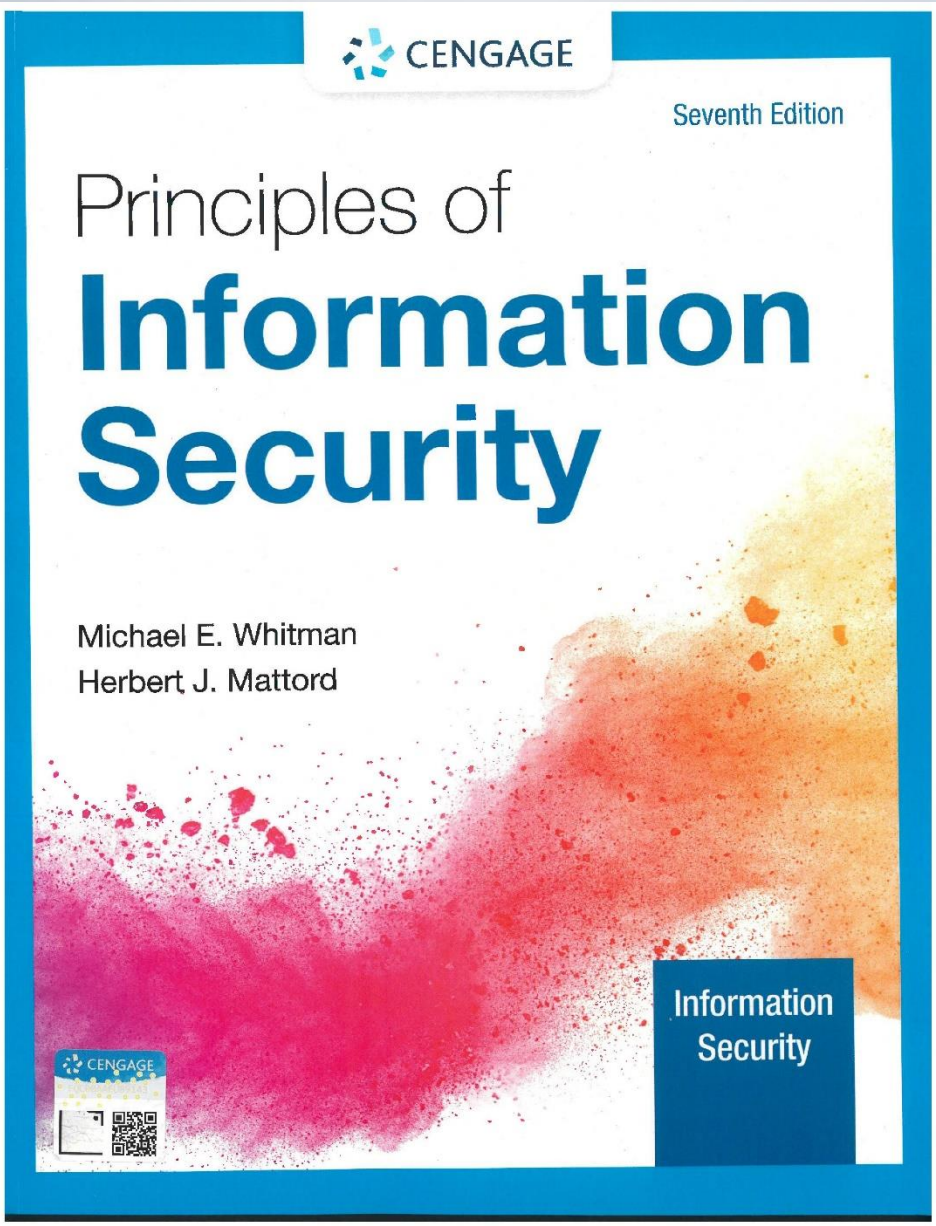
EE 5084
Cyber Security

Course Information

Contact Information

Part 1:	Week 1 to Week 7
Lecturer:	Dr Chan Chee Keong
School:	EEE
Office:	S1-B1b-51
Office Phone:	6790 5377
Email:	eckchan@ntu.edu.sg

Part 2:	Week 8 to Week 13
Lecturer:	Prof Mohammed Yakoob Siyal
Email:	eyakoob@ntu.edu.sg



Textbook

Principles of Information Security, 7th Edition

Michael E. Whitman and Herbert J. Mattord

Continuous Assessment (CA)

- Quiz 1 (OASIS, week 5, 8 Sep 2022) - 20%
- Quiz 2 (OASIS, week 11, 27 Oct 2022) - 20%
- Compulsory

Final Exam

- Closed-book
- 2 hours
- 60% of total marks
- All materials discussed in lectures

Principles of Information Security

Introduction to Information Security

Do not figure on opponents not attacking;
worry about your own lack of preparation.

BOOK OF THE FIVE RINGS

Learning Objectives

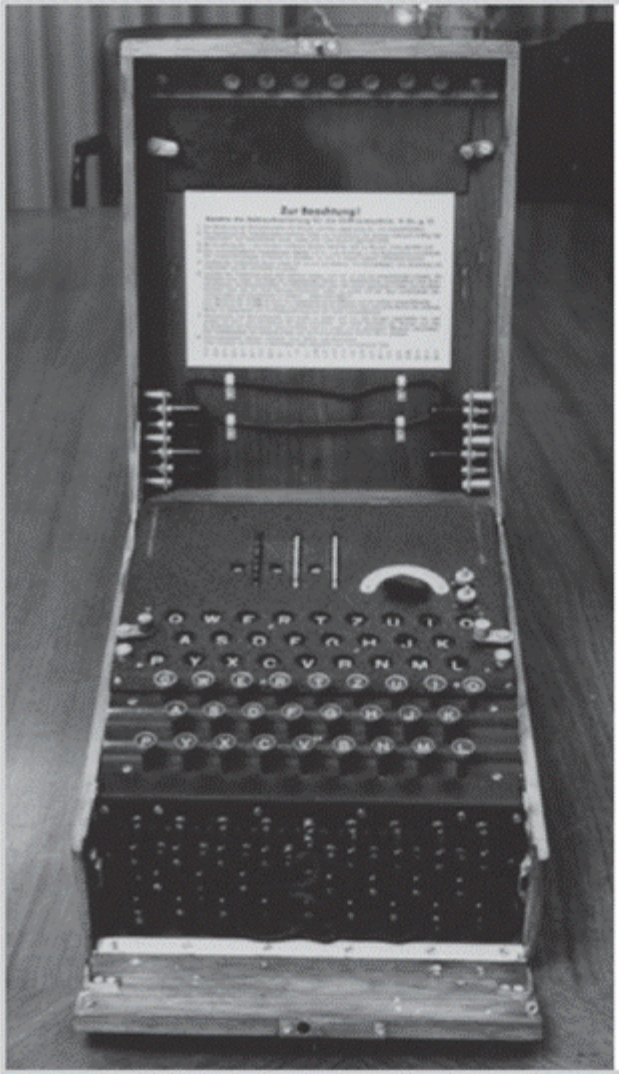
- Recount the history of computer security and how it evolved into information security
- Define information security
- Define key terms and critical concepts of information security
- Describe the information security roles of professionals within an organization

Definition

Information security: defending information from unauthorized access, use, disclosure, disruption, modification, or destruction

The History of Information Security

- Computer security began immediately after the first mainframes were developed.
  - Groups developing code-breaking computations during World War II created the first modern computers.
  - Multiple levels of security were implemented.
- Physical controls limiting access to sensitive military locations to authorized personnel
- Rudimentary in defending against physical theft, espionage, and sabotage



Earlier versions of the German code machine Enigma were first broken by the Poles in the 1930s. The British and Americans managed to break later, more complex versions during World War II. The increasingly complex versions of the Enigma, especially the submarine or *Unterseeboot* version of the Enigma, caused considerable anguish to Allied forces before finally being cracked. The information gained from decrypted transmissions was used to anticipate the actions of German armed forces. "Some ask why, if we were reading the Enigma, we did not win the war earlier. One might ask, instead, when, if ever, we would have won the war if we hadn't read it."

Figure 1-1 The Enigma[1]

Source: National Security Agency. Used with permission.[2]

The 1960s

- Advanced Research Project Agency (ARPA) began to examine the feasibility of redundant networked communications.
- Larry Roberts, founder of the Internet, developed the ARPANET

The 1970s and 80s

- ARPANET grew in popularity, so did the potential for abuse
- Fundamental problems with ARPANET
  - No safety procedures for dial-up connections to ARPANET
  - Nonexistent user identification and authorization to system
- Late 1970s: microprocessor expanded computing capabilities and security threats

The 1970s and 80s (cont'd)

- The Rand Report R-609 - paper that started the study of computer security and identified the role of management and policy issues in it
- The scope of computer security grew from physical security to include:
  - Securing the data
  - Limiting random and unauthorized access to data
  - Involving personnel from multiple levels of the organization in information security

