Module 13

Operating Systems Two

Module Thirteen

- Operating Systems - Part Two

- In this presentation, we are going to talk about :

- Data Security

- Design Options

Overview

- Previously we talked about:

- Resource Allocation

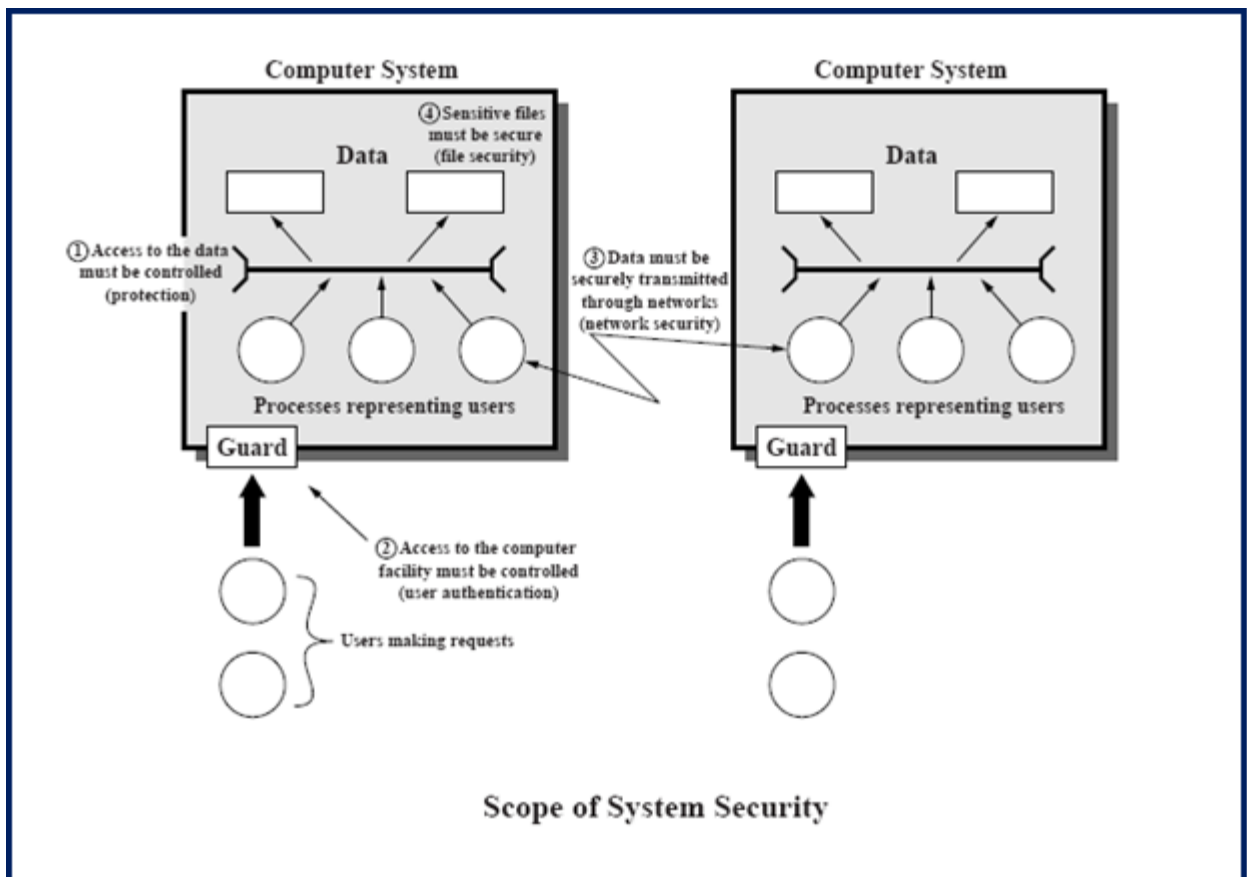   Now: Data Security
                 Design Options
