

Cryptography and Network Security

Lecture 01 - Overview

Ediz SAYKOL

Chapter 0 – Reader’s Guide

Sun
Tzu's
THE
ART
OF
WAR



The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.

Roadmap

- Cryptographic algorithms
 - symmetric ciphers
 - asymmetric encryption
 - hash functions
- Mutual Trust (e.g. key management)
- Network Security
- Computer Security

Standards Organizations

- National Institute of Standards & Technology (NIST)
- Internet Society (ISOC)
- International Telecommunication Union Telecommunication Standardization Sector (ITU-T)
- International Organization for Standardization (ISO)

Chapter 1 – Introduction

- *The combination of space, time, and strength that must be considered as the basic elements of this theory of defense makes this a fairly complicated matter.*
- *Consequently, it is not easy to find a fixed point of departure..*
— *On War, Carl Von Clausewitz*

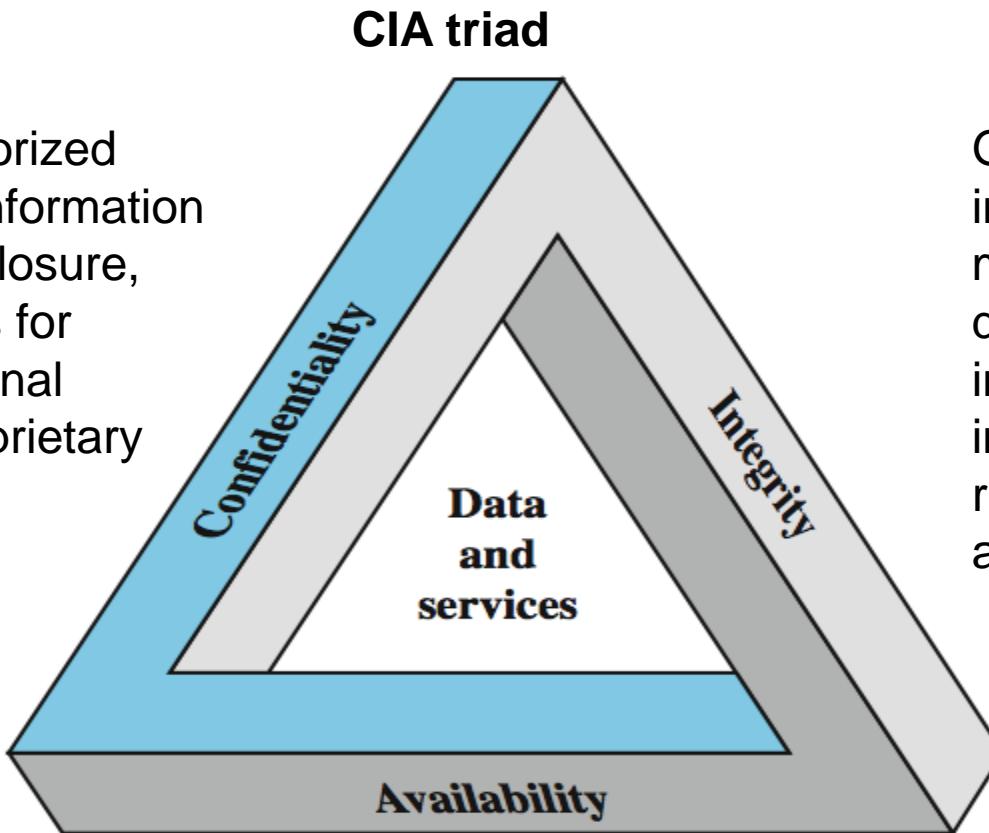


Computer Security

- the protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications)
 - The NIST Computer Security Handbook, 1995

Key Security Concepts

preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.



Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

Ensuring timely and reliable access to and use of information.