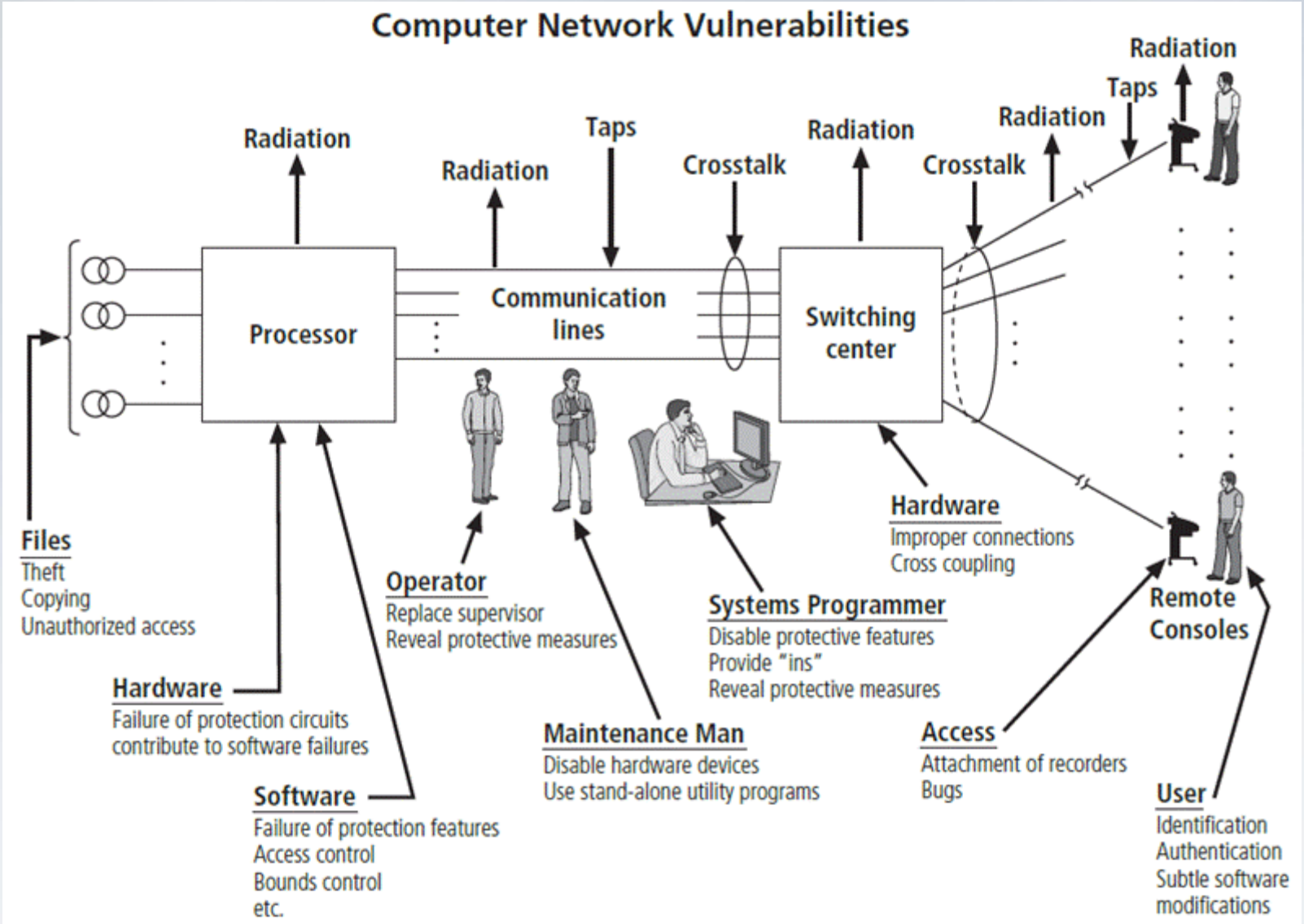


Figure 1-4 Illustration of computer network vulnerabilities from Rand Report R-609

Source: Rand Report R-609. Used with permission.[10]

MULTICS

- Early research focus - Multiplexed Information and Computing Service (MULTICS).
- First operating system was created with security integrated into core functions.
- Mainframe, time-sharing OS was developed in the mid-1960s by General Electric (GE), Bell Labs, and Massachusetts Institute of Technology (MIT).
- Several MULTICS key players created UNIX.
  - Primary purpose of UNIX was text processing

The 1990s

- Networks of computers became prevalent in response to the need to connect them to one another
- Internet became the first global network of computers
- In early Internet deployments, security was treated as a low priority.

2000 to Present

- The Internet brings millions of computer networks into communication with each other—many of them unsecured
- The security of data in a computer was affected by the security of every computer to which it is connected.
- There is a growing threat of cyber attacks
  - increased the awareness of need for improved security.
  - Nation-states engaging in information warfare

Computer 'Nerd' Jailed in Jan. 2003 for Global Virus Attack

- Simon Vallor, a Welsh Web designer and hacker, created one of the most widespread viruses.
- Vallor admitted releasing Gokar
- Gokar: the third most prevalent virus, at one point infecting hundreds of thousands of computers in 46 countries. It clogged networks and crashed computers.
- All were in the form of email attachments.
- When the email was opened, Gokar sent itself to addresses in the user's email directory.
- Crime: violating Computer Misuse Act.
- His plea: guilty.
- His sentence: 2 years in jail.
- Reason for his capture: He boasted in an chat room that "at last there's a Welsh virus" and used his traceable Internet name *Gobo.*
- Like many hackers, he craved fame, which helps law enforcement capture these criminals.

Components of an Information System

- Information system (IS) is an entire set of components necessary to use information as a resource in the organization
  - Software
  - Hardware
  - Data
  - People
  - Procedures
  - Networks

Security Layers

- A successful organization should have multiple layers of security in place to protect:
  - Operations
  - Physical infrastructure
  - People
  - Functions
  - Communications
  - Information

Definition of Security

- Protection of information and its critical elements, including systems and hardware that use, store, and transmit that information
- Covers information security management, data security, and network security
- C.I.A. triangle
  - Is a standard based on confidentiality, integrity, and availability, now viewed as inadequate.
  - Expanded model consists of a list of critical characteristics of information.

C. I. A

The protection afforded to an automated information system connected to internet in order to attain the applicable objectives of preserving the:

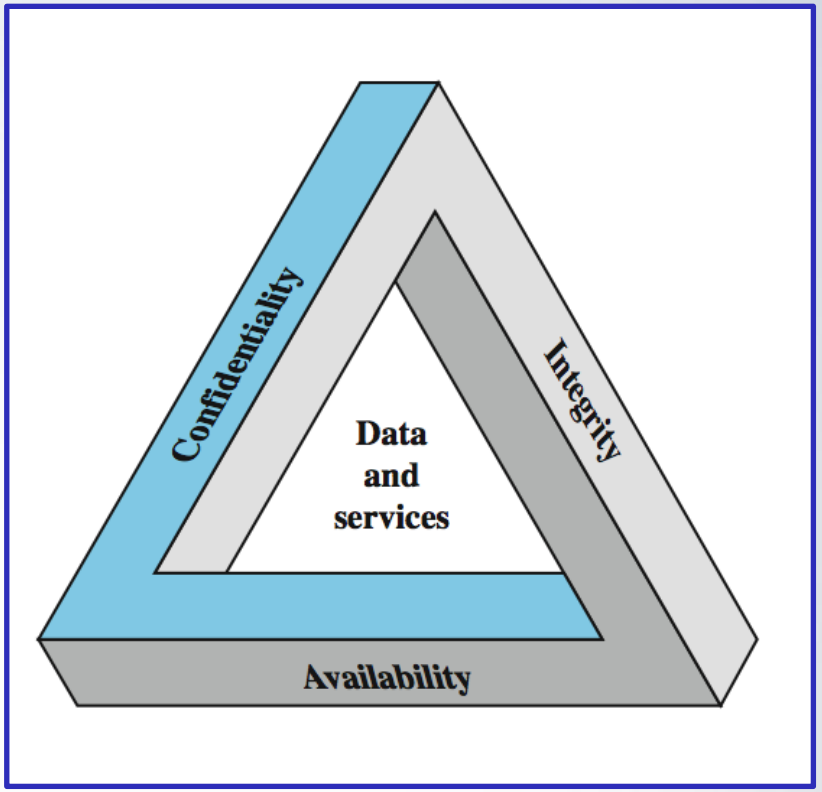
Confidentiality

Integrity

Availability

of information system resources

- Software
- Firmware
- Information/data
- Telecommunications



Examples of Security Requirements

Confidentiality – student grades

Integrity – patient information

Availability – authentication services

Critical Characteristics of Information(1)

- The value of information comes from the characteristics it possesses:
  - Availability
  - Accuracy
  - Authenticity
  - Confidentiality
  - Integrity
  - Utility
  - Possession

Critical Characteristics of Information (2)

- **Availability** enables users who need to access information to do so without interference or obstruction and to retrieve that information in the required format.
- **Accuracy** occurs when information is free from mistakes or errors and has the value that the end user expects. If information contains a value different from the user's expectations due to the intentional or unintentional modification of its content, it is no longer accurate.
- **Authenticity** is the quality or state of being genuine or original, rather than a reproduction or fabrication. Information is authentic when it is the information that was originally created, placed, stored, or transferred.

Critical Characteristics of Information (3)

- **Confidentiality** is the quality or state of preventing disclosure or exposure to unauthorized individuals or systems.
- **Integrity** is the quality or state of being whole, complete, and uncorrupted. The integrity of information is threatened when the information is exposed to corruption, damage, destruction, or other disruption of its authentic state.
- **Utility** is the quality or state of having value for some purpose or end. Information has value when it serves a particular purpose. This means that if information is available, but not in a format meaningful to the end user, it is not useful.
- **Possession** is an attribute of information that describes how the data's ownership or control is legitimate or authorized

Key Information Security Concepts

- Access
- Asset
- Attack
- Control, safeguard, or countermeasure
- Exploit
- Exposure
- Loss
- Protection profile or security posture
- Risk
- Subjects and objects
- Threat
- Threat agent
- Vulnerability

Key Information Security Concepts (cont'd)

- A computer can be the subject of an attack and/or the object of an attack.
  - When the subject of an attack, the computer is used as an active tool to conduct attack.
  - When the object of an attack, the computer is the entity being attacked.

