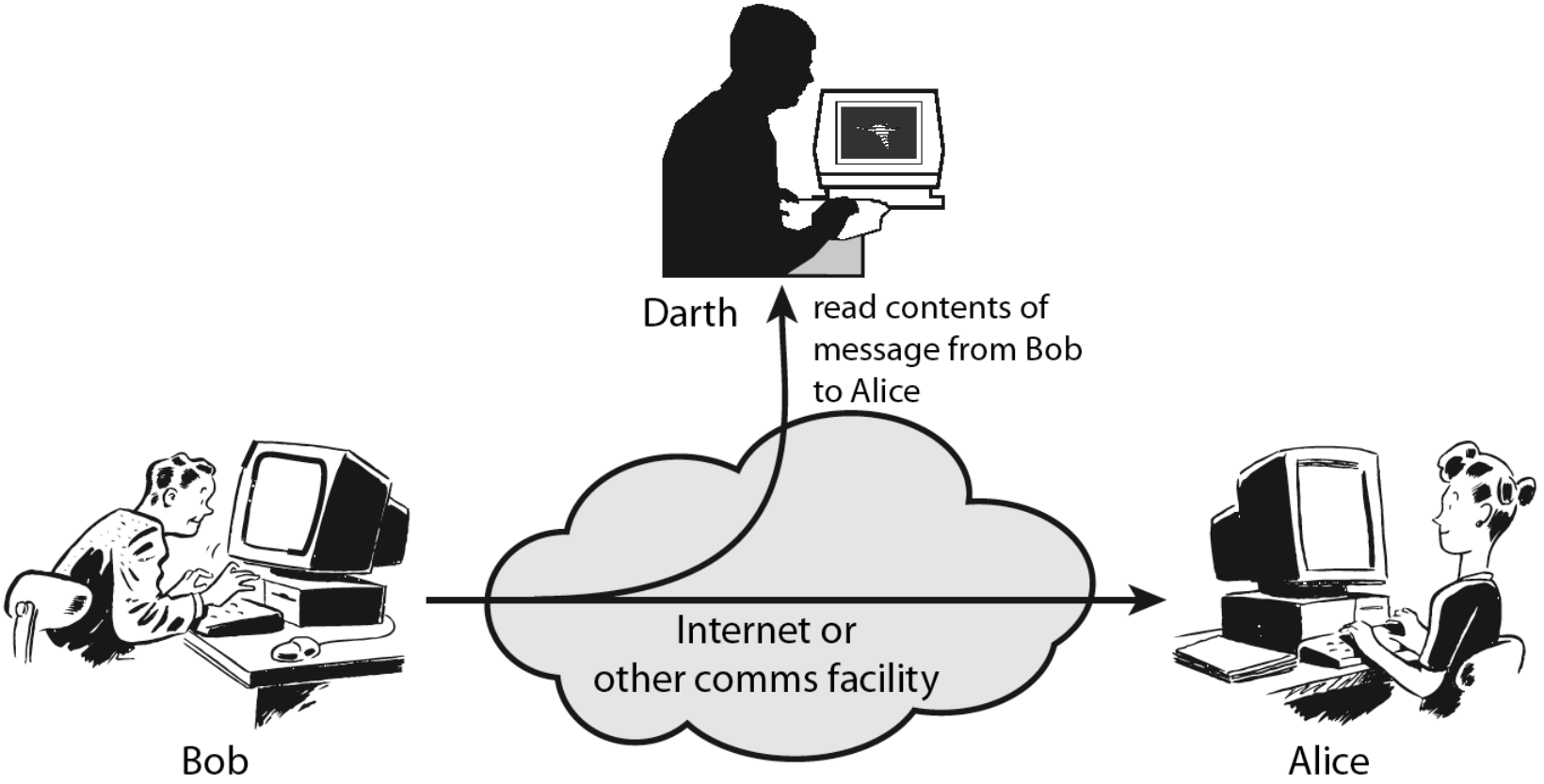
(X.800 – Security for Open Systems Interconnection)

