Network Security

Dr. Dai Tho Nguyen
University of Engineering and Technology
Vietnam National University, Hanoi

Chapter 1

INTRODUCTION

Social Context

- This new century has been characterized by terrorist attacks and security defenses
- IT has also been victim of an unprecedented number of attacks on information
- Information security is now at the core of IT
  - Protecting valuable electronic information
- Demand for IT professionals who know how to secure networks and computers is at a high

Technological Context

- Two major changes in the requirements of information security in recent times
  - Traditionally information security is provided by physical and administrative mechanisms
  - Computer use requires automated tools to protect files and other stored information
  - Use of networks and communications facilities requires measures to protect data during their transmisson

Defining Information Security

- Security
  - A state of freedom from a danger or risk
    - The state or condition of freedom exists because protective measures are established and maintained
- Information security
  - Describes the tasks of guarding information in a digital format
- Information security can be understood by examining its goals and how it is accomplished

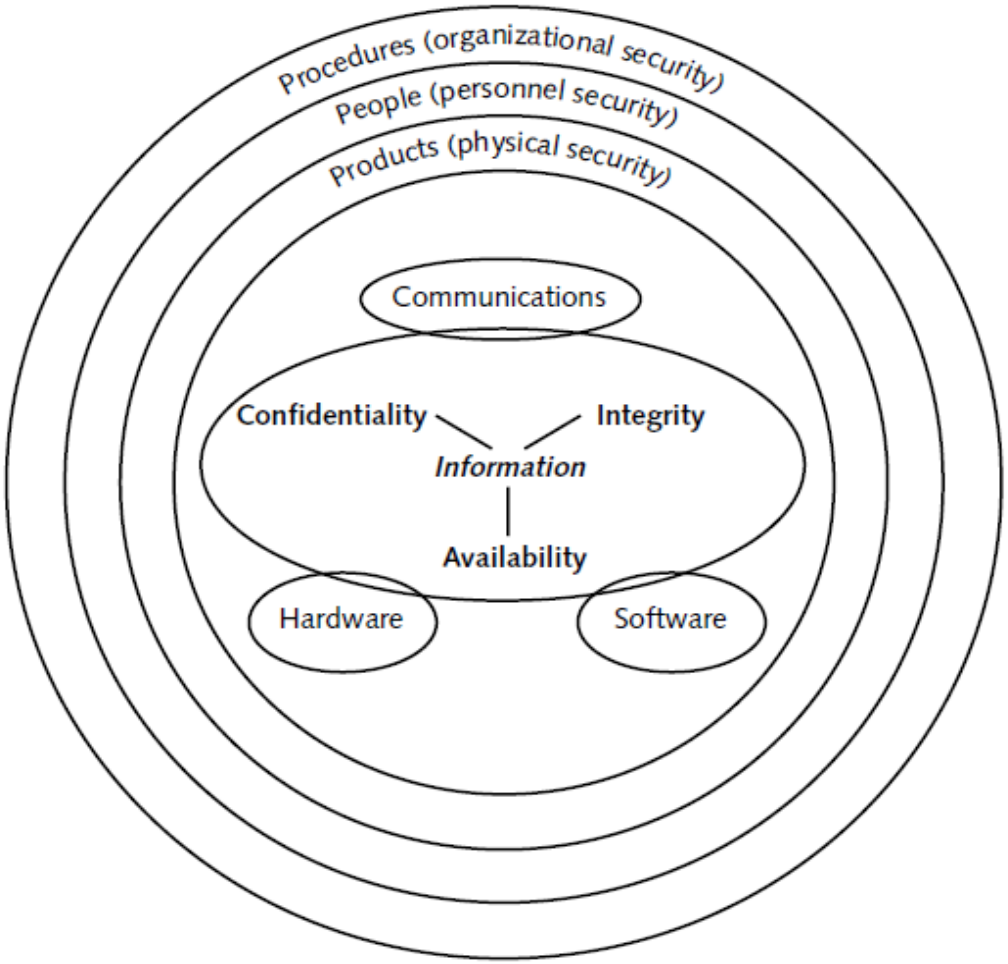
Goals of Information Security

- Ensures that protective measures are properly implemented
- Protects information that has value to people and organizations
  - The value comes from the characteristics **confidentiality**, **integrity**, and **availability**
- Protects the characteristics of information on the devices that store, manipulate, and transmit the information

How Info Security is Accomplished

- Through a combination of 3 entities
  - Hardware, software, and communications
- Three layers of protection
  - Products
    - The physical security around the data
  - People
    - Those who implement and use security products
  - Procedures
    - Plans and policies to ensure correct use of the products

Information Security Components



Information Security Definition

- A more comprehensive definition of information security
  - *That which protects the integrity, confidentiality, and availability of information on the devices that store, manipulate, and transmit the information through products, people, and procedures*

Information Security Concepts (1)

- Confidentiality
  - Preserving authorized restrictions on information access and disclosure
    - Including means for protecting personal privacy and proprietary information
- Integrity
  - Guarding against improper information modification or destruction
    - Including ensuring information nonrepudiation and authenticity

Information Security Concepts (2)

- Availability
  - Ensuring timely and reliable access to and use of information
- Authenticity
  - The property of being genuine and being able to be verified and trusted
- Accountability
  - The security goal that requires for actions of an entity to be traced uniquely to that entity

Information Security Terms (1)

- Asset
  - Something that has a value
- Threat
  - An potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm
    - A threat is a possible danger that might exploit a vulnerability

