IT Security From an Organizational Perspective

Ulrika Norman

Jeffy Mwakalinga

Reference: 1) Enterprise Security.
Robert C. Newman. ISBN: 0-13-047458-4
2) Corporate Computer and Network Security.
Raymond R. Panko. ISBN: 0-13-101774-8

Outline

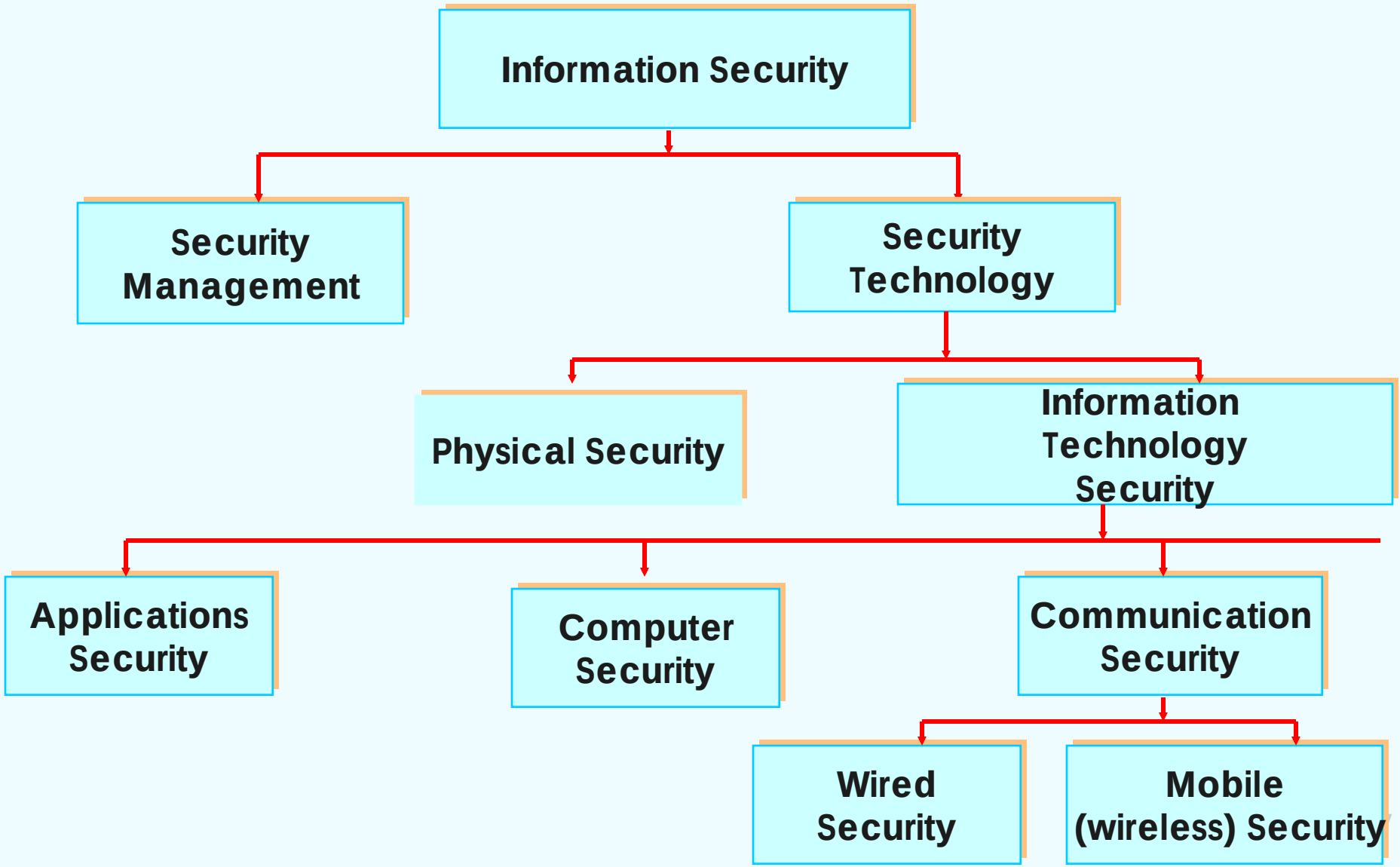
PART I Security Overview

1) Introduction
2) Security Services and Implementation
3) Overview of Existing Security Systems
4) Implementing Security in a System

PART II: Organizational Security

1) Introduction
2) Securing Information Systems of an Organization
3) Corporate Security Planning
4) Adding a Security Department

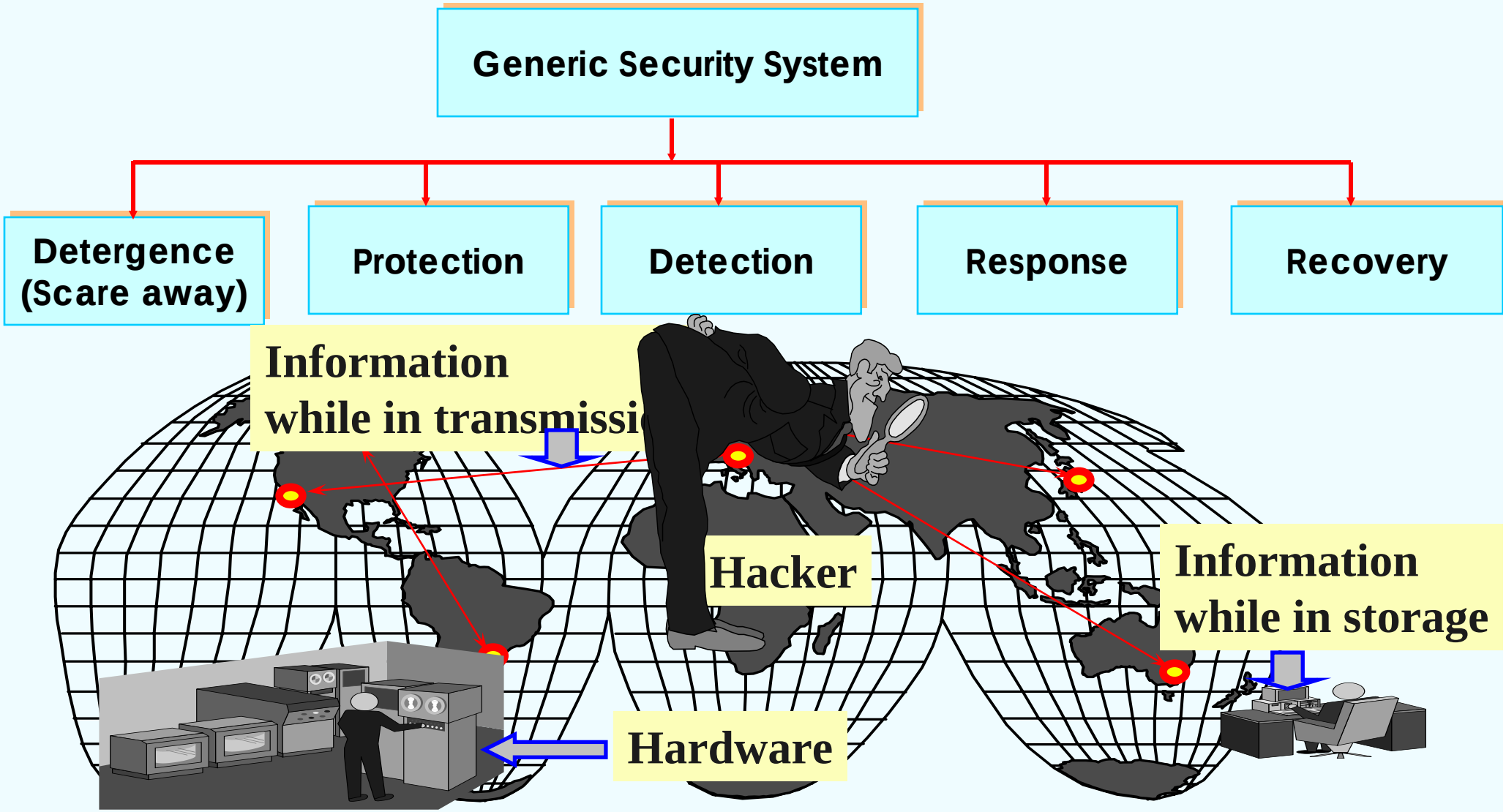
Introduction



Introduction

Information security is defined as methods and technologies for deterrence (scaring away hackers), protection, detection, response, recovery and extended functionalities

Generic Security Principles



PART I: Security Overview

- Introduction
- Security Services and Implementation
- Overview of Existing Security Systems
- Implementing security in a system

Security Services and Implementation : Confidentiality

- Confidentiality
- Authentication
- Access Control
- Integrity
- Non-repudiation
- Availability

To keep a message secret to those that are not authorized to read it

Security Services: Authentication

- Confidentiality
- **Authentication**
- Access Control
- Integrity
- Non-repudiation
- Availability

To verify the identity of the user / computer

Security Services: Access Control

- Confidentiality
- Authentication
- Access Control
- Integrity
- Non-repudiation
- Availability

To be able to tell who can do what with which resource

Security Services: Integrity

- Confidentiality
- Authentication
- Access Control
- Integrity
- Non-repudiation
- Availability

To make sure that a message has not been changed while on Transfer, storage, etc

Security Services: Non-repudiation

- Confidentiality
- Authentication
- Access Control
- Integrity
- Non-repudiation
- Availability

To make sure that a user/server can't deny later having participated in a transaction

Security Services: Availability

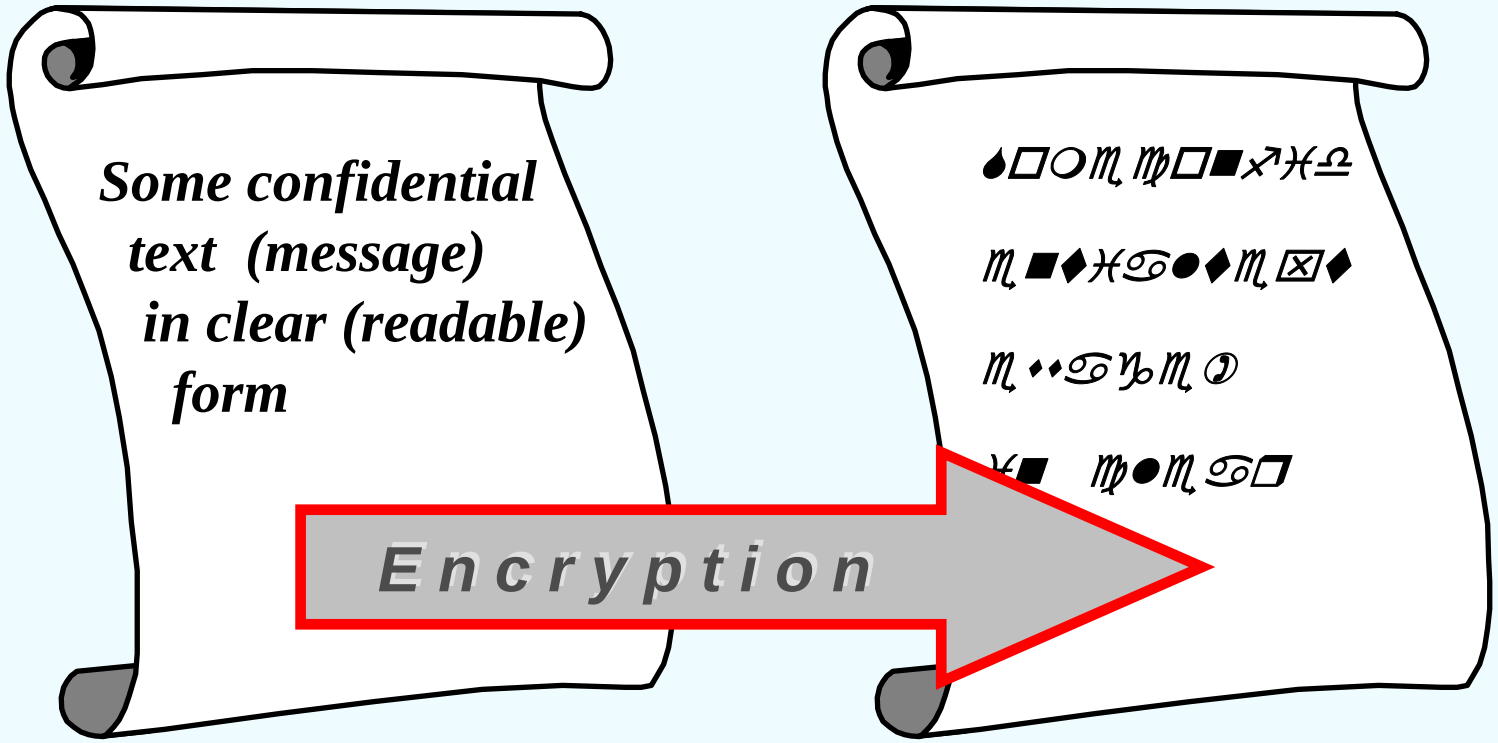
- Confidentiality
- Authentication
- Access Control
- Integrity
- Non-repudiation
- Availability

To make sure that the services are always available to users.

