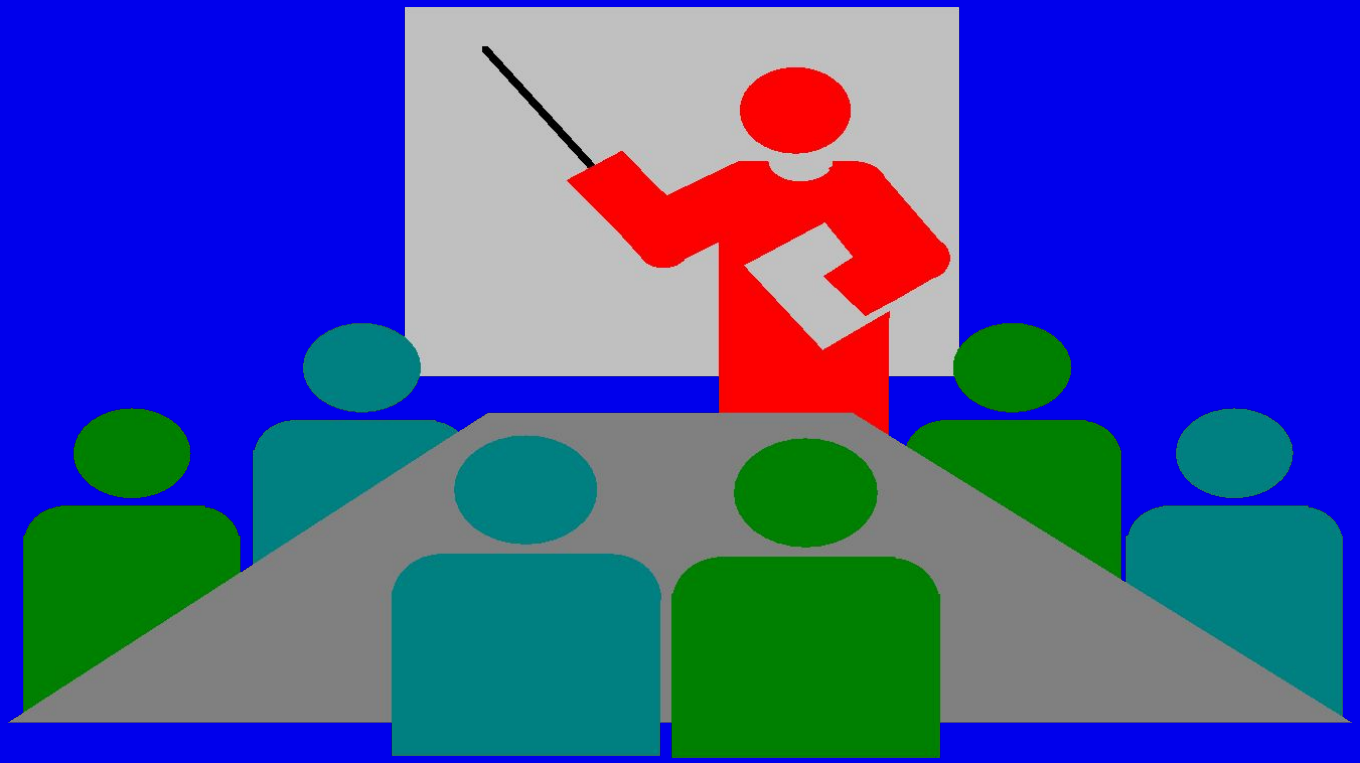
Network Security

Dr.Eng.Bader Ahmad



REFERENCE

Cryptography and Network Security
Fifth Edition

by William Stallings

This course covers the following topics :

- Introduction
- Networks vulnerabilities and attack
- Web security
- Wireless network security
- I P security
- Network intrusion detection