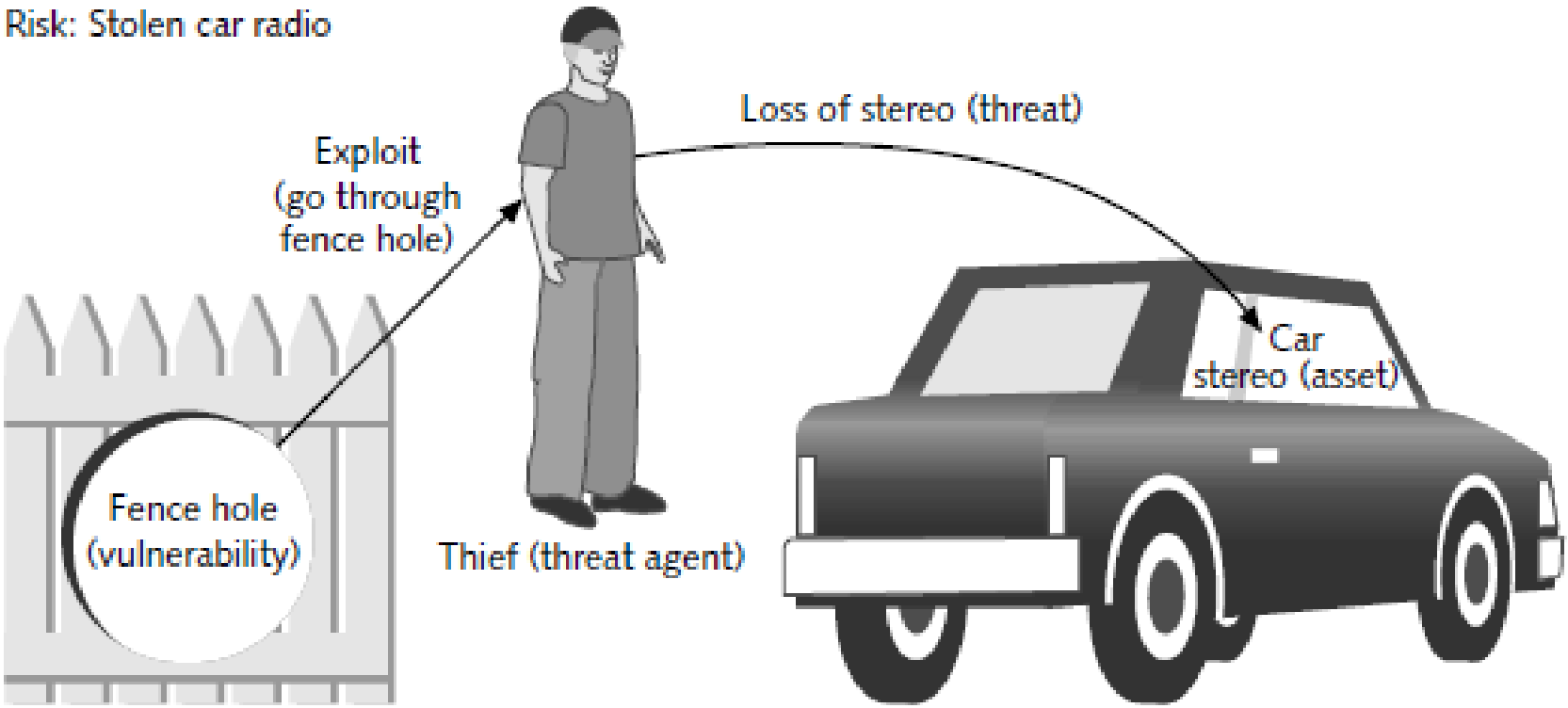
Information Security Terms (2)

- Threat agent
  - A person or thing that has the power to carry out a threat
- Attack
  - An assault on system security that derives from an intelligent threat or act
    - A deliberate attempt to evade security services and violate the security policy of a system
  - Often means the same thing as threat

Information Security Terms (3)

- Vulnerability
  - Weakness that allows a threat agent to bypass security
- Risk
  - The likelihood that a threat agent will exploit a vulnerability
  - Realistically risk cannot ever be entirely eliminated
  - Three options when dealing with risks
    - Accept the risk, diminish the risk, or transfer the risk

Example of Security Terms



Security 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

Computer Security Challenges (1)

- Not as simple as it might first appear
- Must always consider potential attacks on security features to develop
- Security procedures often counterintuitive
- Must decide where to deploy security mechanisms
- Involve more than an algorithm or protocol and require secret information

Computer Security Challenges (2)

- Battle of wits between attacker and designer or administrator
- Not perceived as benefit until fails
- Requires regular, even constant, monitoring
- Too often an afterthought to be incorporated after design is complete
- Regarded as impediment to efficient and user-friendly use of system or information

Attacker Profiles (1)

- Hackers
  - People with special knowledge of computer systems
  - Black-hat hackers
    - Hack computing systems for their own benefit
  - White-hat hackers
    - Hack for finding loopholes and developing solutions
  - Grey-hat hackers
    - Often wear a white hat but may also wear a black hat

Attacker Profiles (2)

- Script kiddies
  - People who use scripts and programs developed by black-hat hackers to attack computing systems
  - They don't know how to write hacking tools or understand how an existing hacking tool works, but could inflict a lot of damage
- Cyber spies
  - Collecting intelligence through intercepted network communications

Attacker Profiles (3)

- Vicious employees
  - People who intentionally breach security to harm their employers
- Cyber terrorists
  - Terrorists who use computer and network technologies to carry out attacks and produce public fear
- Hypothetical attackers
  - All attackers except cyber terrorists