Examples of Security Requirements

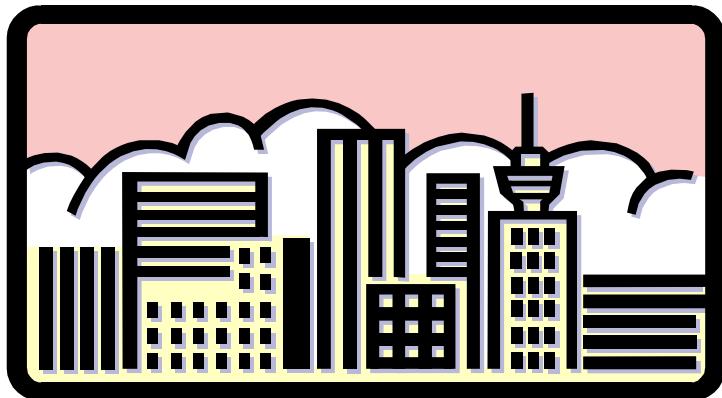
- confidentiality – student grades
- integrity – patient information
- availability – authentication service

Computer Security Challenges

1. not simple
2. must consider potential attacks
3. procedures used counter-intuitive
4. involve algorithms and secret info
5. must decide where to deploy mechanisms
6. battle of wits between attacker / admin
7. not perceived on benefit until fails
8. requires regular monitoring
9. too often an after-thought
10. regarded as impediment to using system

OSI Security Architecture

- ITU-T X.800 “Security Architecture for OSI”
- defines a systematic way of defining and providing security requirements