Aim of Course

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

Standards Organizations

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

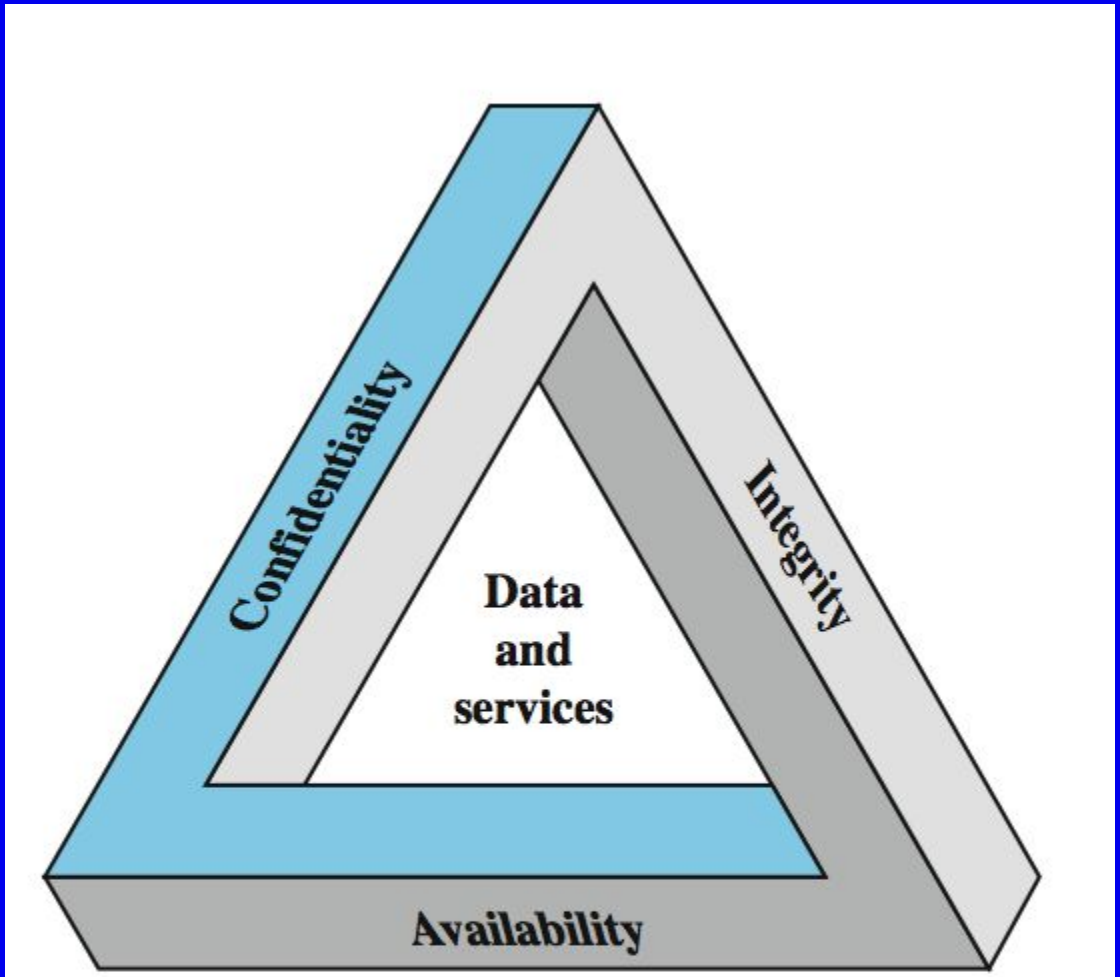
Background

- 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

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, information/data, and telecommunications .

Key Security Concepts



(Figure 1.1).

Key Security Concepts

- These three concepts form what is often referred to as the **CIA triad** (Figure 1.1). The three concepts embody the fundamental security objectives for both data and for information and computing services. FIPS PUB 199 provides a useful characterization of these three objectives in terms of requirements and the definition of a loss of security in each category:

Key Security Concepts

- **Confidentiality** (covers both data confidentiality and privacy): preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.

Key Security Concepts

- **Integrity** (covers both data and system integrity): Guarding against modification or destruction of information, and includes ensuring information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.

