Chapter 1 Computer and Network Security Concepts

Introduction

The art of war teaches us 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

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

Cryptographic algorithms and protocols

Symmetric encryption

- Used to conceal the contents of blocks or streams of data of any size, including messages, files, encryption keys, and passwords

Asymmetric encryption

- Used to conceal small blocks of data, such as encryption keys and hash function values, which are used in digital signatures

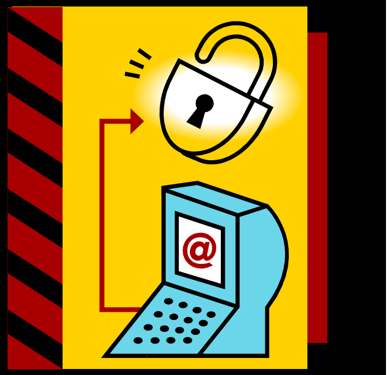
Data integrity algorithms

- Used to protect blocks of data, such as messages, from alteration

Authentication protocols

- Schemes based on the use of cryptographic algorithms designed to authenticate the identity of entities

Network and Internet Security



measures to deter, prevent, detect, and correct security violations that involve the transmission of information

Outline

- □ Computer Security Concepts
- □ The OSI Security Architecture
- □ Security Attacks
- □ Security Services
- □ Security Mechanisms
- □ Fundamental Security Design Principles
- □ Attack Surfaces and Attack Trees
- □ A model for Network Security
- □ Standards

Outline

- ❑ Computer Security Concepts
- ❑ The OSI Security Architecture
- ❑ Security Attacks
- ❑ Security Services
- ❑ Security Mechanisms
- ❑ Fundamental Security Design Principles
- ❑ Attack Surfaces and Attack Trees
- ❑ A model for Network Security
- ❑ Standards

Organizational Security

What’s it about?

- keeping information within organization secure
- establishing and enforcing security policies
- management level concern

Typical Issues

- risk assessment (systematic process for identifying, analyzing, and controlling risk)
- asset identification
- threat and vulnerability assessment
- user responsibilities, Internet use policy
- incident response team
- disaster recovery plan

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

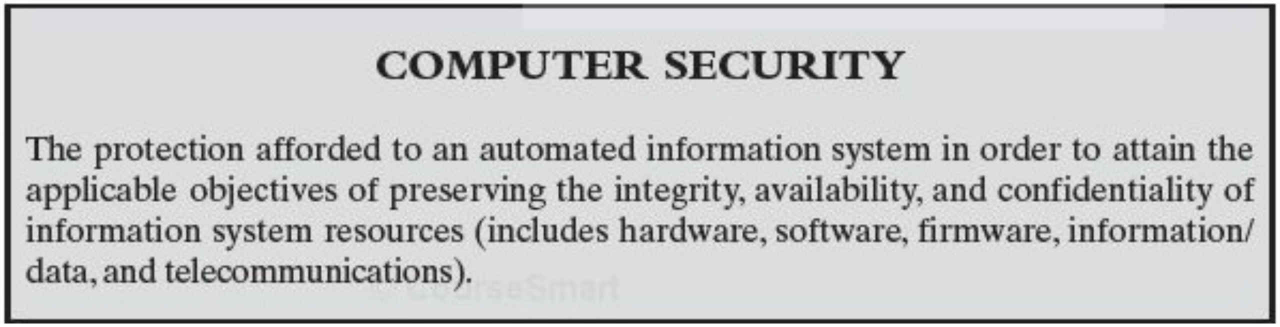
Computer Security

What’s it about?

- protection of data stored on a computer
- controlled use of resources (operating system, physical access)
- operating system (OS) and software security

Typical Issues

- authentication (passwords, biometrics, tokens, smart cards)
- access control (typically done by operating software)
- accounting
- OS patches, software updates
- installation of anti-virus and spam software



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).

Network Security

Network Security - measures to protect data during their transmission

Internet Security - measures to protect data during their transmission over a collection of interconnected networks

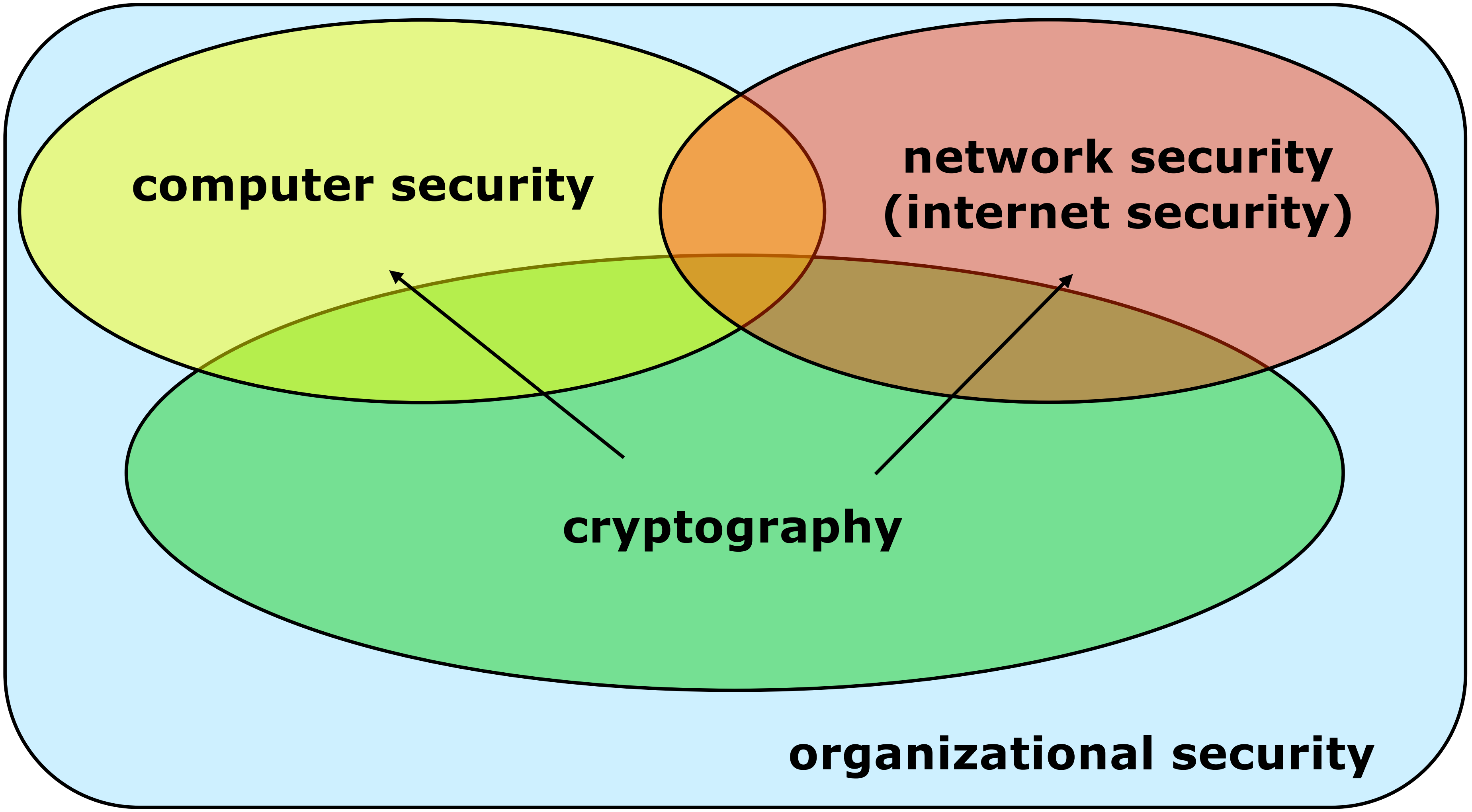
What are they about?

- secure communication and data transmission
- protection against network (and networked) attacks

Typical Issues

- network security services
- Virtual Private Networks (VPN)
- Denial of Service (DoS) attacks
- Spoofing (e.g., ARP spoofing)
- Firewalls
- Intrusion Detection Systems (IDS)
- Honeypots and Honeynets

Information Security



Cryptography

- from Greek: *kryptós*, "hidden", and *gráphein*, "to write“
- art of secret writing:
  - traditionally, the study of means of converting information from its normal, comprehensible form into an incomprehensible format, rendering it unreadable without secret knowledge [the art of *encryption*]
  - study of means of converting information from its normal, comprehensible form into an incomprehensible format, rendering it unreadable without secret knowledge [wikipedia.com]
- **Past:** Cryptography helped ensure secrecy in important communications, such as those of spies, military leaders, and diplomats.
- **In recent decades, cryptography has expanded its remit in two ways**
  - mechanisms for more than just keeping secrets: schemes like digital signatures and digital cash, for example.
  - in widespread use by many civilians, and users are not aware of it.