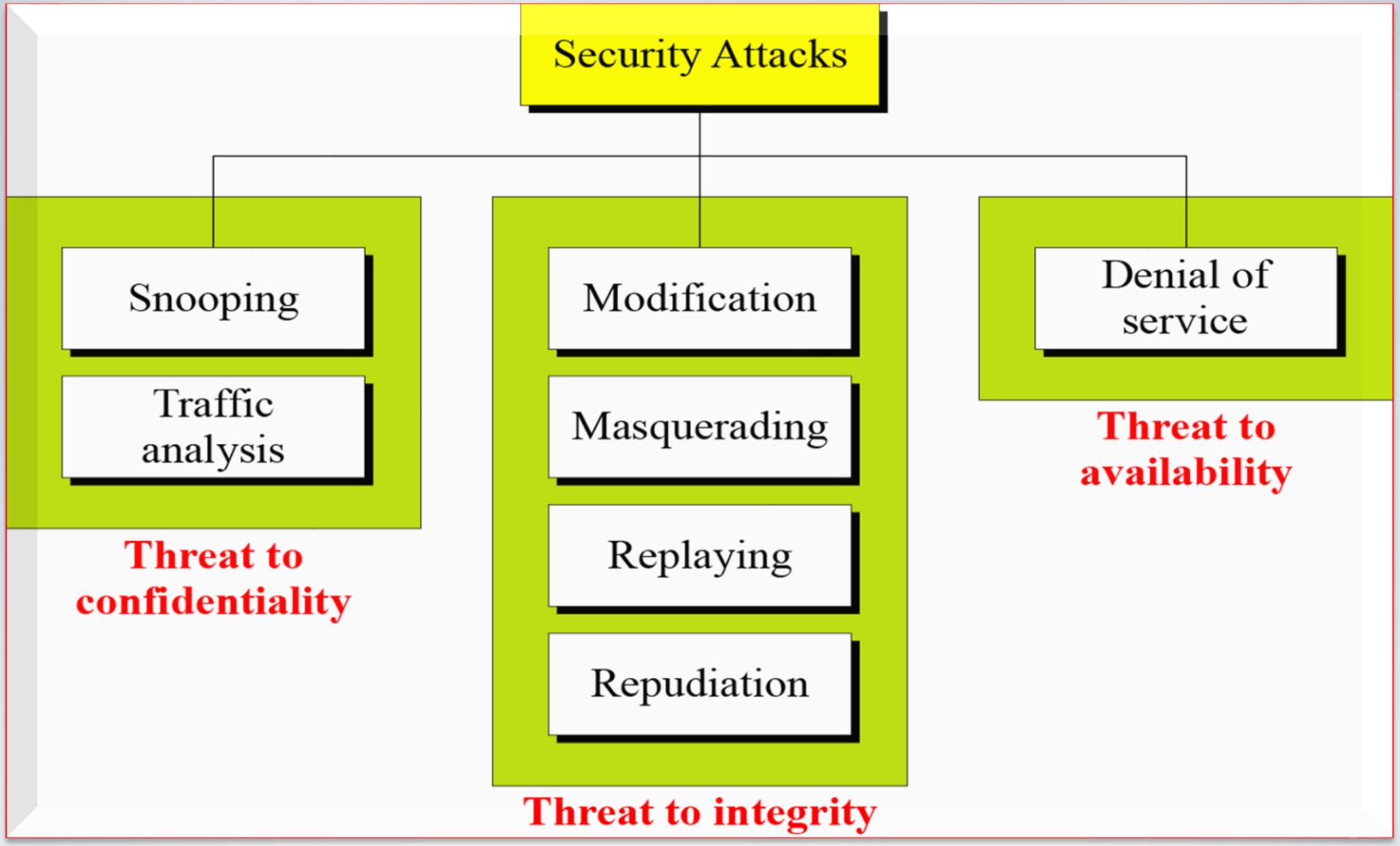
Threats and Attacks

Can be:

- Intentional (by hackers) OR
- Unintentional (eg., lightning strike)

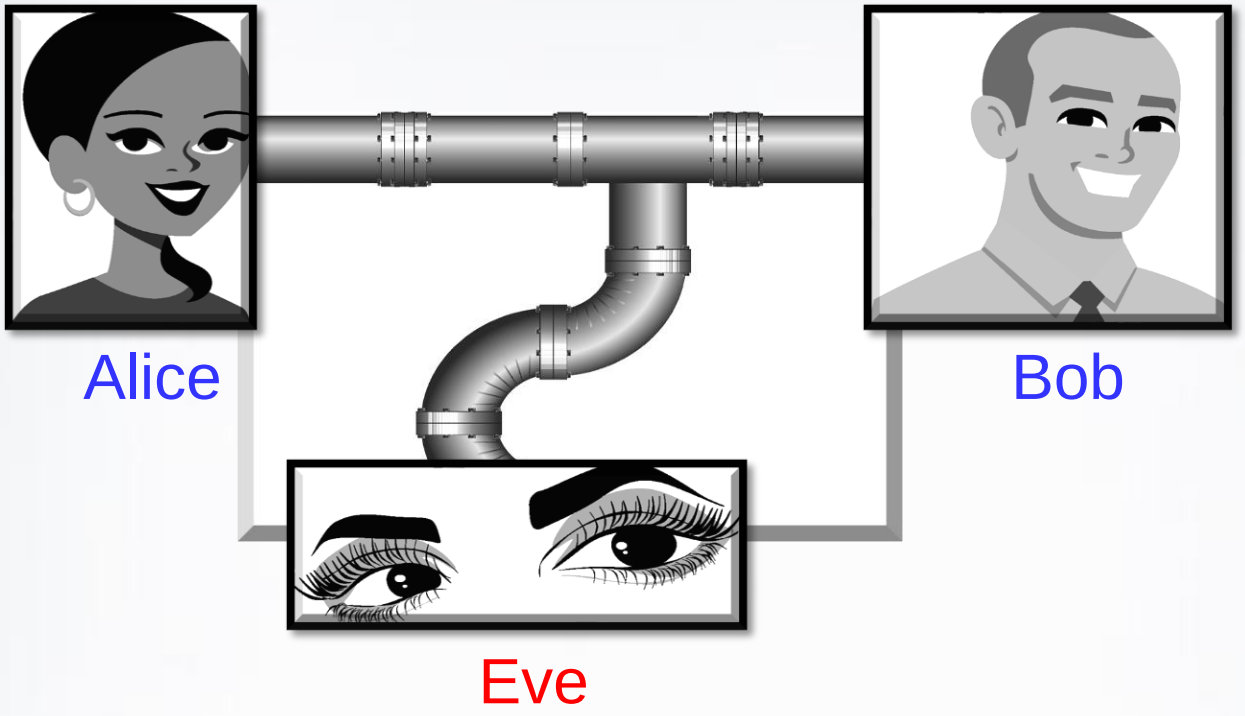
- Passive (snooping/eavesdropping or traffic analysis) OR
- Active (modification, masquerading, replaying or repudiation)

- Direct (by hacker pc) OR
- Indirect (via compromised computers, eg., distributed Denial of Services)


Security Attacks
Snooping
Traffic analysis
Threat to confidentiality
Modification
Masquerading
Replaying
Repudiation
Threat to integrity
Denial of service
Threat to availability

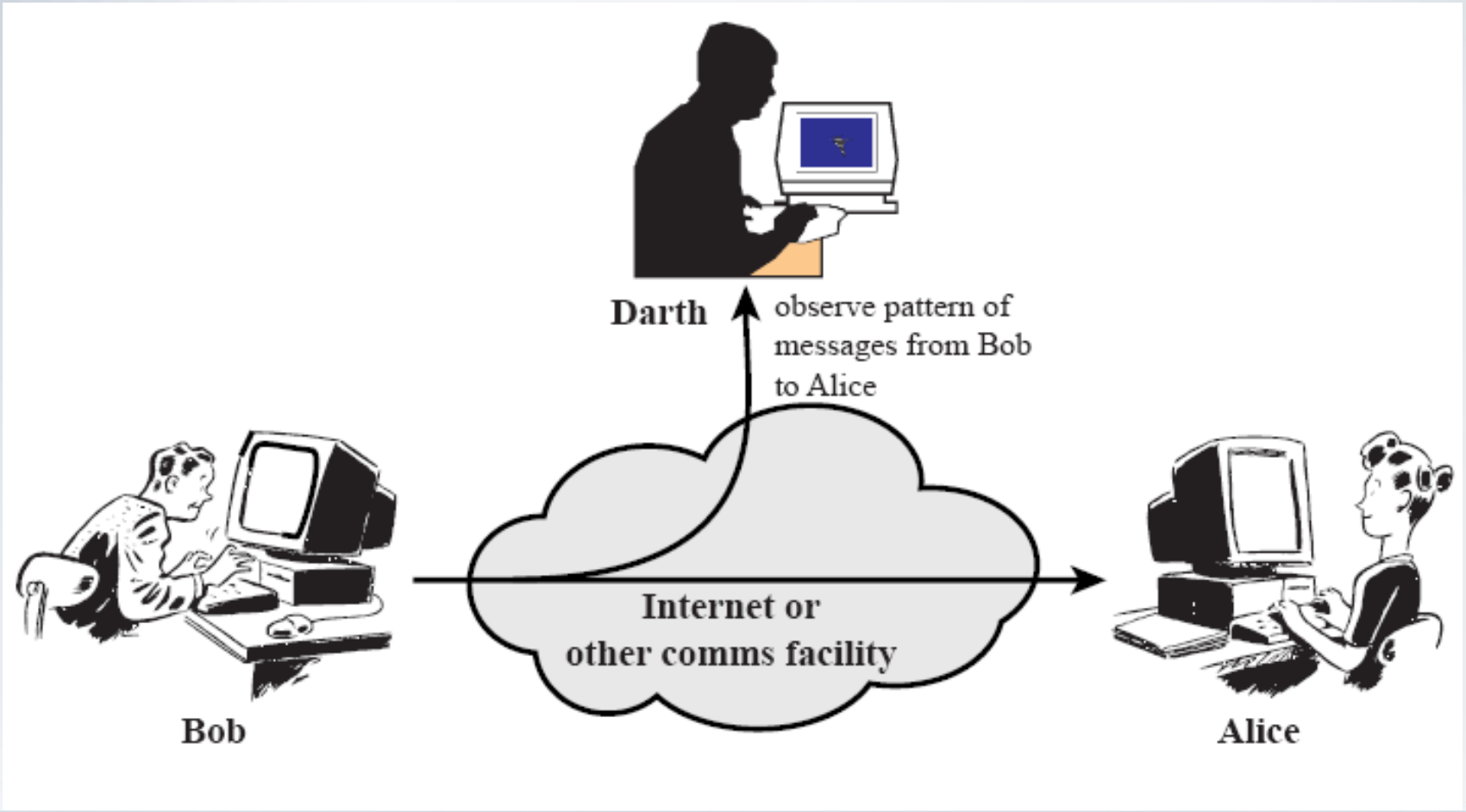
Threats and Attacks

- **SNOOPING/EAVESDROPPING**
  - The interception of information intended for someone else during its transmission over a communication channel.