OSI Security Architecture

- Goals
  - Assess effectively the security needs of an organization
  - Evaluate and choose security products and policies
- ITU-T X.800 “Security Architecture for OSI”
- A systematic way of defining and satisfying security requirements
- Provides a useful, if abstract, overview of concepts we will study

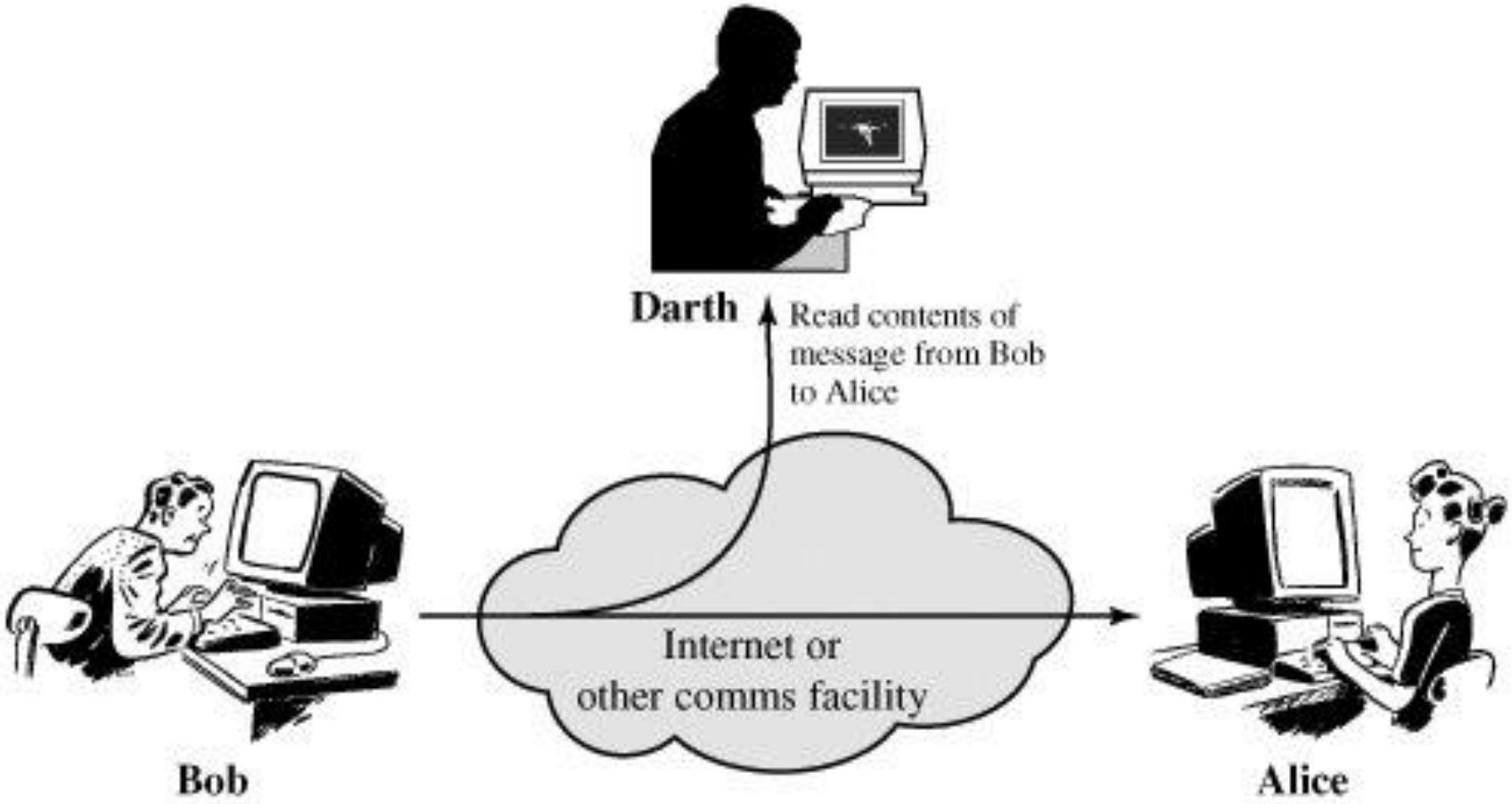
Aspects of Security

- Security attack
  - Action that compromises the security of information
- Security mechanism
  - Process that is designed to detect, prevent, or recover from a security attack
- Security service
  - Service that enhances the security of data processing systems and information transfers