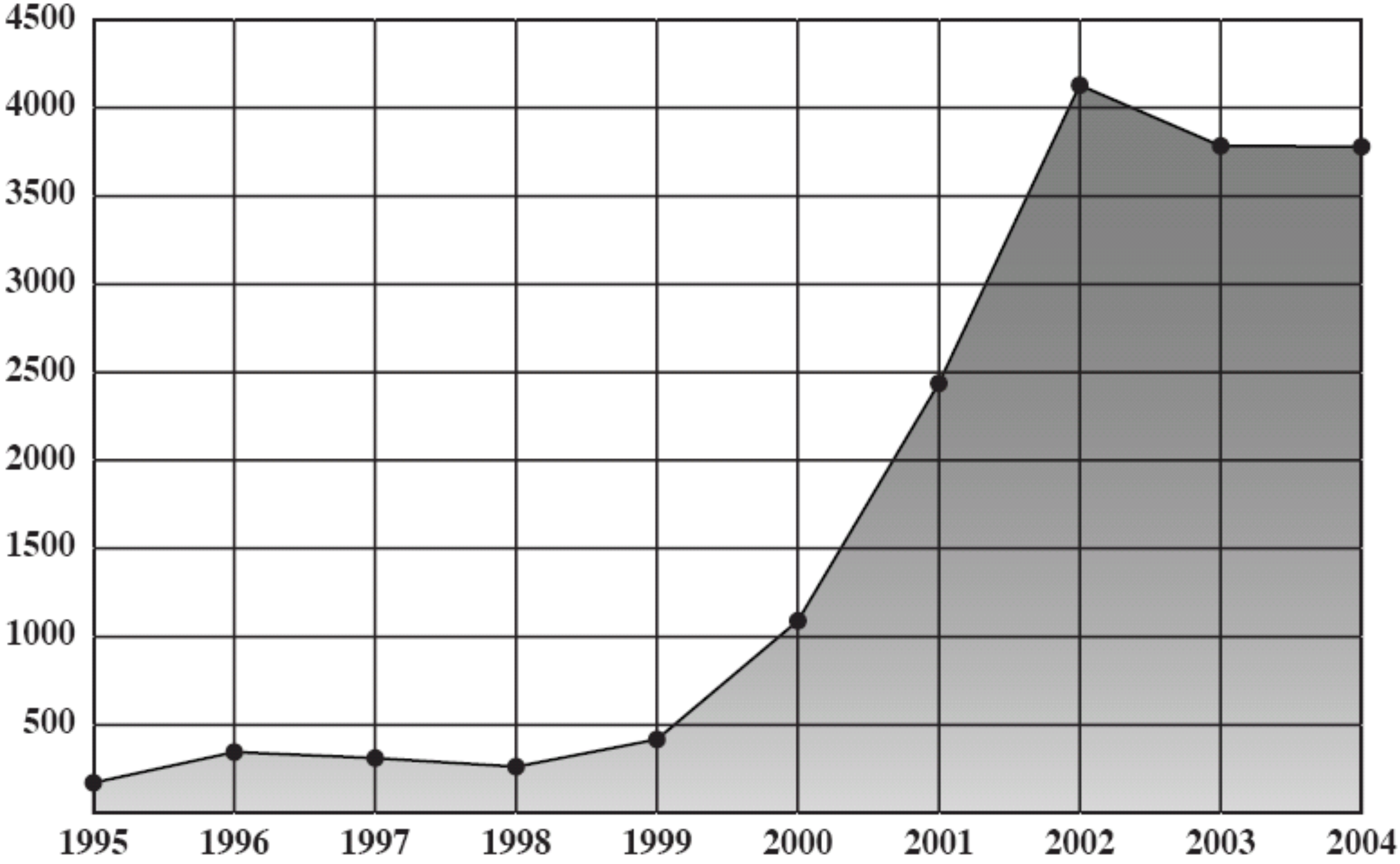
Crypto-graphy, -analysis, -logy

- **Cryptanalysis**:
  - also from Greek: *analýein*: “to loosen”, “to untie”
  - breaking of cryptographic systems (“*code breaking”*)
- **Cryptology**: includes cryptography and cryptanalysis
- In practice, "cryptography" is also often used to refer to the field as a whole; **crypto** is an informal abbreviation.
- **Cryptography** is an interdisciplinary subject,
  - linguistics
  - Mathematics: number theory, information theory, computational complexity, statistics and combinatorics
  - engineering

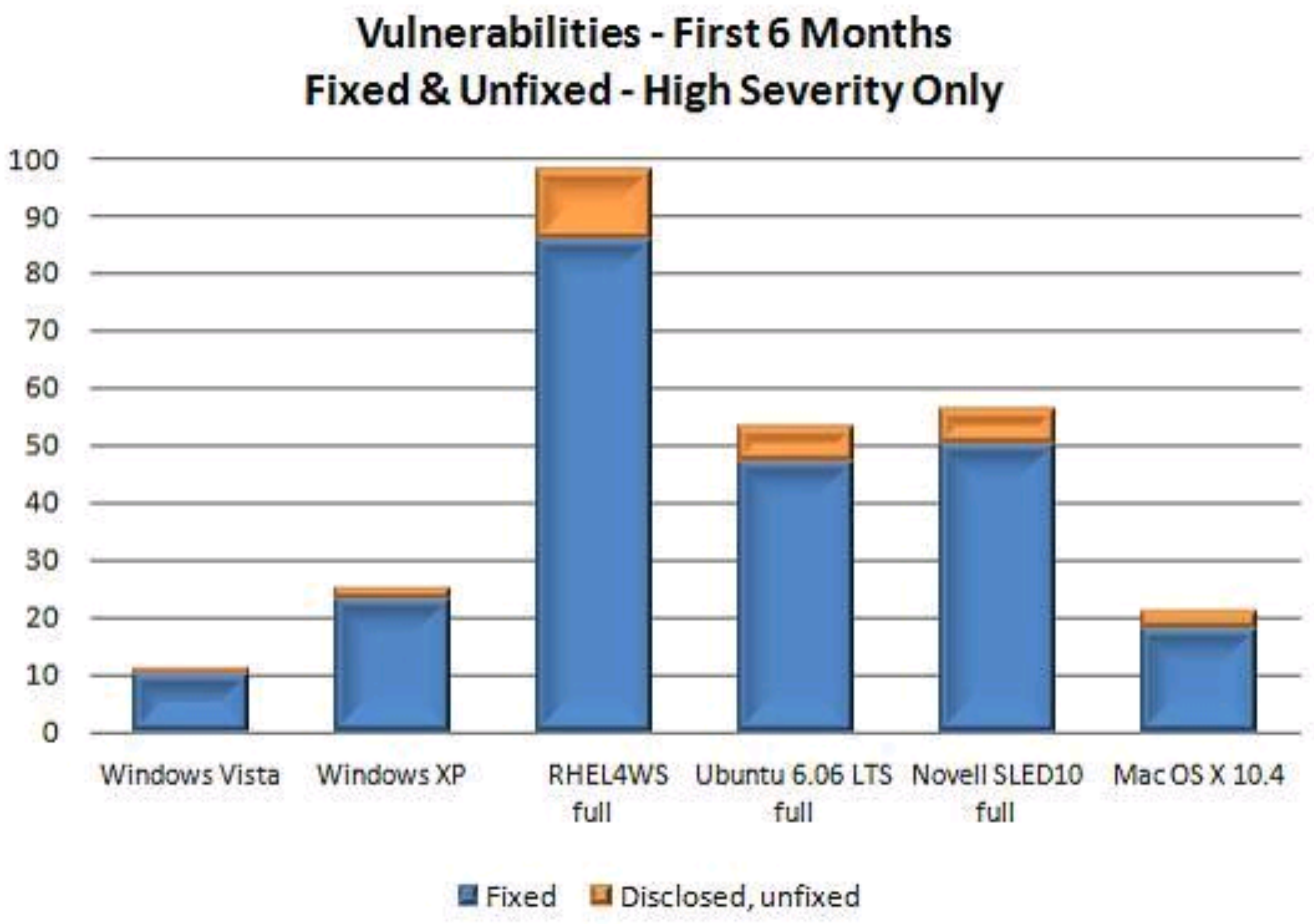
Close, but different fields

- **Steganography**
  - the study of hiding the very *existence* of a message, and not necessarily the *contents* of the message itself (for example, microdots, or invisible ink)
- **Traffic analysis**
  - which is the analysis of patterns of communication in order to learn secret information