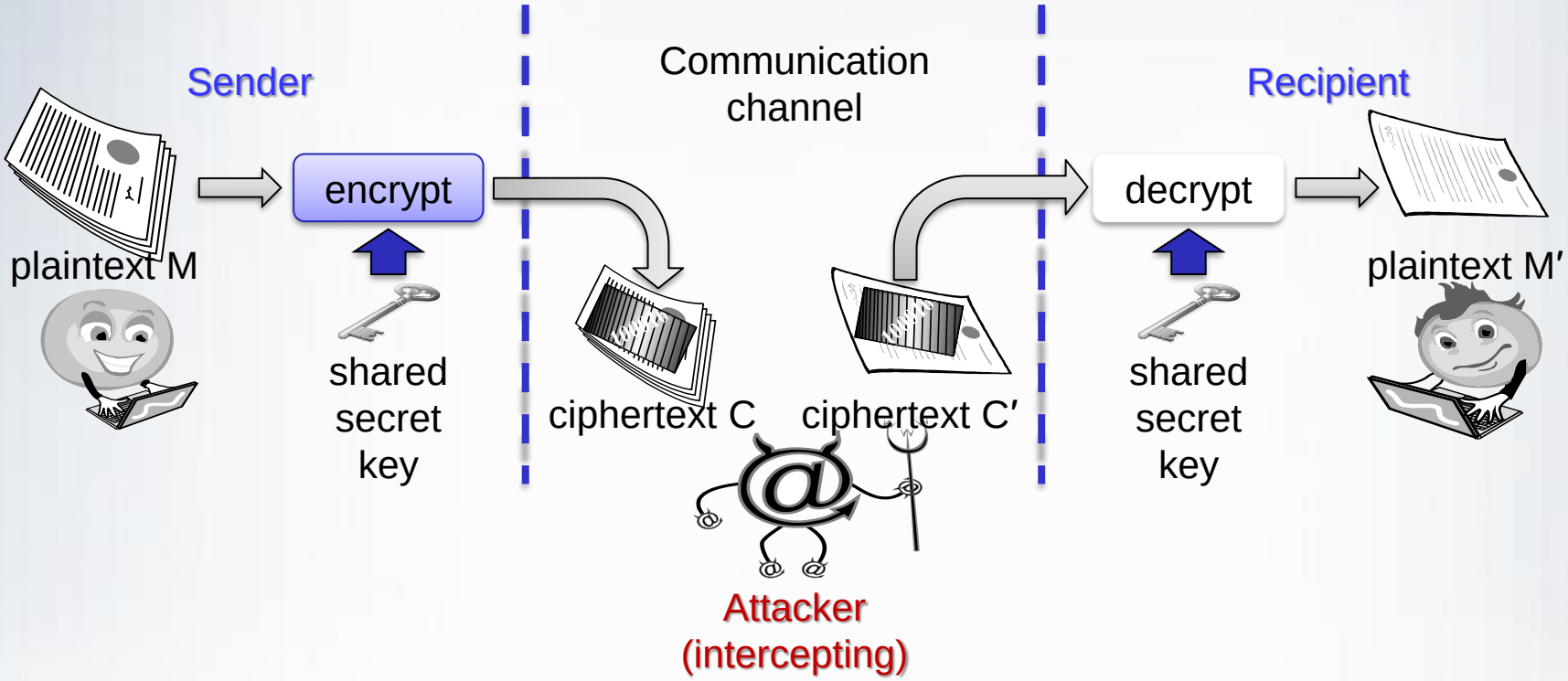
Threats and Attacks

- **TRAFFIC ANALYSIS**
  - Observe patterns of message



Threats and Attacks

- **ALTERATION OR MODIFICATION**
  - Unauthorized modification of information.
    - **Example:** The man-in-the-middle attack, where a network stream is intercepted, modified, and retransmitted.



Threats and Attacks

MASQUERADING

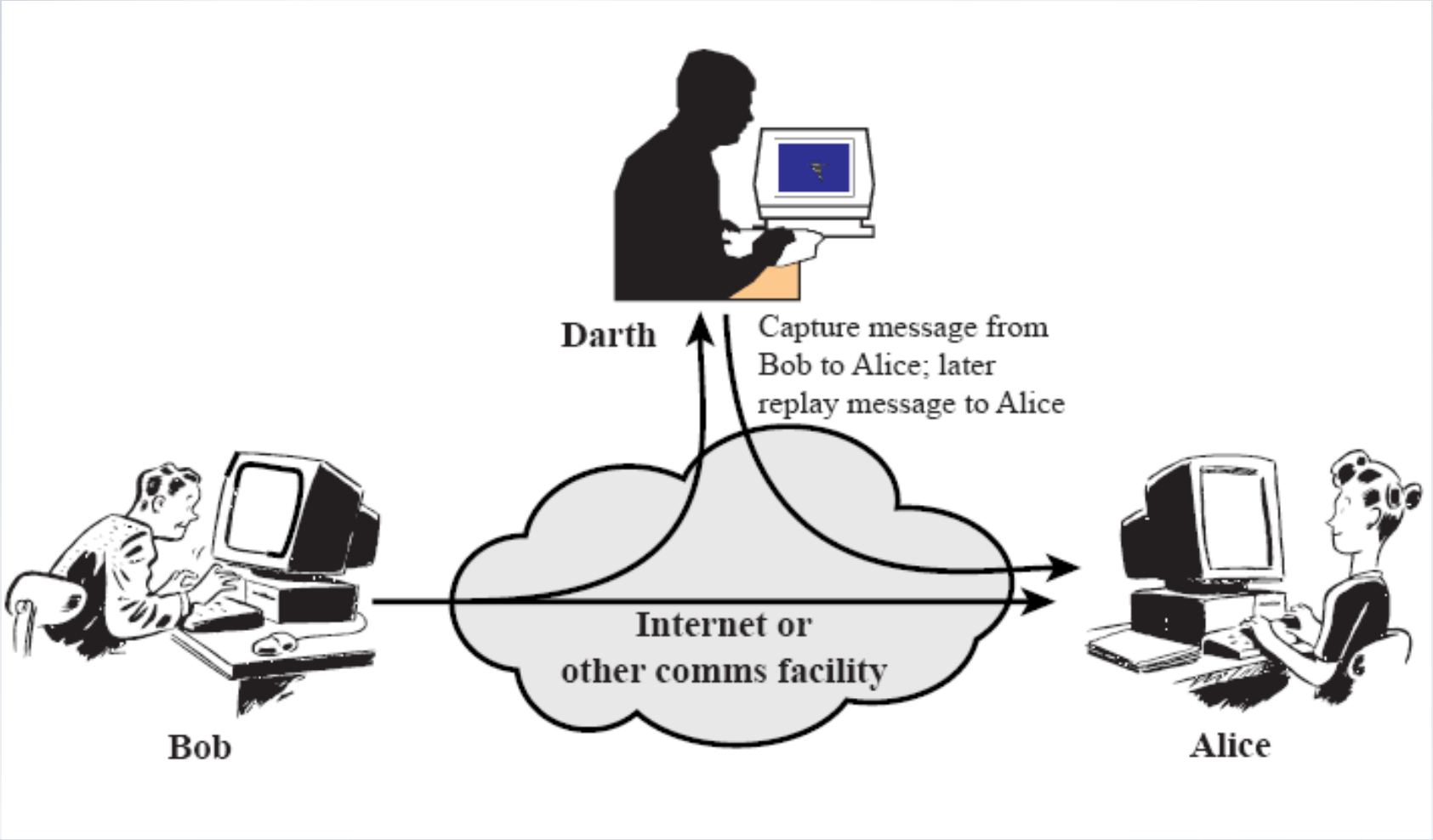
The fabrication of information that is purported to be from someone who is not actually the author.

"From: Alice"

(really is from Eve)

Threats and Attacks

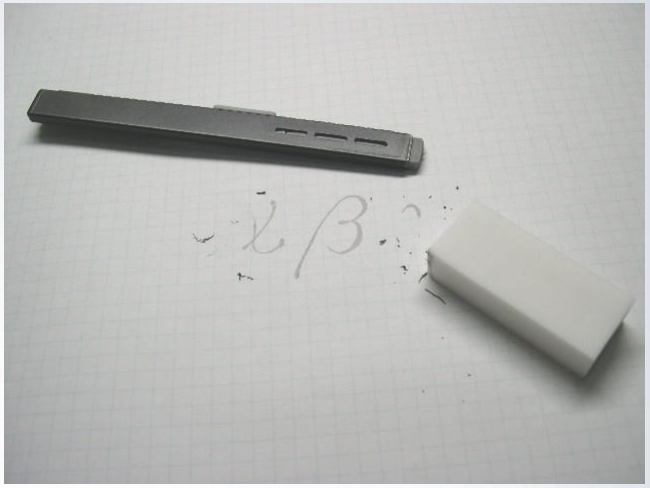
- **REPLAYING**
  - Capture message then replay later



Threats and Attacks

REPUDIATION

The denial of a commitment or data receipt. This involves an attempt to back out of a contract or a protocol that requires the different parties to provide receipts acknowledging that data has been received.



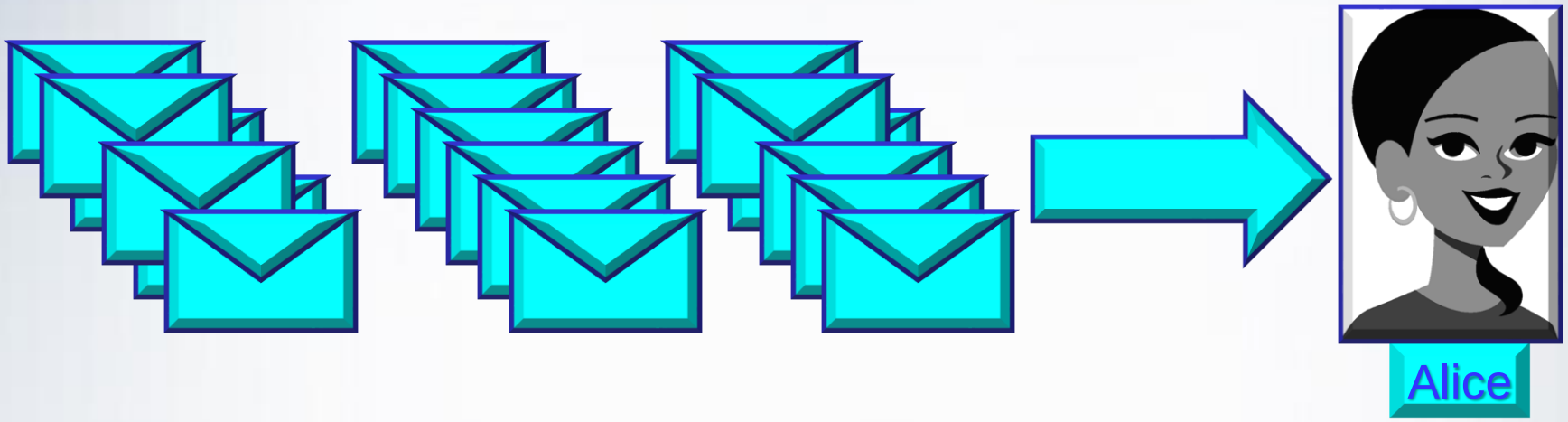
A repudiation attack happens when an application or system does not adopt controls to properly track and log users' actions, thus permitting malicious manipulation or forging the identification of new actions. This attack can be used to change the authoring information of actions executed by a malicious user in order to log wrong data to log files. Its usage can be extended to general data manipulation in the name of others, in a similar manner as spoofing mail messages. If this attack takes place, the data stored on log files can be considered invalid or misleading.