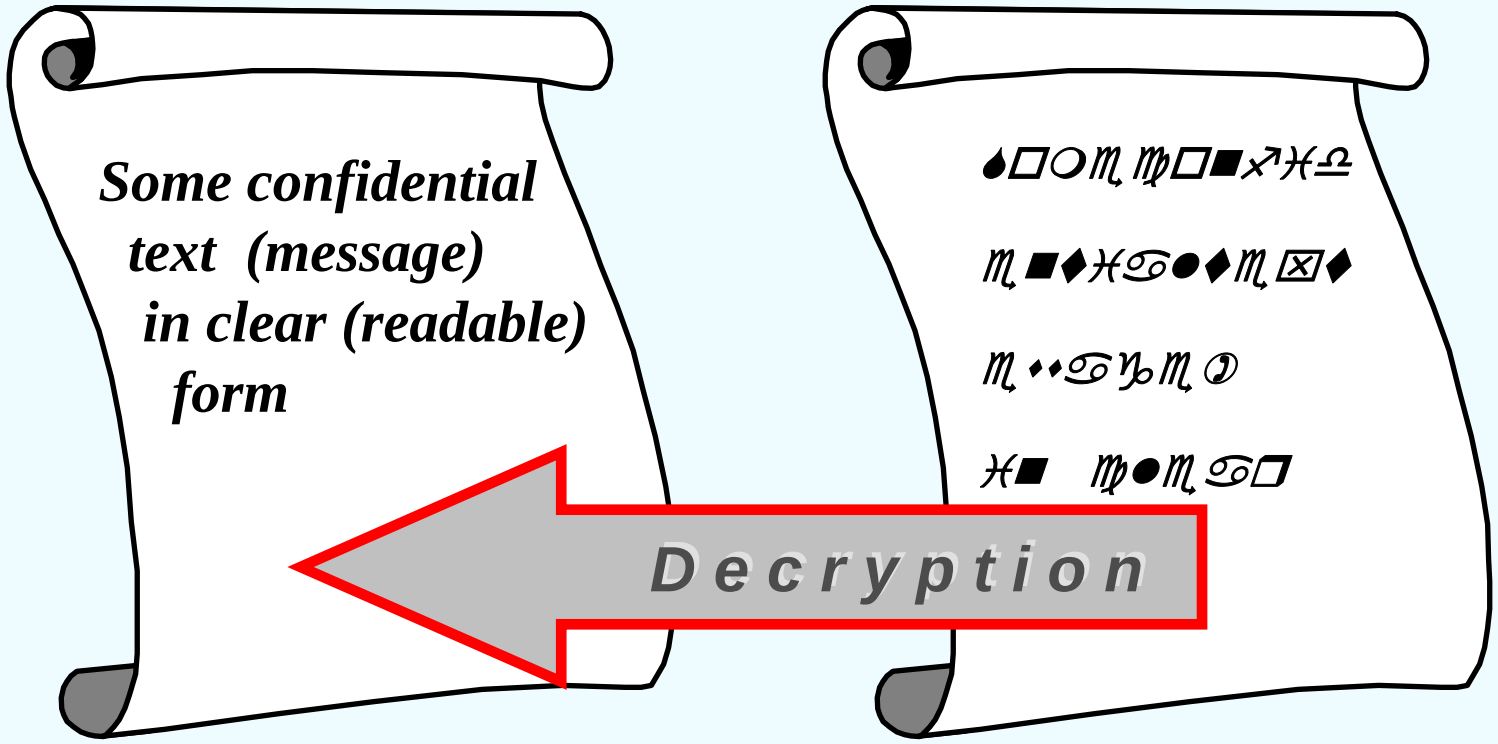
Providing Security Services: Confidentiality

- **We use cryptography** → Science of transforming information so it is secure during transmission or storage
  - **Encryption:**
    Changing original text into a secret, encoded message
  - **Decryption:**
    Reversing the encryption process to change text back to original, readable form

Encryption


Some confidential
text (message)
in clear (readable)
form
Encryption

Decryption


Some confidential
text (message)
in clear (readable)
form
Decryption

Example

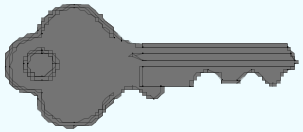
STOCKHOLM

A B C D E F G . . . . X Y Z

L G T U W O M . . . . I A C

VWRFNKROP

Symmetric Key Encryption – One Key System



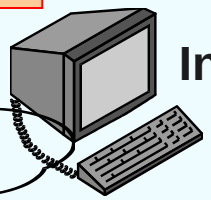
Symmetric Key

Note:
A single key is used to encrypt and decrypt in both directions.

Plaintext "Hello"

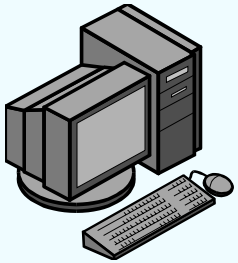
Encryption Method & Key

Ciphertext "11011101"

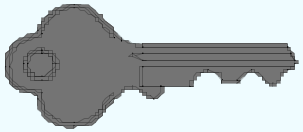


Interceptor

Internet



Anders

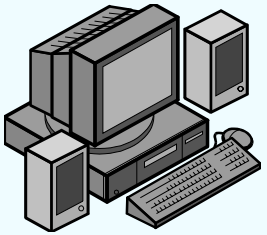


Same Symmetric Key

Ciphertext "11011101"

Decryption Method & Key

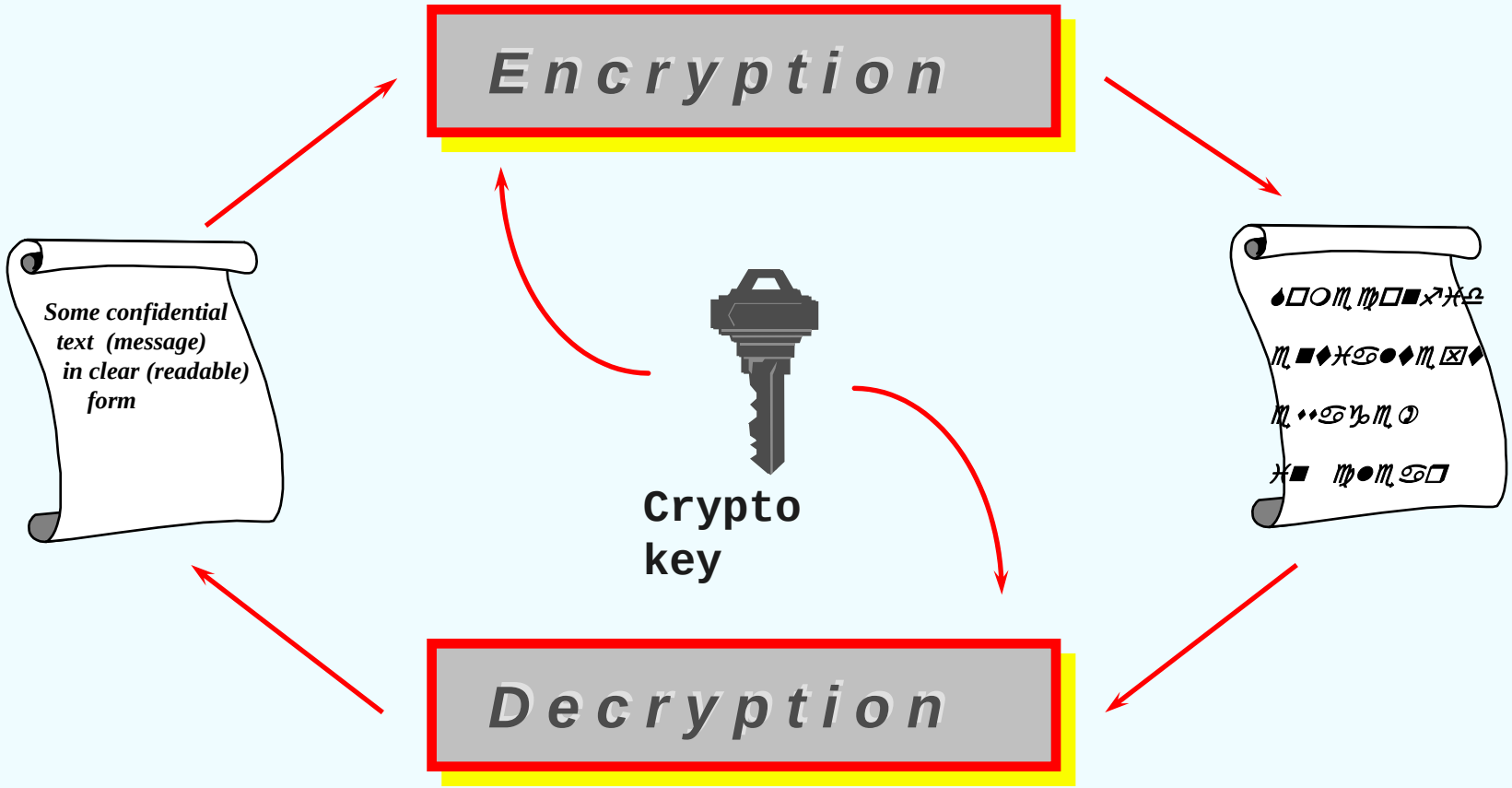
Plaintext "Hello"



Karin

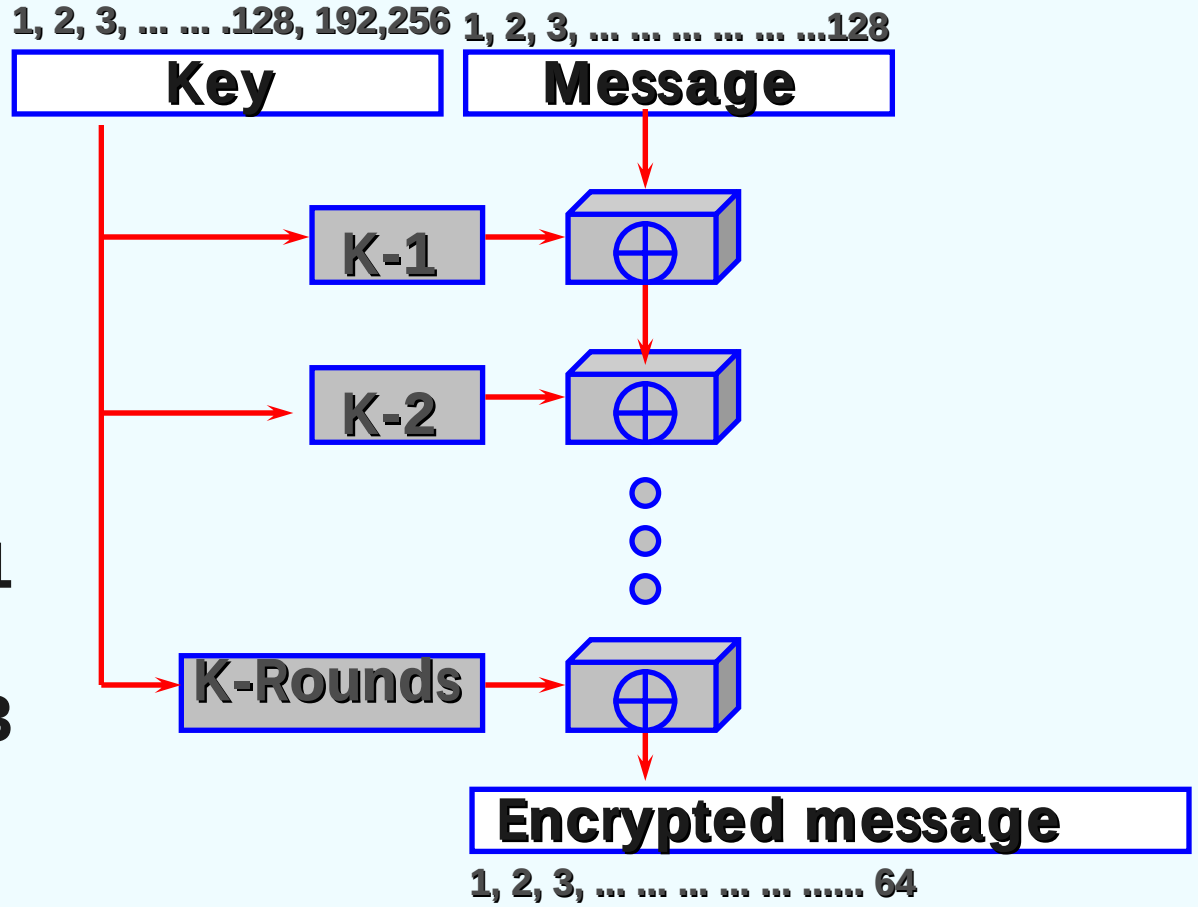
Single Key System: Symmetric System

Same secret key is used to encrypt and decrypt messages. Secret Key must remain secret



