Introduction to Security

Udaya Parampalli

Introduction

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.

***—The Art of War,* Sun Tzu**

Information Security

- What is Cryptography
  - “Secret Writing”
  - Refers to the techniques required for protecting data between authorized parties on information communication technologies in the presence of potentially malicious elements.
  - Refers to a range of techniques such as Encryption, Signature, Hash functions, assuring Privacy, Integrity, and Authentication of data in the digital world.
- What is Information Security?
  - A broad topic of exchange and processing of information on modern computers and networks.
  - Confidentiality, Integrity, and Availability.
- What is Cyber Security?
  - Refers to management of attacks and risks by adversarial and malicious elements on computers and networks that support modern businesses and economy involving business, government, and community.

Stallings take: Introduction to Information Security

- What is Information Security?
  - It is a large topic dealing with many aspects of transmission and processing of information in modern day computers, networks and communication systems.
  - It is about ensuring that systems managing information behave exactly way they are constructed and specified to behave.

Components

- Specification and Policy.
- Implementation and Mechanism.
- Correctness and assurance.
- Background and nature of the users.

- We concentrate on Implementation and Mechanism aspects of Information Security.

Three important concerns of Information security:

- Confidentiality
  - In simple terms, confidentiality of information or data ensures that the access is given only to authorized individuals.
- Integrity
  - Information integrity ensures that enough safe guarding mechanisms exists so that authorized individuals get the **right** information and any changes to the information by intentional and un intentional means will be detected.
- Availability
  - Information or data availability ensures that the information is authorized available to the users.