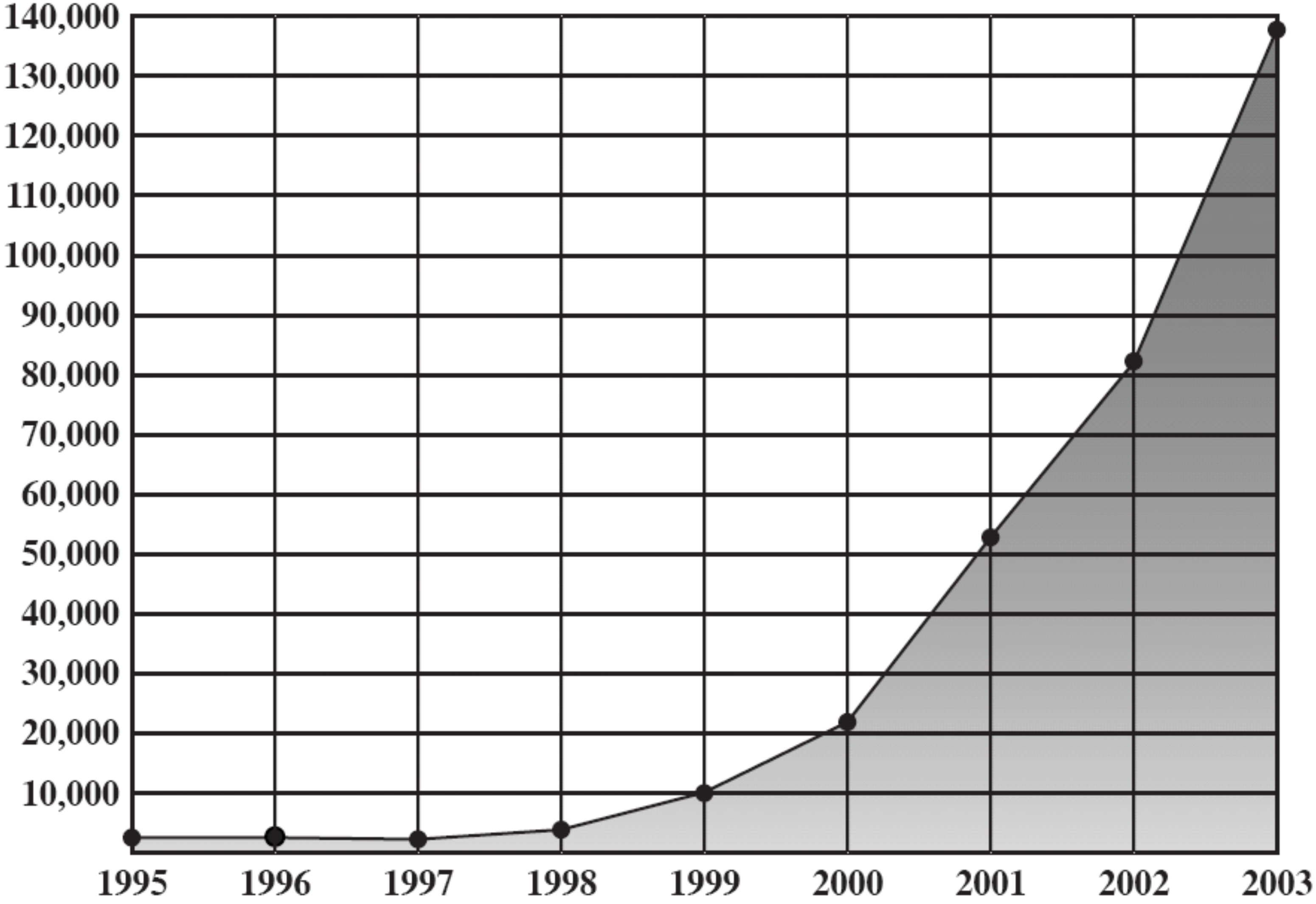
Vulnerabilities Reported



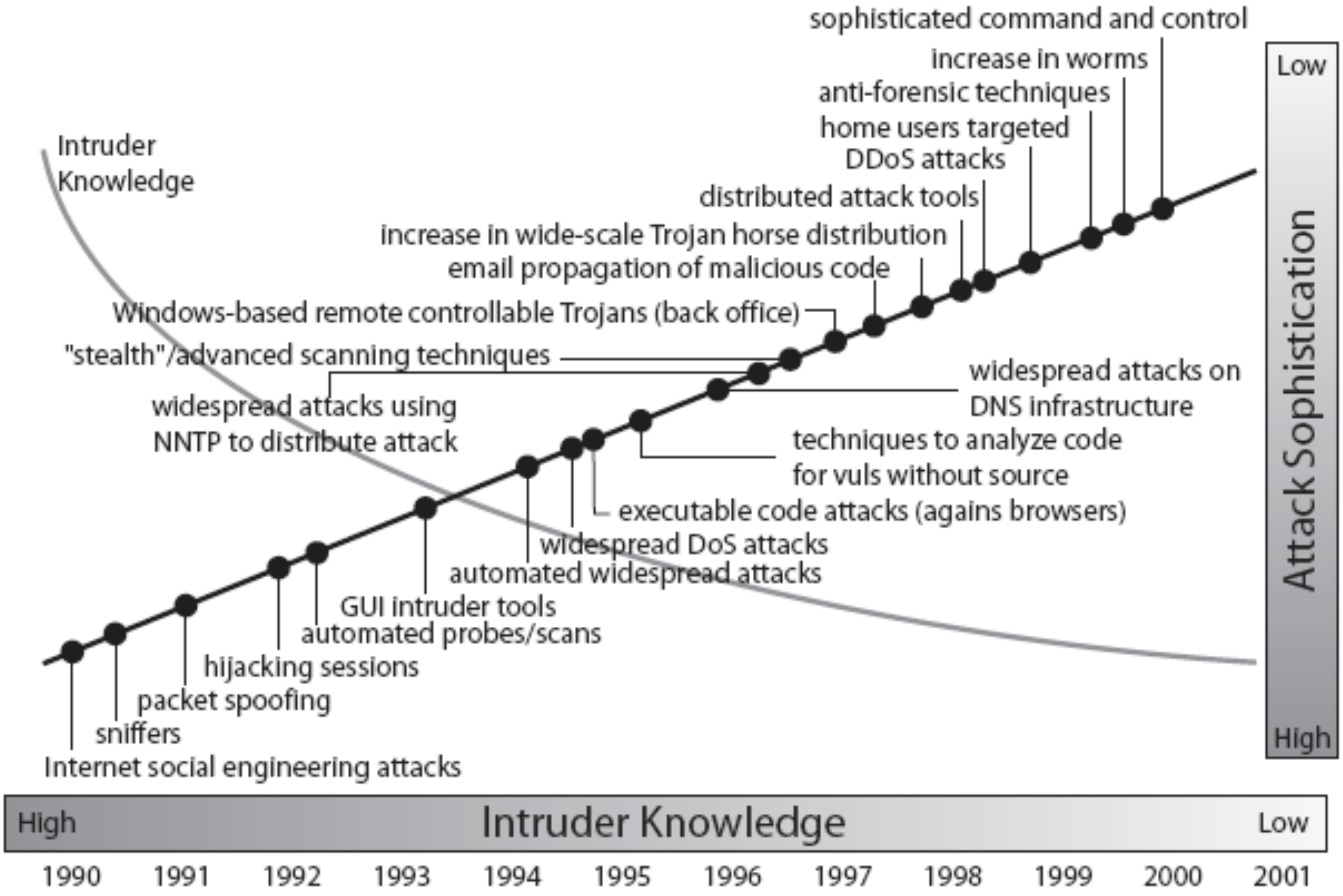
Vulnerabilities – First 6 Months (by Microsoft)