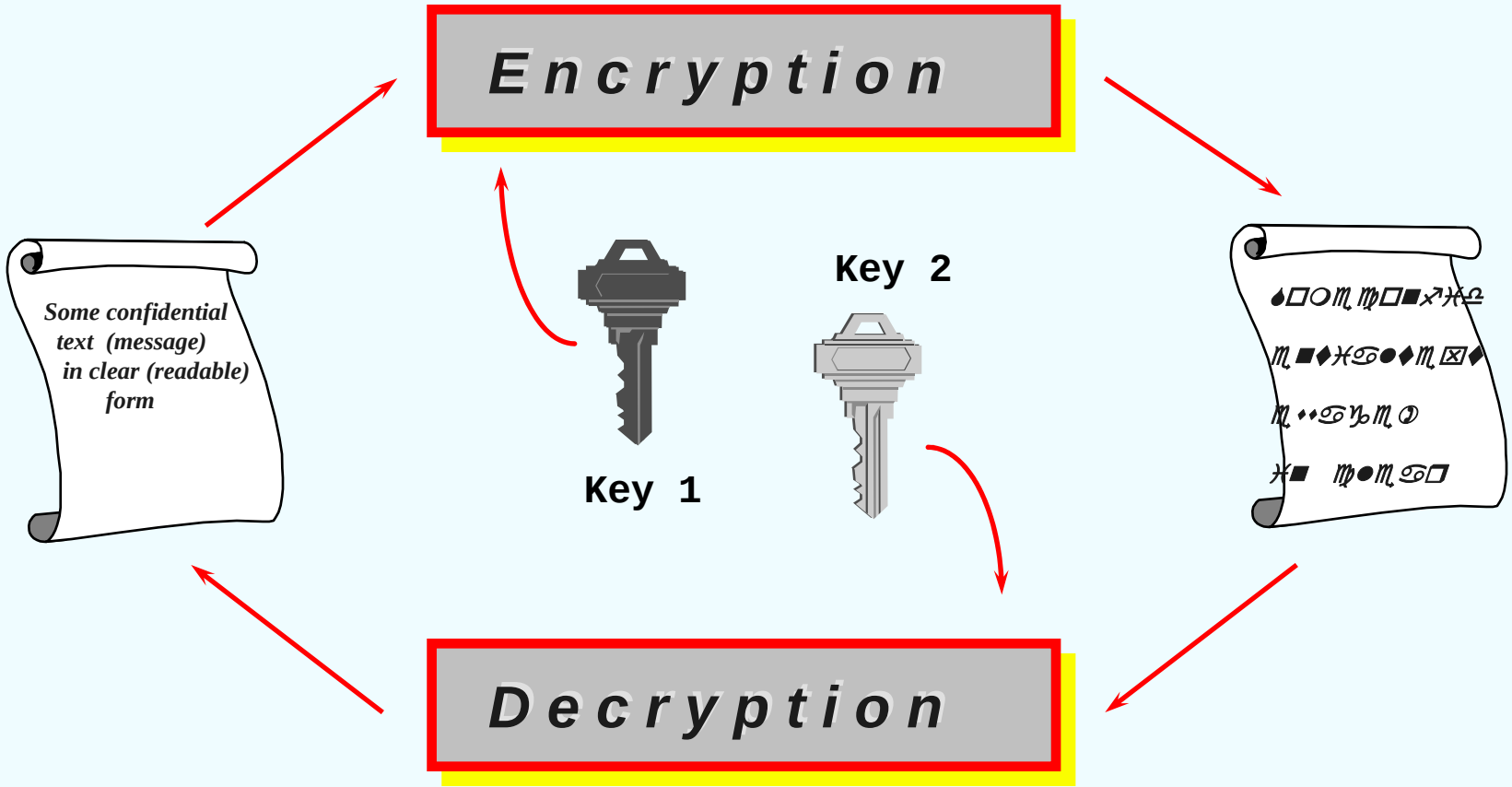
Advanced Encryption Algorithm (AES)

If key = 128
Rounds = 9
If key = 192
Rounds = 11
If key = 256
Rounds = 13



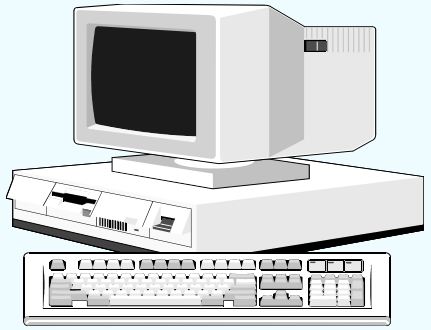
Two Keys System: Asymmetric System

System with two keys: Private key and Public key. Example: Rivest Shamir Adleman system (RSA)

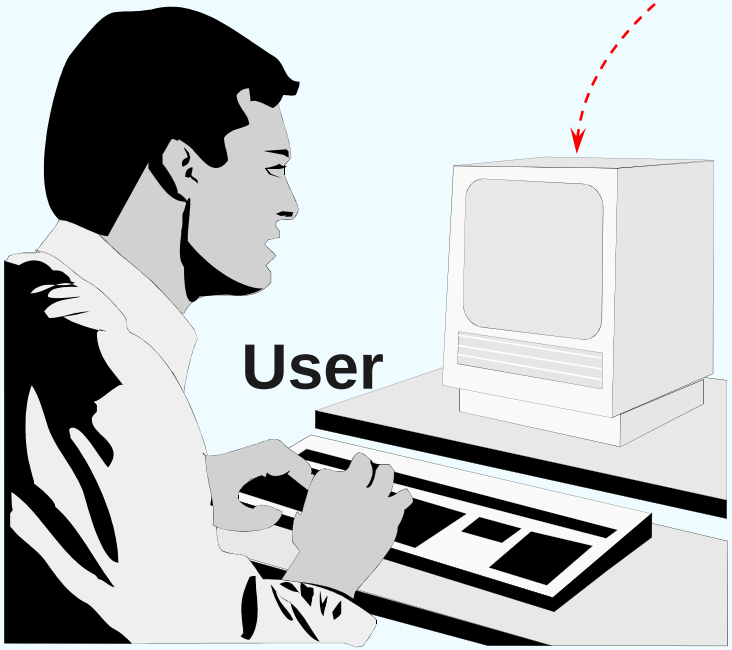


Providing Security Services: Authentication

-something who you are
-something what you have
-something what you know
-where you are - terminal



WWW Server

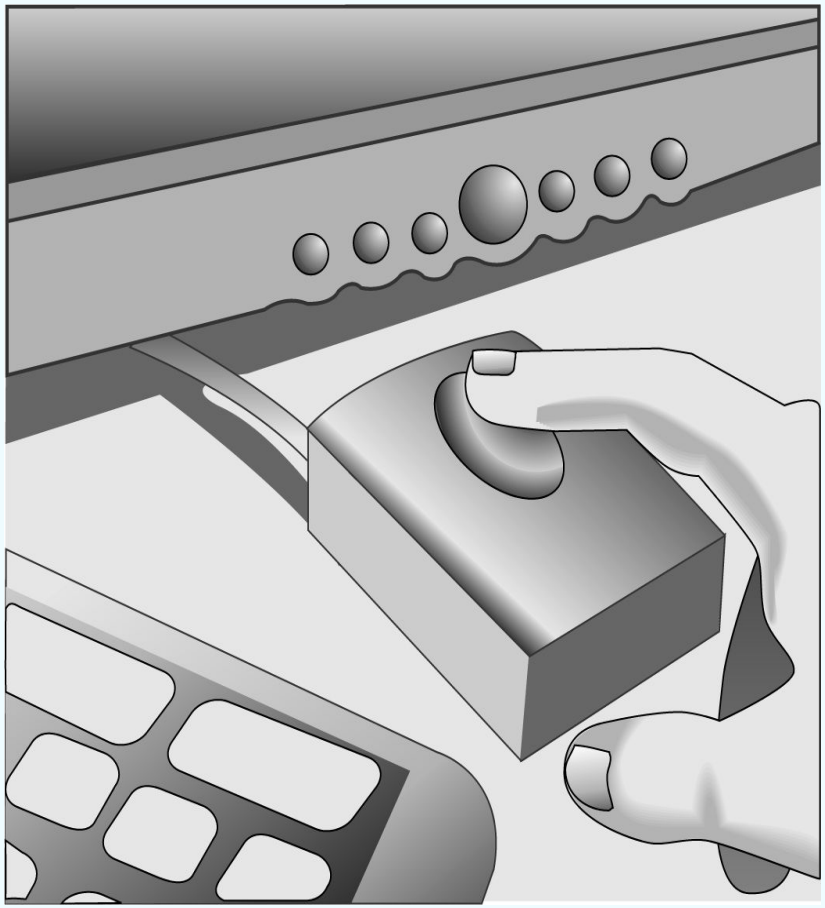


User

Authentication (continued)

- Passwords
- Smart cards
- certificates
- Biometrics
  - Biometrics used for door locks, can also be used for access control to personal computers
  - Fingerprint scanners

Fingerprint scanner



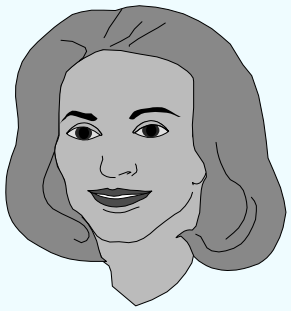
Providing Security Services: Access Control

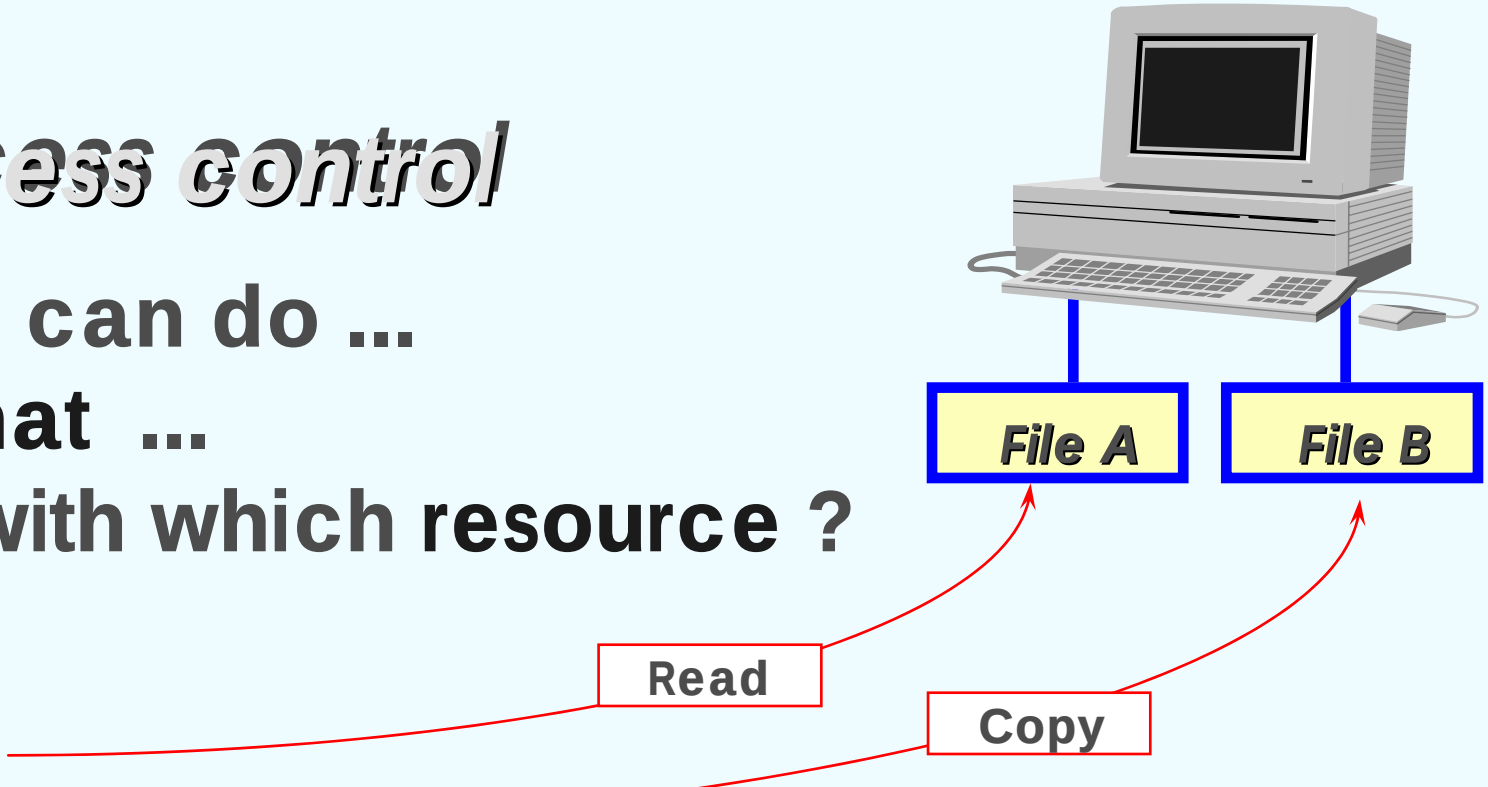
Access control

Who can do ...

what ...

with which resource ?