- International Standard
- 5 Categories
- 14 Services

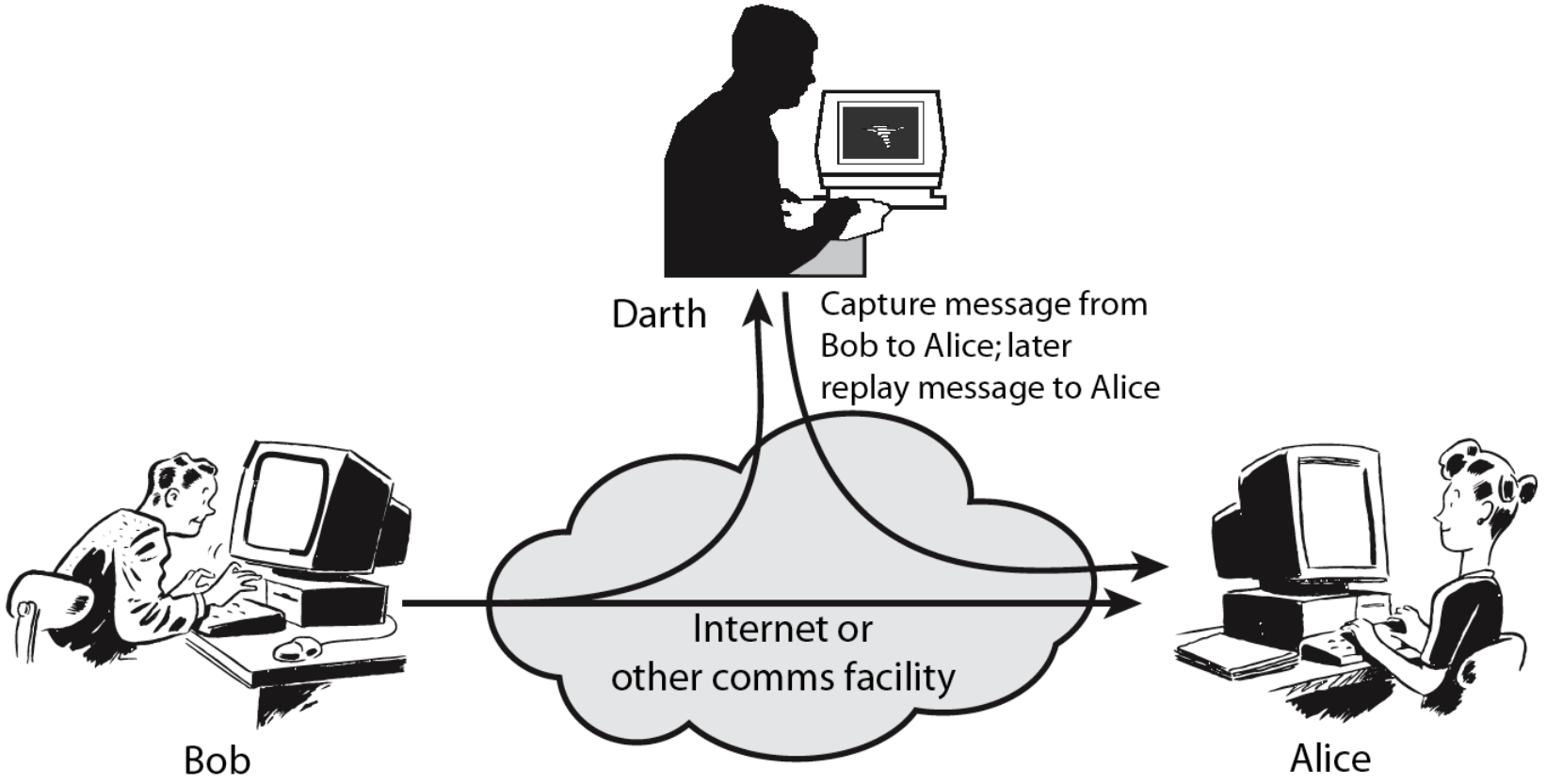
Security Attack

- any action that compromises the security of information owned by an organization
- information security is about how to prevent attacks, or failing that, to detect attacks on information-based systems
- often *threat* & *attack* used to mean same thing
- have a wide range of attacks
- can focus of generic types of attacks
  - passive
  - active