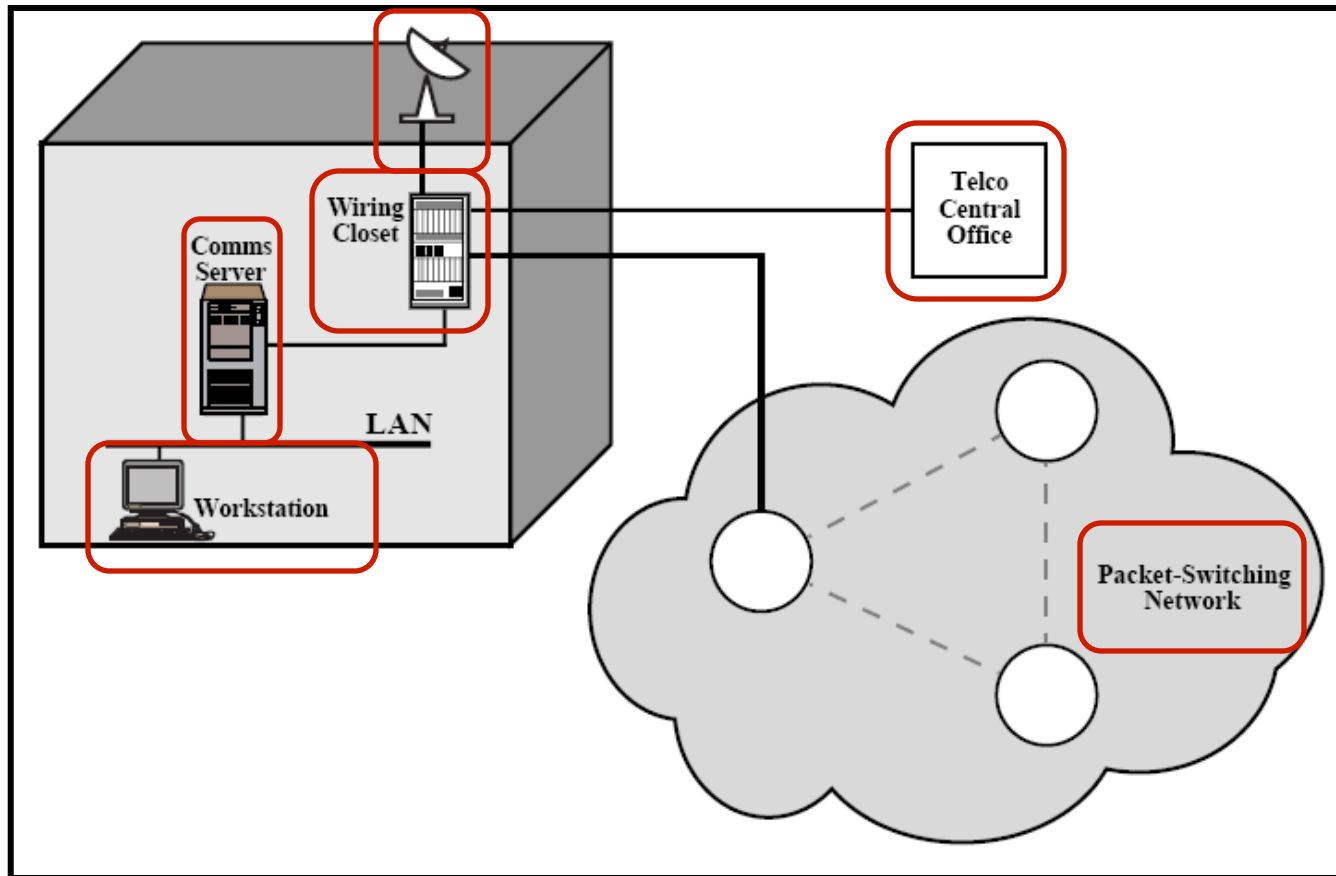
System Security

Access to data

Access to facility

Remote access

Sensitive data

Computer System

Data

④ Sensitive files must be secure (file security)

① Access to the data must be controlled (protection)

③ Data must be securely transmitted through networks (network security)