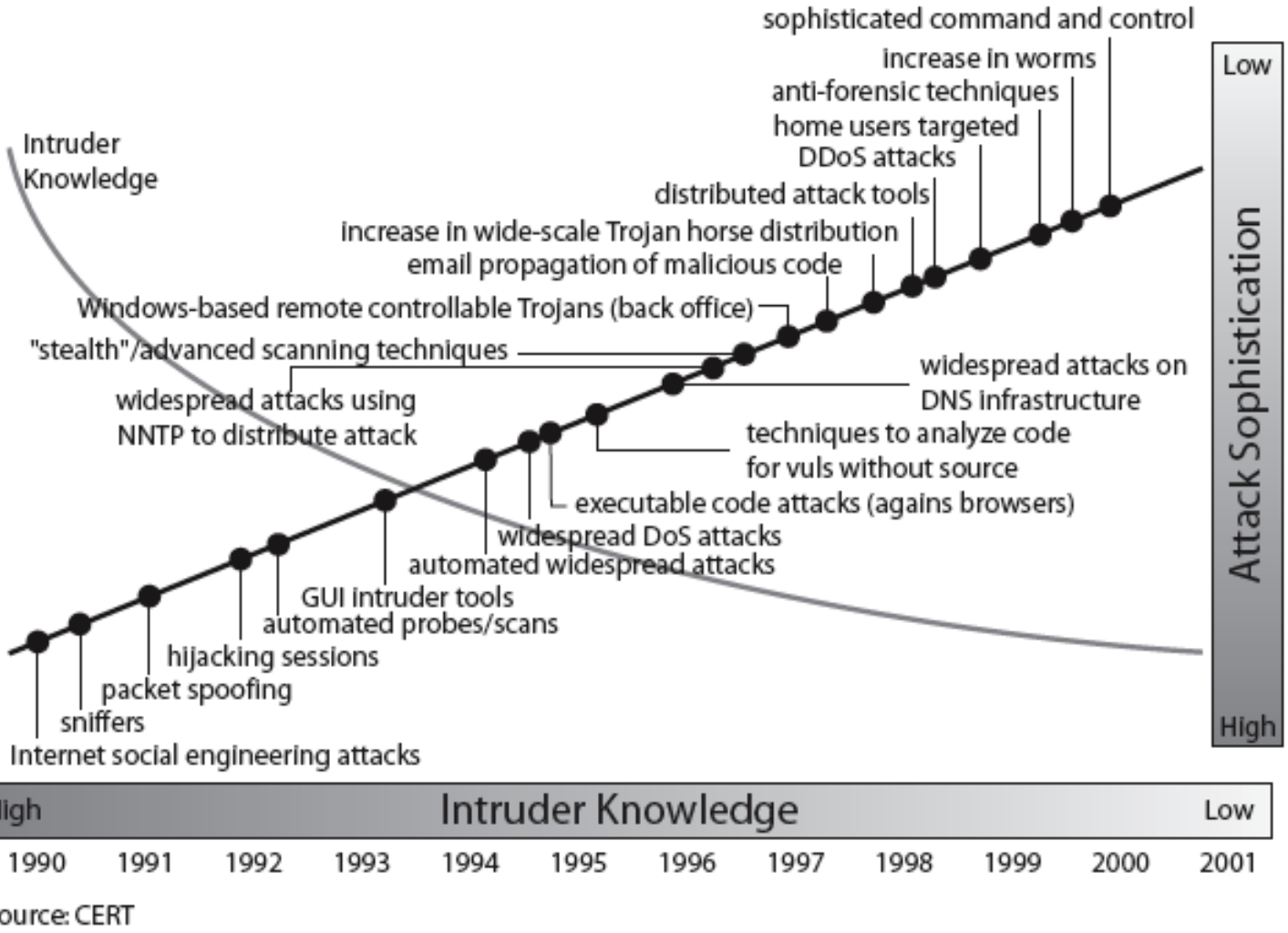
Other Concerns

- Physical Security.
  - This relates to the protection of all computing related products, equipments and facilities. We do not deal in detail this aspect, but should not be neglected.
- Perception of Security.
  - This is about how users feel about the security of their environment.
- Privacy.
  - This relates to the rights of the users.

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

Security Trends



Source: CERT

OSI Security Architecture

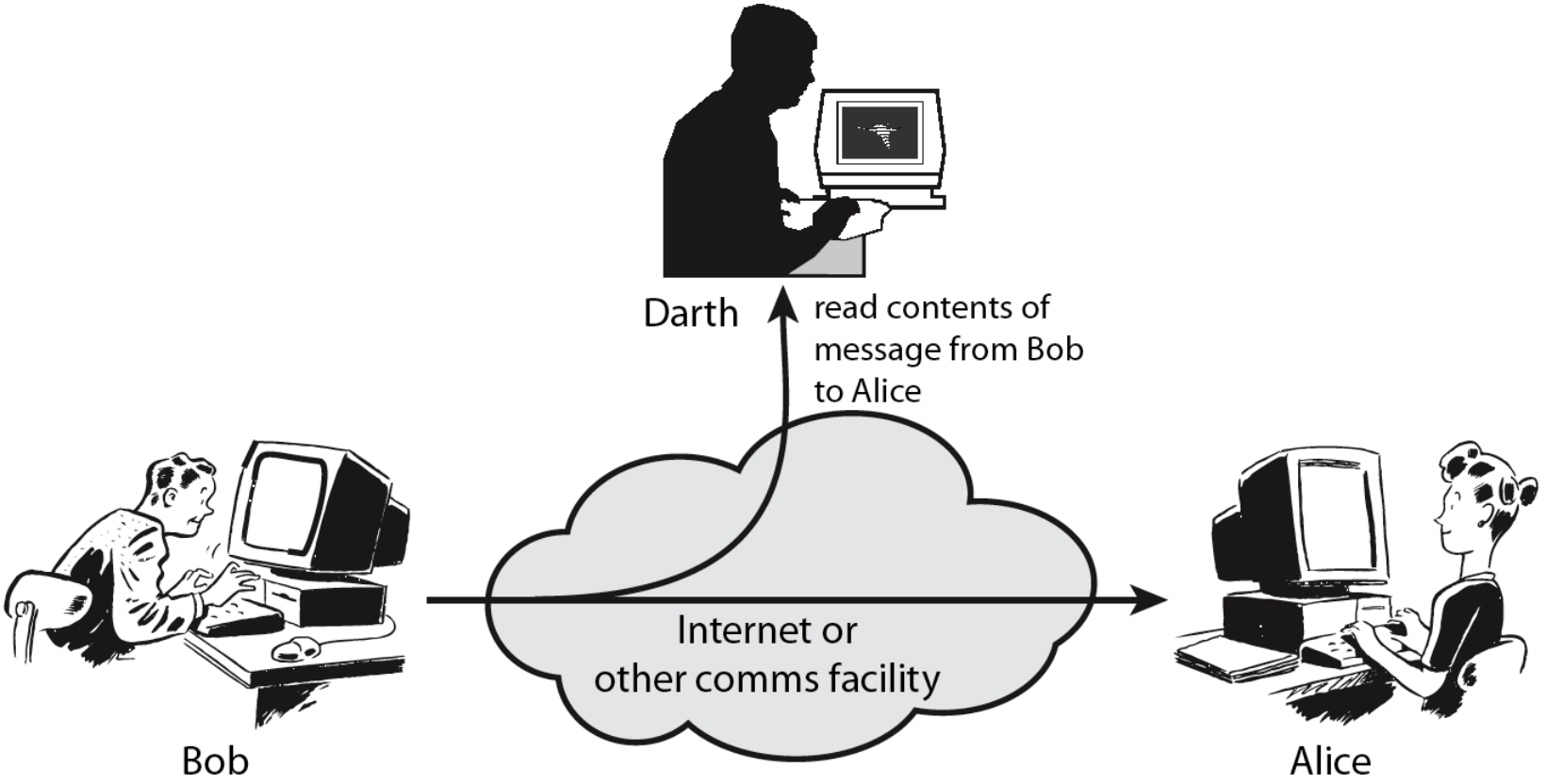
How to define the requirements for security in networked world and characterizing the approaches to satisfy those requirements?