Incidents Reported



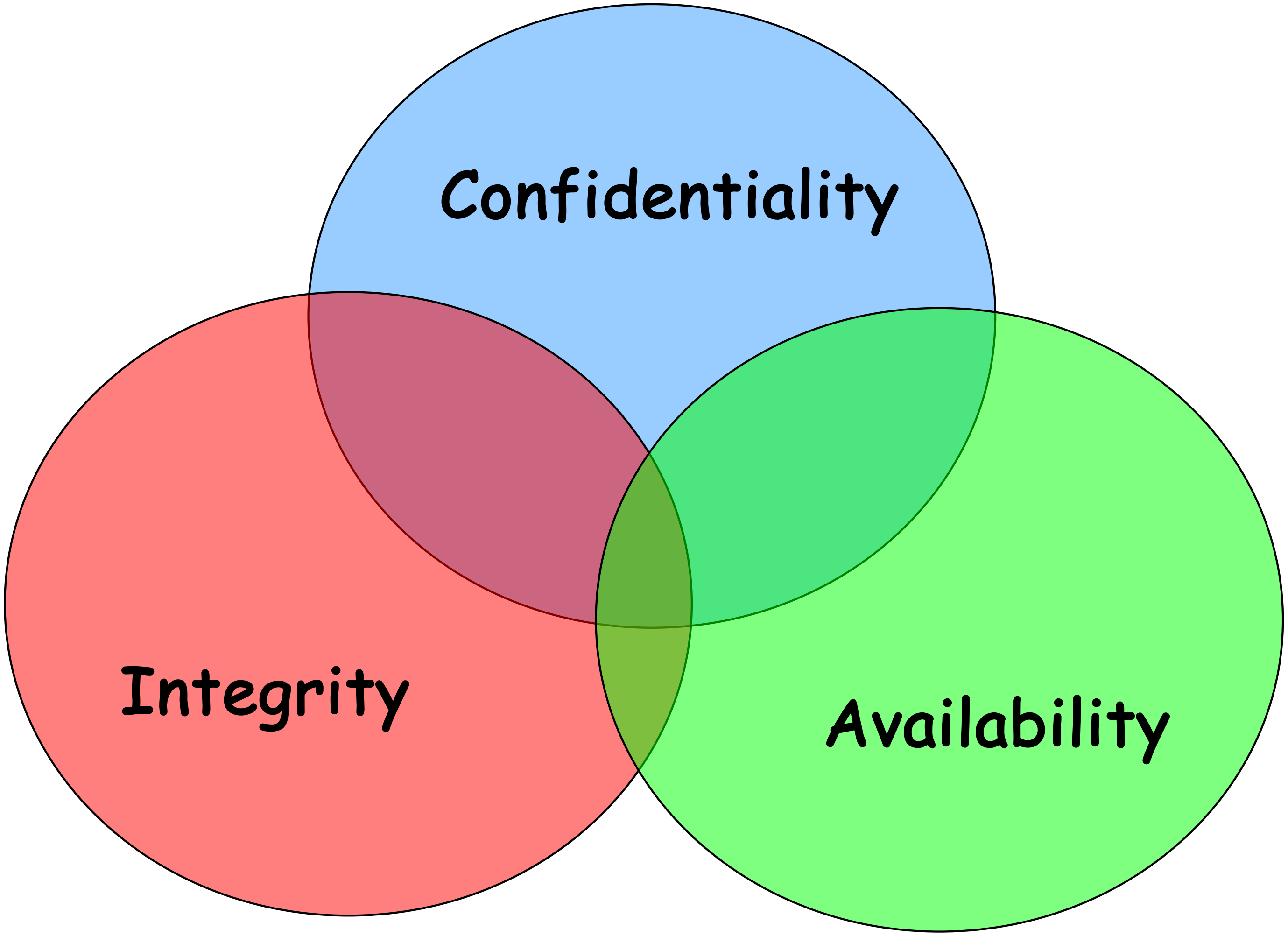
Security Trends



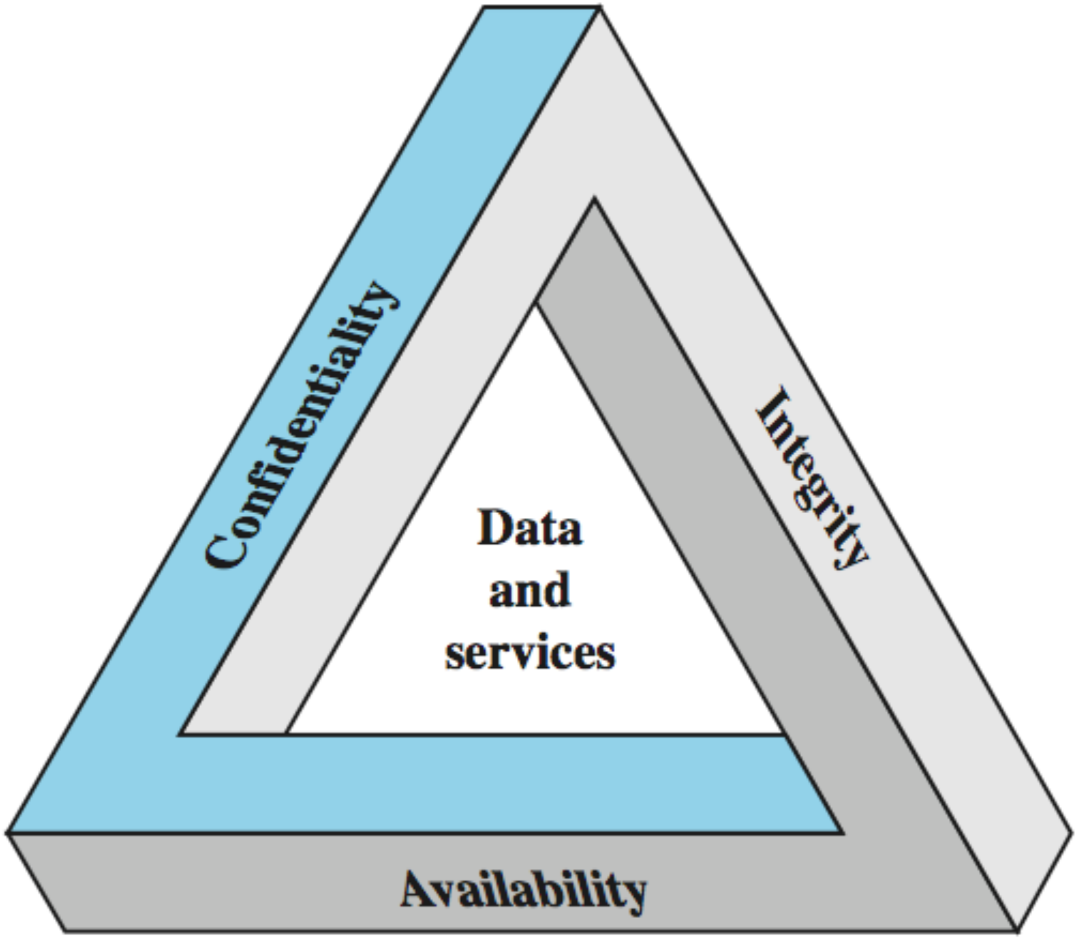
Source: CERT

Security Goals

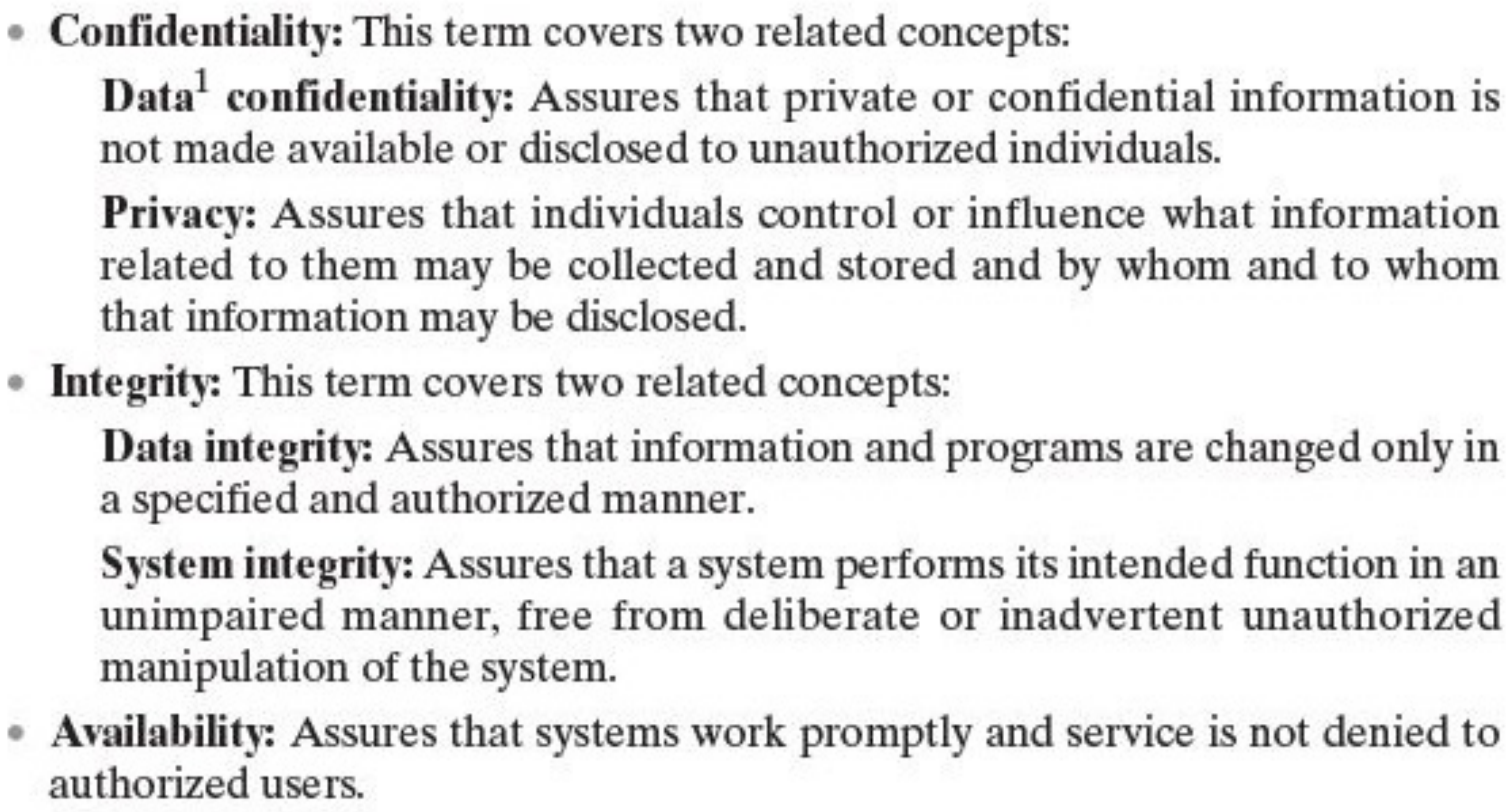
- Also, nonrepudiation



Key Security Concepts



CIA Triad



- **Confidentiality:** This term covers two related concepts:

  Data[1] confidentiality: Assures that private or confidential information is not made available or disclosed to unauthorized individuals.