Key Security Concepts

- **Availability:** Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.

Key Security Concepts

- Although the use of the CIA triad to define security objectives is well established, some in the security field feel that additional concepts are needed to present a complete picture. Two of the most commonly mentioned are:

Key Security Concepts

- • **Authenticity:** The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator.
- • **Accountability:** The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.

Levels of Impact

- can define 3 levels of impact from a security breach
  - Low
  - Moderate
  - High

Levels of Impact

- **Low:** The loss could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions,

Levels of Impact

- but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

Levels of Impact

- **Moderate:** The loss could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. A serious adverse effect means that, for example, the loss might (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;

Levels of Impact

- (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious, life-threatening injuries.

Levels of Impact

- **High:** The loss could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. A severe or catastrophic adverse effect means that, for example, the loss might (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions;

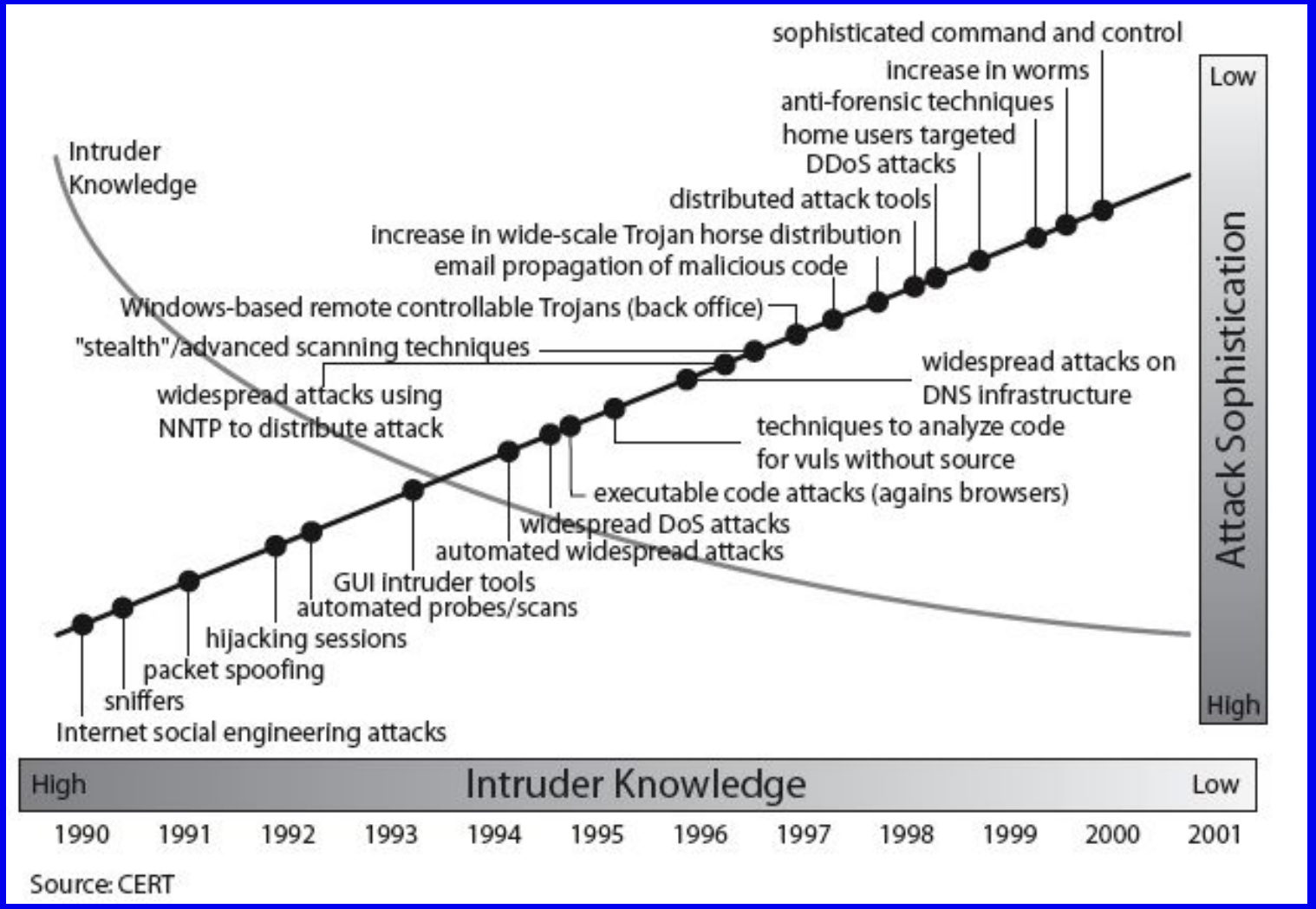
Levels of Impact

- • (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

Definitions

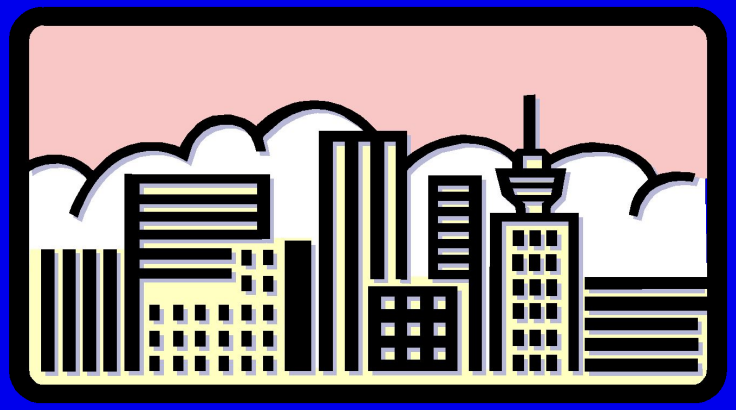
- **Computer Security** - generic name for the collection of tools designed to protect data and to thwart hackers
- **Network Security** - measures to protect data during their transmission
- **Internet Security** - measures to protect data during their transmission over a collection of interconnected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