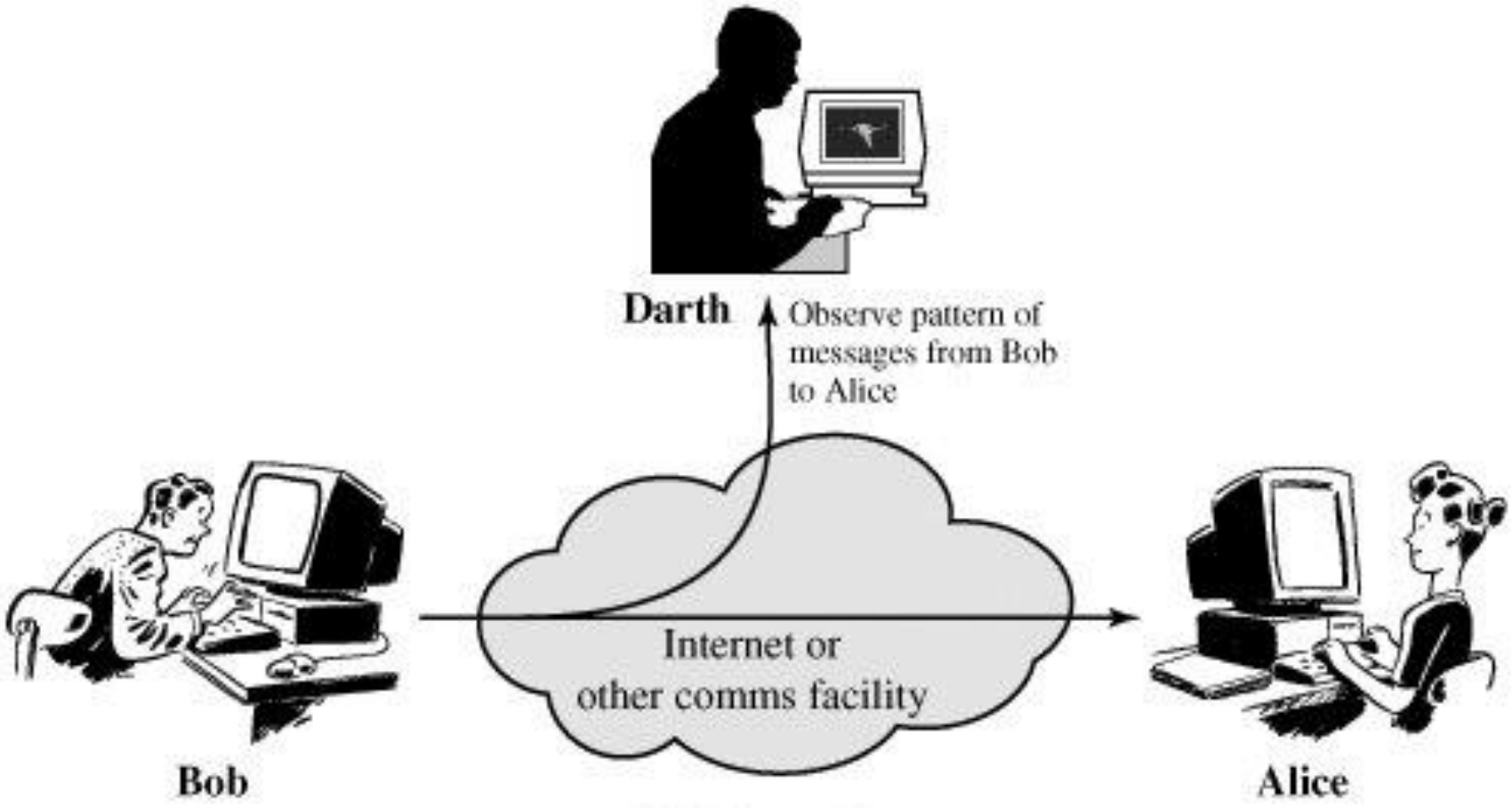
Passive Attacks

- Attempt to learn or make use of information but does not affect system resources
  - Do not involve any alteration of the data
- Two types
  - Release of message contents
  - Traffic analysis
- Emphasis on prevention rather than detection
  - Usually by means of encryption