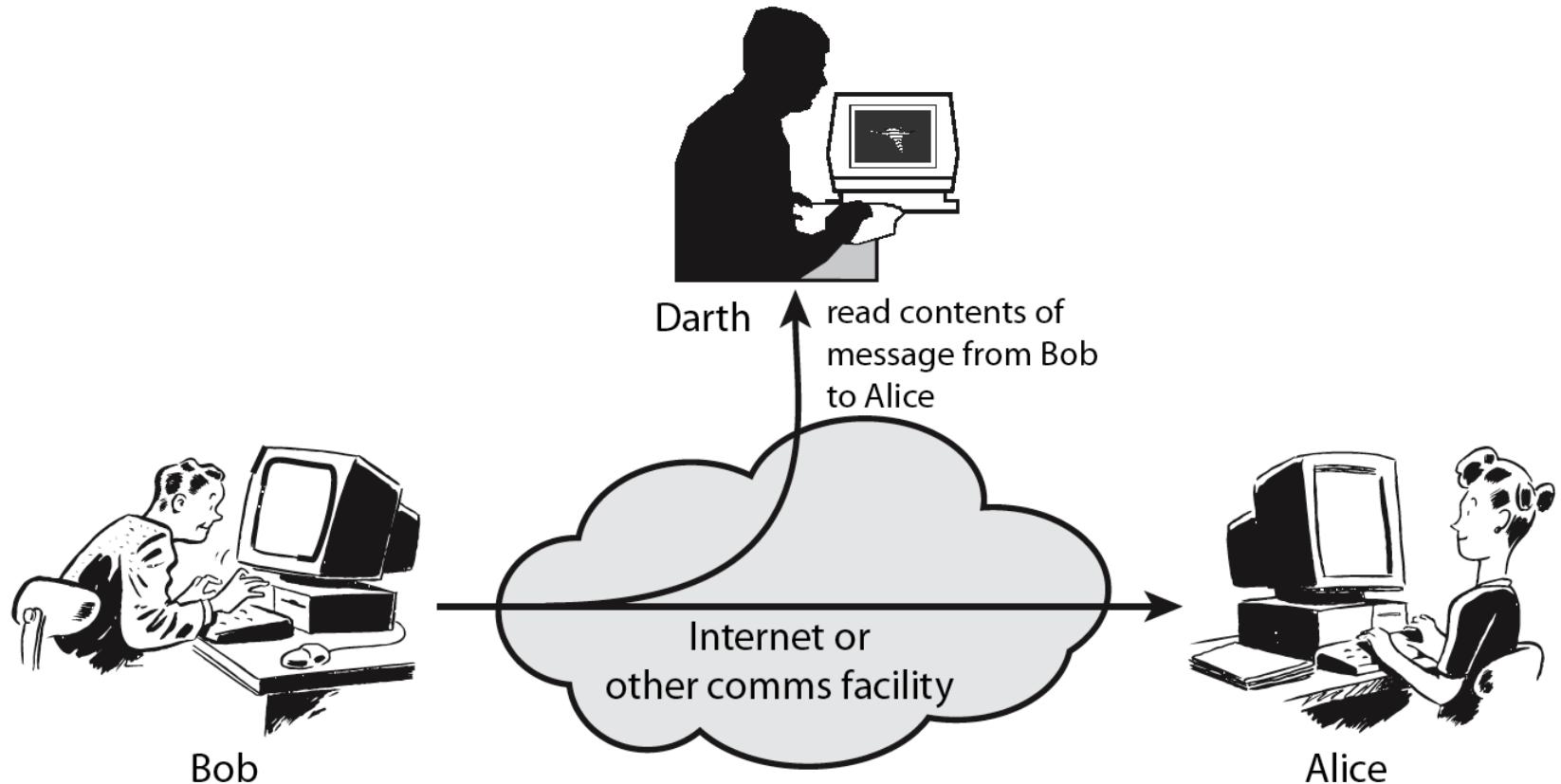
Aspects of Security

- **Security attack:** Any action that compromises the security of information owned by an organization.
- **Security mechanism:** A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.
- **Security service:** A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