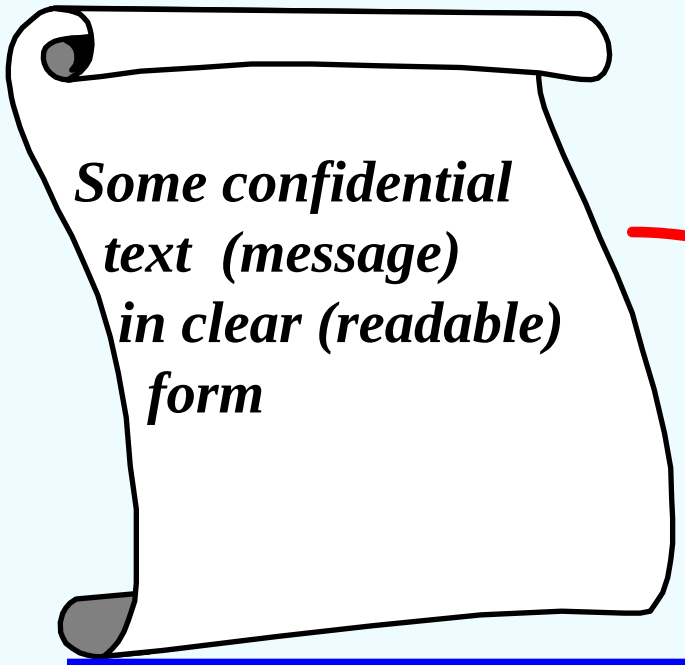




Access Control Matrix

	File1	File2	File3	File4	File5	File6
Subject1		*read,*				
Subject2			*write*			
Subject3						
Subject4						
Subject5					*delete*	
Subject6						

Providing Security Services: Integrity



Change to Binary form

10111000110011010101010010011101 0011 1010 1001

It is called Message Digest

Compress (Hashing)

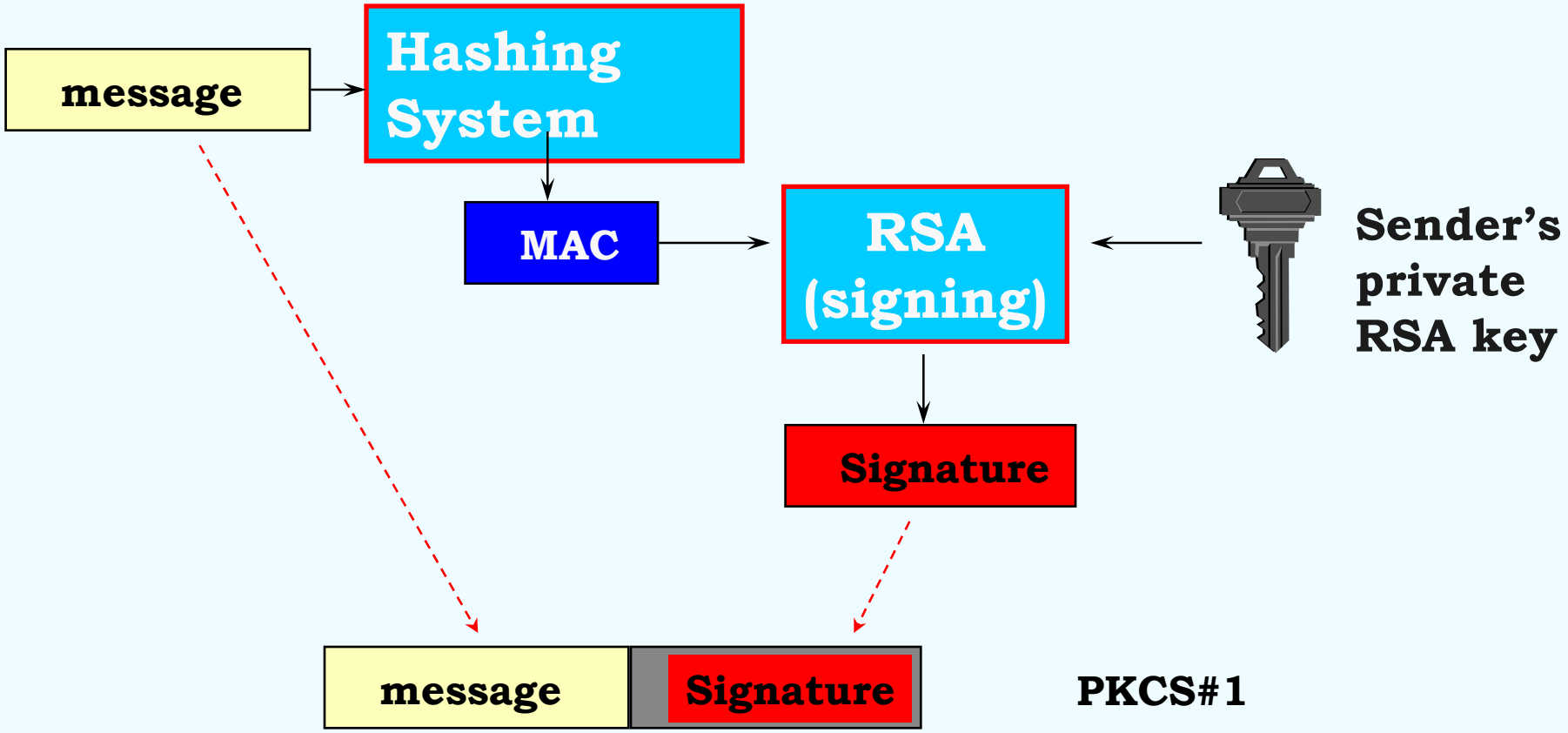
1101 0011 1010 1001

Providing Integrity

Message Digest ~ Message Authentication Code (MAC)

Providing Security Services: Non-repudiation - Signatures

14



PART I: Security Overview

- Introduction
- Security Services
- **Overview of Existing Security Systems**
- **Implementing security in a system**

Overview of Existing Security Systems : Firewalls
Used even for Deterring (Scaring attackers)

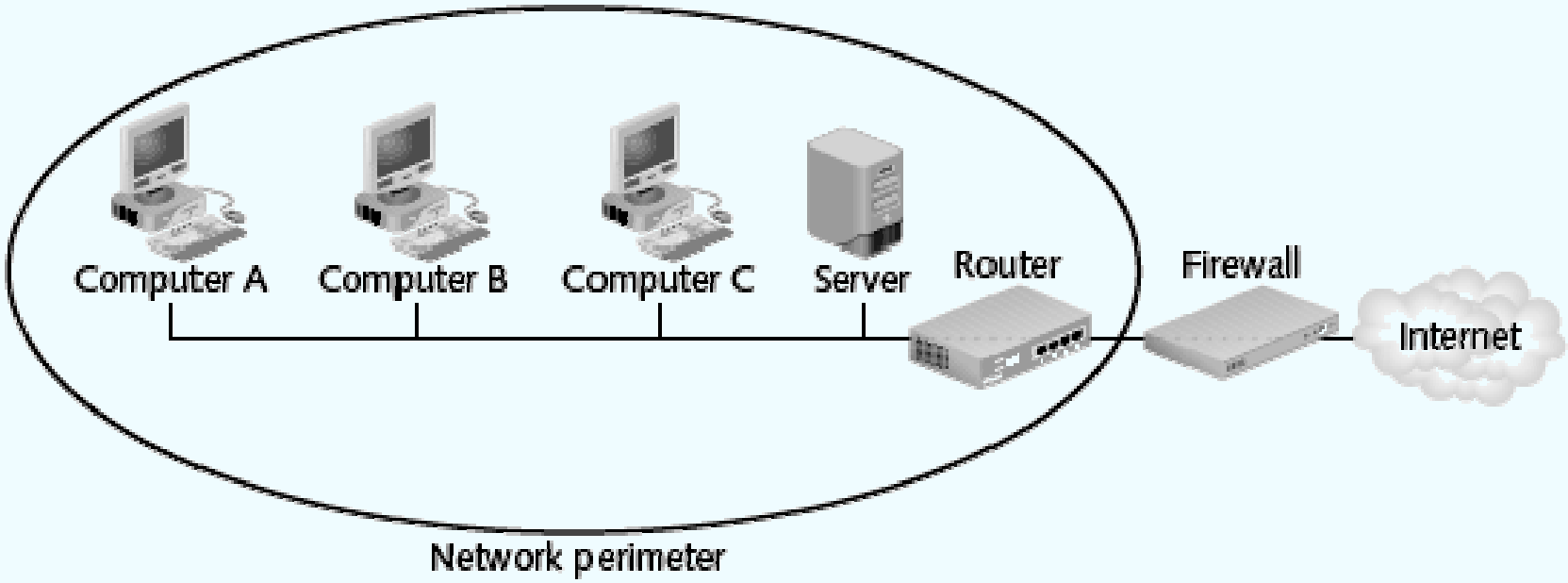


Figure 5-11 Firewall position in network

Firewalls → Designed to prevent malicious packets from entering

Software based → Runs as a local program to protect one computer (**personal firewall**) or as a program on a separate computer (**network firewall**) to protect the network

Hardware based → separate devices that protect the entire network (network firewalls)

Overview of Existing Security Systems : Detection - Intrusion Detection Systems

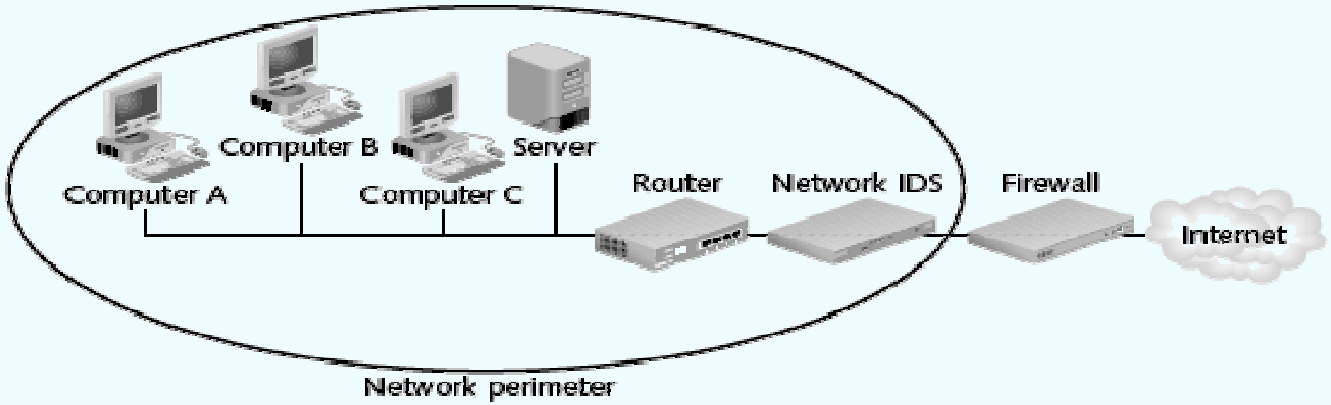


Figure 5-12 IDS system

Intrusion Detection System (IDS) → Examines the activity on a network

Goal is to detect intrusions and take action

Two types of IDS:

Host-based IDS → Installed on a server or other computers (sometimes all)
Monitors traffic to and from that particular computer

Network-based IDS → Located behind the firewall and monitors all network traffic

Overview of Existing Security Systems :
Network Address Translation (NAT)

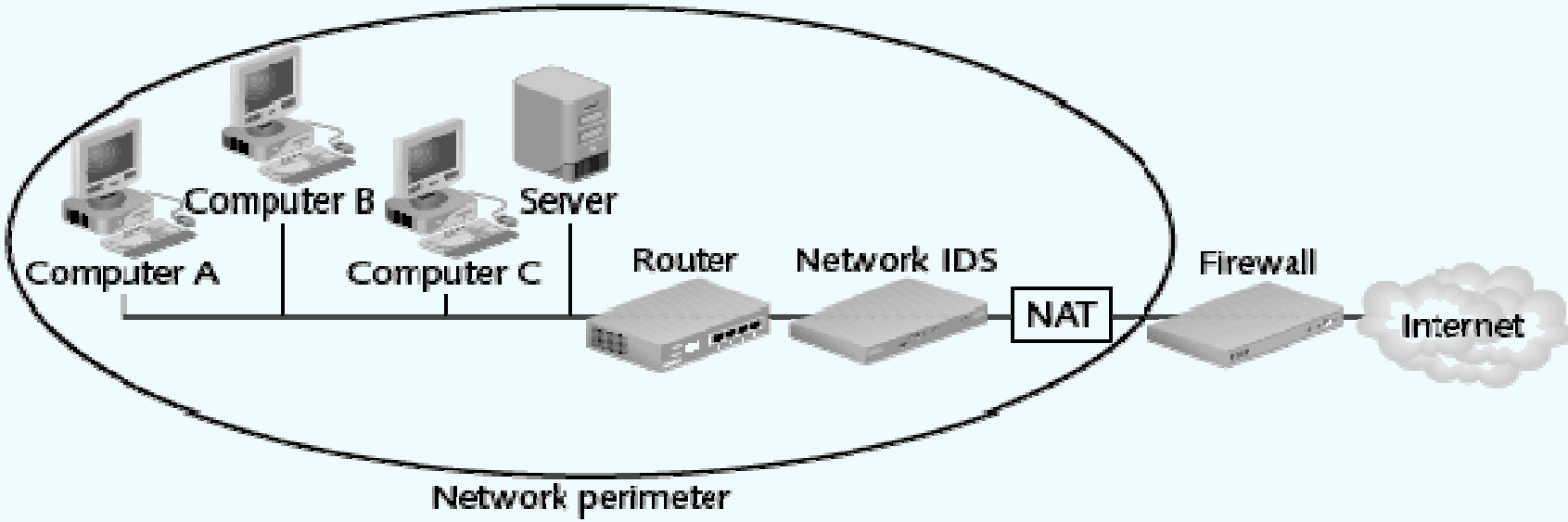


Figure 5-13 Network address translation position

Network Address Translation (NAT) Systems → Hides the IP address of network devices