Security Trends



OSI Security Architecture

- 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



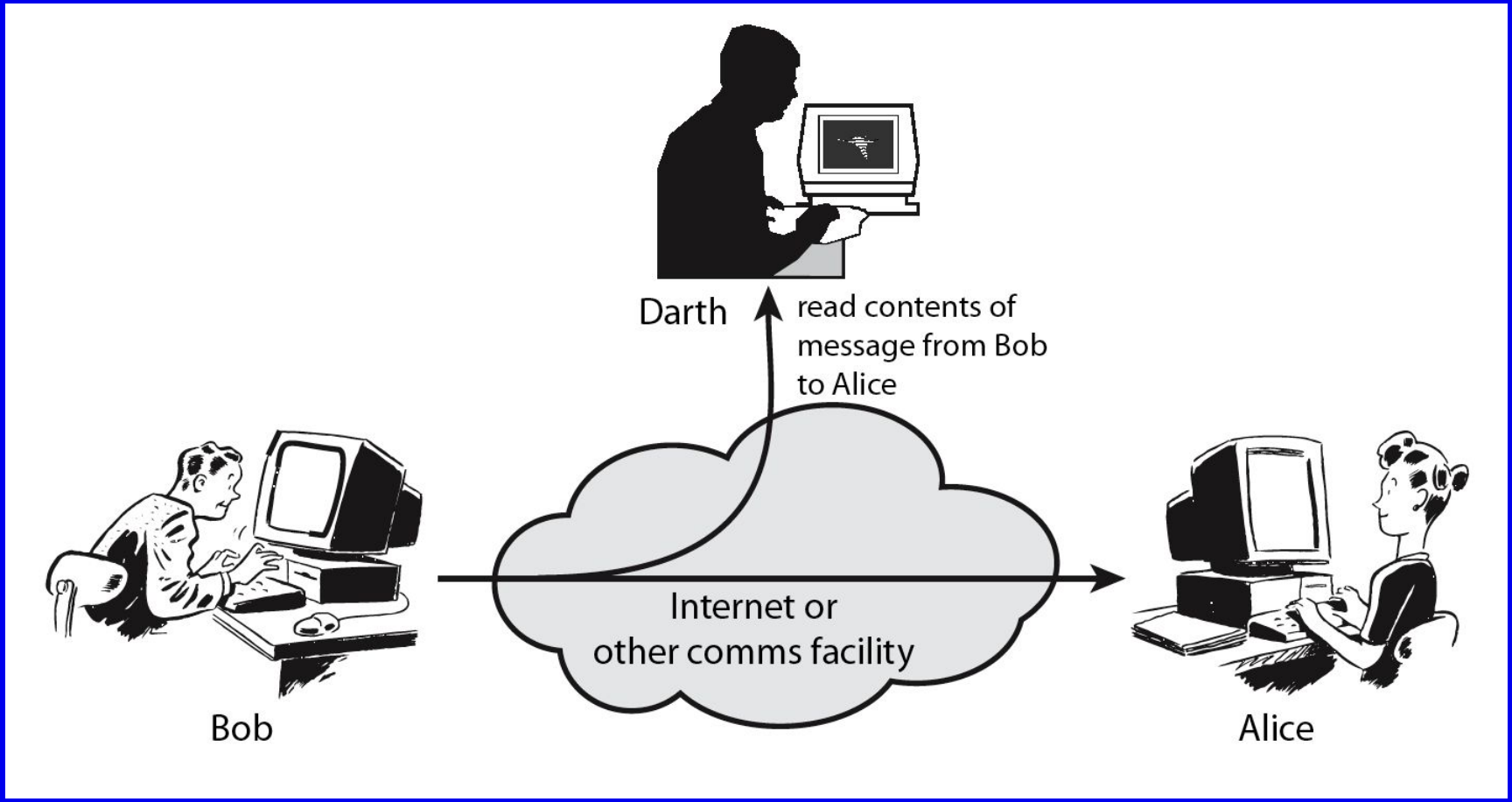
Aspects of Security

- consider 3 aspects of information security:
  - **security attack**
  - **security mechanism**
  - **security service**
- note terms
  - *threat* – a potential for violation of security
  - *attack* – an assault on system security, a deliberate attempt to evade 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
- have a wide range of attacks
- can focus of generic types of attacks
  - passive
  - active