Nonrepudiation is the assurance that someone cannot deny something. Typically, nonrepudiation refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.

To repudiate means to deny. For many years, authorities have sought to make repudiation impossible in some situations. You might send registered mail, for example, so the recipient cannot deny that a letter was delivered. Similarly, a legal document typically requires witnesses to signing so that the person who signs cannot deny having done so.

Threats and Attacks

- **DENIAL-OF-SERVICE**
  - The interruption or degradation of a data service or information access.
  - **Example:** Email spam, to the degree that it is meant to simply fill up a mail queue and slow down an email server.

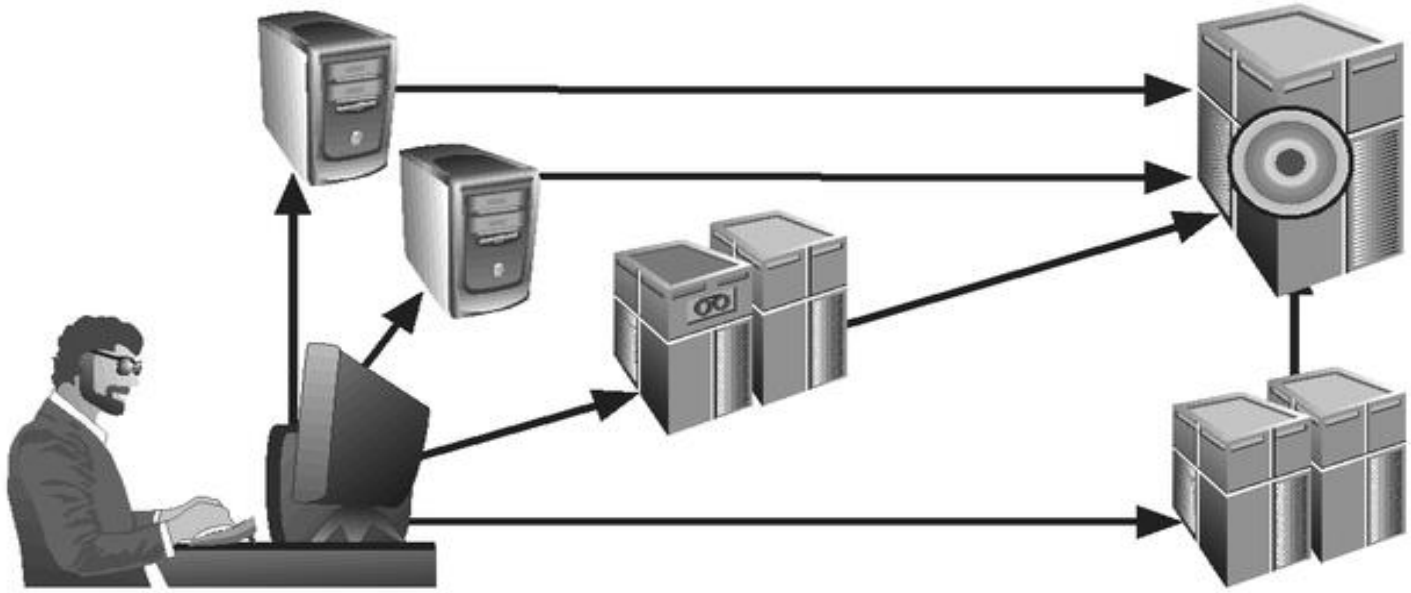


Threats and Attacks

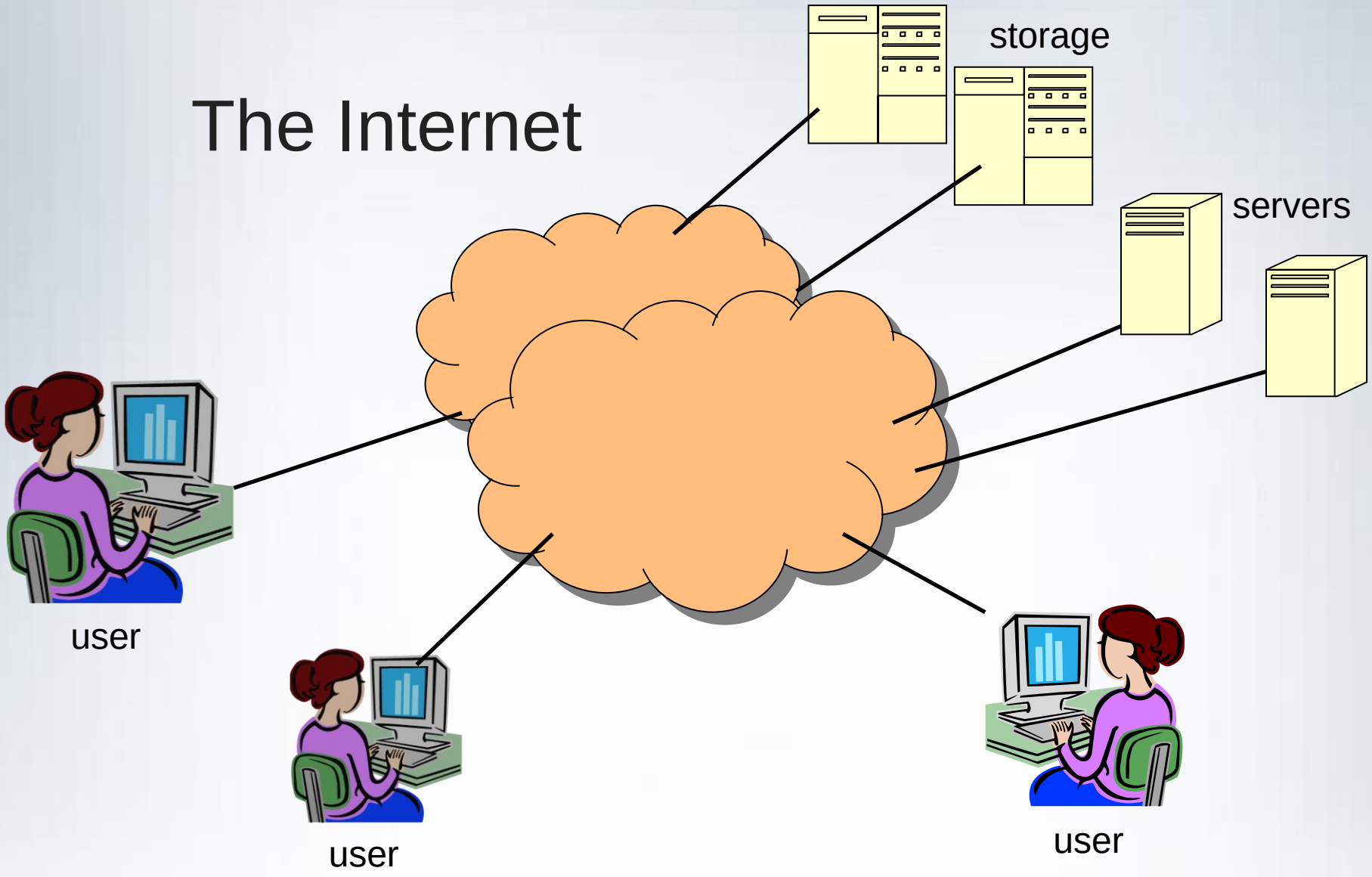
- **DISTRIBUTED DENIAL-OF-SERVICE**

In a denial-of-service attack, a hacker compromises a system and uses that system to attack the target computer, flooding it with more requests for services than the target can handle.