Release of Message Contents



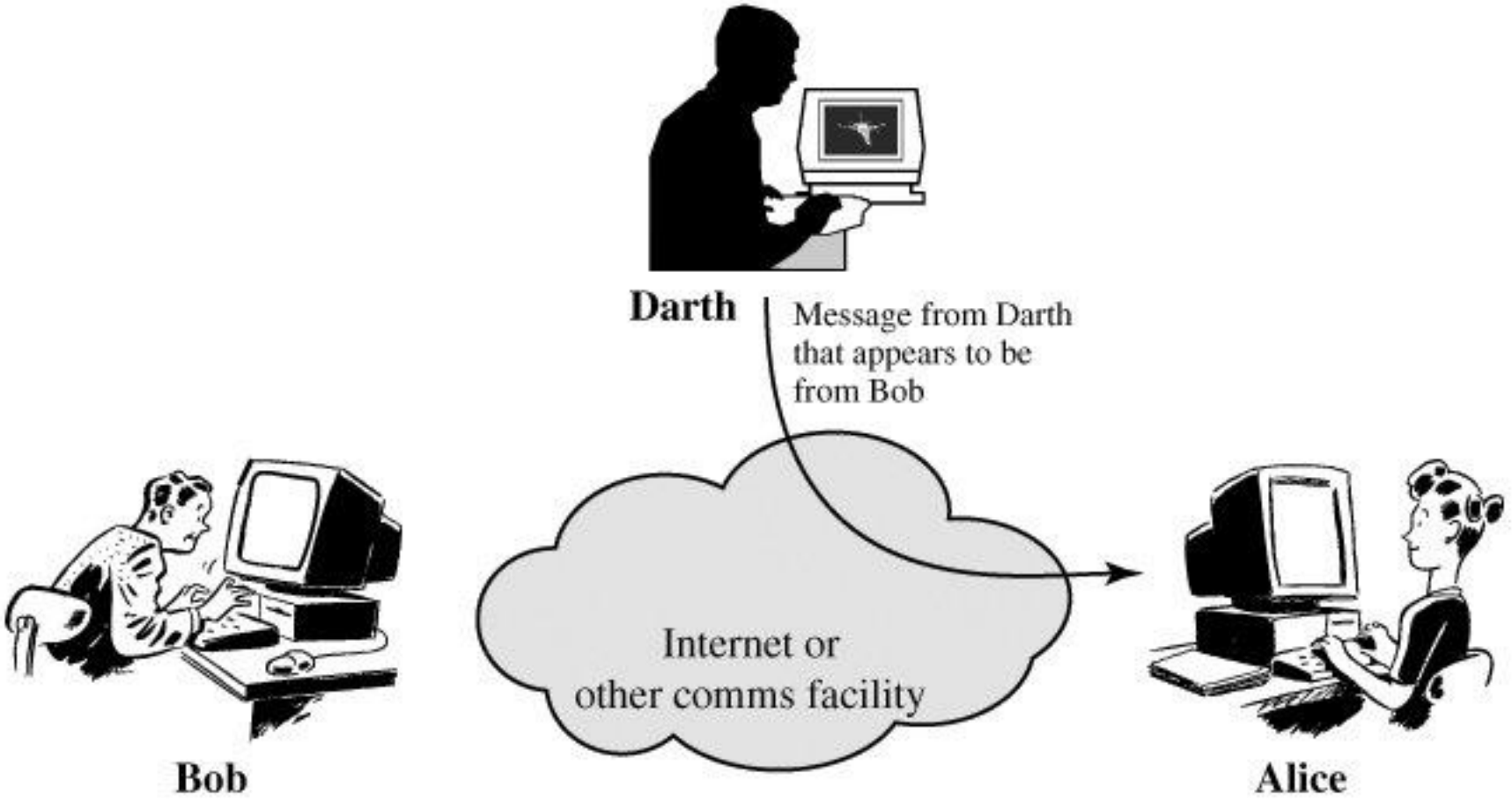
Traffic Analysis



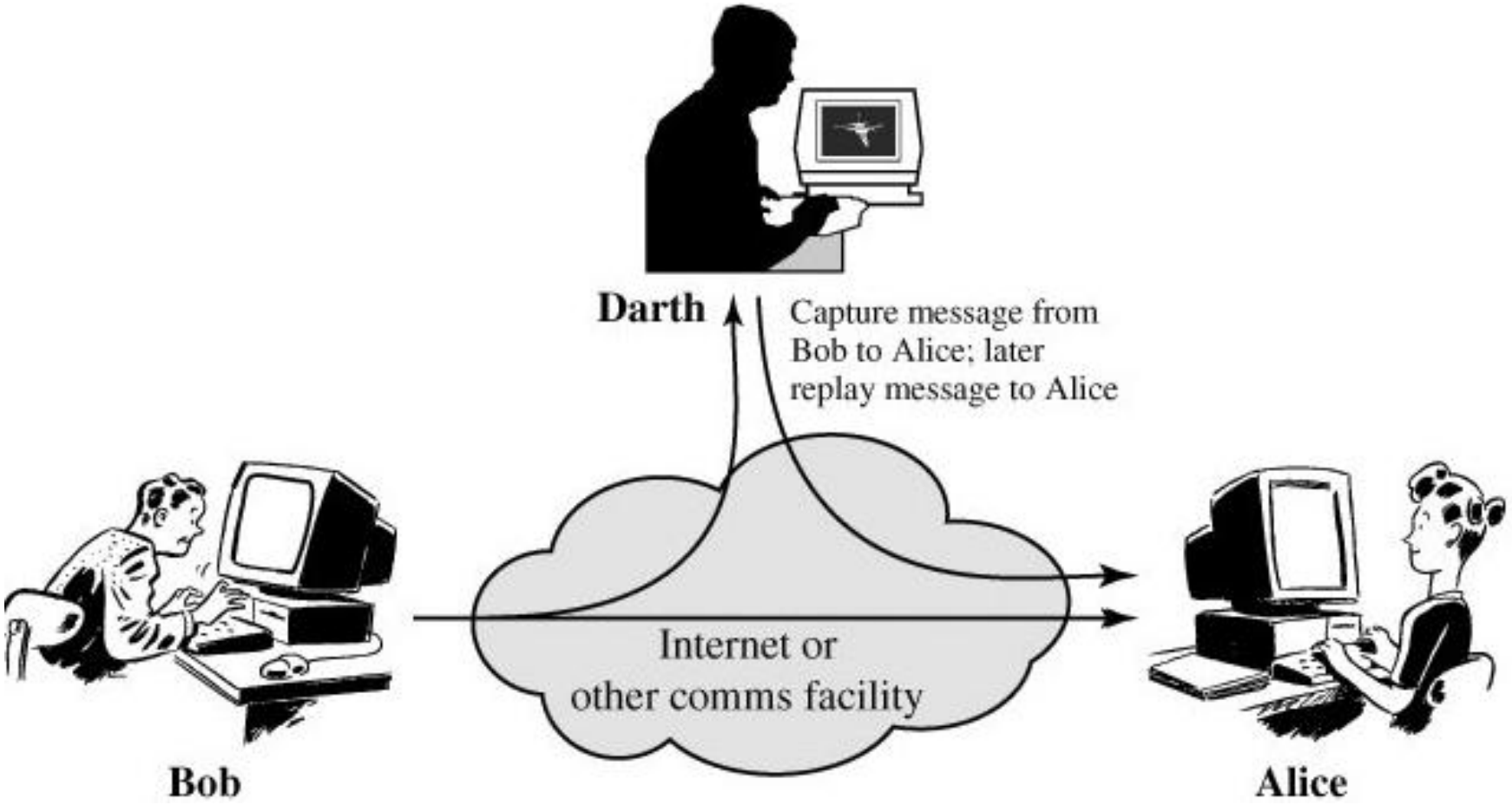
Active Attacks

- Involve some modification of the data stream or the creation of a false stream
- Four types
  - Masquerade
  - Modification of messages
  - Replay
  - Denial of service
- The goal is to detect active attacks and to recover from disruption or delays
  - Detection may contribute to prevention