Located just behind the firewall. NAT device uses an alias IP address in place of the sending machine's real one "You cannot attack what you can't see"

Overview of Existing Security Systems : Proxy Servers

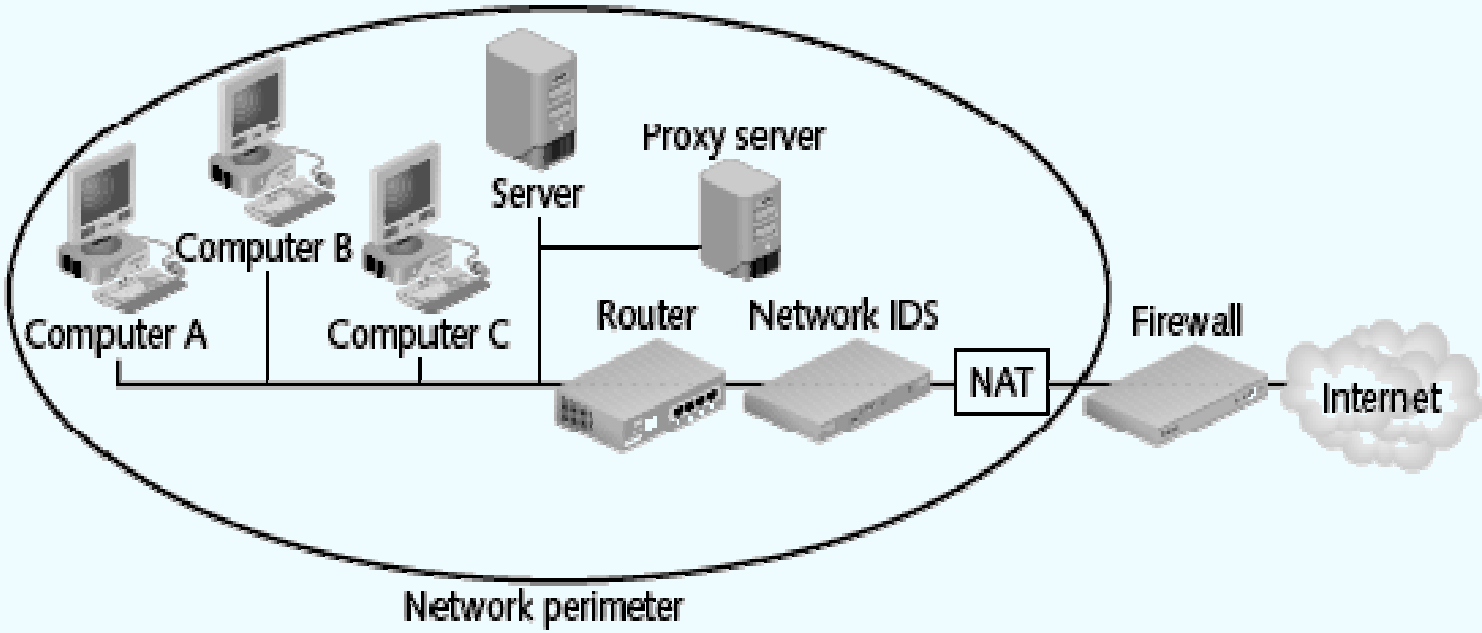


Figure 5-15 Proxy server location

Proxy Server → Operates similar to NAT, but also examines packets to look for malicious content **Replaces the protected computer's IP address with the proxy server's address**

Protected computers never have a direct connection outside the networkThe proxy server intercepts requests. Acts "on behalf of" the requesting client

Adding a Special Network called Demilitarized Zone (DMZ)

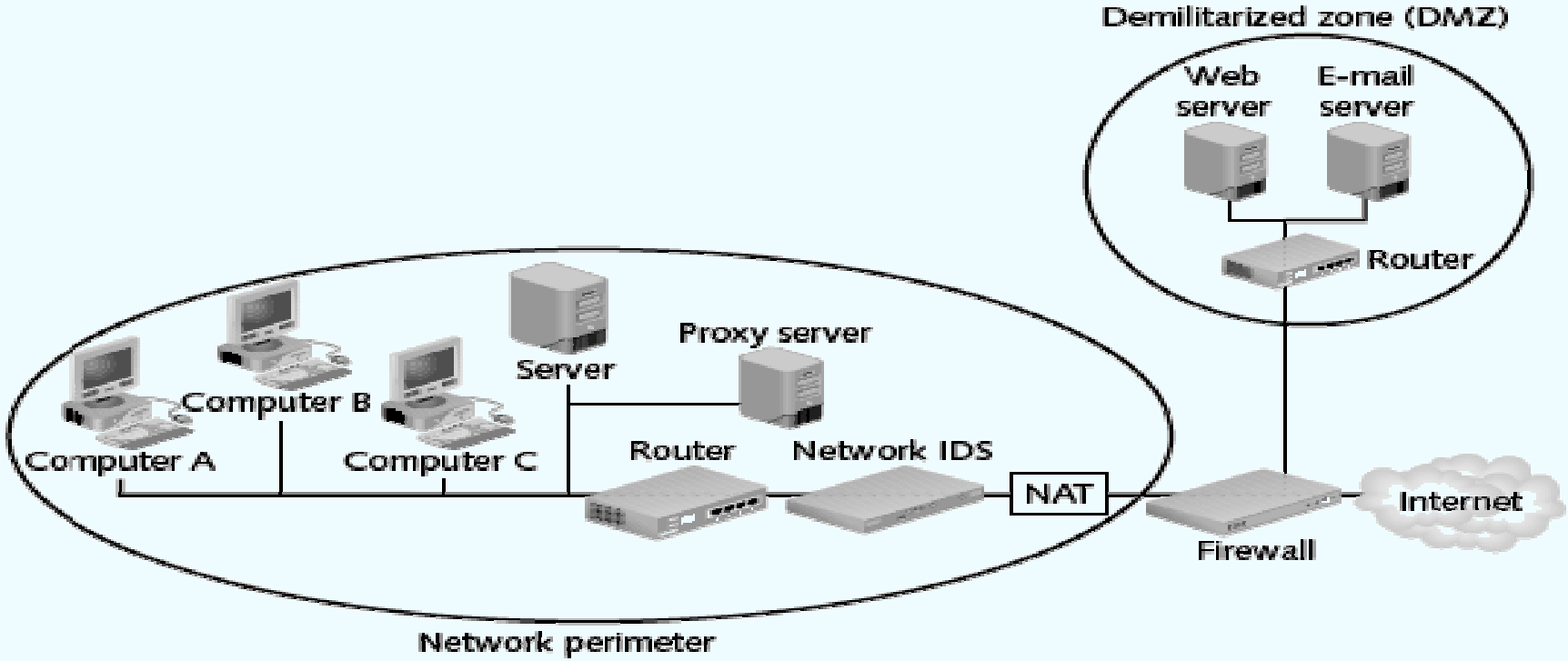


Figure 5-17 DMZ set up outside the secure network perimeter

Demilitarized Zones (DMZ) → Another network that sits outside the secure network perimeter. Outside users can access the DMZ, but not the secure network

Some DMZs use two firewalls. This prevents outside users from even accessing the internal firewall → Provides an additional layer of security

Overview of Existing Security Systems : Virtual Private Networks (VPN)

- **Virtual Private Networks (VPNs)** → A secure network connection over a public network
  - **Allows mobile users to securely access information**
  - **Sets up a unique connection called a tunnel**

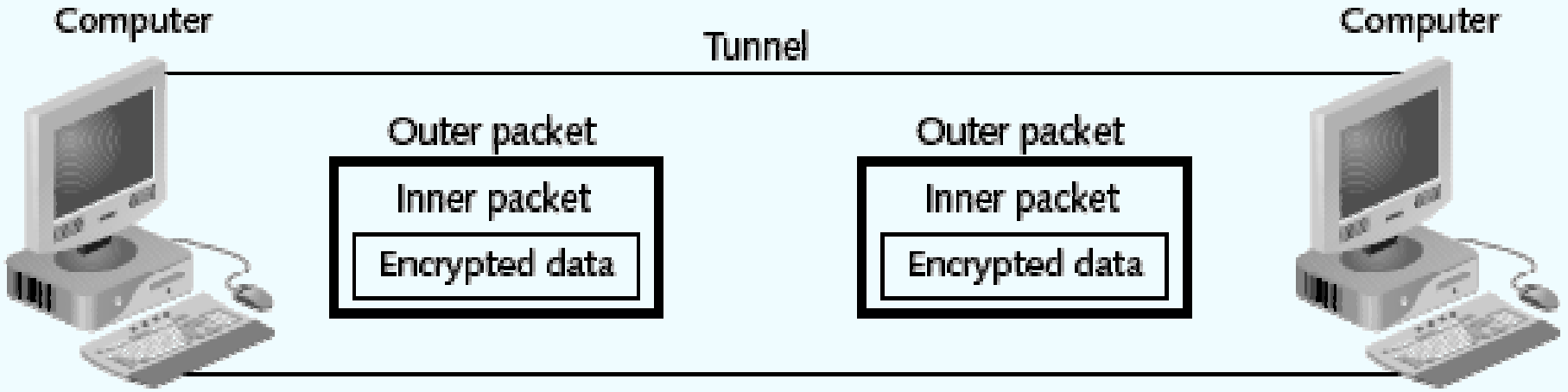


Figure 5-20 VPN transmission

Overview of Existing Security Systems : Virtual Private Networks (VPN)

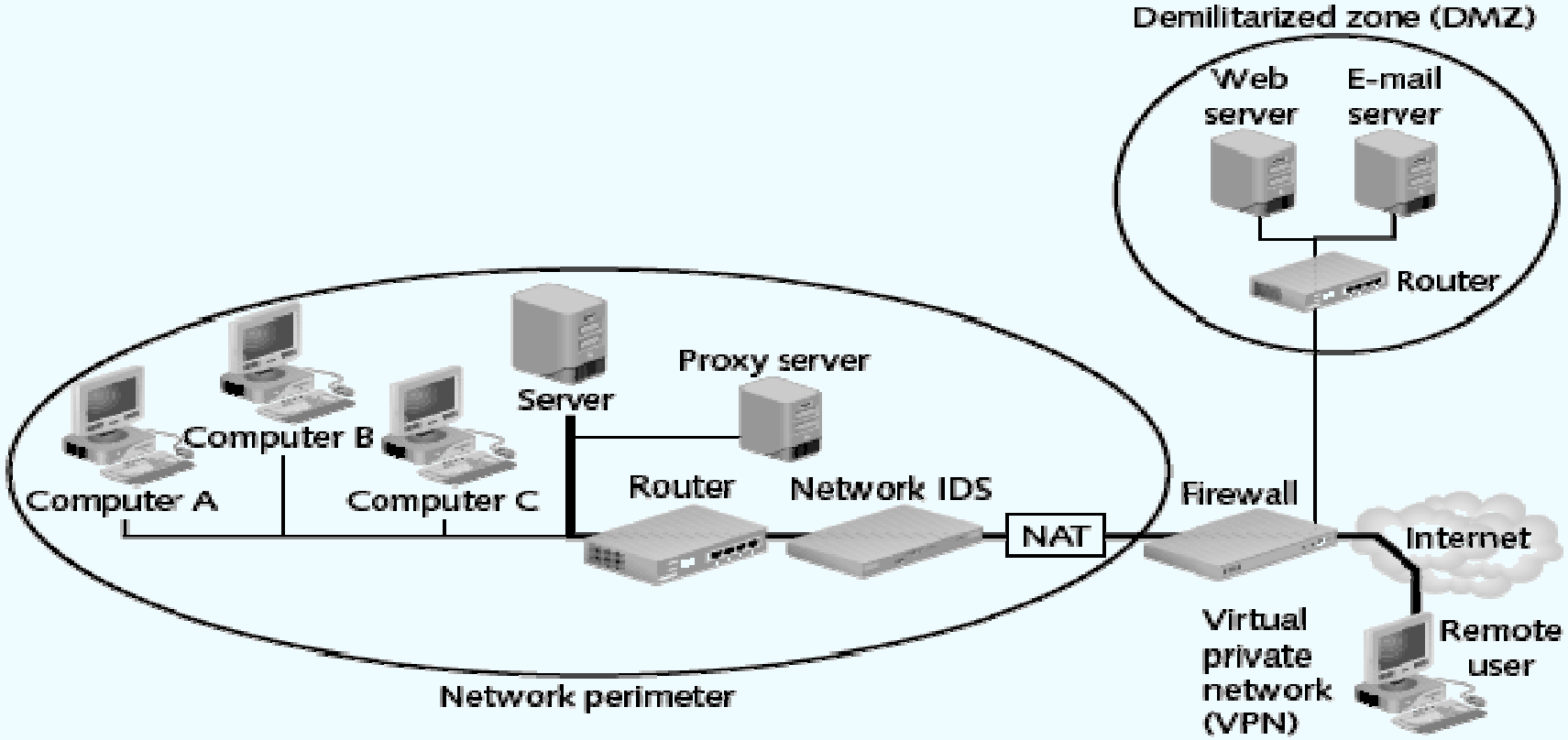


Figure 5-19 Virtual private network (VPN)