  Privacy: Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

- **Integrity:** This term covers two related concepts:

  Data integrity: Assures that information and programs are changed only in a specified and authorized manner.

  System integrity: Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

- **Availability:** Assures that systems work promptly and service is not denied to authorized users.

Computer Security Objectives

Confidentiality

- Data confidentiality
  - Assures that private or confidential information is not made available or disclosed to unauthorized individuals
- Privacy
  - Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed

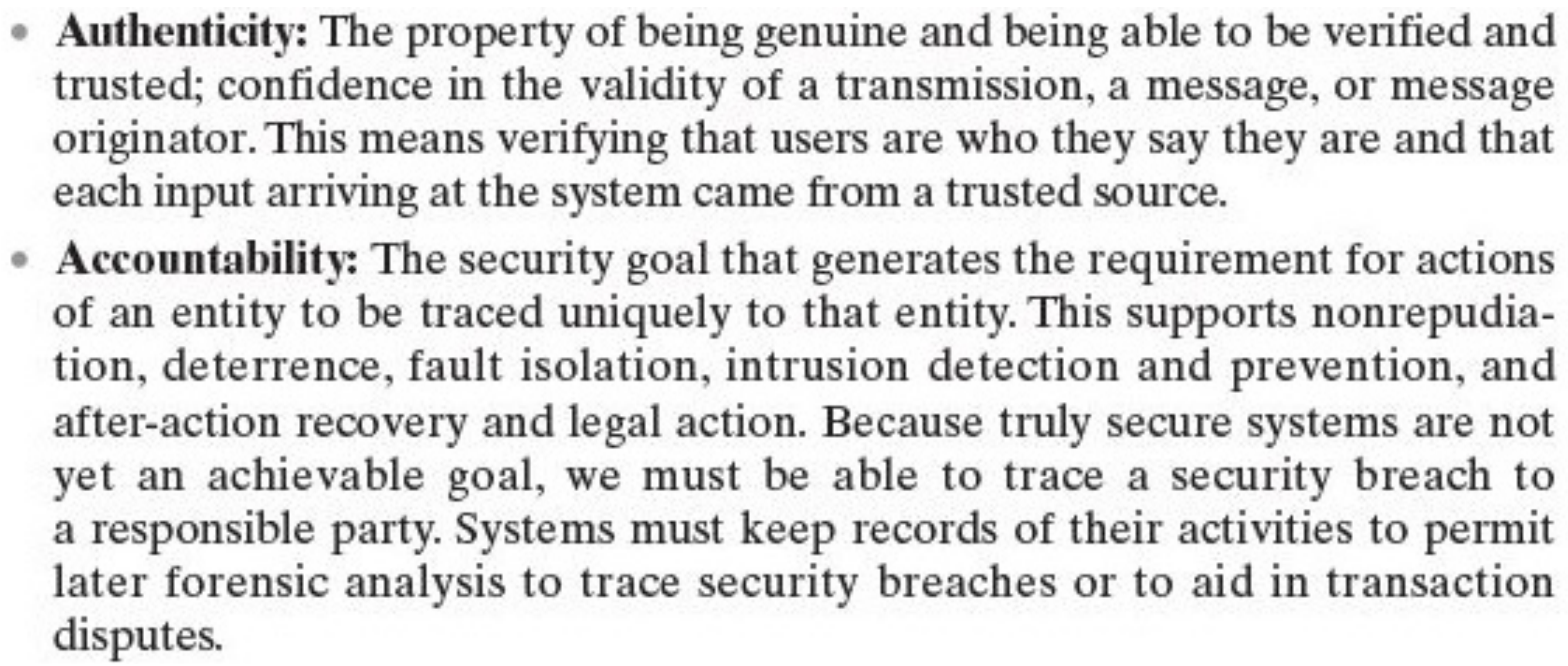
Integrity

- Data integrity
  - Assures that information and programs are changed only in a specified and authorized manner
- System integrity
  - Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system

Availability

- Assures that systems work promptly and service is not denied to authorized users

Two more



- **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. This means verifying that users are who they say they are and that each input arriving at the system came from a trusted source.
- **Accountability:** The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action. Because truly secure systems are not yet an achievable goal, we must be able to trace a security breach to a responsible party. Systems must keep records of their activities to permit later forensic analysis to trace security breaches or to aid in transaction disputes.

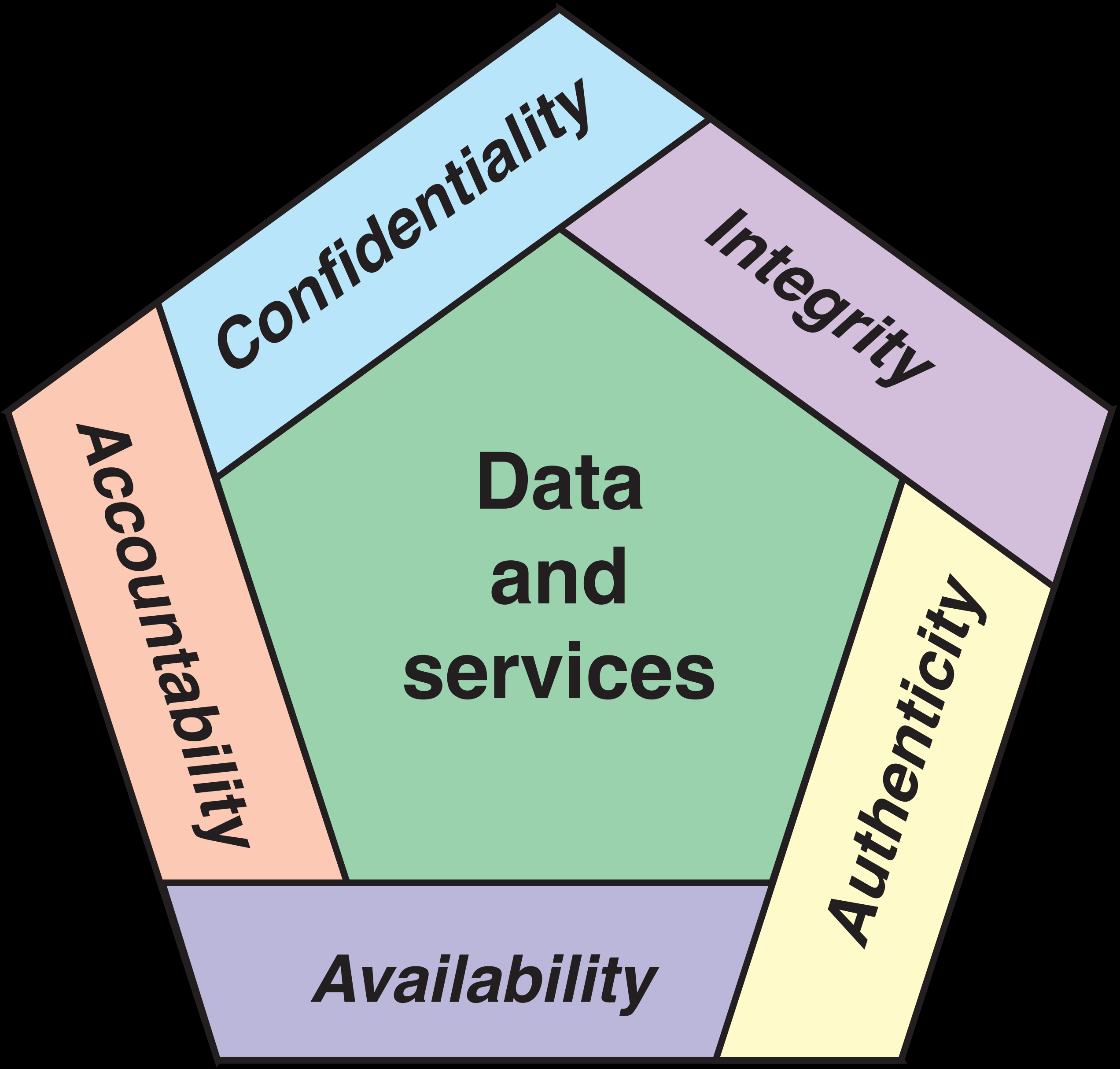


Figure 1.1 Essential Network and Computer Security Requirements

Levels of Impact

- **can define 3 levels of impact from a security breach**
  - Low (minor)
  - Moderate (significant)
  - High (major)

- **Considerations:**
  - mission capability to an extent and duration that the organization is able to perform its primary functions, and the effectiveness of the functions
  - organizational assets
  - financial loss
  - harm to individuals

Examples

- **Confidentiality**
  - High: student grade information
  - Moderate: student enrollment information
  - Low: directory information
- **Integrity**
  - High: a hospital patient’s allergy information stored in a database
  - Moderate: online forum
  - Low: online polls
- **Availability**
  - High: authentication services for critical systems , applications and devices
  - Moderate: a public web site for a university
  - Low: an online telephone directory

Computer Security Challenges

- Security is not simple
- Potential attacks on the security features need to be considered
- Procedures used to provide particular services are often counter-intuitive
- It is necessary to decide where to use the various security mechanisms
- Requires constant monitoring
- Is too often an afterthought

- **Security mechanisms typically involve more than a particular algorithm or protocol**
- **Security is essentially a battle of wits between a perpetrator and the designer**
- **Little benefit from security investment is perceived until a security failure occurs**
- **Strong security is often viewed as an impediment to efficient and user-friendly operation**

Outline

- ❑ Computer Security Concepts
- ❑ **The OSI Security Architecture**
- ❑ Security Attacks
- ❑ Security Services
- ❑ Security Mechanisms
- ❑ Fundamental Security Design Principles
- ❑ Attack Surfaces and Attack Trees
- ❑ A model for Network Security
- ❑ Standards

Overview

Security Attack

- action that compromises the security of information
- wide range of attacks

Security Mechanism

- mechanism to detect, prevent, or recover from security attack

Security Service

- service that enhances security of data processing systems and information transfers
- intended to counter security attacks
- make use of one or more security mechanisms

Threats and Attacks (RFC 4949)

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.

