Security

Chapter 16

* Three keys computer security goals:

1. Confidentiality
   - 1.1 Data Confidentiality — authorized entity
   - 1.2 Privacy
2. Integrity
   - 2.1 Data Integrity — authorized entity, authorized mechanism
   - 2.2 System Integrity — a system peforms in an unimpaired manner
3. Availability — services is not denied to authorized users — dinial of services
4. Authenticity — property of being genuine and able to be verified and trusted for
   - confidence in validity of transmission; both messages and message origina
5. Accountability — ability to trace a security breach to a responsible party or aid in transaction disputes

The National Institute of Standards and Technology (NIST) defines computer security as:

"The protection afforded to an automated IS in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of IS resources."

Table 14.2 Computer and Network Assets, with Examples of Threats

	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service.		
Software	Programs are deleted, denying access to users.	An unauthorized copy of software is made.	A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task.
Data	Files are deleted, denying access to users.	An unauthorized read of data is performed. An analysis of statistical data reveals underlying data.	Existing files are modified or new files are fabricated.
Communication Lines	Messages are destroyed or deleted. Communication lines or networks are rendered unavailable.	Messages are read. The traffic pattern of messages is observed.	Messages are modified, delayed, reordered, or duplicated. False messages are fabricated.

→ viruses
→ s/w piracy

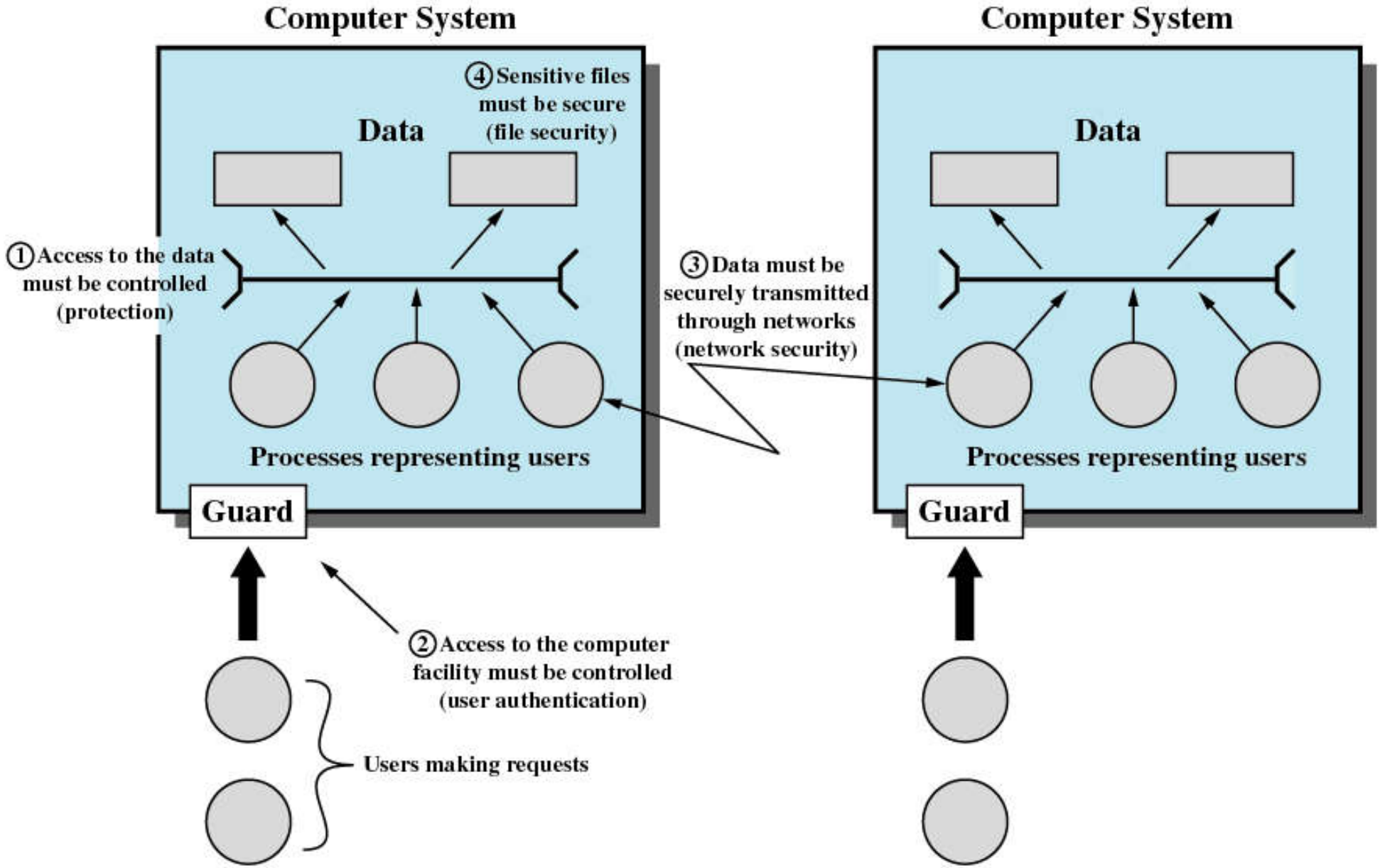
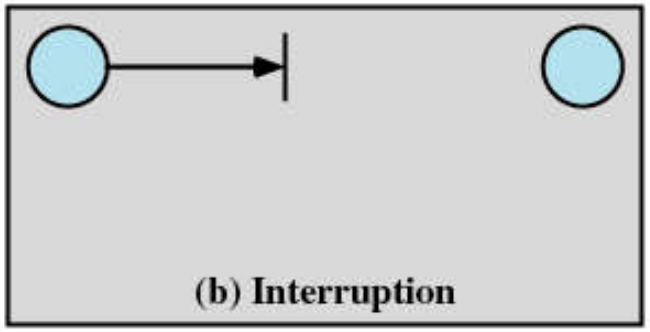