Overview of Existing Security Systems : Honeypots

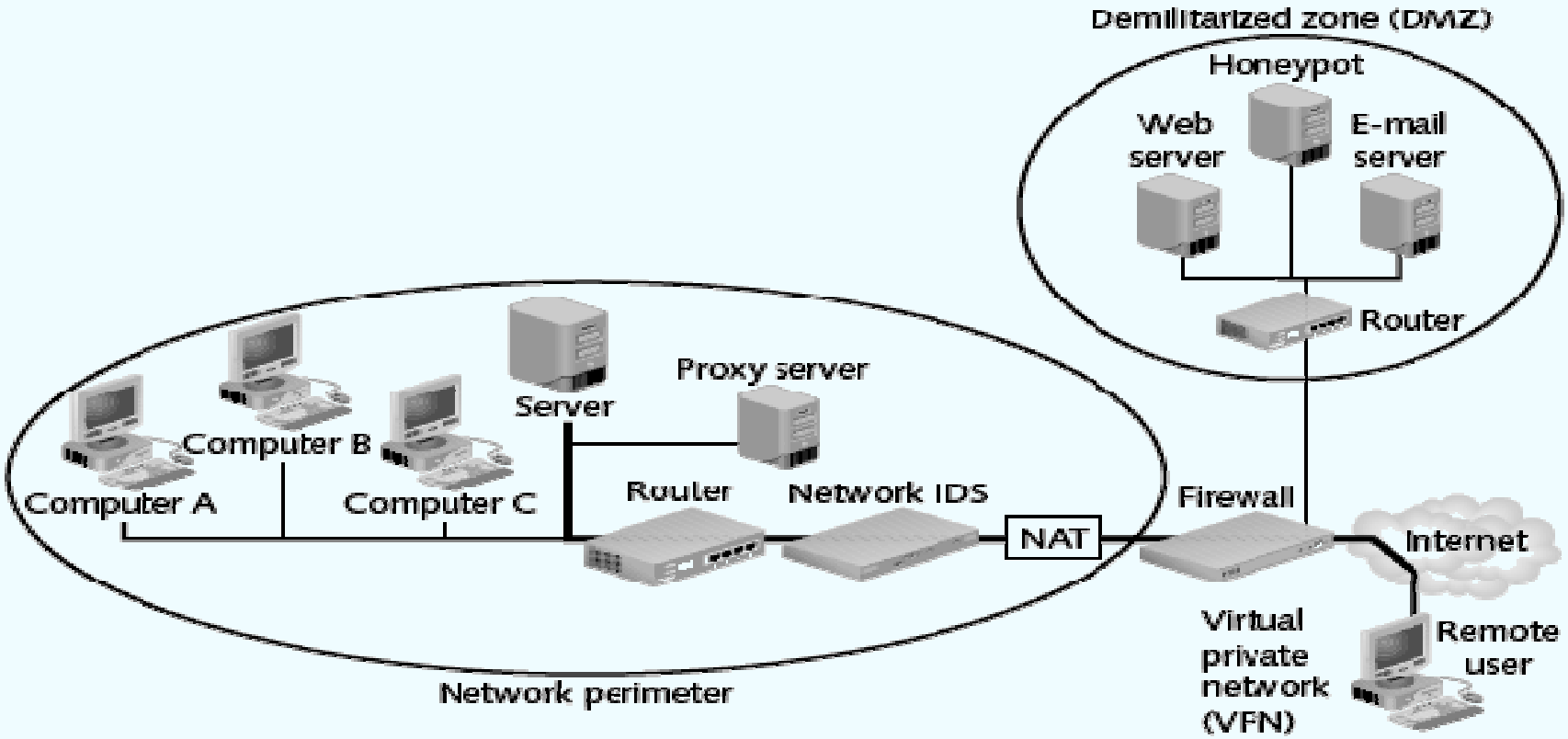


Figure 5-21 Honeypot

Honeypots → Computer located in a DMZ and loaded with files and software that appear to be authentic, but are actually imitations

Intentionally configured with security holes

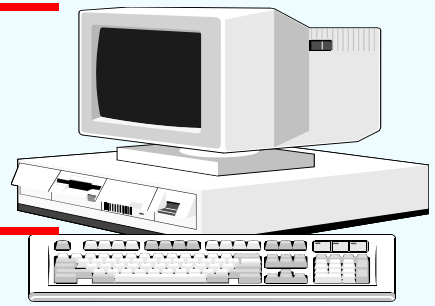
Goals: Direct attacker's attention away from real targets; Examine the techniques used by hackers

Overview of Existing Security Systems : Secure Socket Layer (SSL)

SSL is used for securing communication between clients and servers. It provides mainly confidentiality, integrity and authentication

Client

Establish SSL connection - communication protected



WWW Server

PART I: Security Overview

- Introduction
- Security Services and Implementation
- Overview of Existing Security Systems
- **Implementing security in a system**

Implementing Security in a System Involves:

Patching software
- Getting the latest versions

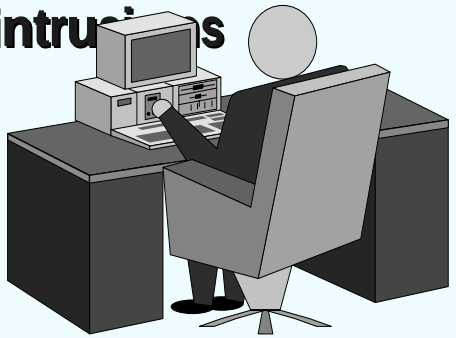
Hardening systems
- by using different security systems available

Blocking attacks – By having different security tools to prevent attacks

Testing defenses Regularly testing from outside and inside the network or an organization

Protecting one Computer

- **Operating system hardening is the process of making a PC operating system more secure**
  - **Patch management**
  - **Antivirus software – to protect your pc from viruses**
  - **Antispyware software**
  - **Firewalls – to deter (scare), protect**
  - **Setting correct permissions for shares**
  - **Intrusion detection Systems – to detect intrusions**
  - **Cryptographic systems**



Protecting a Wired Network

Use Firewalls, Intrusion Detection Systems, Network Address Translation, Virtual Private net Networks, honey pots, cryptographic systems, etc

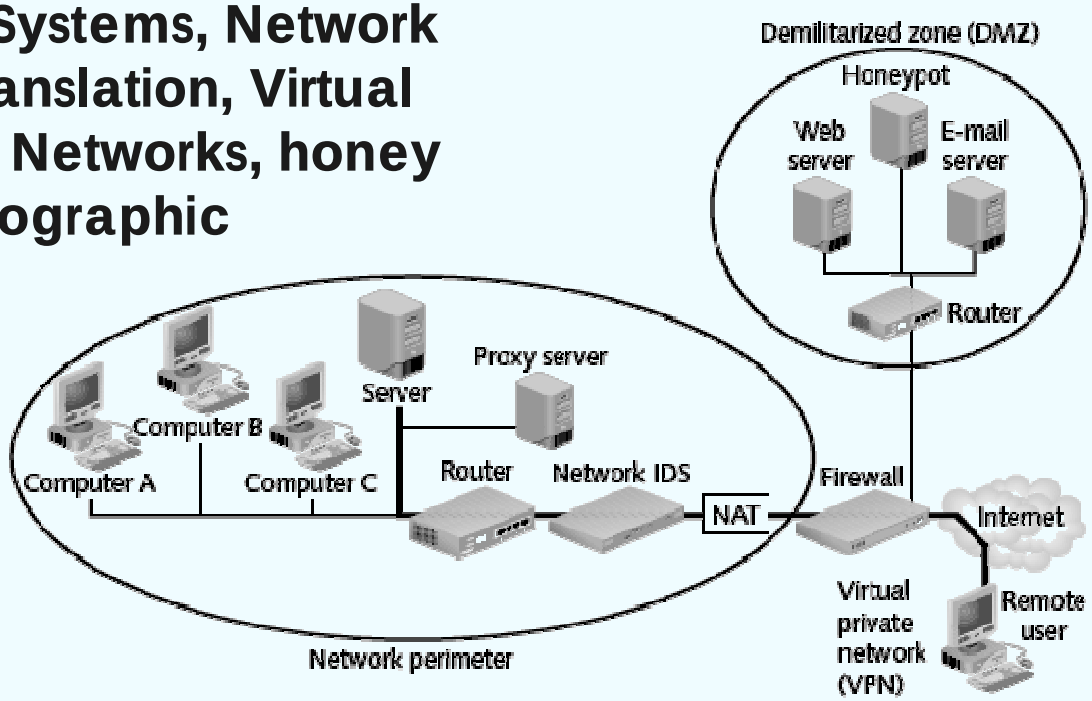


Figure 5-21 Honeypot

Protecting a Wireless Local Area Network (WLAN)