Security Service

- **a processing or communication service that is provided by a system to give a specific kind of protection to system resources [RFC 2828]**
- **a service, provided by a layer of communicating open systems, which ensures adequate security of the systems or of data transfers [OSI X.800]**
- **replicates functions normally associated with physical documents**
  such as:
  - discriminate between original and copy, determine modifications
  - proof and date of sending/receiving a document
  - ensure that document is read only by authorized persons
  - (notarized) signature

RFC 2828: Internet Security Glossary, May 2000 --> check out www.ietf.org
OSI X.800: Security Architecture for Open Systems Interconnection, 1991

Security Mechanism

- **a mechanism designed to detect, prevent, or recover from security attack**
- **a process (or a device incorporating such a process) that can be used in a system to implement a security service that is provided by or within the system [RFC 2828]**
- **examples are authentication exchange, checksum, digital signature, encryption, traffic padding**
- **no single mechanism is sufficient to achieve complete security**
- **many mechanisms are based on cryptographic techniques e.g., data encryption, hash functions, digital signatures**

Security Threat

According to RFC 2828

- a ***potential for violation of security***, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm
- a possible danger that might exploit a vulnerability
- either "intentional" (“intelligent”) or "accidental”
- U. S. Government usage:
  The technical and operational capability of a hostile entity to detect, exploit, or subvert friendly information systems and the demonstrated, presumed, or inferred intent of that entity to conduct such activity.
- “threat action”: assault on system security

Outline

- ❑ Computer Security Concepts
- ❑ The OSI Security Architecture
- ❑ Security Attacks
- ❑ Security Services
- ❑ Security Mechanisms
- ❑ Fundamental Security Design Principles
- ❑ Attack Surfaces and Attack Trees
- ❑ A model for Network Security
- ❑ Standards

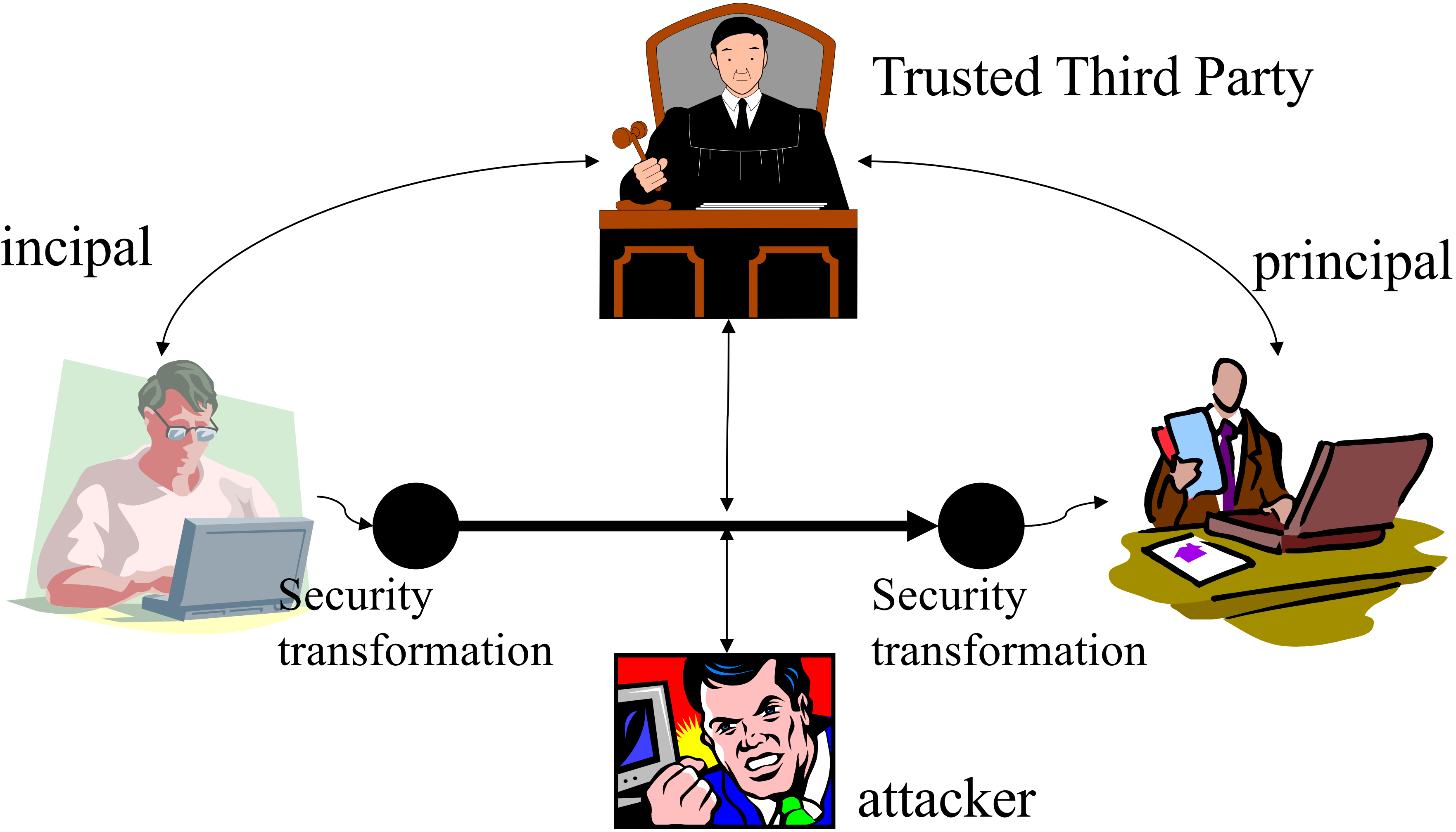
Security Attack

According to RFC 2828:

- an ***assault on system security*** that derives from an intelligent threat, i.e., 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
- “active” vs. “passive”
- “insider” vs. “outsider”