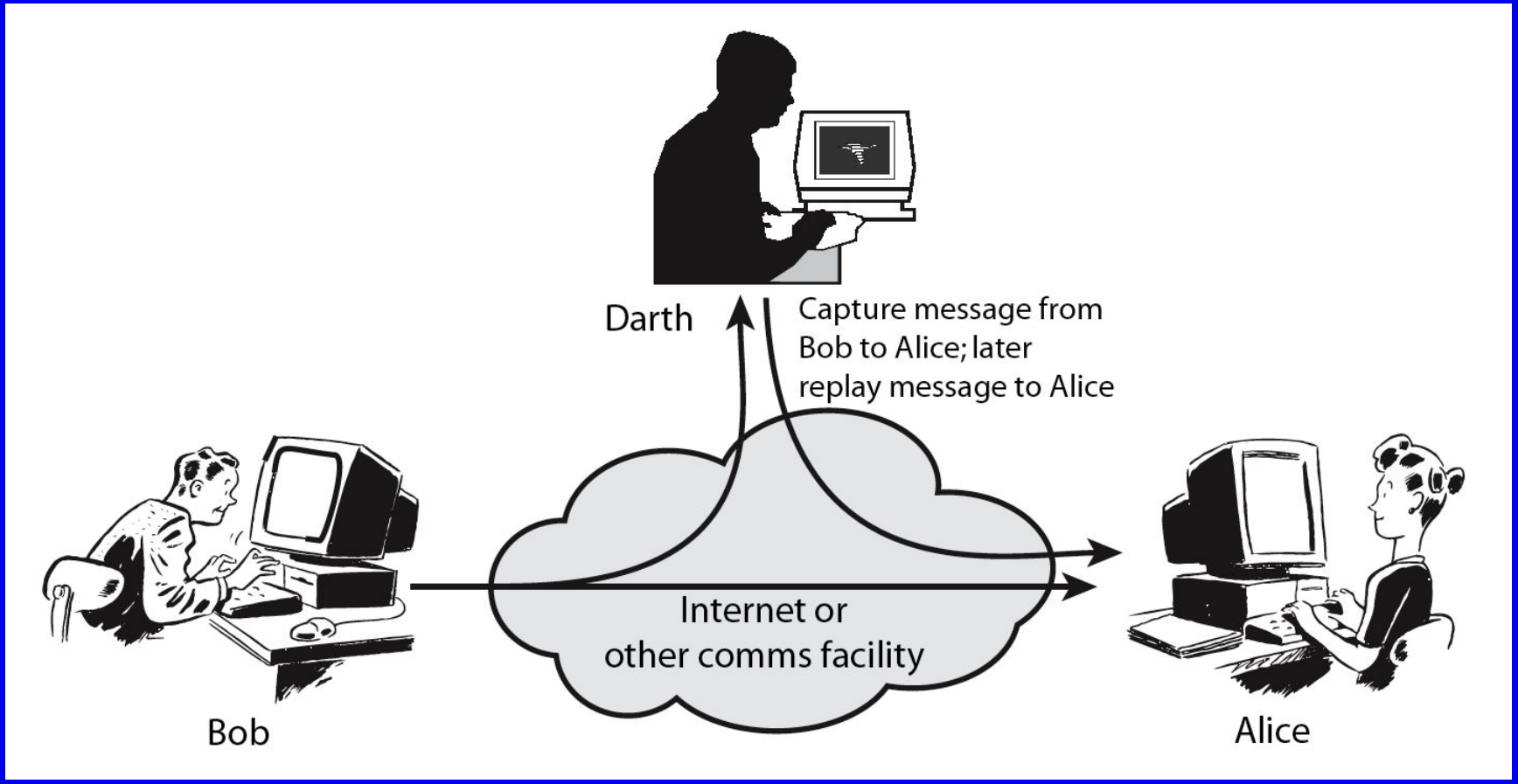
Passive Attacks



Passive Attacks

- **Have "passive attacks" which** attempt to learn or make use of information from the system but does not affect system resources.
- By eavesdropping on, or monitoring of, transmissions to:
  - + obtain message contents or
  - + monitor traffic flows
- Are difficult to detect because they do not involve any alteration of the data.

Active Attacks



Active Attacks

- “active attacks” which attempt to alter system resources or affect their operation.
- By modification of data stream to:
  - masquerade of one entity as some other
  - replay previous messages (as shown above in Stallings Figure 1.4b)
  - modify messages in transit
  - denial of service

Active Attacks

- Active attacks present the opposite characteristics of passive attacks. Whereas passive attacks are difficult to detect, measures are available to prevent their success. On the other hand, it is quite difficult to prevent active attacks absolutely, because of the wide variety of potential physical,software,and network vulnerabilities. Instead, the goal is to detect active attacks and to recover from any disruption or delays caused by them.