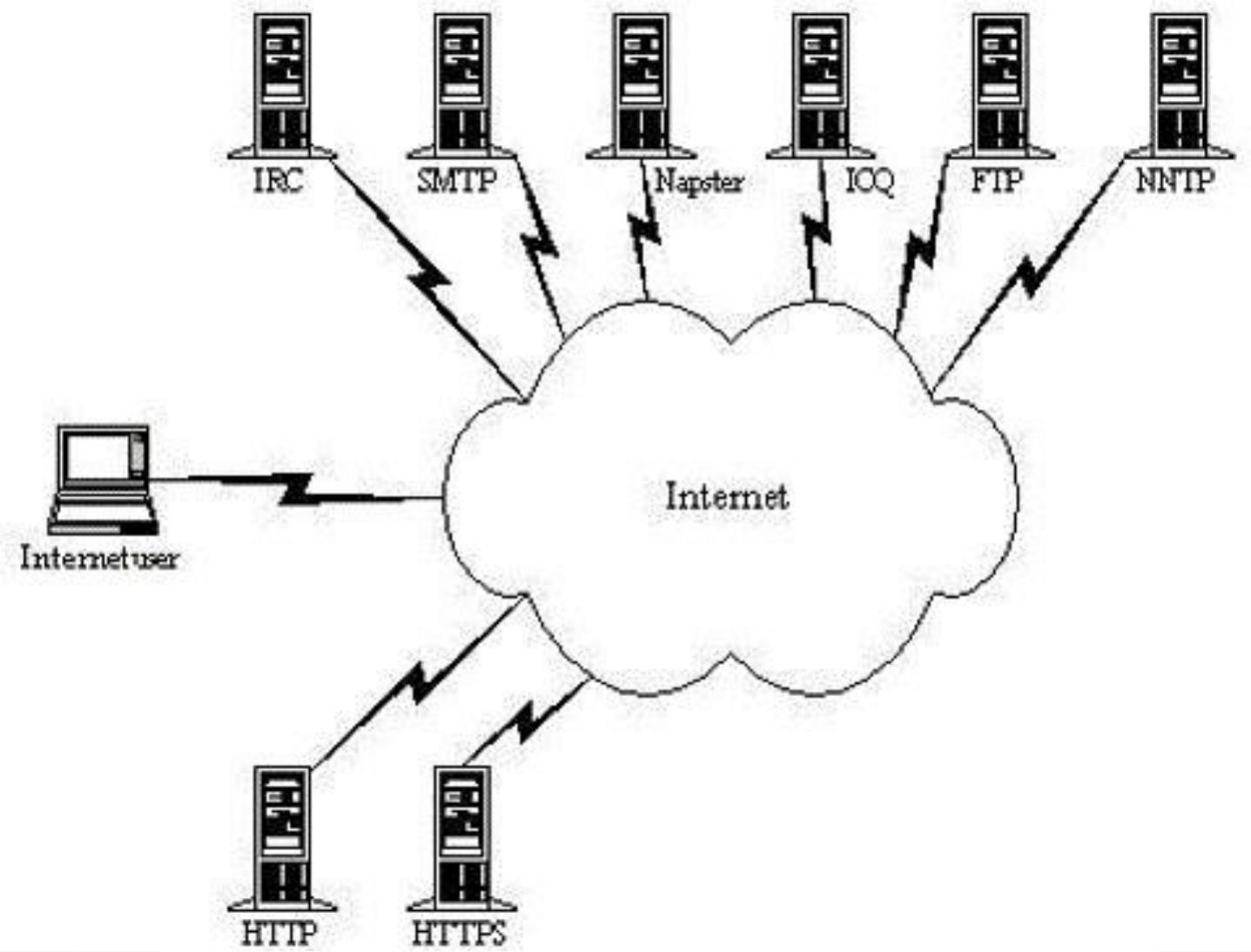
In a distributed denial-of-service attack, dozens or even hundreds of computers (known as zombies) are compromised, loaded with DoS attack software and then remotely activated by the hacker to conduct a coordinated attack.