Processes representing users

Guard

② Access to the computer facility must be controlled (user authentication)

Users making requests

Computer System

Data

Processes representing users

Guard

Scope of System Security

Points of Vulnerability

Data Security

- File Access Control

    Read/Write/Execute/Append

    User/Group/Library

- Passwords on User Accounts

- Hardware - Software cooperation

    Memory Protection

    Supervisor Mode

    Privileged Instructions - executed only by the monitor,
   an interrupt occurs if a program tries these instructions

   Privileged I/O channels: System Console

Data Security

- Access control

  regulate user access to the system

- Information flow control

  regulate flow of data within the system and its delivery to users

- Certification

  proving that access and flow control perform according to specifications

- Secure Building

- Encryption

- RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described it in 1978.
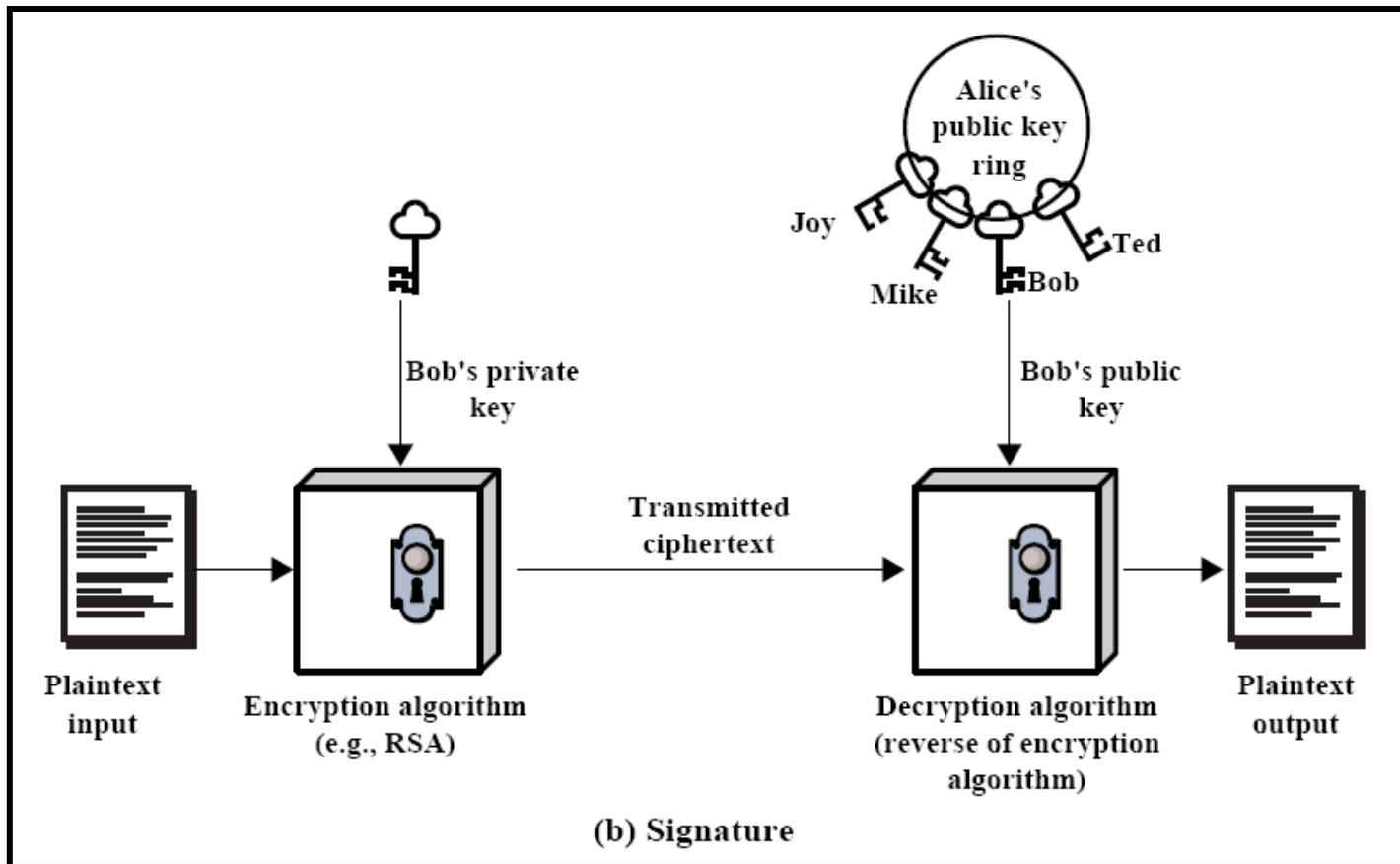
Taxonomy of malicious programs
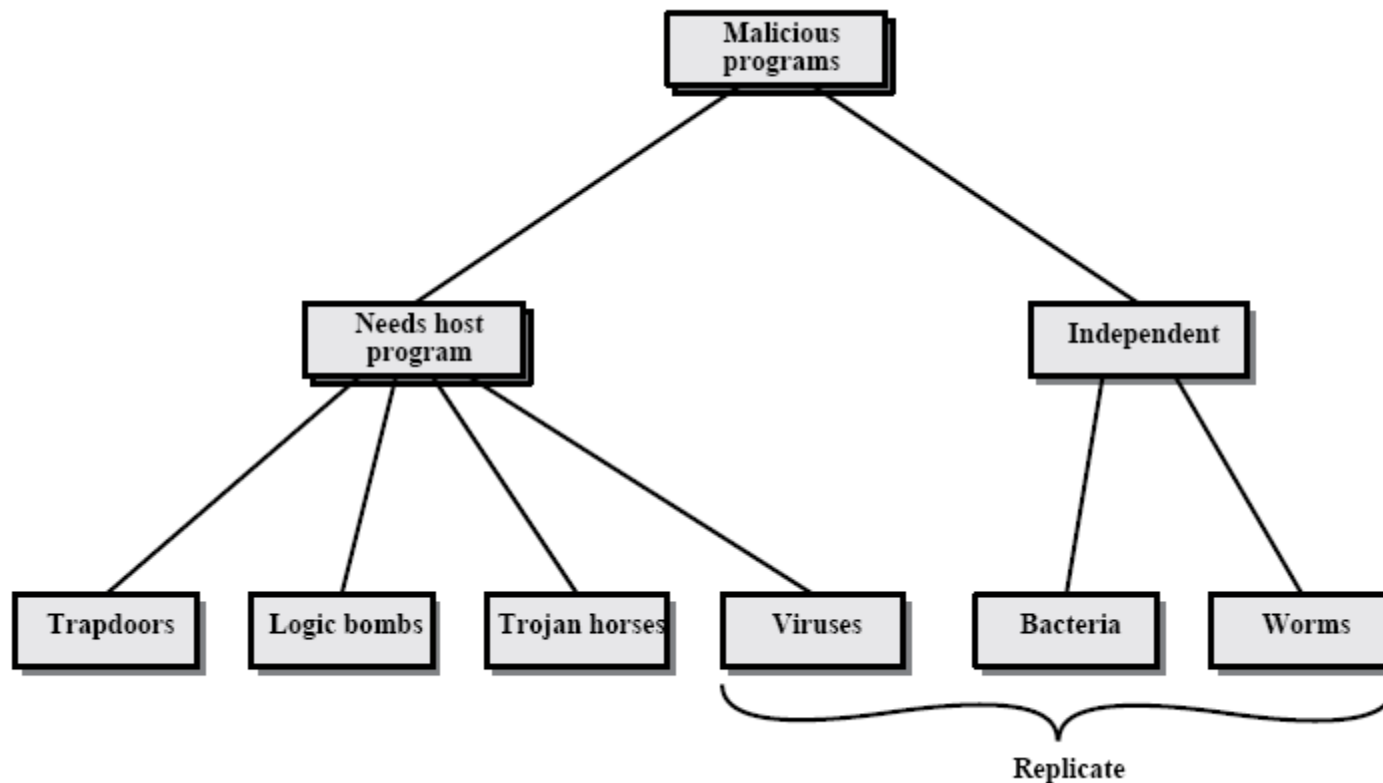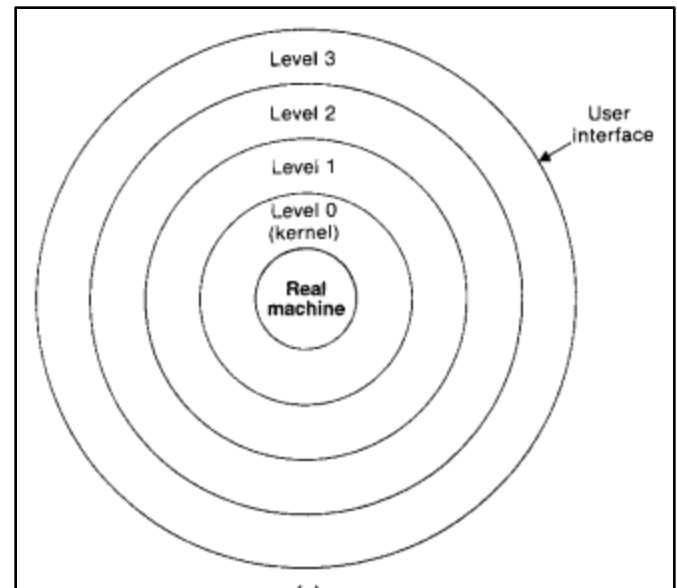
Public Key Encryption