Passive Attacks



Active Attacks



ATTACKS

- PASSIVE:
  System unaltered(inchanger),
  – hard to detect, easier to prevent

- ACTIVE:
  System altered,
  – easier to detect, hard to prevent

ATTACKS

- PASSIVE:
  eavesdropping (ecouter), monitoring (surveillance), message release (communiquer des messages), traffic analysis (analyse le trajet)

- ACTIVE:
  replay, masquerade(impersonation), modification, denial of service(supression,overload)

Security Services

- Authentication (peer-entity, data-origin)
- Access Control
- Data Confidentiality (connection, connectionless, selective-field, traffic-flow)
- Data Integrity (connection[recovery, no-recovery, selective-field], connectionless[no-recovery,selective-field])
- NonRepudiation (origin, destination)

Security Services

Authentication

Data Origin (m not protected)

$A(m) \rightarrow_m B$

$B(m,A) \rightarrow \text{AUTHENTIC}_{(\text{sincere})}(A)?$

Peer Entity (c is protected message)

$A \leftarrow c \rightarrow B$

$S(A,B) \rightarrow \text{AUTHENTIC}(A,B)?$

$S(c,\text{masquerador},\text{replay}) \rightarrow \text{SECURE}(c)?$

Security Services
Access Control

Access REQUEST:

A(m) →m

{Host/System}

Host MATCHES m to A:

{Host/System}(m,A) →m’ A

A GRANTED (translating) read/write access:

A(m’) ←→

{Host/System}

Security Services

Confidentiality

CONNECTION:

$$A \overset{c_K}{\leftrightarrow} B \qquad \text{(e.g. TCP)}$$

CONNECTIONLESS:

$$A \rightarrow m_K \; B$$

SELECTIVE-FIELD:

$$A \overset{c_K | c'}{\leftrightarrow} B$$

TRAFFIC-FLOW:

$$A \; \{\leftrightarrow\} \; B$$

Security Services

Integrity

CONNECTION-RECOVERY:

c modification/destruction

A →m B(m) →recover → m

CONNECTION-NO RECOVERY:

c modification/destruction

A →m B(m) →detect → !!

SELECTIVE FIELD:

c modification/destruction

A →m|m' B(m) →detect(m) → !!

Security Services

Non-Repudiation

SENDER VERIFICATION:

A →m,[A] B(m,[A]) → m⇔A

RECEIVER VERIFICATION:

A →m B

B →[m],[B] A([m],[B]) → m⇔B

Security Services
Availability

- Upon request
- Denial of Service
- Attack Countermeasures:
  - Authentication
  - Encryption
  - Physical Response