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 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 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"

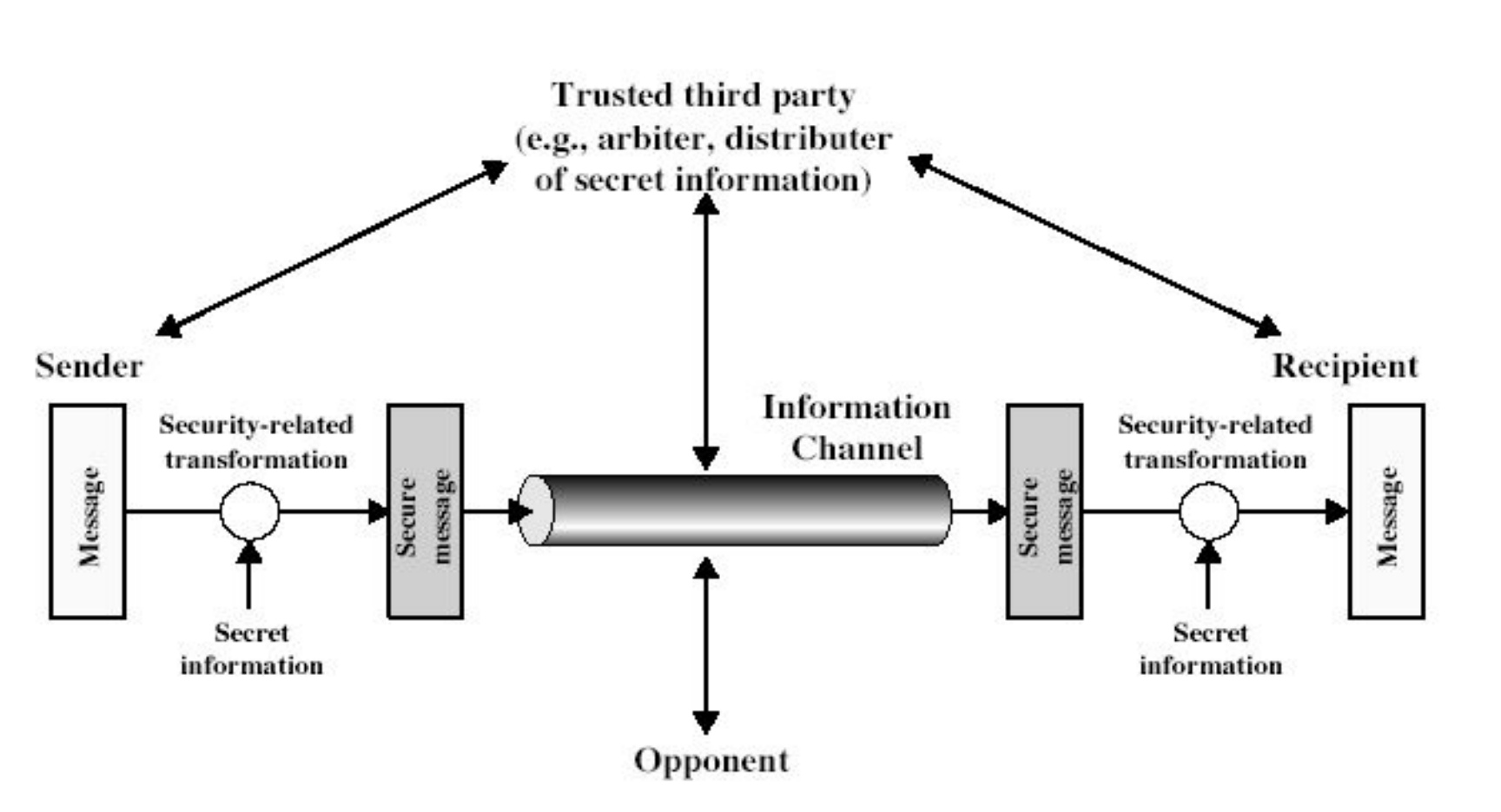
Security Services (X.800)

- **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 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

- In considering the place of encryption, its useful to use the following two models
- The first, illustrated in Figure 1.5, models information flowing over an insecure communications channel, in the presence of possible opponents. Hence an appropriate **security transform (encryption algorithm)** can be used, with suitable **keys**, possibly negotiated using the presence of a **trusted third party**.