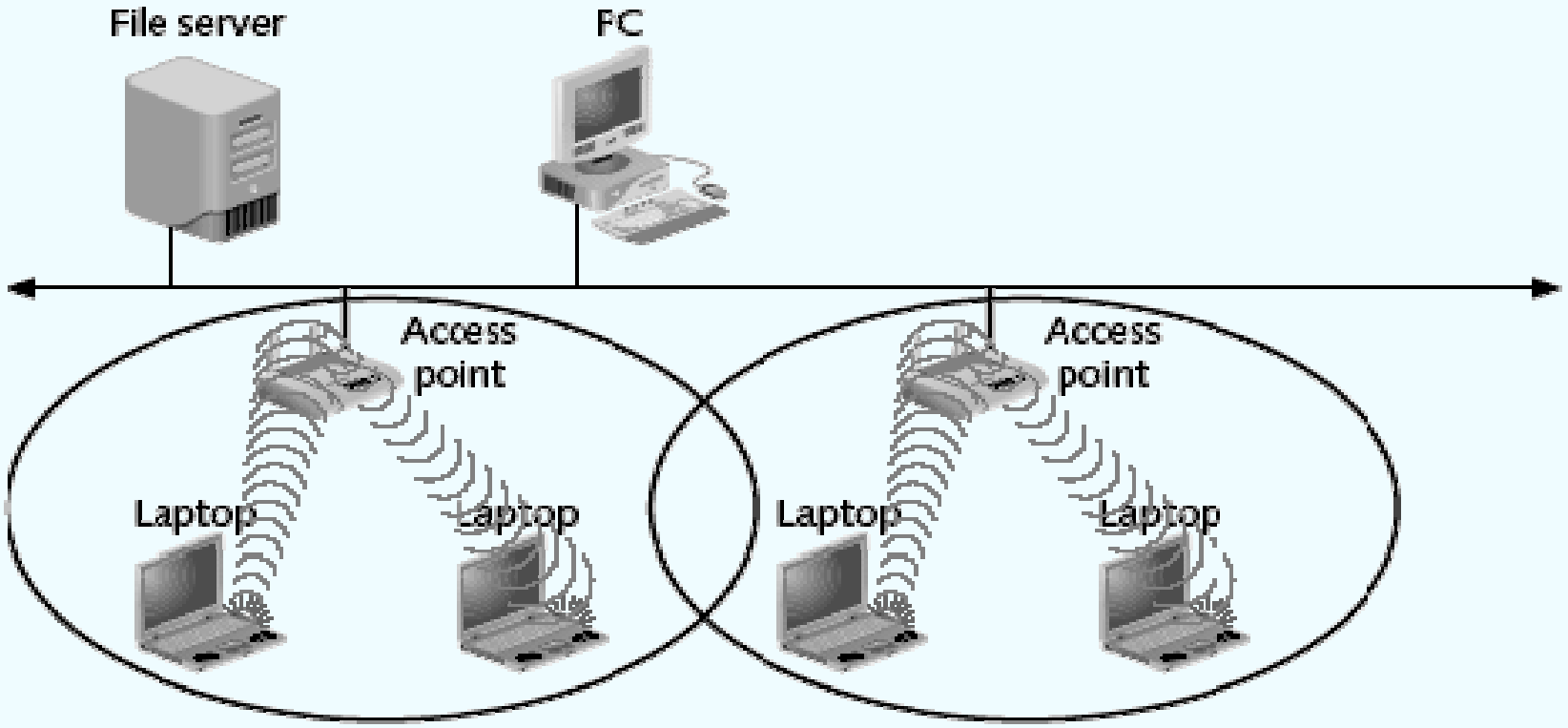


Figure 5-22 Wireless local area network

Security in a Wireless LAN

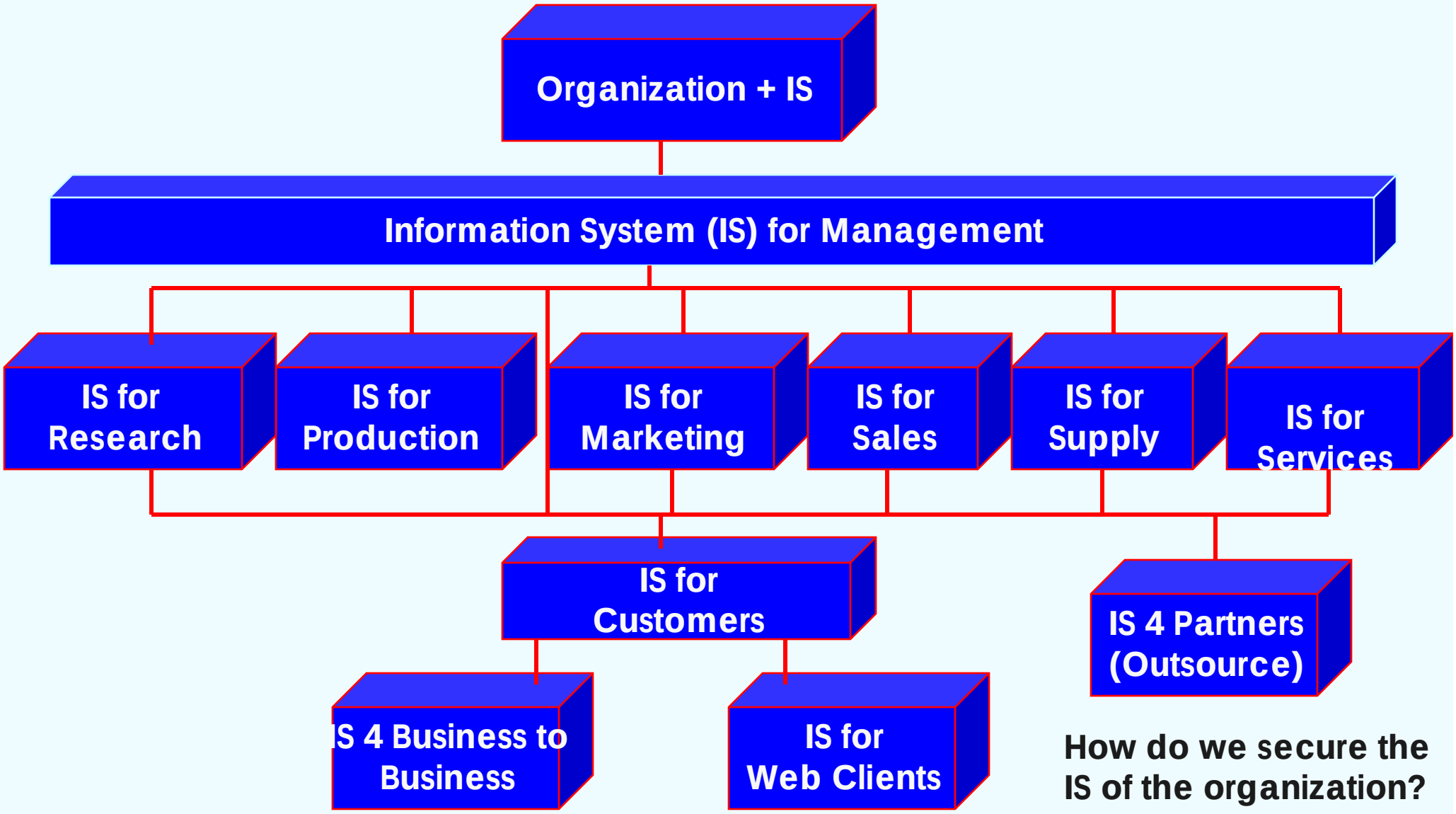
- WLANs include a different set of security issues
- Steps to secure:
  - Turn off broadcast information
  - MAC address filtering
  - Encryption
  - Password protect the access point
  - Physically secure the access point
  - Use enhanced WLAN security standards whenever possible
  - Use cryptographic systems

PART II: Organizational Security

- Introduction
- Securing Information Systems of an Organization
- Corporate Security Planning
- Adding a security Department

Introduction - Traditional Organization

Introduction: Adding Information System

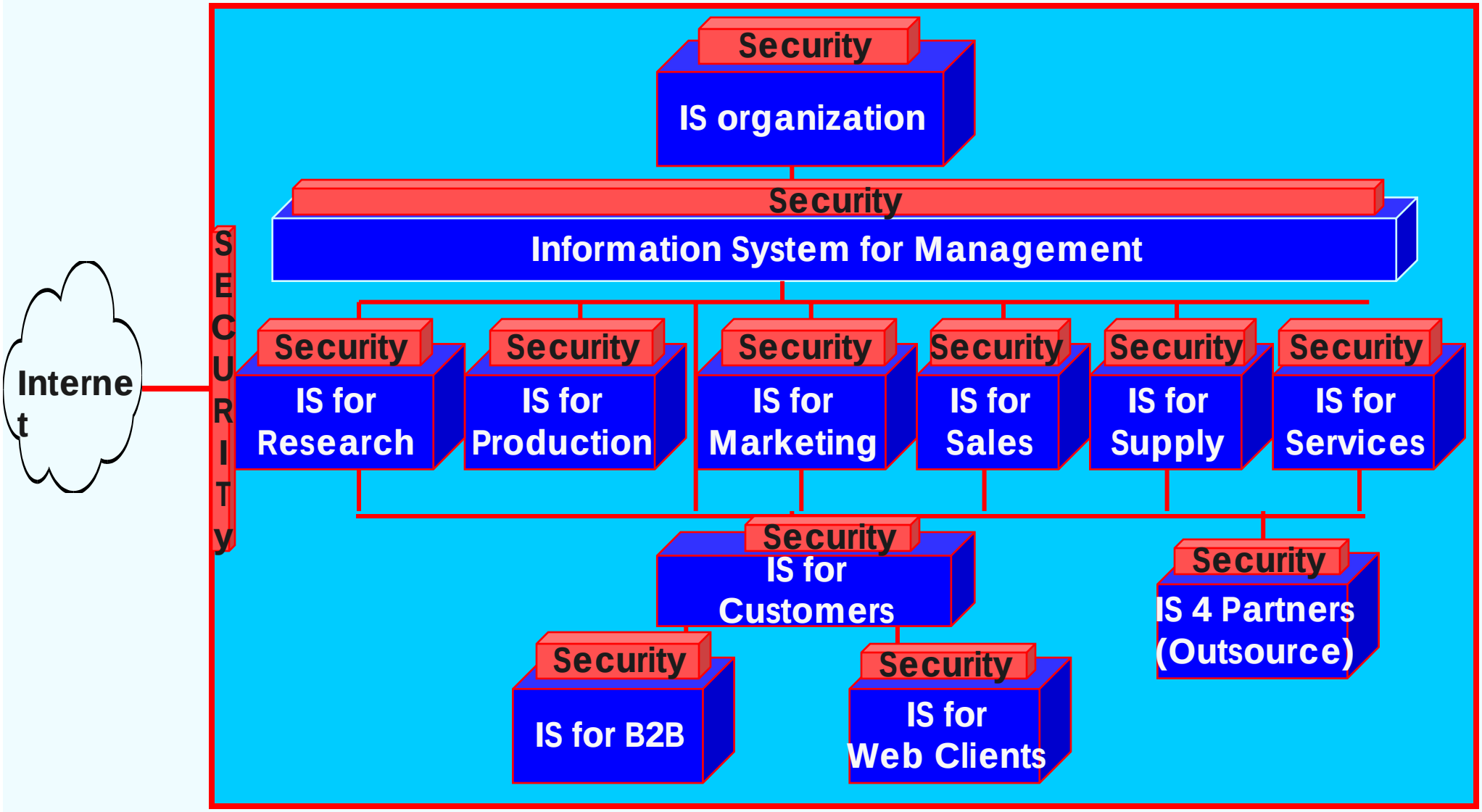


How do we secure the IS of the organization?

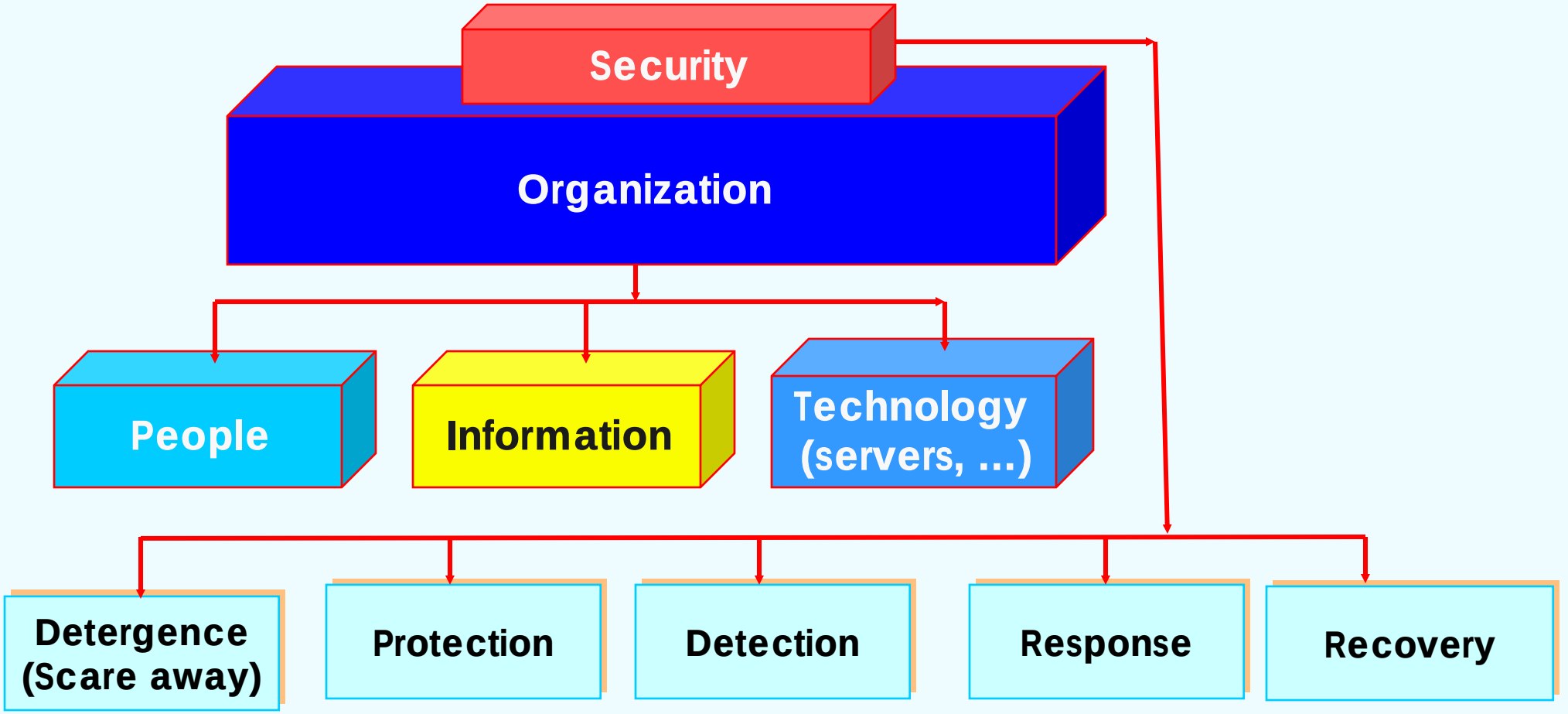
PART II: Organizational Security

- Introduction
- Securing Information Systems of an Organization
- Corporate Security Planning
- Adding a security Department

Securing Information Systems of an Organization



Holistic (Generic) Security Approach



Analysis

Detergence (Scare away)	Protection	Detection	Response	Recovery
How much to spend on Deterrence?	How much to spend on Protection?	How much to spend on Detection?	How much to spend on Response?	How much to spend on Recovery?
10%?	50%?	20%?	10%?	10%?
How much responsibility on employees?	How much responsibility on employees?	How much responsibility on employees?	How much responsibility on employees?	How much responsibility on employees?
How much responsibility on organization?	How much responsibility on organization?	How much responsibility on organization?	How much responsibility on organization?	How much responsibility on organization?
How much responsibility on government?	How much responsibility on government?	How much responsibility on government?	How much responsibility on government?	How much responsibility on government?

Analysis continued

Detergence (Scare away)	Protection	Detection	Response	Recovery
Implementation By Software x% By People y% By Hardware z%	Implementation: By Software? n% By People s% By Hardware t%	Implementation By Software m% By People p% By Hardware h%	Implementation By Software f% By People g% By Hardware r%	Implementation By Software k% By People d% By Hardware c%
Which standards to use for deterring?	Which standards to use for Protection?	Which standards to use for detection?	Which standards to use for response?	Which standards to use for Recovery?