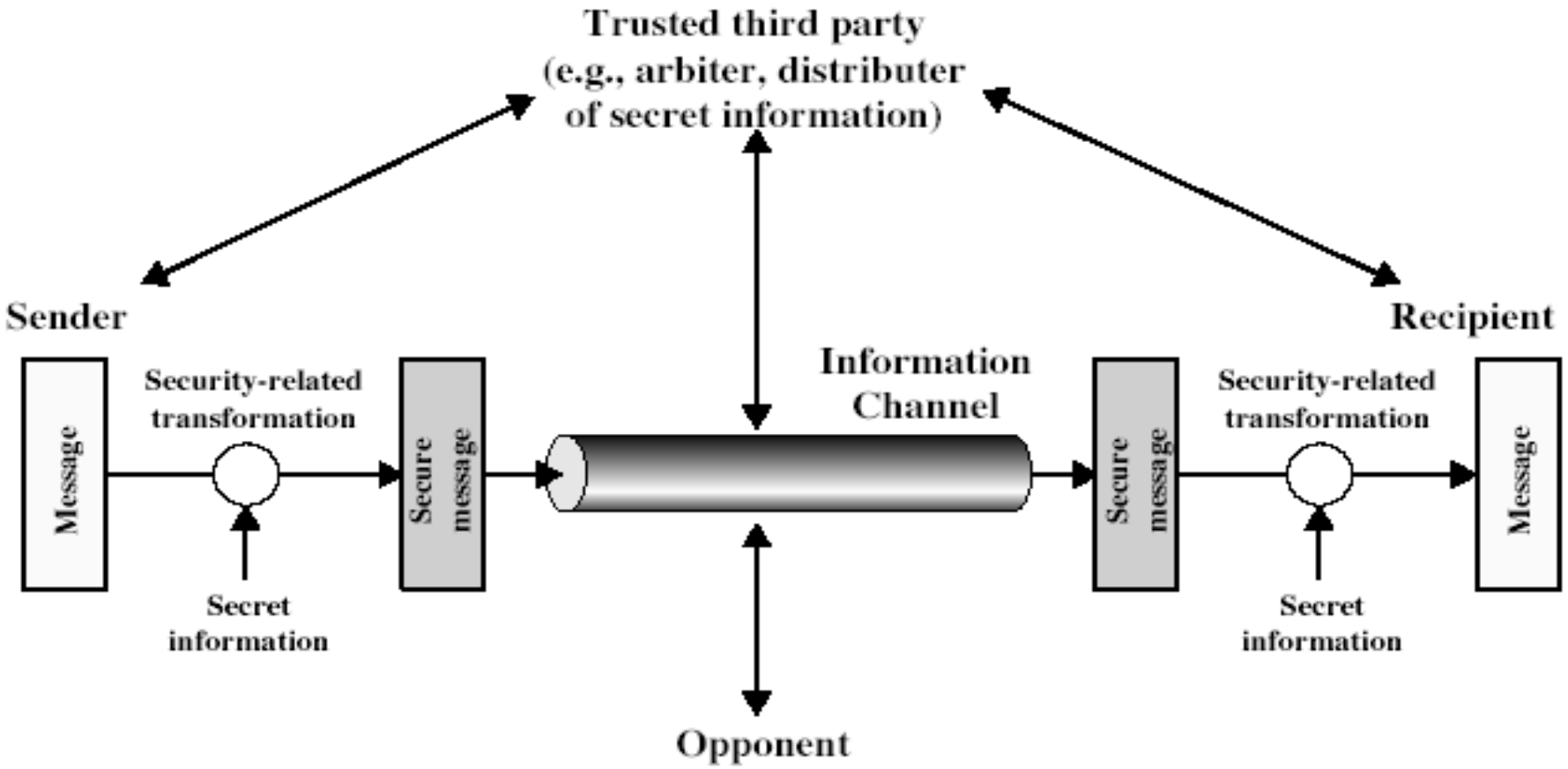
SECURITY MECHANISMS (X.800) - specific

- Encipherment (chiffrement) – unintelligible (incomprehensible)
- Signature – data tag to ensure
  a) Source b) Integrity c) anti-forgery (anti-contrefaçon)
- Access Control
- Data Integrity
- Authentication
- Traffic Padding – prevent traffic analysis
- Routing Control – adapt upon partial failure
- Notarization (legalization) – trusted third party

SECURITY MECHANISMS
(X.800) - pervasive

- Trusted Functionality
- Security Label
- Event Detection
- Audit Trail
- Recovery