Note: “threat” and “attack” often mean the same thing

Network Security Model



Trusted Third Party

principal

principal

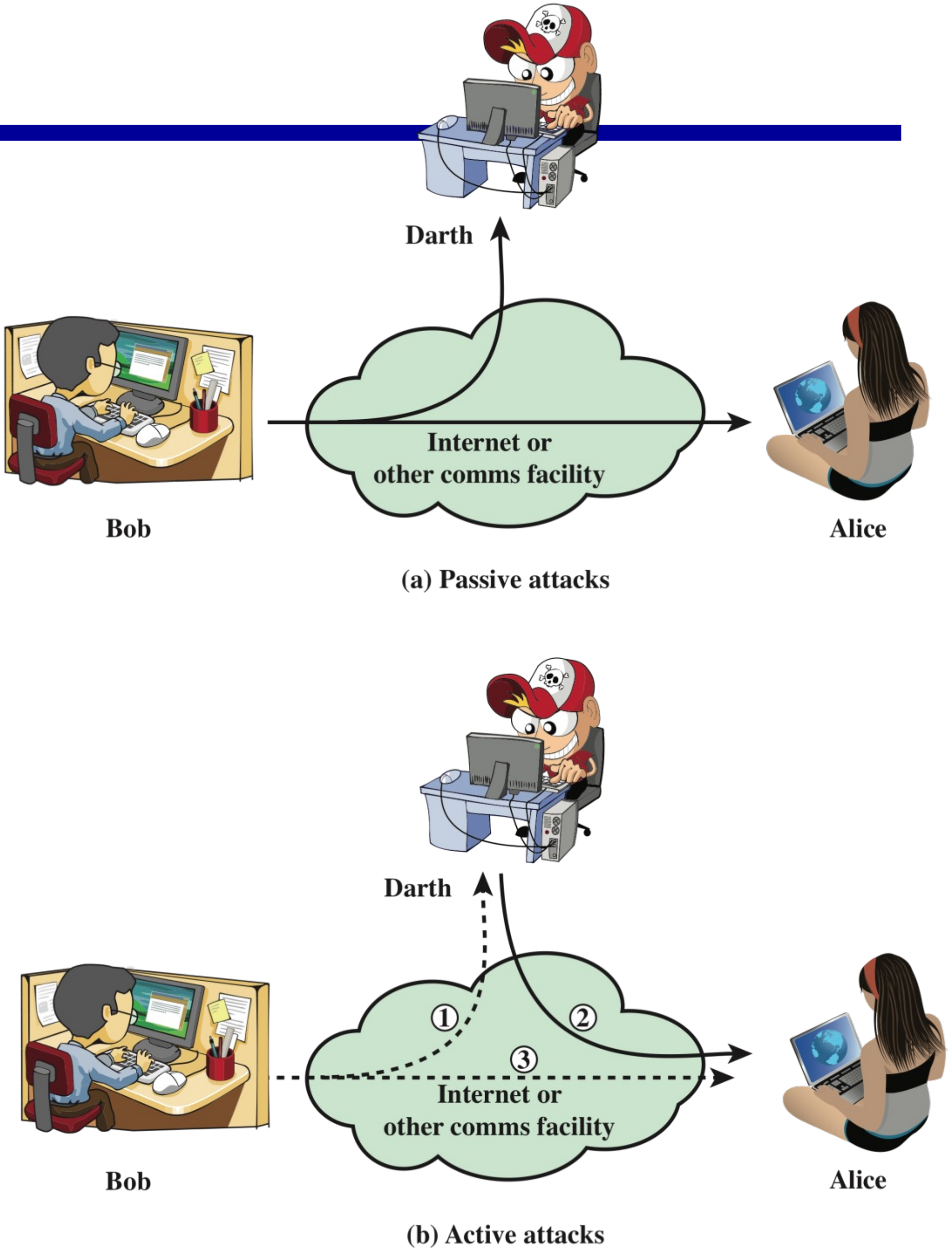
Security transformation

Security transformation

attacker

Attacks

- **Passive attacks**
  - Interception
    - Release of message contents
    - Traffic analysis
- **Active attacks**
  - Interruption, modification, fabrication
    - Masquerade
    - Replay
    - Modification
    - Denial of service


Darth
Bob
Internet or other comms facility
Alice
Darth
①
②
③
Bob
Internet or other comms facility
Alice

(a) Passive attacks

(b) Active attacks

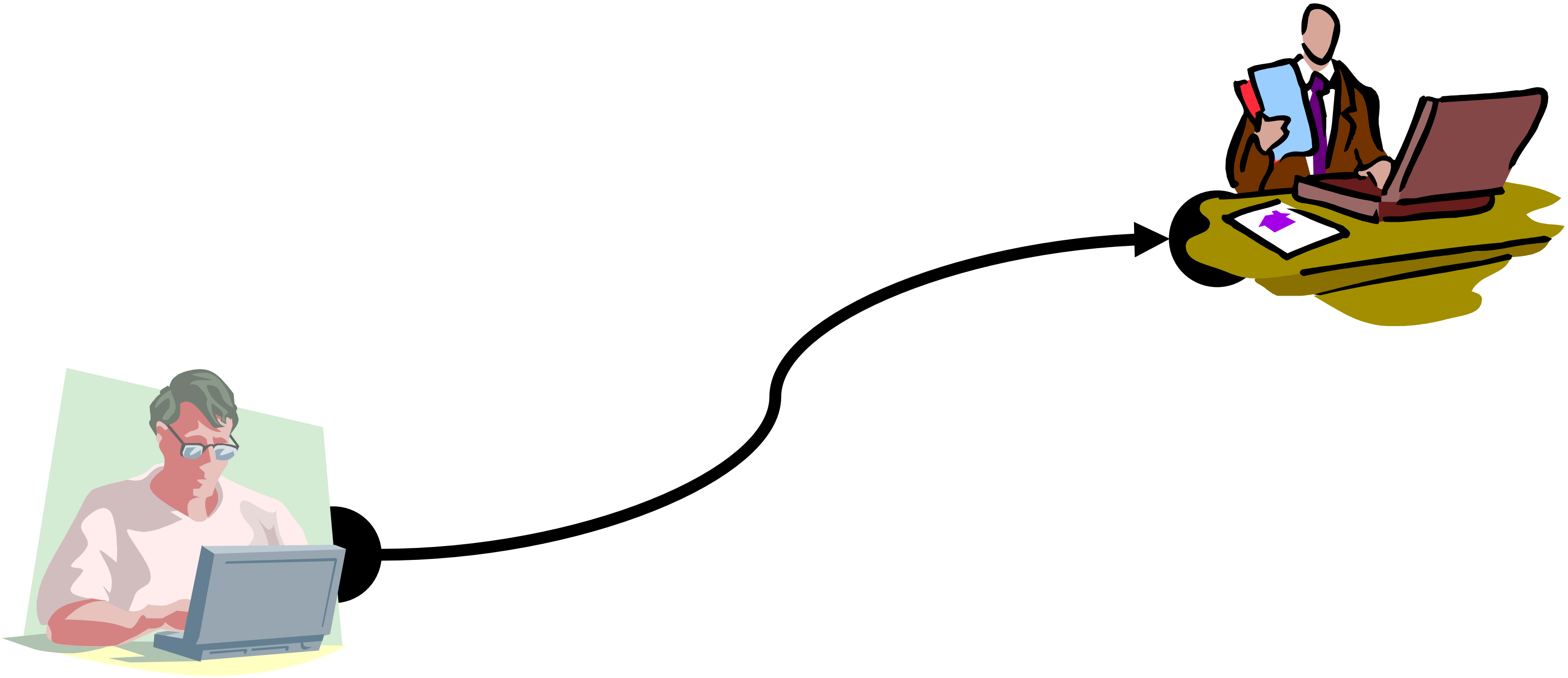
Figure 1.1 Security Attacks

Passive Attacks

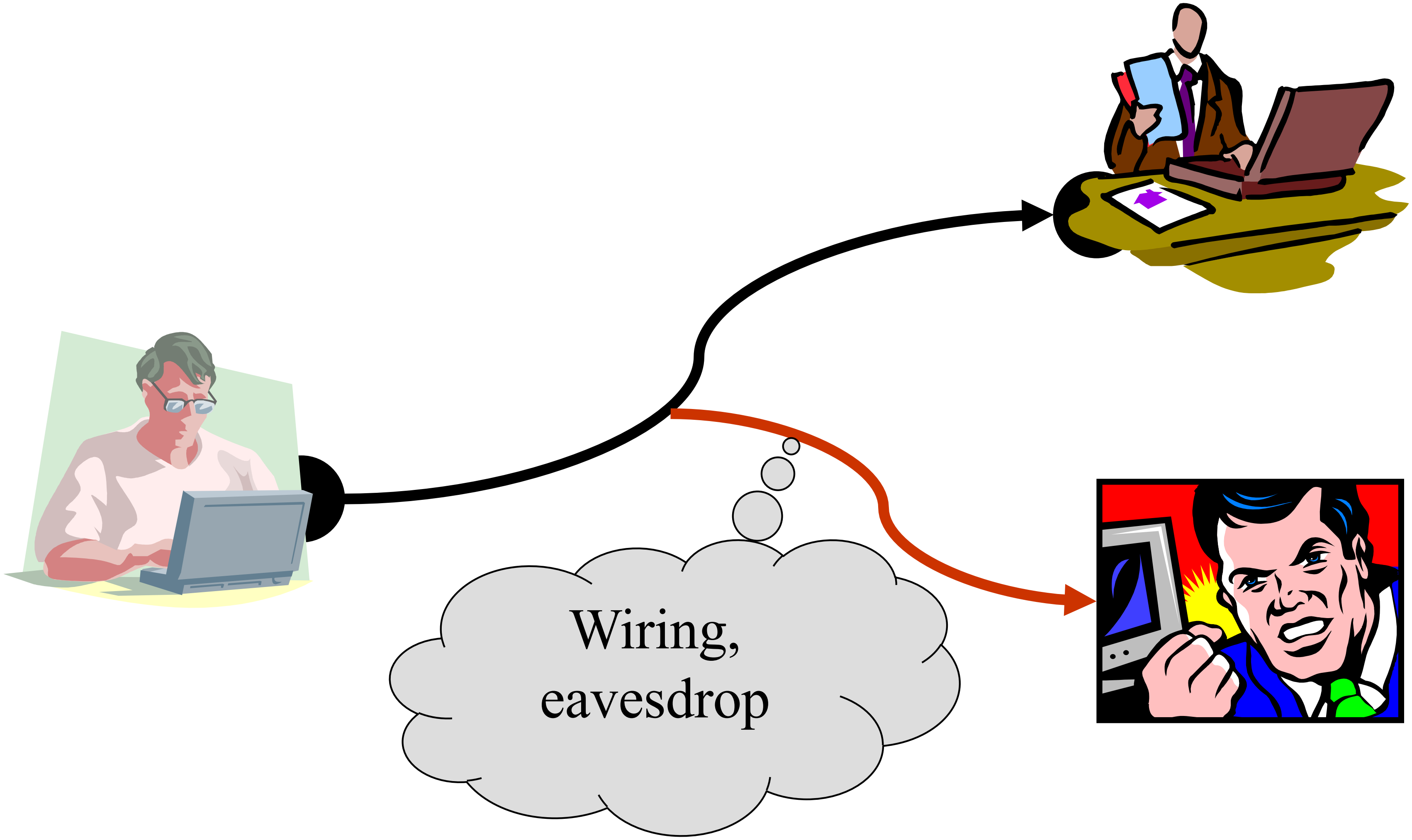
- **Are in the nature of eavesdropping on, or monitoring of, transmissions**
- **Goal of the opponent is to obtain information that is being transmitted**