Model for Network Security

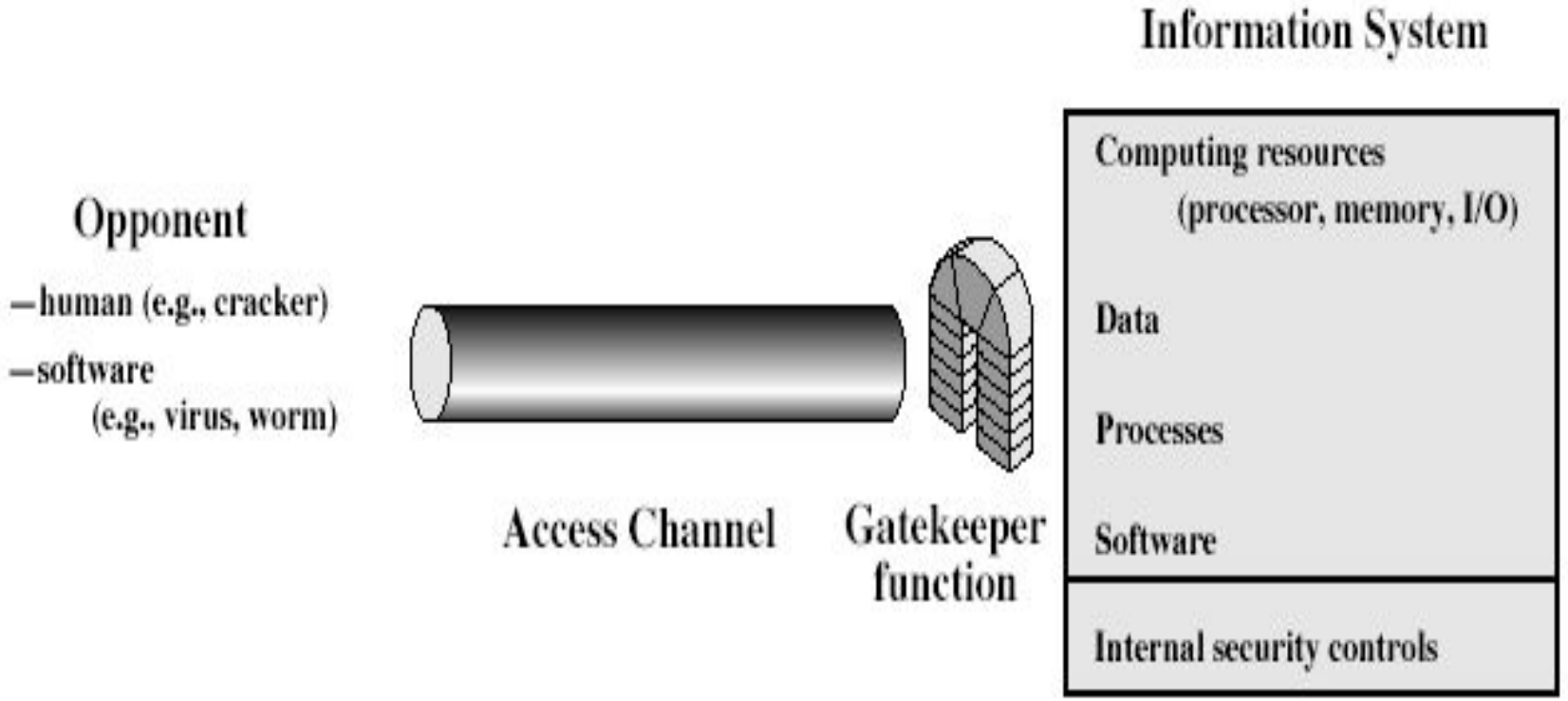
- using this model requires to:(there are four basic tasks in designing a particular security service)

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 Security

- The second, illustrated in Figure 1.6, model is concerned with controlled access to information or resources on a computer system, in the presence of possible opponents. Here appropriate controls are needed on the access and within the system, to provide suitable security. Some cryptographic techniques are useful here also.

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
- standards organizations
- security concepts:
  - confidentiality, integrity, availability
- X.800 security architecture
- security attacks, services, mechanisms
- models for network (access) security