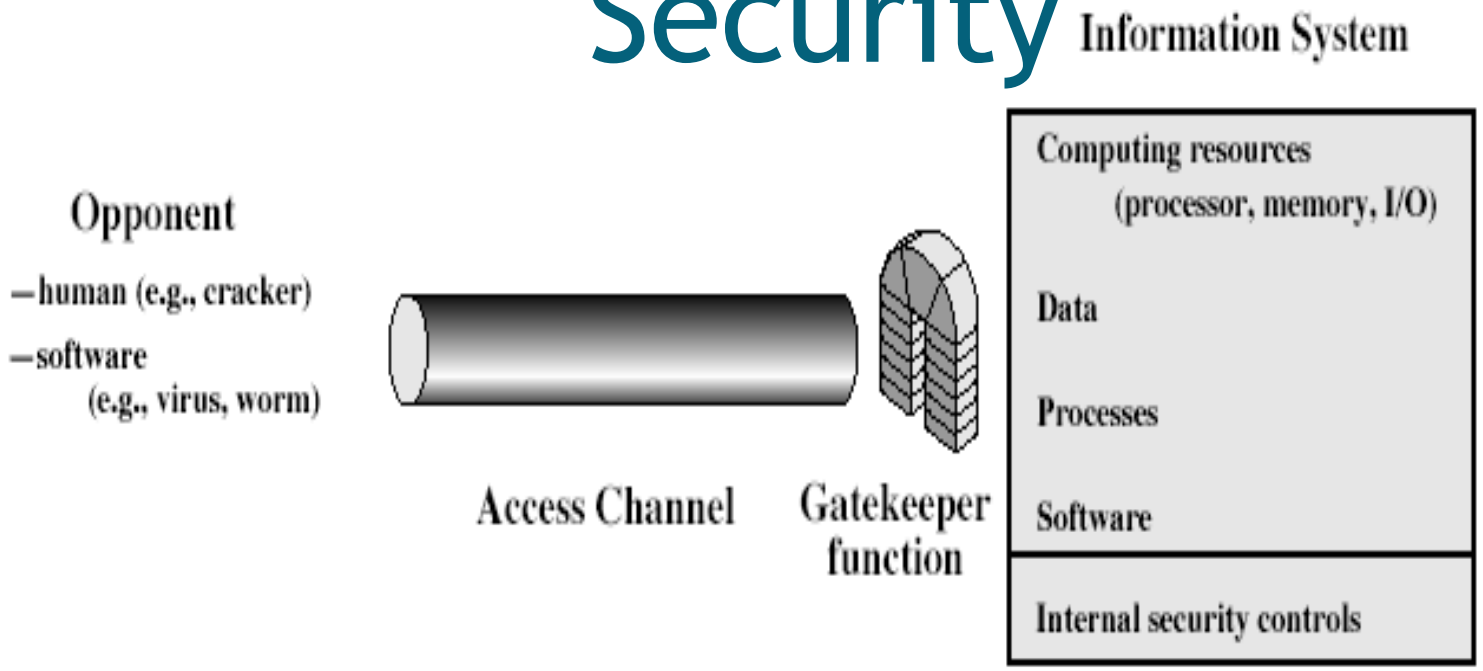
Model for Network Security



Model for Network Security

- using this model requires us to:
  1. design a suitable algorithm for the security transformation
  2. generate the secret information (keys) used by the algorithm
  3. develop methods to distribute and share the secret information
  4. specify a protocol enabling the principals to use the transformation and secret information for a security service

Model for Network Access Security



- Gatekeeper: password-based login, screening logic
- Internal controls: monitor activity, analyse stored info

Model for Network Access Security

- using this model requires us to:
  1. select appropriate gatekeeper functions to identify users
  2. implement security controls to ensure only authorised users access designated information or resources
- trusted computer systems may be useful to help implement this model

Summary

- have considered:
  - definitions for:
    - computer, network, internet security
- security attacks, services, mechanisms
- models for network (access) security