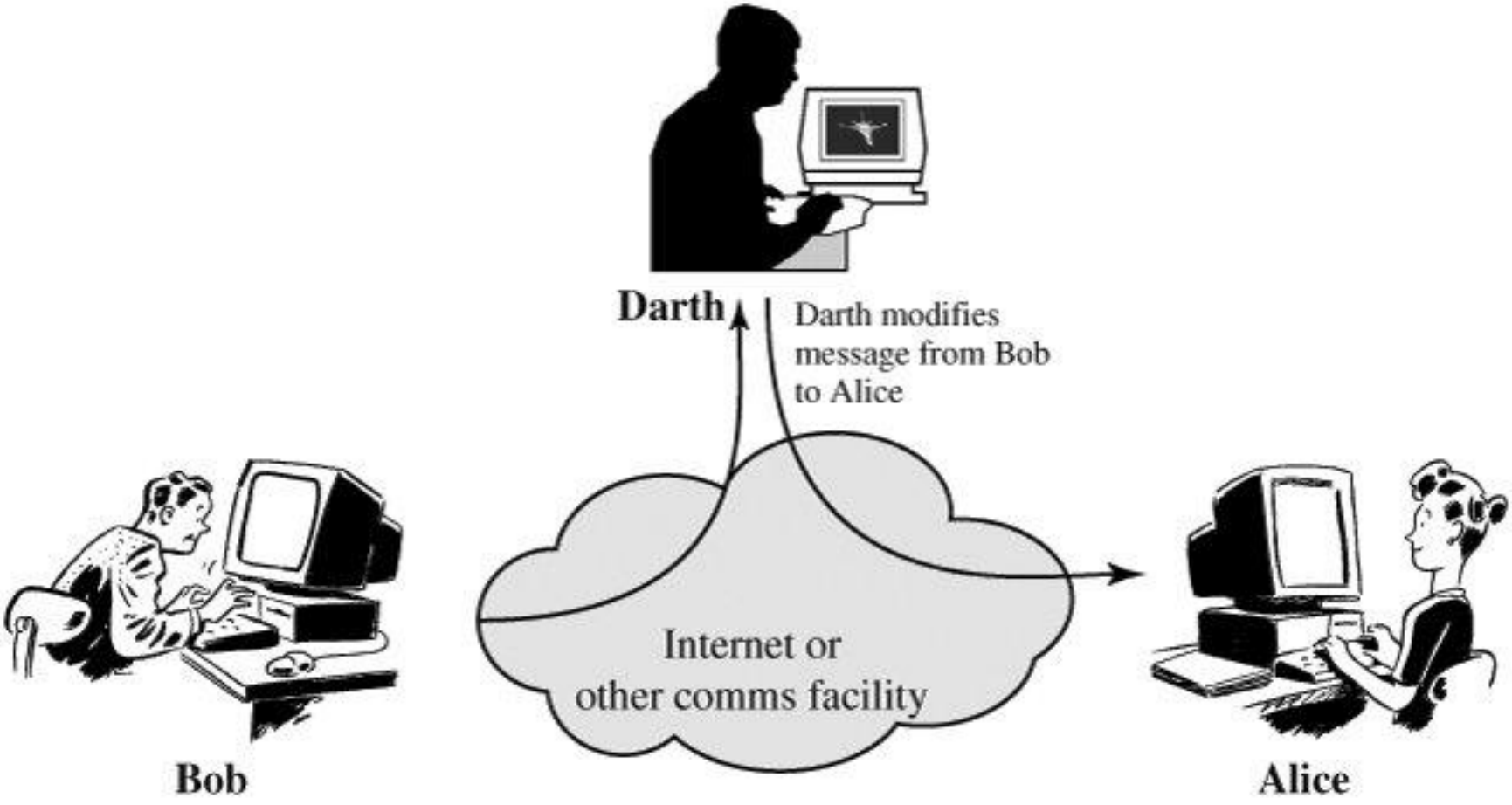
Masquerade


Darth
Message from Darth
that appears to be
from Bob
Internet or
other comms facility
Bob
Alice