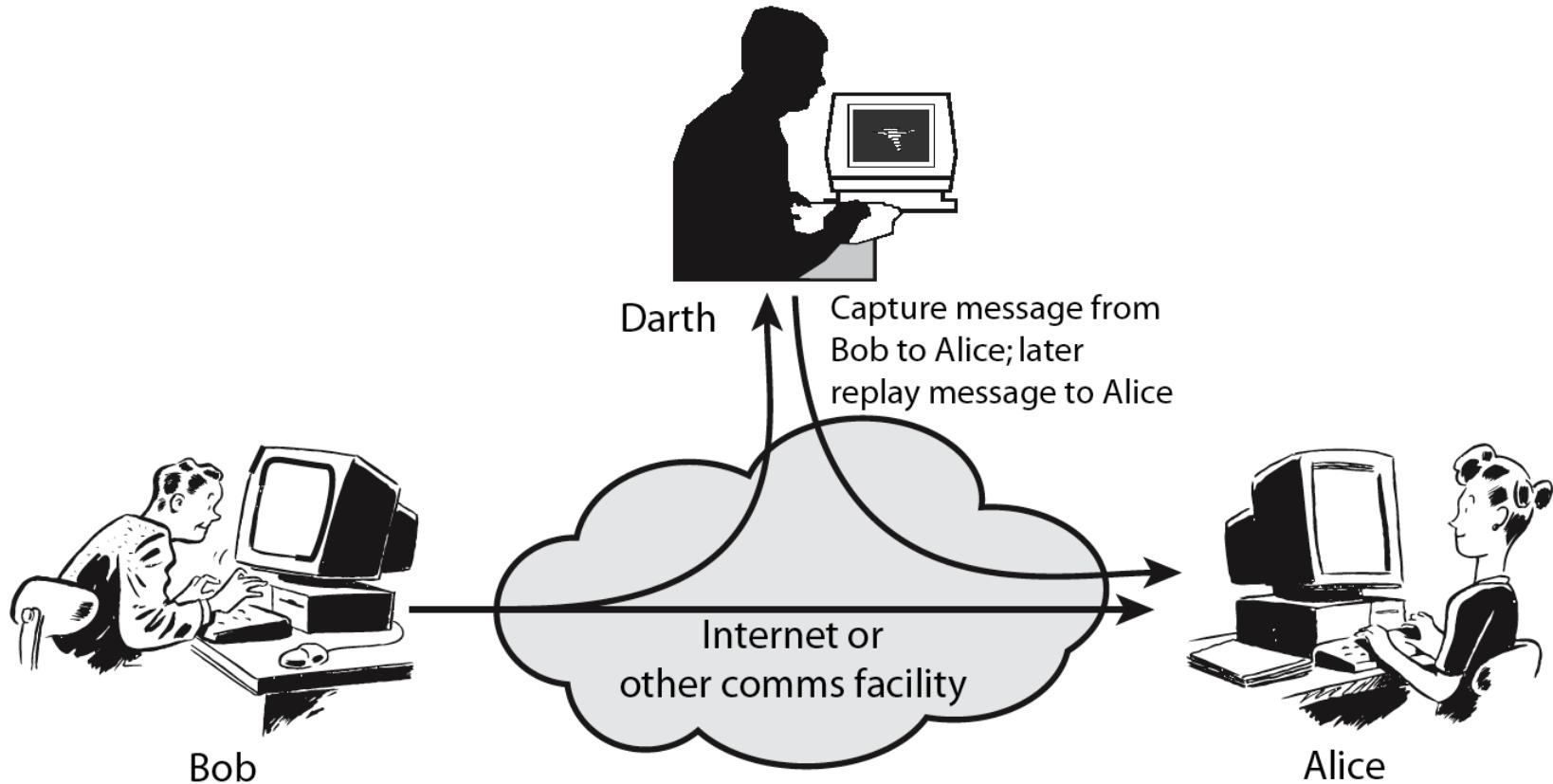
Threat and Attack

- *Internet Security Glossary*.
- **Threat** - A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.
- **Attack** - An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

Passive Attacks



Active Attacks



Security Service

- enhance security of data processing systems and information transfers of an organization
- intended to counter security attacks
- using one or more security mechanisms
- often replicates functions normally associated with physical documents
 - which, for example, have signatures, dates; need protection from disclosure, tampering, or destruction; be notarized or witnessed; be recorded or licensed

Security Services

- X.800:
“a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers”
- RFC 2828:
“a processing or communication service provided by a system to give a specific kind of protection to system resources”

Security Services (X.800)

- **Authentication** - assurance that communicating entity is the one claimed
 - have both peer-entity & data origin authentication
- **Access Control** - prevention of the unauthorized use of a resource
- **Data Confidentiality** –protection of data from unauthorized disclosure
- **Data Integrity** - assurance that data received is as sent by an authorized entity
- **Non-Repudiation** - protection against denial by one of the parties in a communication
- **Availability** – resource accessible/usable