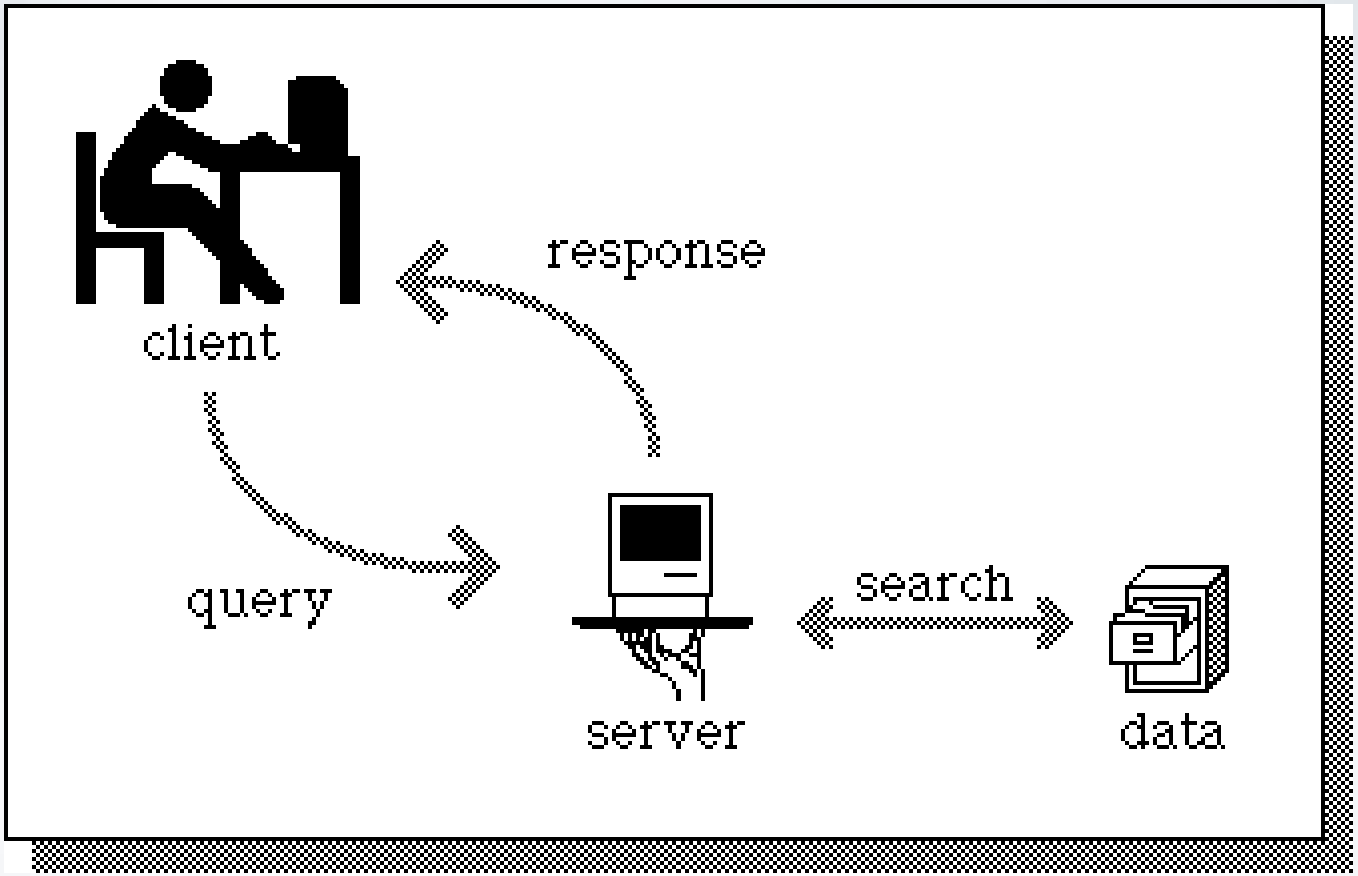
The Internet



The Internet – users and servers

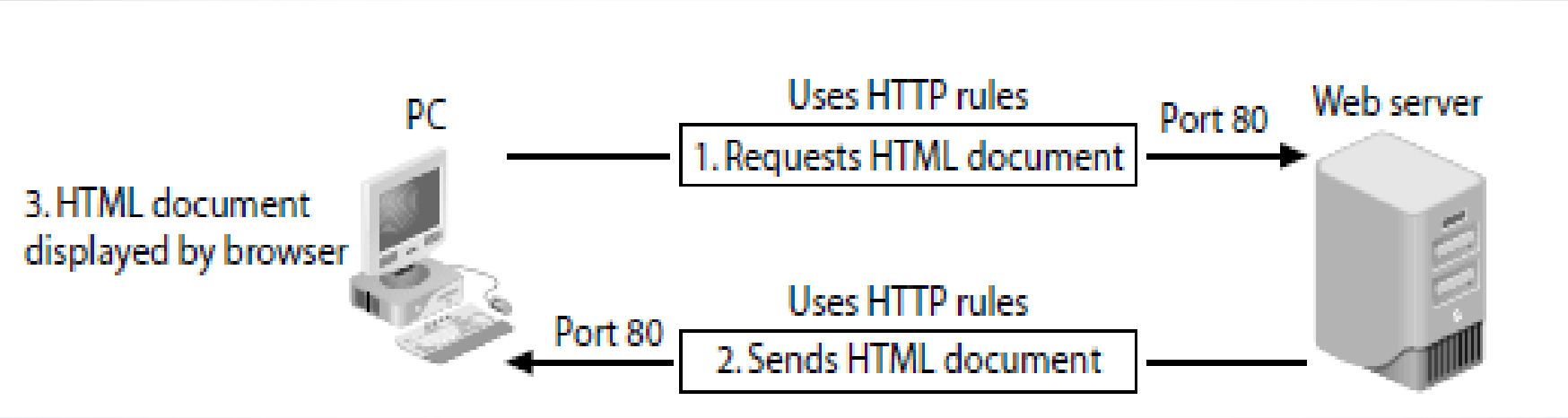


Server-Client – internet/intranet

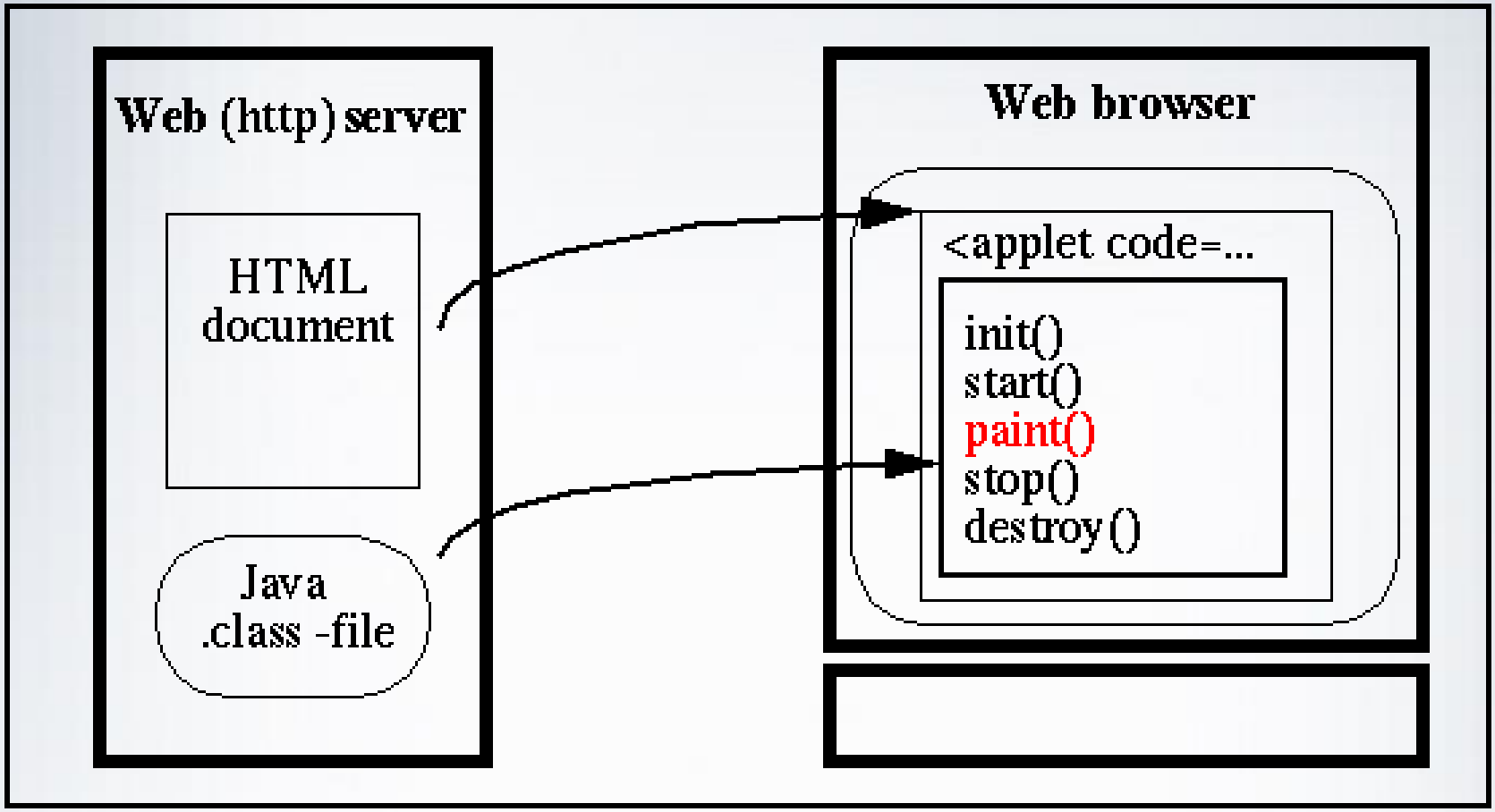


The World Wide Web

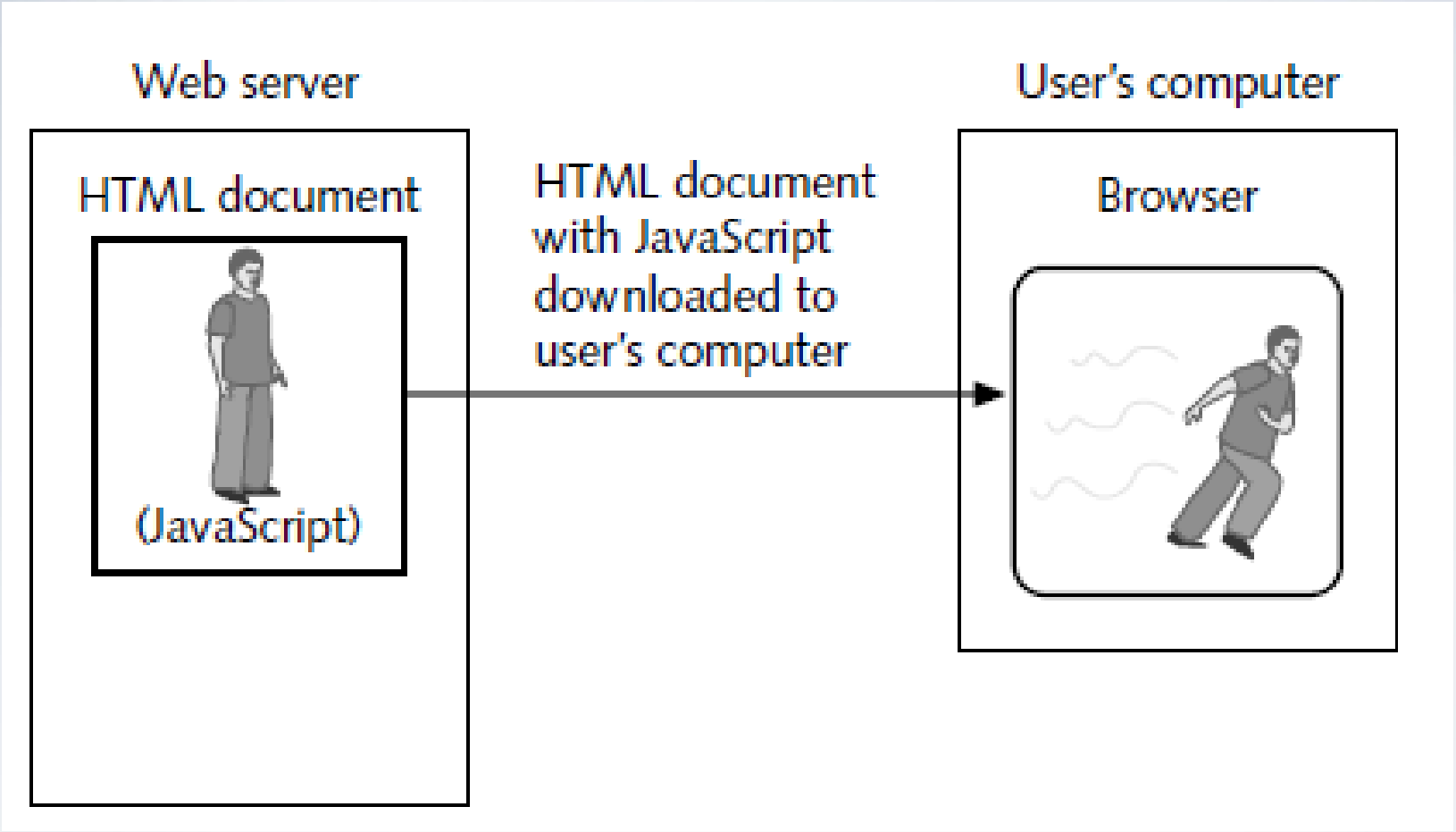
- **TRANSFER-AND-STORE PROCESS**
  - Entire document is transferred and then stored on the local computer before the browser displays it
  - Creates opportunities for sending different types of malicious code to the user's computer



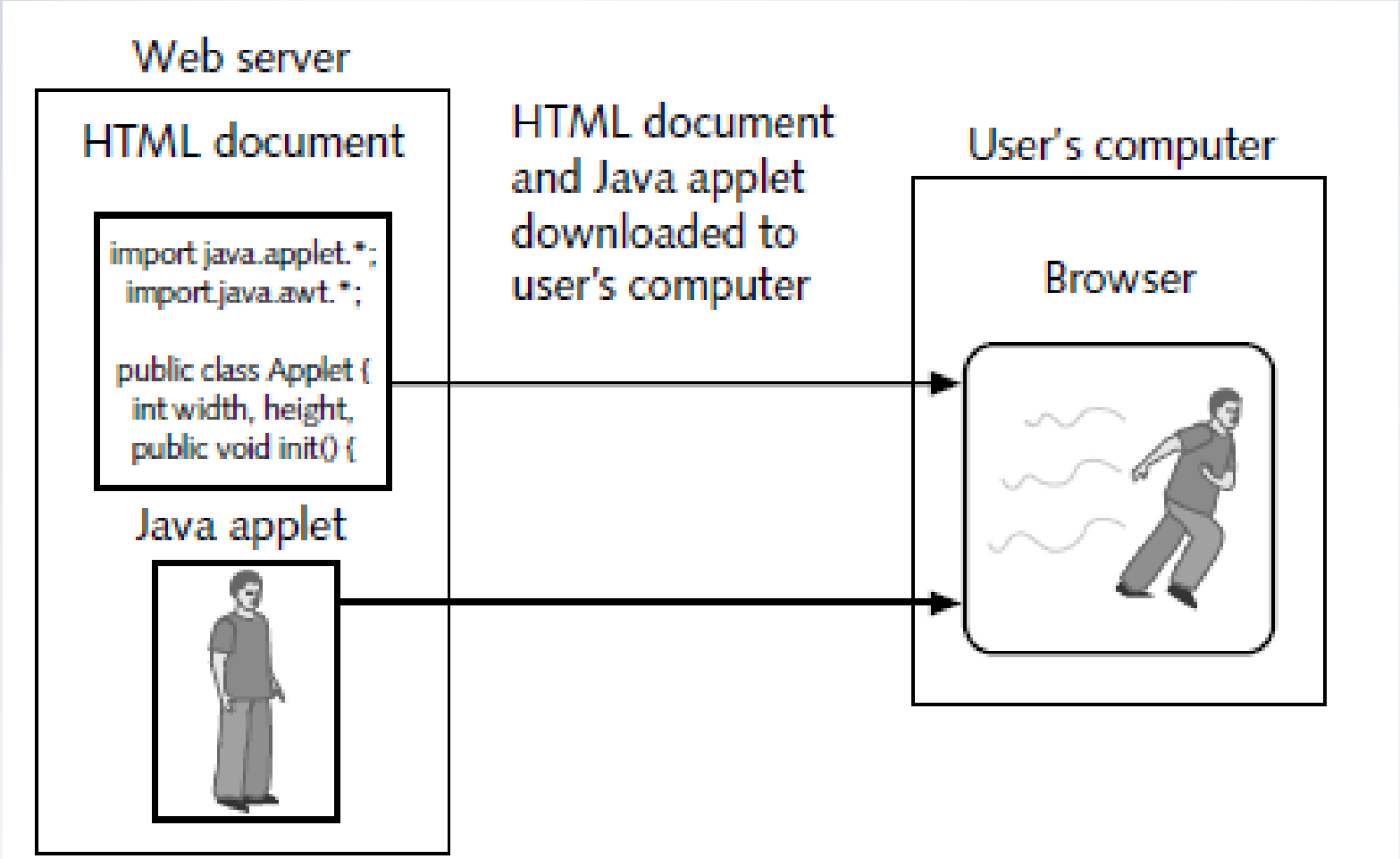
Web page programming
Security (Java, …)