- ITU-T X.800 “Security Architecture for OSI”
- defines a systematic way of defining and providing security requirements
- for us it provides a useful, if abstract, overview of concepts we will study
- Three main aspects:
  - Security attacks
  - Security Mechanisms.
  - Security services.

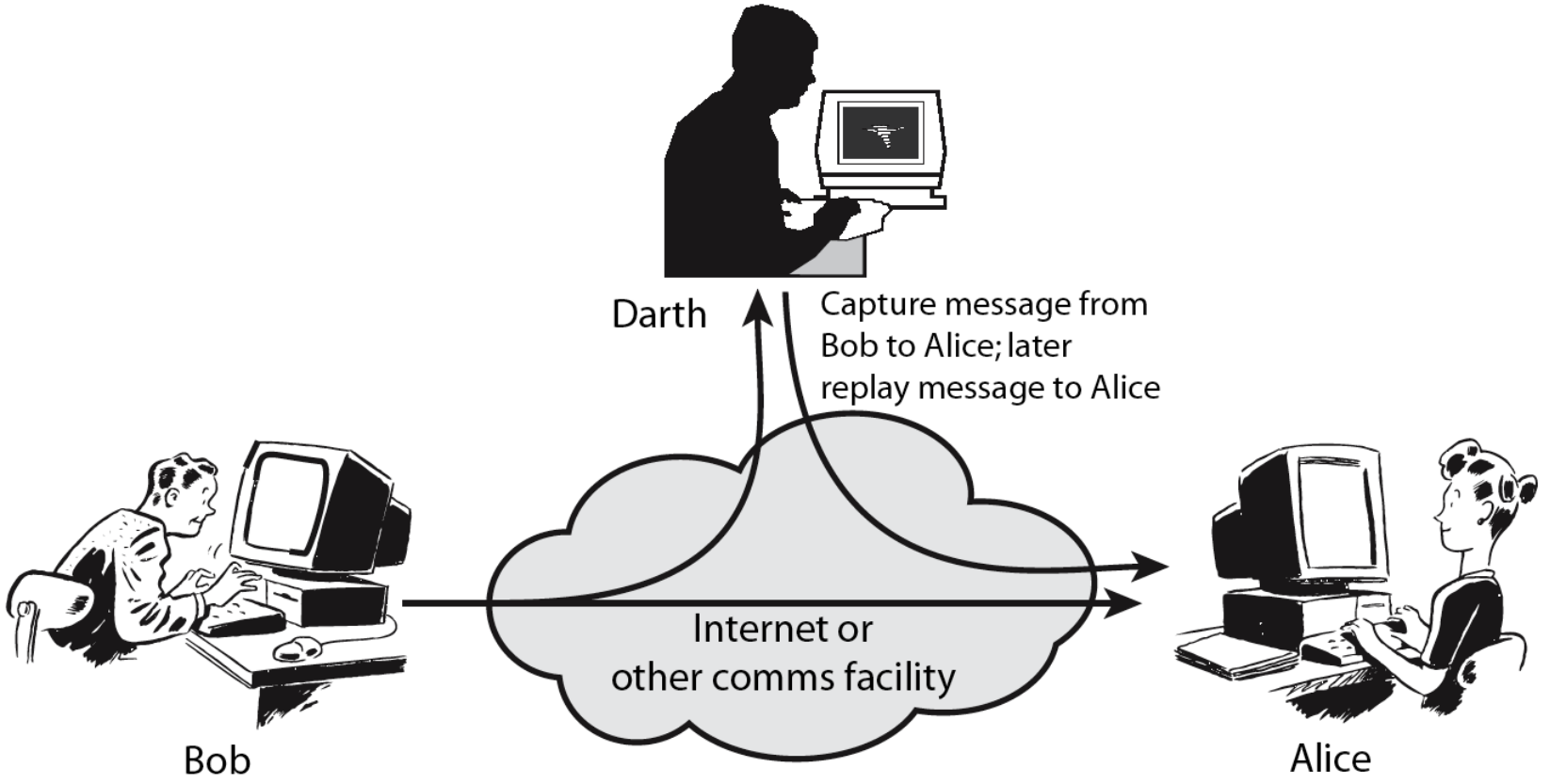
Security Attack

- 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 (threat is attack in waiting)