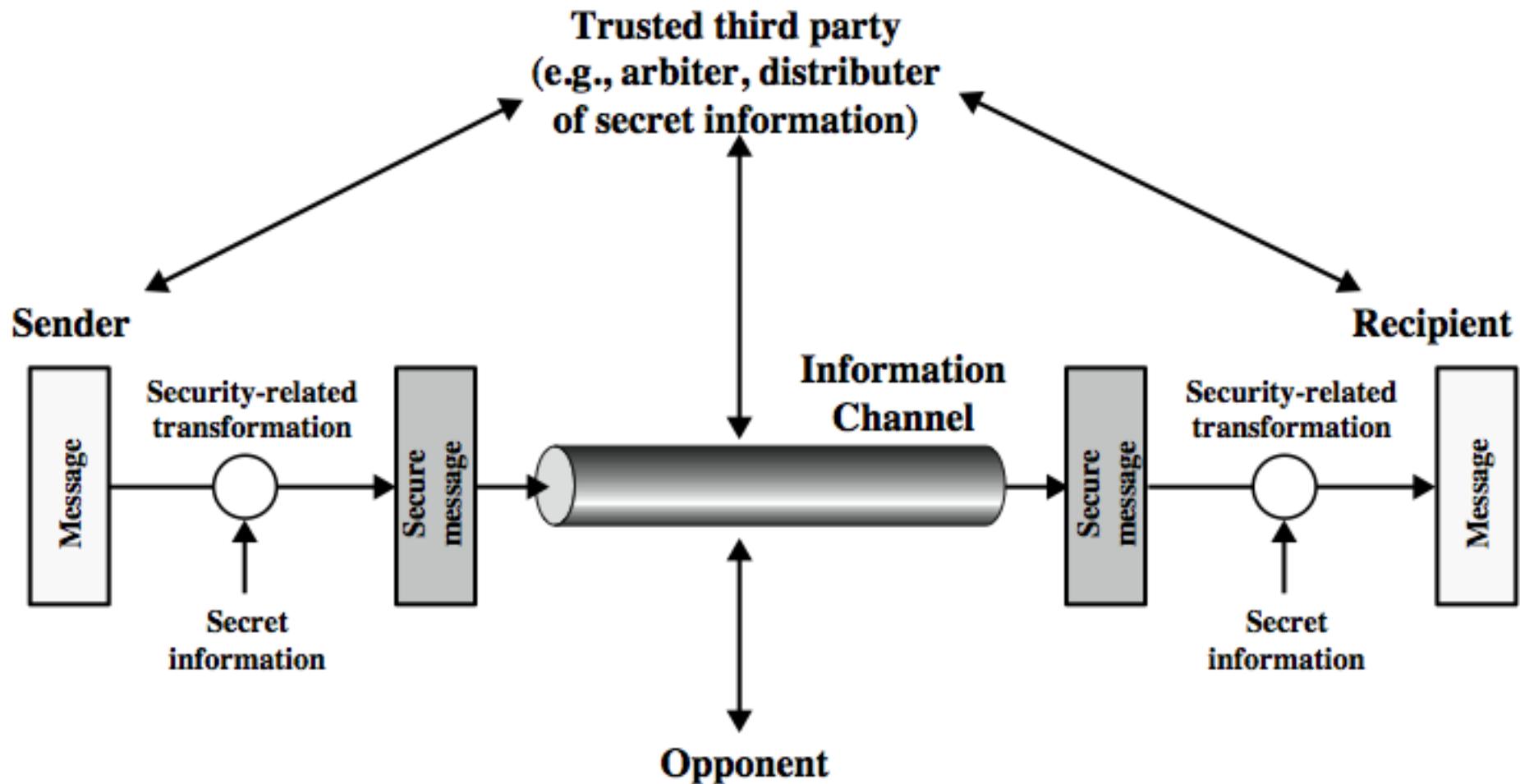
Security Mechanism

- feature designed to detect, prevent, or recover from a security attack
- no single mechanism that will support all services required
- however one particular element underlies many of the security mechanisms in use:
 - **cryptographic techniques**

Security Mechanisms (X.800)

- specific security mechanisms:
 - encipherment, digital signatures, access controls, data integrity, authentication exchange, traffic padding, routing control, notarization
- pervasive security mechanisms:
 - trusted functionality, security labels, event detection, security audit trails, security recovery

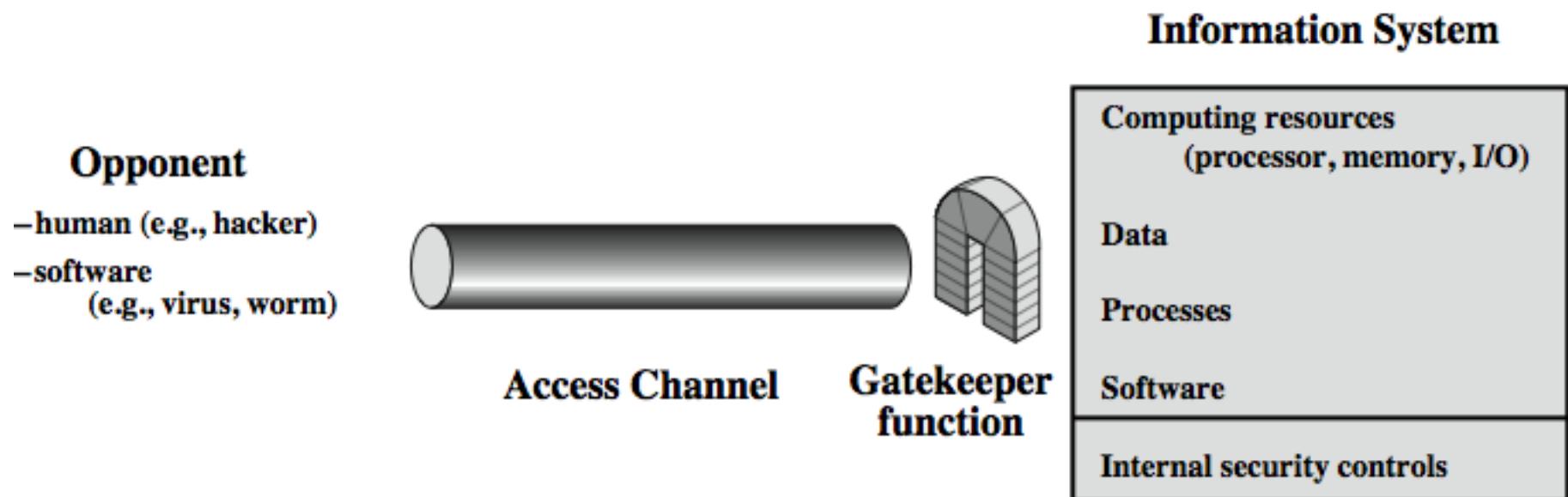
Model for Network Security



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



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