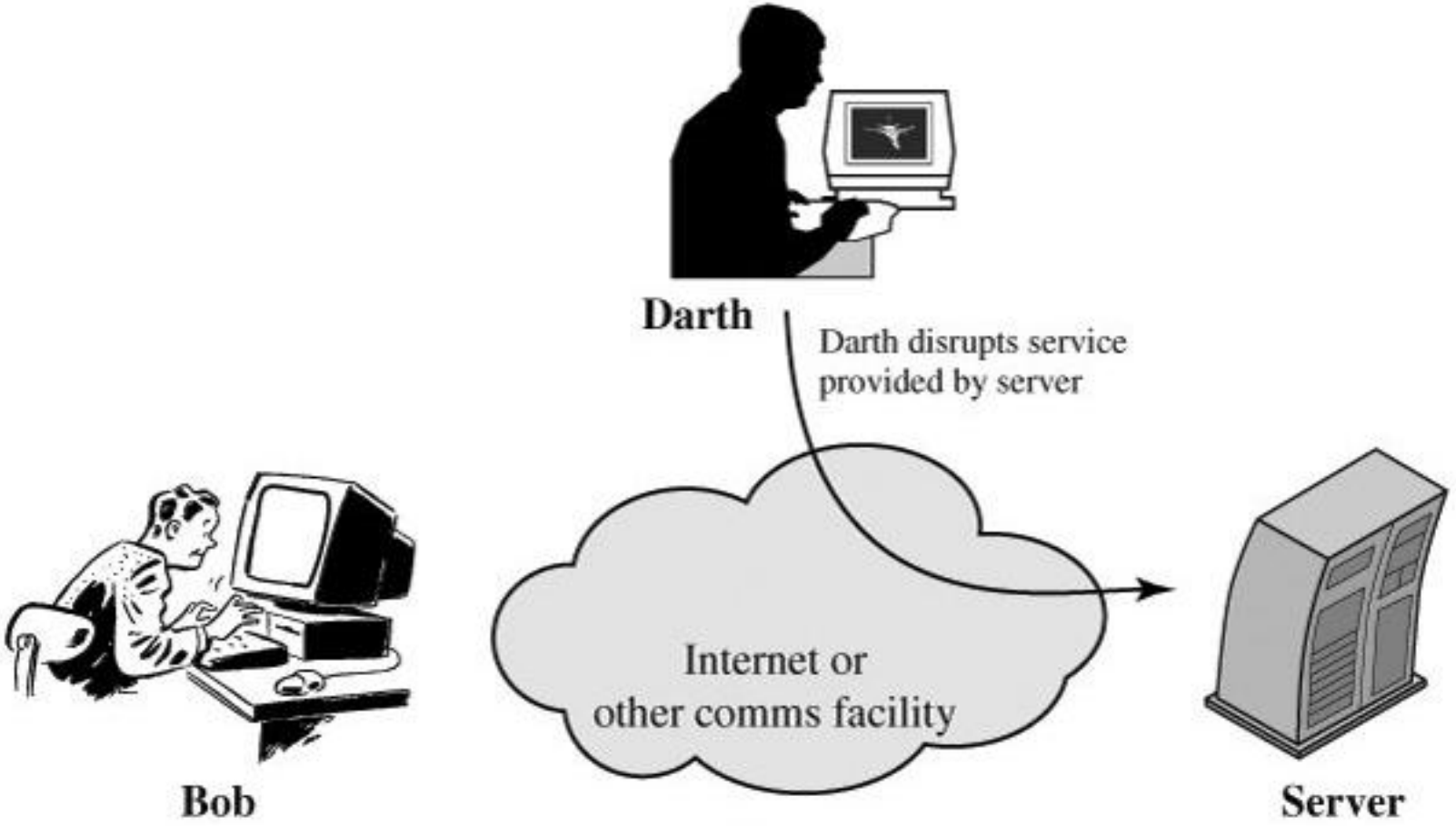
Replay


Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice

Modification of Messages



Denial of Service



Security Services

- X.800
  - Services provided by a protocol layer of communicating open systems, ensuring adequate security of the systems or of data transfers
- RFC 2828
  - Processing or communication services provided by a system to give a specific kind of protection to system resources
- Intended to counter security attacks

Security Services (X.800) (1)

- Authentication
  - Assurance that communicating entity is the one that it claims to be
- Access control
  - Prevention of unauthorized use of a resource
- Data confidentiality
  - Protection of data from unauthorized disclosure

Security Services (X.800) (2)

- Data integrity
  - Assurance that data received are exactly as sent by an authorized entity
- Non-repudation
  - Protection against denial by one of the entities involved in a communication
- Availability
  - Assurance that a resource is accessible and usable