Downloaded JavaScript Code



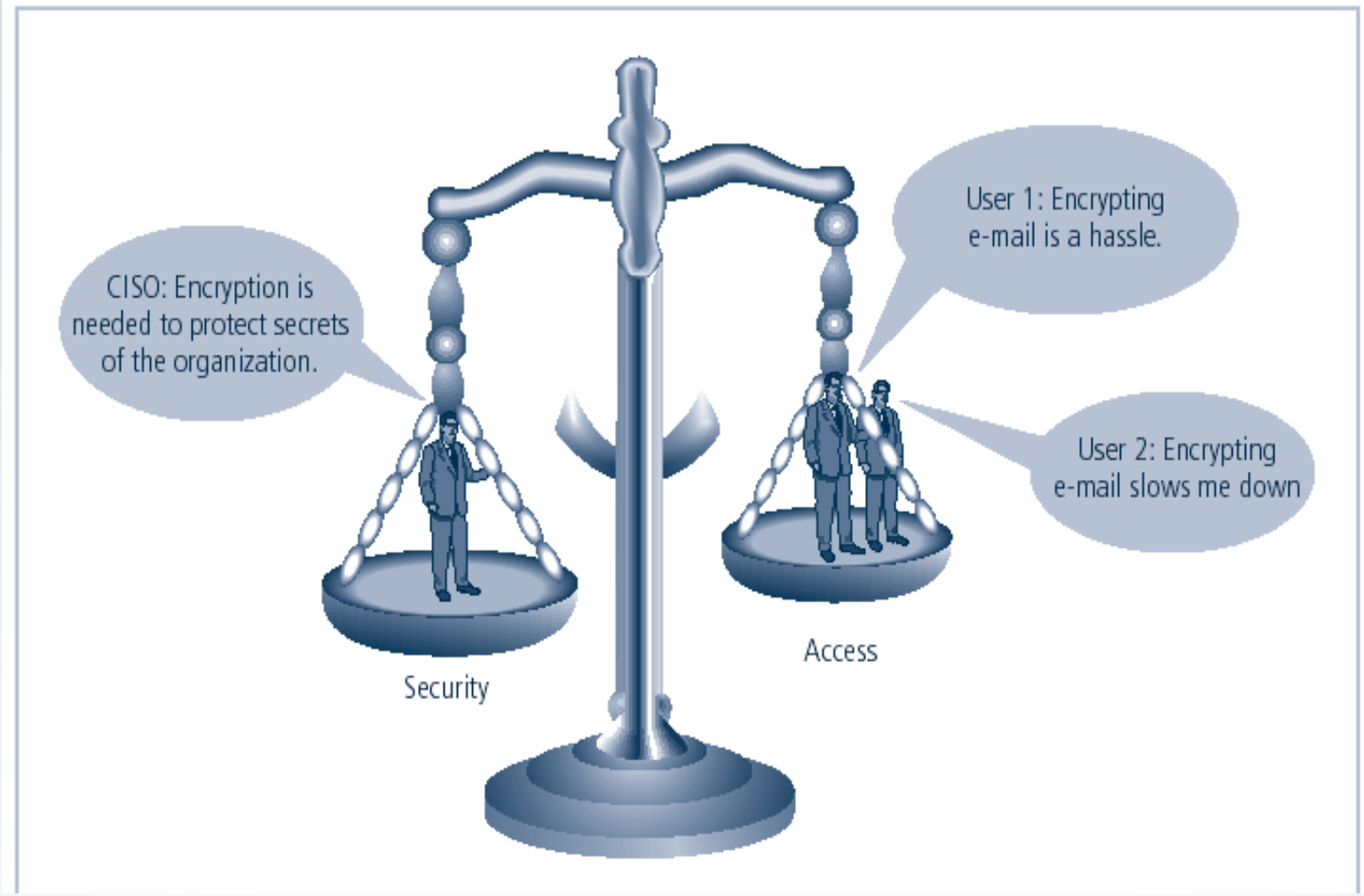
Downloaded Java Applet



Balancing Information Security and Access

- Impossible to obtain perfect information security - it is a process, not a goal
- It is a balance between protection and availability
- The level of security must balance against reasonable access, yet offer adequate protection against threats

Impossible to obtain perfect Information Security

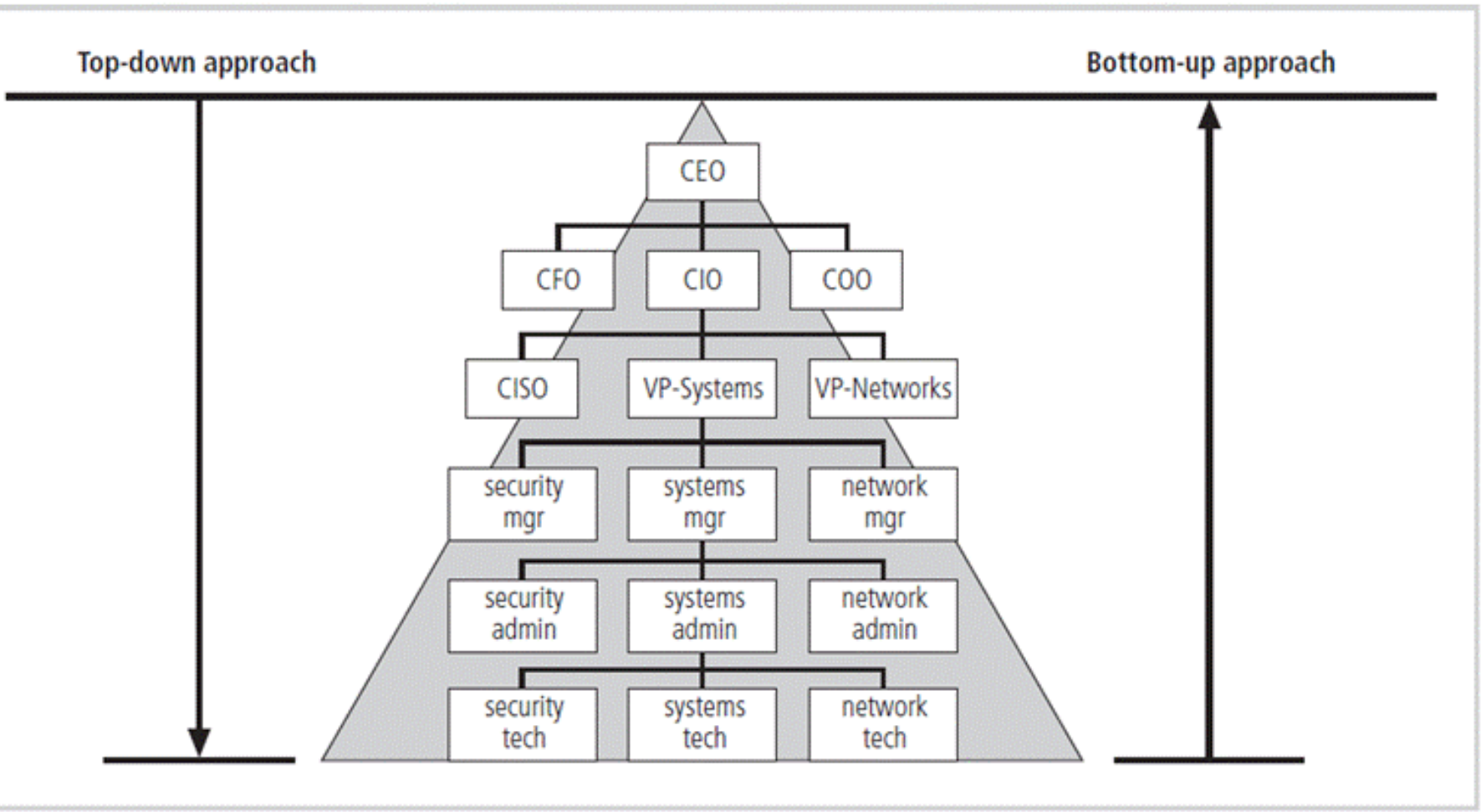


Information Security Implementation Bottom-Up Approach

- Begins at grassroots level where systems administrators attempt to improve security of their systems.
- Main advantage is the ability to tap on the technical expertise of individual administrators
- Seldom works because it did not have the following
  - Participant support
  - Organizational staying power

Information Security Implementation Top-Down Approach

- Begins at upper management level
  - Issue policy, procedures, and processes
  - Dictate goals and expected outcomes of project
  - Determine accountability for each required action
- A preferred approach


Top-down approach
Bottom-up approach
CEO
CFO
CIO
COO
CISO
VP-Systems
VP-Networks
security mgr
systems mgr
network mgr
security admin
systems admin
network admin
security tech
systems tech
network tech
© Cengage Learning 2015

Security Professionals and the Organization

- Diverse group of professionals are required
- Senior/upper management is a very important component.
- Additional staffs are needed to offer administrative support and technical expertise - to implement the details of an IS program.

Senior Management

- Chief information officer (CIO)
  - Senior technology officer
  - Advise the senior executives on strategic planning
- Chief information security officer (CISO)
  - Performs assessment, management, and implementation of IS in the organization
  - Reports directly to the CIO

Information Security Project Team

- A team of people who are experienced in one or multiple aspects of technical and nontechnical areas:
  - Champion
  - Team leader
  - Security policy developers
  - Risk assessment specialists
  - Security professionals
  - Systems administrators
  - End users

Data Responsibilities

- Data owners: senior management responsible for the security and use of a particular set of information
- Data custodian: responsible for information and systems that process, transmit, and store it
- Data users: individuals with an information security role

Communities of Interest

- Group of individuals united by similar interests/values within an organization
  - Information security management and professionals
  - Information technology management and professionals
  - Organizational management and professionals

Information Security: Is It an Art or a Science?

- Implementation of information security is often described as a combination of art and science.
- “Security artisan” idea: based on the way individuals perceive system technologists and their abilities

Security as Art

- No hard and fast rules nor many universally accepted complete solutions
- No manual for implementing security through entire system

Security as Science

- Dealing with technology designed for rigorous performance levels
- Specific conditions cause virtually all actions in computer systems.
- Almost every fault, security hole, and systems malfunction is a result of interaction of specific hardware and software.
- If developers had sufficient time, they could resolve and eliminate faults.

Security as a Social Science

- Social science examines the behavior of individuals interacting with systems.
- Security begins and ends with the people that interact with the system, intentionally or otherwise.
- Security administrators can greatly reduce the levels of risk caused by end users and create more acceptable and supportable security profiles.

Summary

- A short history
- Components and layers
- CIA
- Characteristics of Information
- Threats and attacks
- A fine balance
- Bottom up vs top-down
- IS professionals and roles
- Art, Science or Social Science