- **Two types of passive attacks are:**
  - The release of message contents
  - Traffic analysis

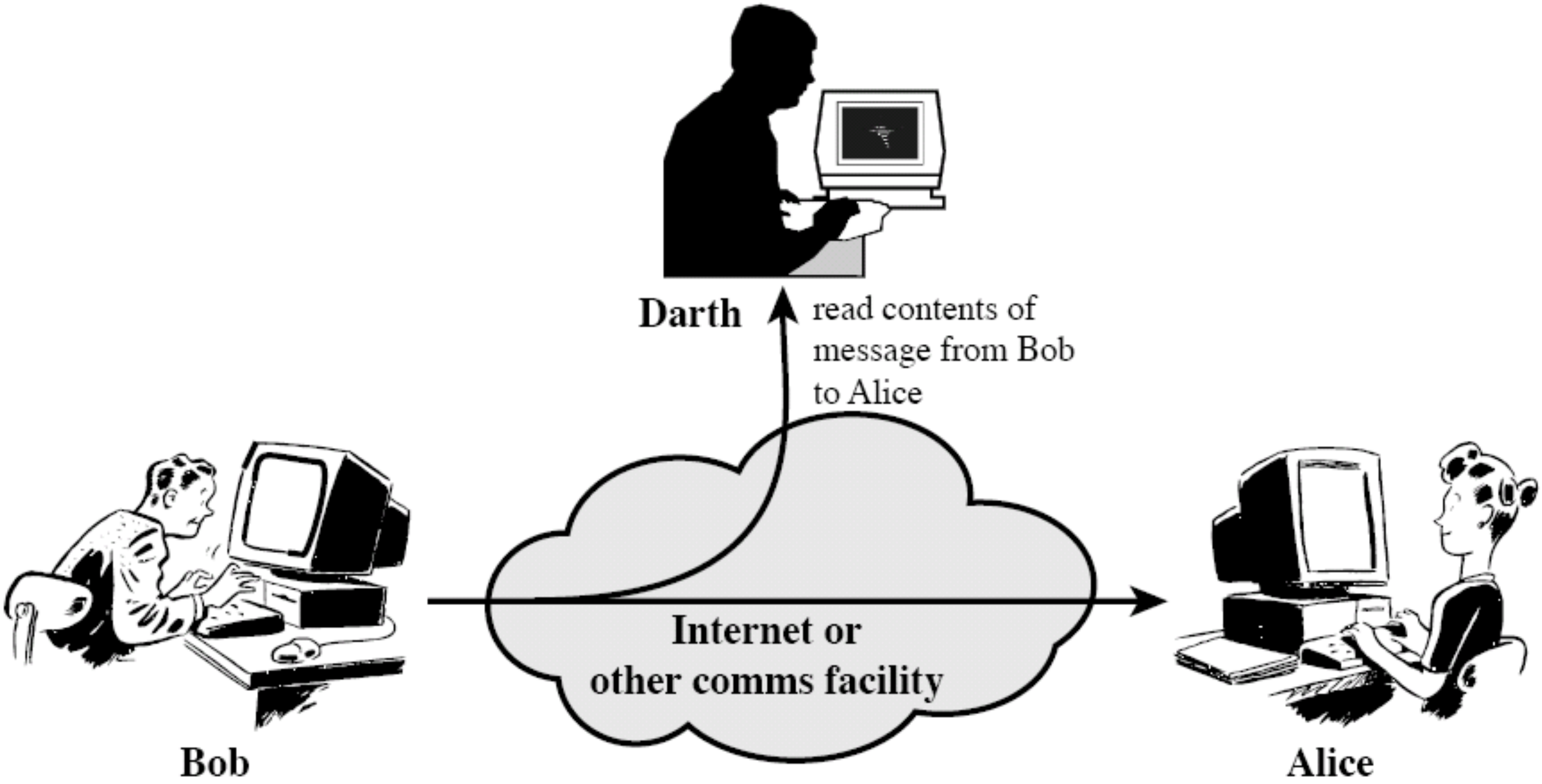
Information Transferring



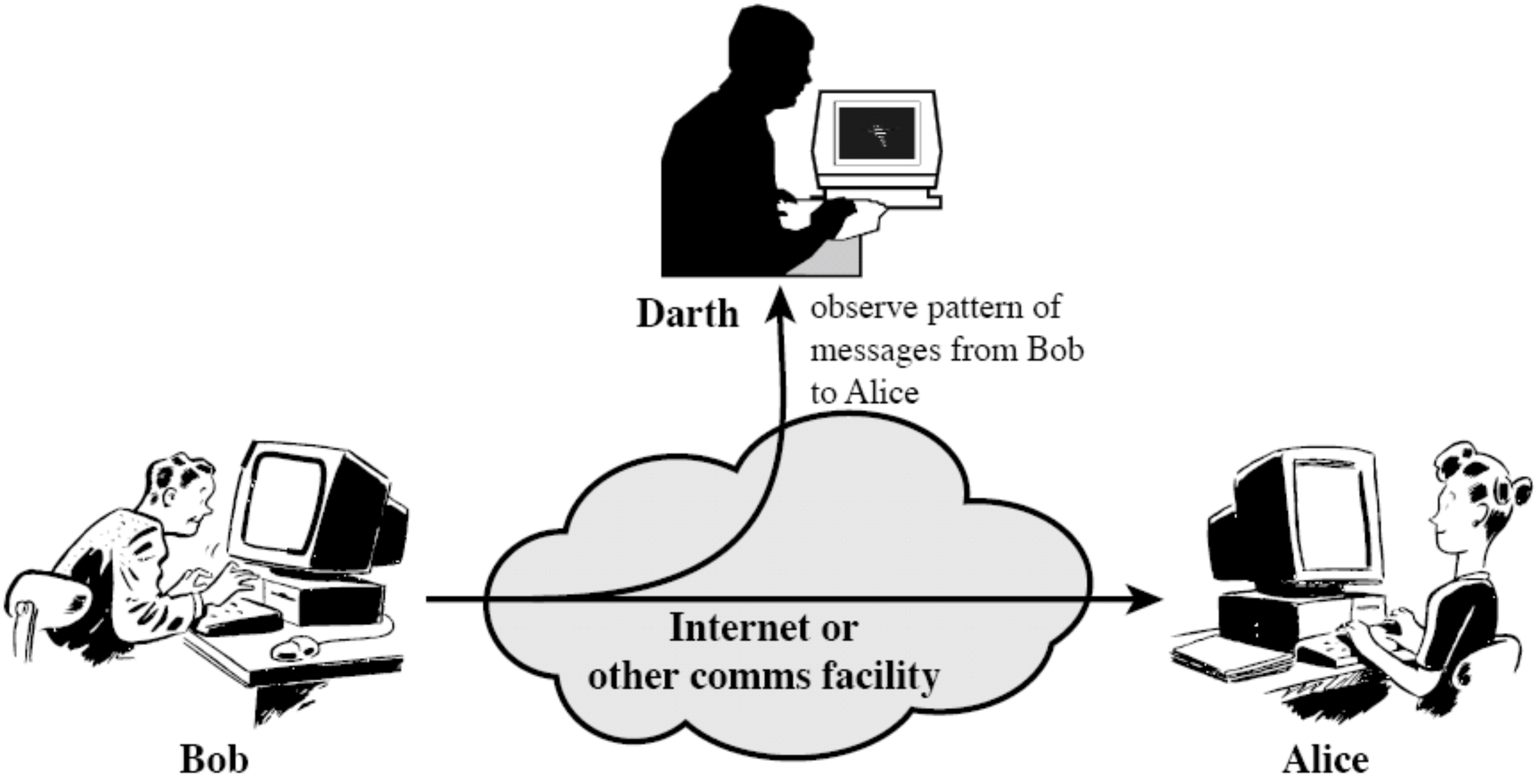
Passive Attack: Interception (snooping)



Passive Attack: Release of Message Contents



Passive Attack: Traffic Analysis


Darth
observe pattern of messages from Bob to Alice
Internet or other comms facility
Bob
Alice

Active Attacks

- **Involve some modification of the data stream or the creation of a false stream**
- **Difficult to prevent because of the wide variety of potential physical, software, and network vulnerabilities**
- **Goal is to detect attacks and to recover from any disruption or delays caused by them**

Masquerade

- Takes place when one entity pretends to be a different entity
- Usually includes one of the other forms of active attack

Replay

- Involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect

Modification of messages

- Some portion of a legitimate message is altered, or messages are delayed or reordered to produce an unauthorized effect

Denial of service

- Prevents or inhibits the normal use or management of communications facilities