- We have a wide range of attacks
- We can focus of generic types of attacks
  - passive
  - active

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 the communicating entity is the one claimed
- **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

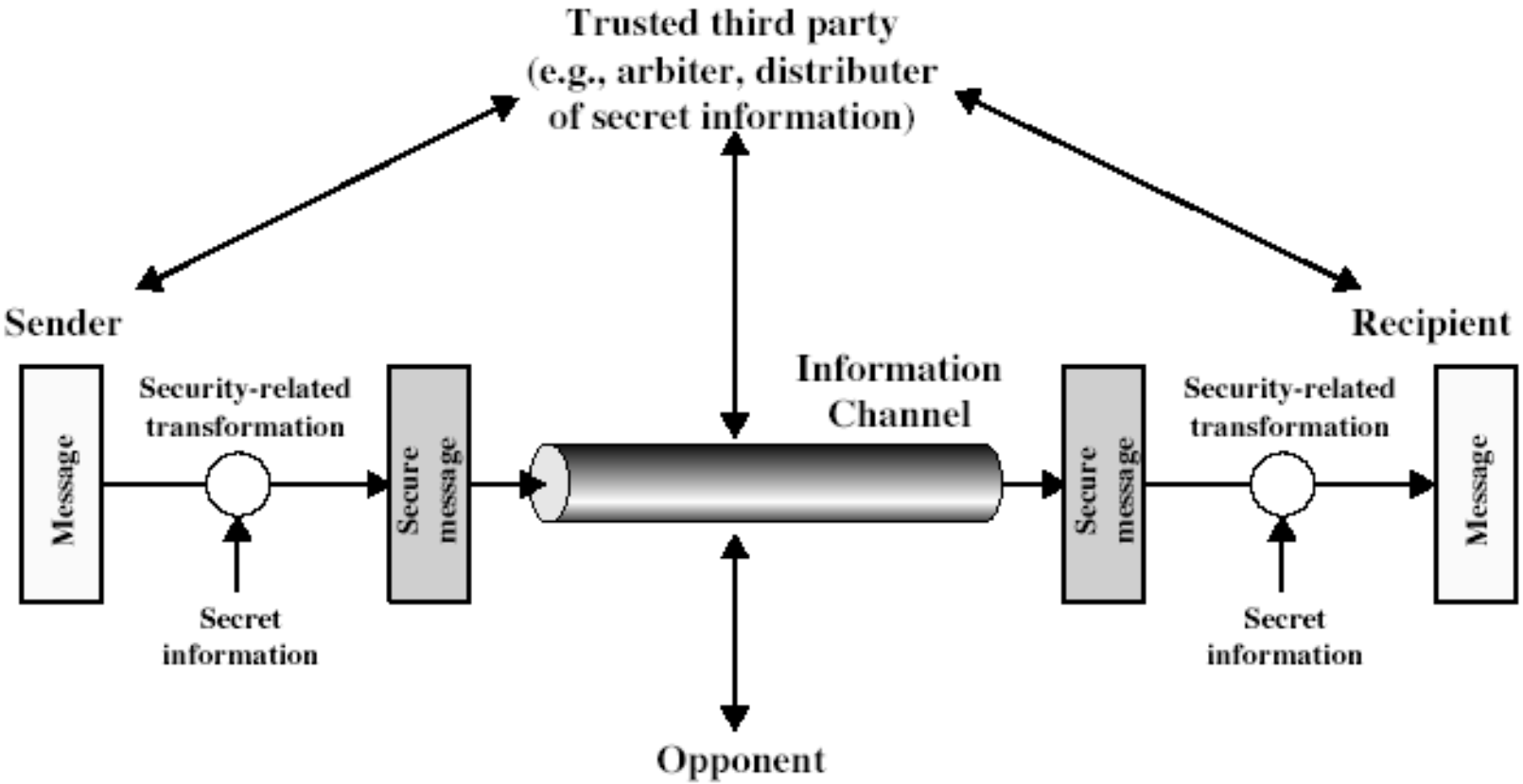
Security Mechanism

- 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**
- hence our focus on this topic