To do the analysis we need corporate security planning?

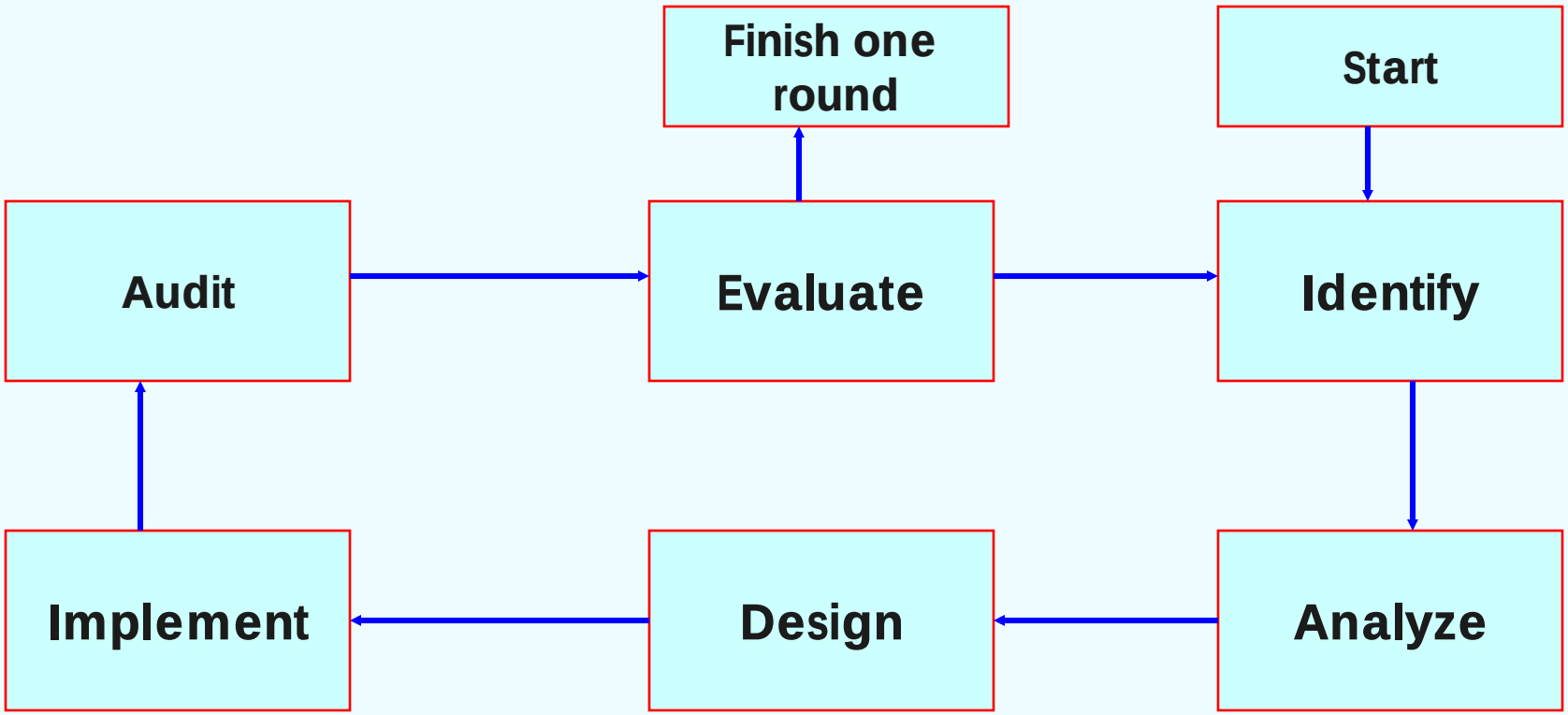
PART II: Organizational Security

- Introduction
- Securing Information Systems of an Organization
- **Corporate Security Planning**
- **Adding a security Department**

Corporate Security Planning

- Security requirements Assessment
- Business Continuity Planning
- How to perform network management?
- Administration
- How to test and troubleshoot?

Security requirements Assessment: Continuous process



Identify the organization's security issues and assets
Analyze security risks, threats and vulnerabilities
Design the security architecture and the associated processes
Audit the impact of the security technology and processes
Evaluate the effectiveness of current architecture and policies

Business Continuity Planning (1)

- A business continuity plan specifies how a company plans to restore core business operations when disasters occur

Business Process Analysis

- Identification of business processes and their interrelationships
- Prioritizations of business processes

Communicating, Testing, and Updating the Plan

- Testing (usually through walkthroughs) needed to find weaknesses
- Updated frequently because business conditions change and businesses reorganize constantly

Business Continuity Planning - continued

- **Disaster Recovery**
  - Disaster recovery looks specifically at the technical aspects of how a company can get back into operation using backup facilities
- **Backup Facilities**
  - Hot sites
    - Ready to run (with power, computers): Just add data
  - Cold sites
    - Building facilities, power, communication to outside world only
    - No computer equipments
    - Might require too long to get operating
- **Restoration of Data and Programs**
- **Testing the Disaster Recovery Plan**

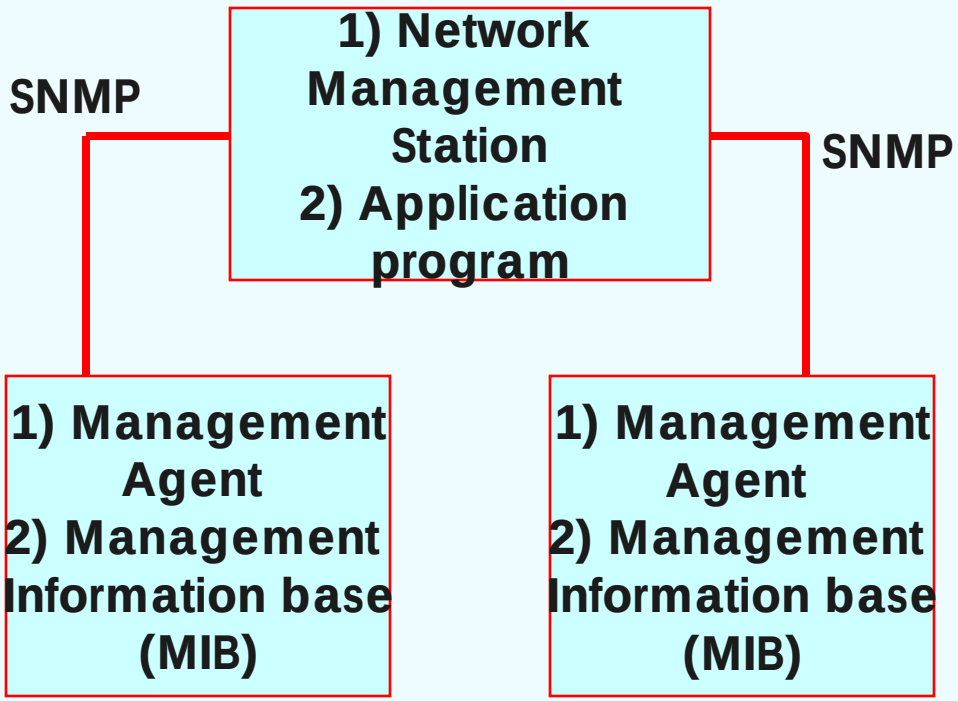
Network management Functions (ISO)

- **Fault Management**
  - Ability to detect, isolate, and correct abnormal conditions that occur in a network.
- **Configuration management**
  - Ability to identify components configure them according to the security policy
- **Performance Management**
  - Ability to evaluate activities of the network and improve network performance
- **Security management**
  - Ability to monitor, control access, securely store information, examine audit records; etc.
- **Accounting management**

  The ability to track the use of network resources. Identify costs and charges related to the use of network resources

Some Network management Standards

- **Simple Network Management Protocol (SNMP)**



- **Common Management Information protocol (CMIP).**

  The main functions provided by this protocol are : alarm reporting, access control, accounting, event report management, lo control, object management, state management, security audit, test management, summarization, relation management.

Administration

- Computer and Network administration section
- Duties:

1) Software installation and upgrade
2) Database access approval and maintenance
3) User identities and password management
4) Back up and restoral processes
5) Training employees about security awareness

How to test and troubleshoot?

- Test whether the systems and components are behaving in accordance to the security plans
- Test from inside the organization and from outside the organization
- Trouble shooting: Define the situation, prioritize the problem, develop information about the problem, identify possible causes, eliminate the possibilities one at a time, ensure the fix does not cause additional problems, document the solution

PART II: Organizational Security

- Introduction
- Securing Information Systems of an Organization
- Corporate Security Planning
- **Adding a security Department**

Adding a security Department

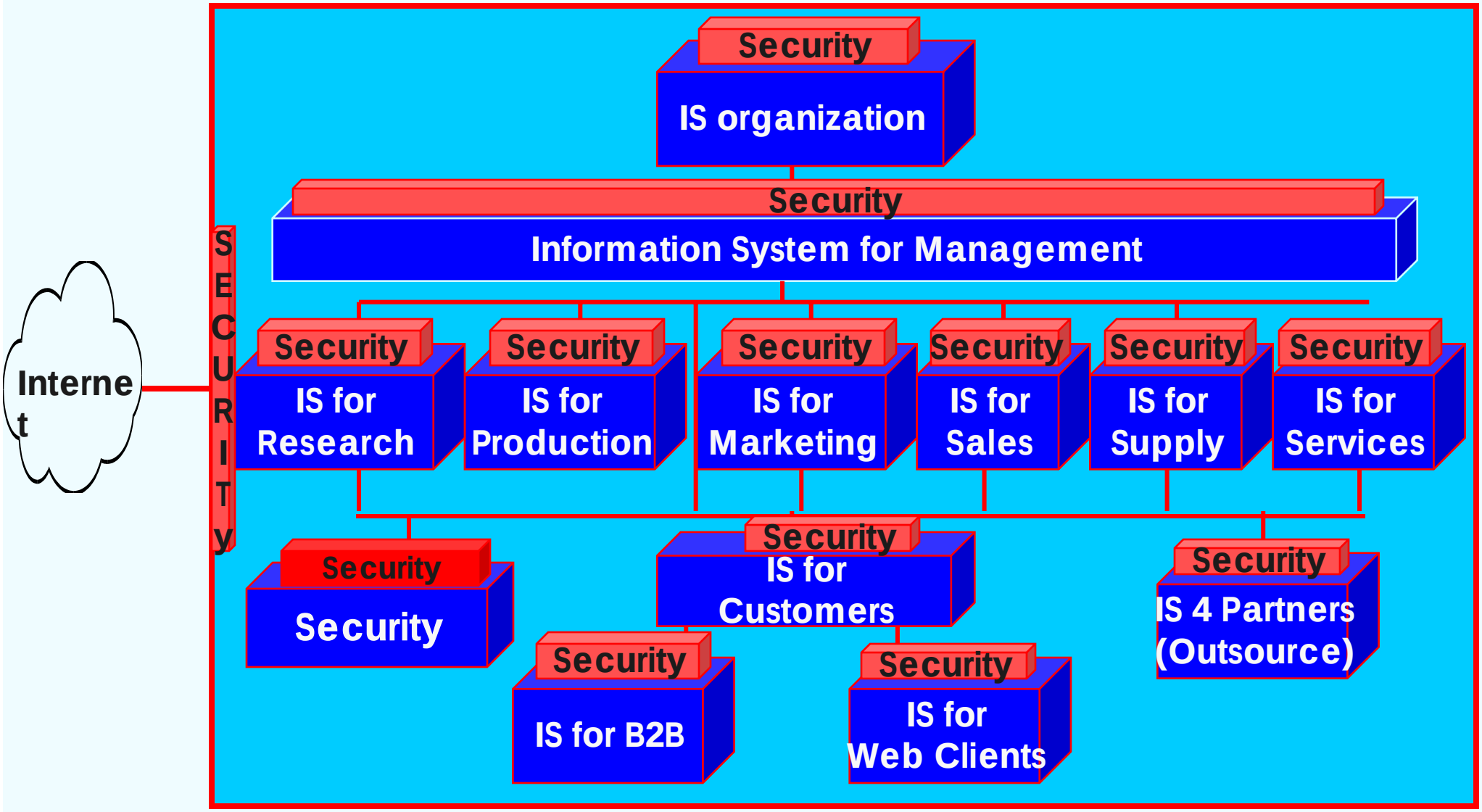
- Security Management section

1) Security planning
2) Security requirements Assessment
3) Business continuity planning

- Security Technology section

1) Computer and Network administration
2) Network management
3) Testing and troubleshooting

Organization with a Security Department



PART II: Organizational Security

- Introduction
- Securing Information Systems of an Organization
- Corporate Security Planning
- Adding a security Department

Summary

PART I Security Overview

1) **Introduction**
2) **Security Services and Implementation**
3) **Overview of Existing Security Systems**
4) **Implementing Security in a System**

- **PART II: Organizational Security**

1) Introduction

2) Securing Information Systems of an Organization

3) Corporate Security Planning

4) Adding a Security Department

Questions