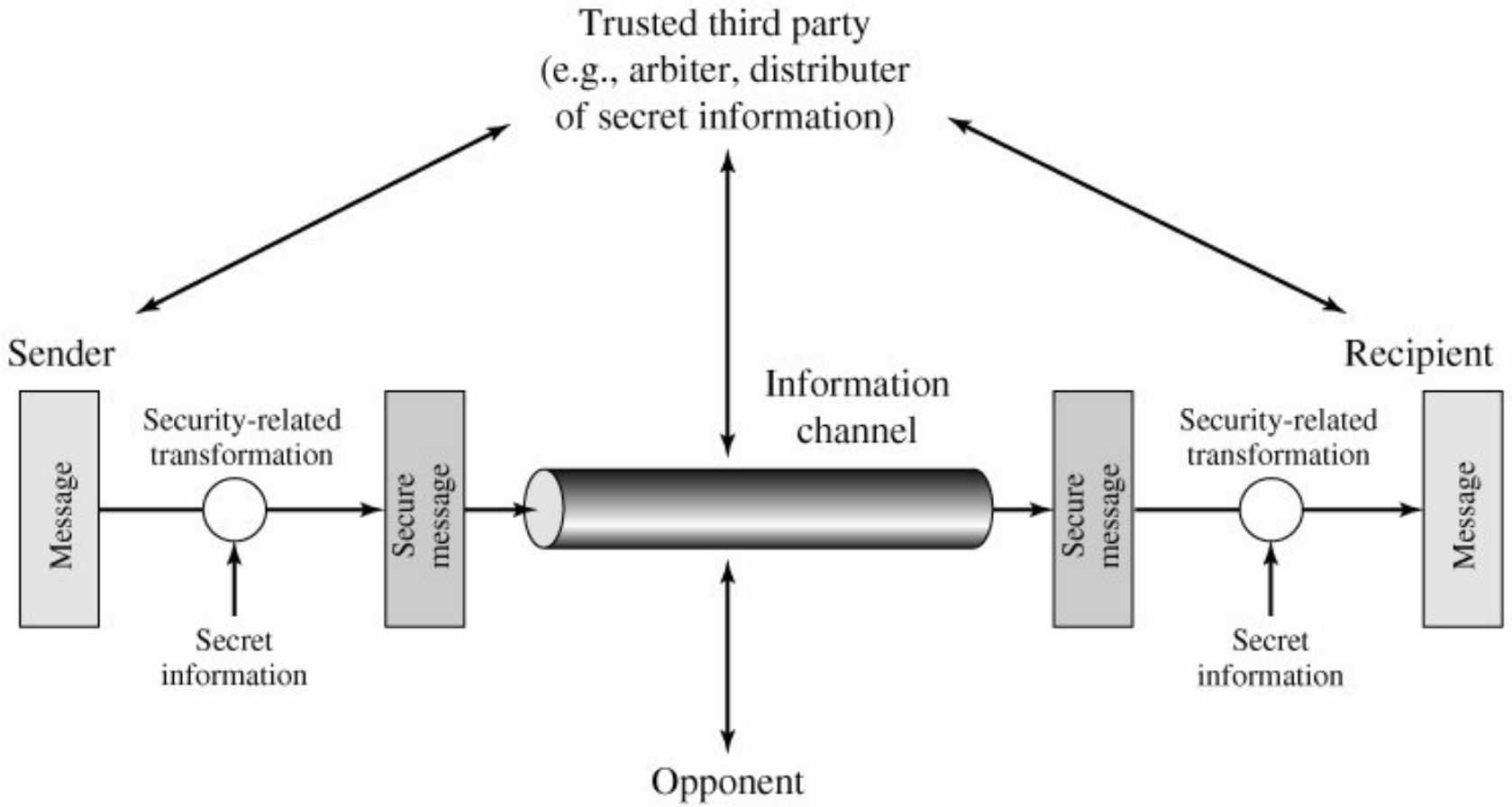
Security Mechanisms

- A security service makes use of one or more security mechanisms
- No single mechanism that will support all security services
- One particular element underlies many of the security mechanisms in use
  - Cryptographic techniques

Security Mechanisms (X.800)

- Specific security mechanisms
  - Implemented in a specific protocol layer
  - Encipherment, digital signature, access control, data integrity, authentication exchange, traffic padding, routing control, notarization
- Pervasive security mechanisms
  - Trusted functionality, security labels, event detection, security audit trails, security recovery
  - Not specific to any particular security service or protocol layer

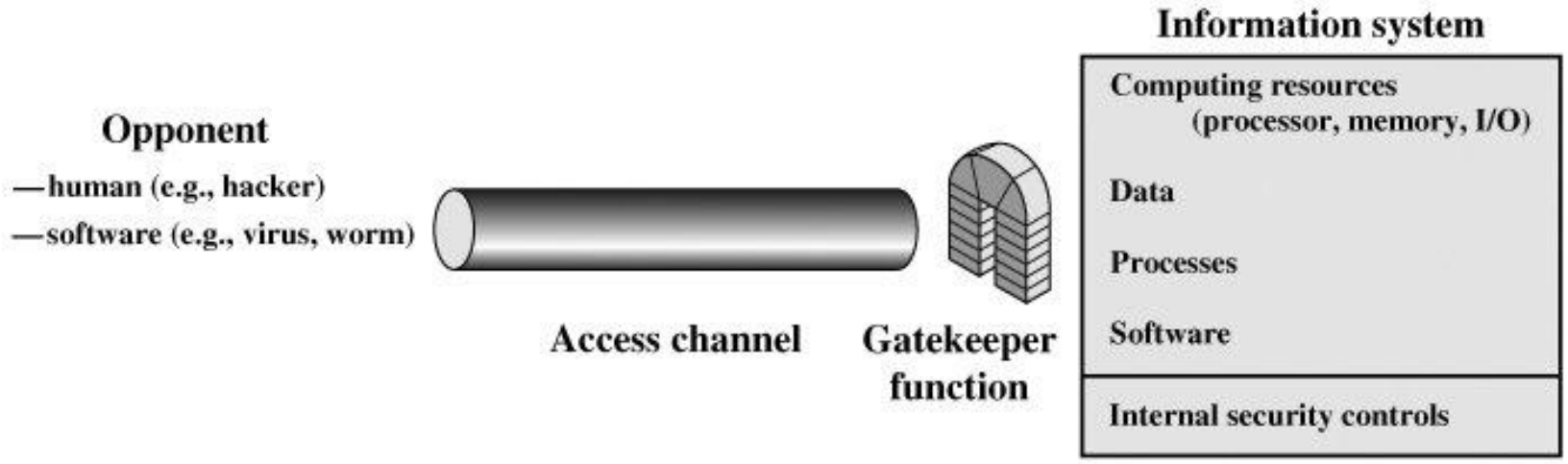
Model for Network Security



Tasks in Network Security Model

- Design an algorithm for performing the security-related transformation
- Generate the secret information to be used with the algorithm
- Develop methods for the distribution and sharing of the secret information
- Specify a protocol enabling the principals to use the security algorithm and secret information for a security service

Model for Network Access Security



Tasks in Network Access Security

- Gatekeeper function
  - Password-based login procedures designed to deny access to all but authorized users
  - Screening logic designed to detect and reject worms, viruses, and other similar attacks
- Internal security controls
  - Monitor activity and analyze stored information to detect the presence of unwanted intruders

Summary

- Motivations
- Security definitions, concepts, and terms
- Computer security challenges
- Attacker profiles
- X.800 security architecture
  - Security attacks, services, mechanisms
- Models for network (access) security