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

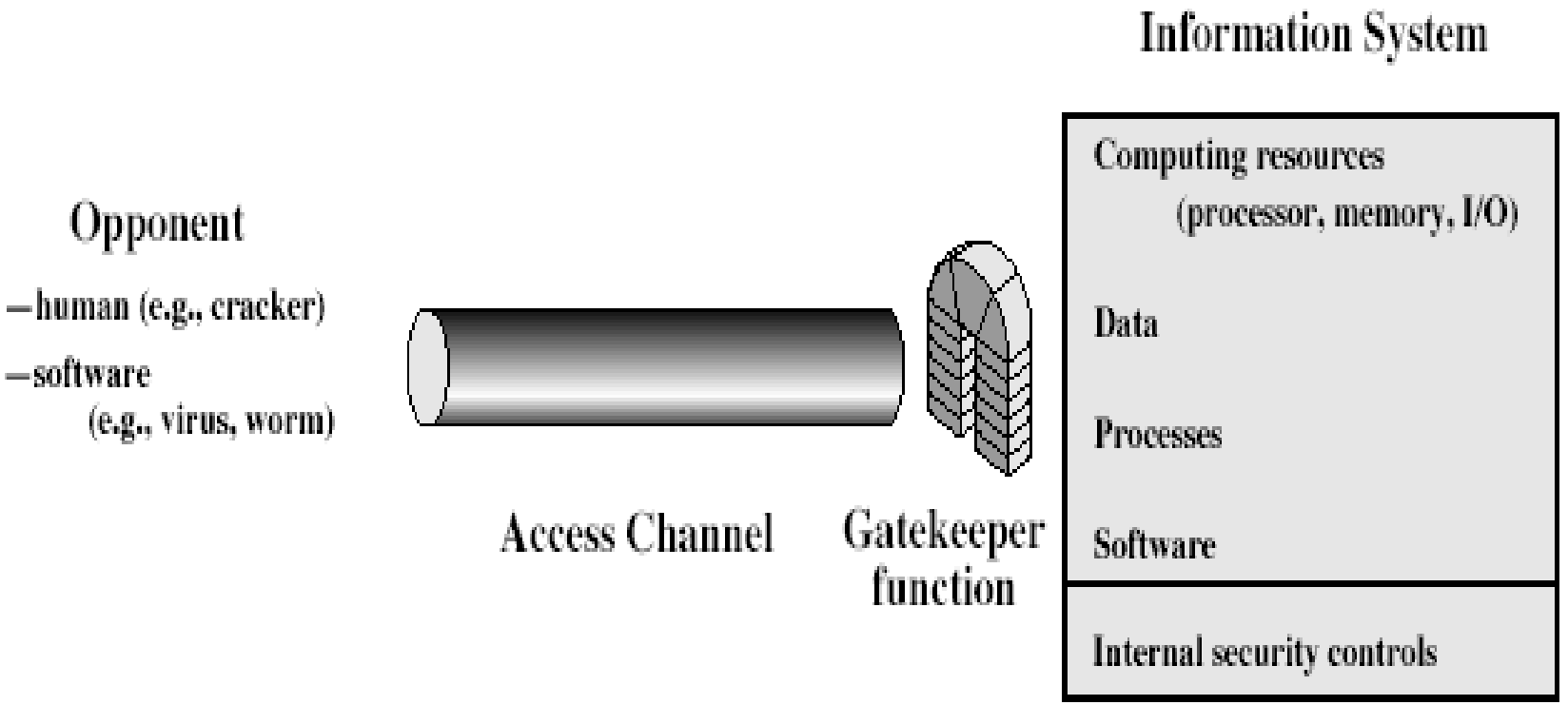
Model for Network Security



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
- trusted computer systems may be useful to help implement this model

Summary

- have considered:
  - definitions for:
    - computer, network, internet security
- X.800 standard
- security attacks, services, mechanisms
- models for network (access) security