(a) Encryption

Public Key Encryption

(b) Signature
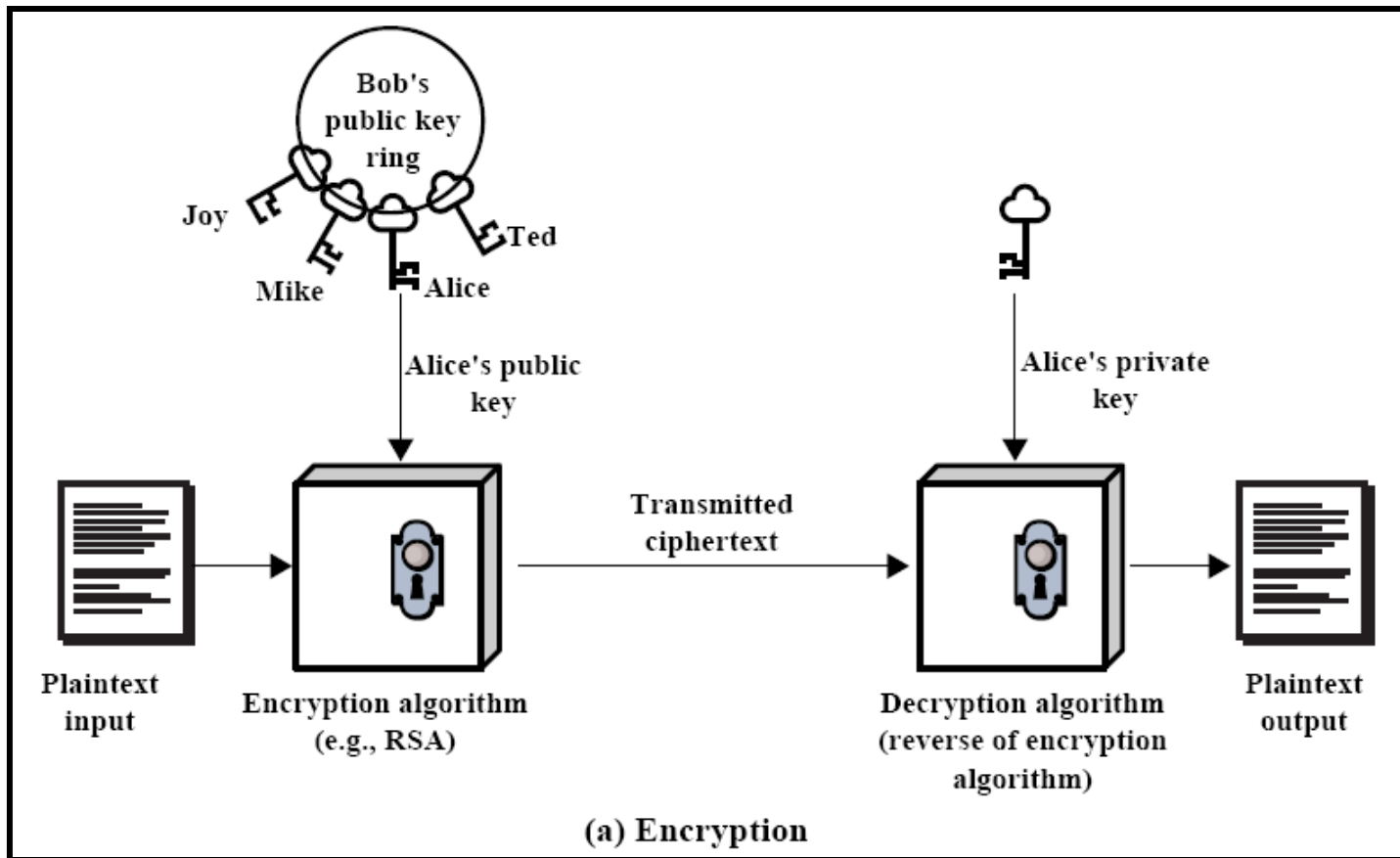
Design Options

- Hierarchical Structure
    - Kernel - dispatch, resource manager
    - level 1 - I/O Supervisor
    - level 2 - memory manager
    - level 3 - file manager

    - Strict Hierarchy
    - Transparent

- Virtual Machine Monitor

- Multi - processor
    - Loosely coupled
    - Tightly coupled

Operating System Design

Level	Name	Objects	Example Operations
13	Shell	User programming environment	Statements in shell language
12	User processes	User processes	Quit, kill, suspend, resume
11	Directories	Directories	Create, destroy, attach, detach, search, list
10	Devices	External devices, such as printer, displays and keyboards	Create, destroy, open, close, read, write
9	File system	Files	Create, destroy, open, close read, write
8	Communications	Pipes	Create, destroy, open. close, read, write
7	Virtual Memory	Segments, pages	Read, write, fetch

Operating System Design

Level	Name	Objects	Example Operations
6	Local secondary store	Blocks of data, device channels	Read, write, allocate, free
5	Primitive processes	Primitive process, semaphores, ready list	Suspend, resume, wait, signal
4	Interrupts	Interrupt-handling programs	Invoke, mask, unmask, retry
3	Procedures	Procedures, call stack	Mark stack, call, return
2	Instruction Set	Evaluation stack,micro-program interpreter, scalar and array data	Load, store, add, subtract branch
1	Electronic circuits	Registers, gates, buses, etc.	Clear, transfer, activate, complement

Operating System Characteristics

- Micro-kernel architecture - assigns only a few essential functions to the kernel.
    - address space
    - Inter-process communication (IPC)
    - basic scheduling

- Multithreading - process is divided into threads that can run simultaneously.

- Thread - dispatchable unit of work, executes sequentially, and is interruptible.

- Process is a collection of one or more threads.

Operating System Characteristics

- Symmetric multiprocessing

    There are multiple processors.

    These processors share same main memory and I/O facilities.

    All processors can perform the same functions.

- Distributed operating systems

    Provides the illusion of a single main memory.

    Used for distributed file system.

- Object-oriented design

    Used for adding modular extensions to a small kernel.

    Enables programmers to customize an operating system without disrupting system integrity.

Review

- Operating Systems: Part Two

- Hardware Independent Tasks

  – File Processing
  – Job Scheduling
  – Resource Allocation
  – Data Security

- Design Options