Figure 16.1 Scope of System Security [MAEK87]

Types of Threats

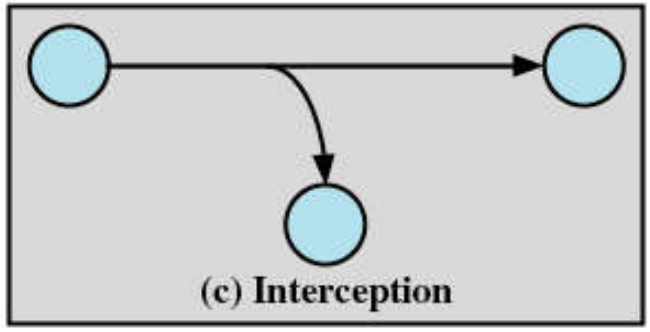
- Interruption
  - An asset of the system is destroyed of becomes unavailable or unusable
  - Attack on availability
  - Destruction of hardware
  - Cutting of a communication line
  - Disabling the file management system



Types of Threats

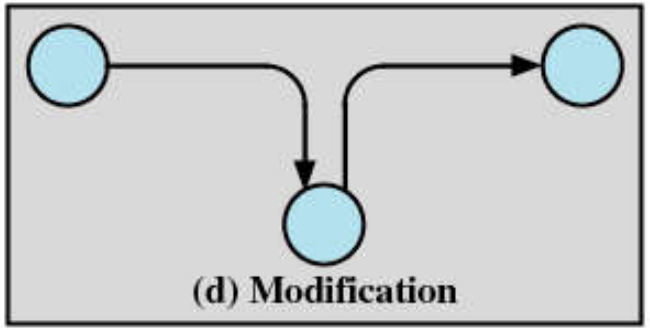
- Interception
  - An unauthorized party gains access to an asset
  - Attack on confidentiality
  - Wiretapping to capture data in a network
  - Illicit copying of files or programs

illegitimato



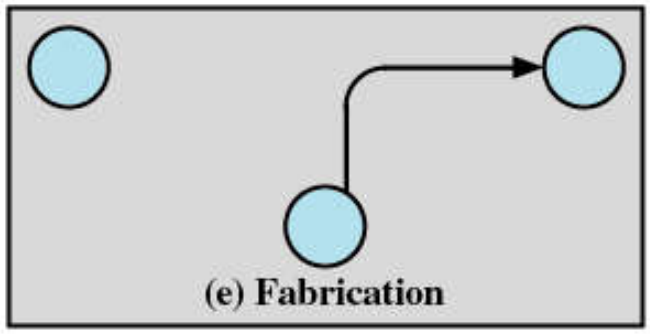
Types of Threats

- Modification
  - An unauthorized party not only gains access but tampers with an asset
  - Attack on integrity
  - Changing values in a data file
  - Altering a program so that it performs differently
  - Modifying the content of messages being transmitted in a network



Types of Threats

- Fabrication
  - An unauthorized party inserts counterfeit objects into the system
  - Attack on authenticity
  - Insertion of spurious messages in a network
  - Addition of records to a file



Computer System Assets

- Hardware
  - Threats include accidental and deliberate damage
- Software
  - Threats include deletion, alteration, damage
  - Backups of the most recent versions can maintain high availability

Computer System Assets

- Data
  - Involves files
  - Security concerns ~~fro~~ of availability, secrecy, and integrity
  - Statistical analysis can lead to determination of individual information which threatens privacy

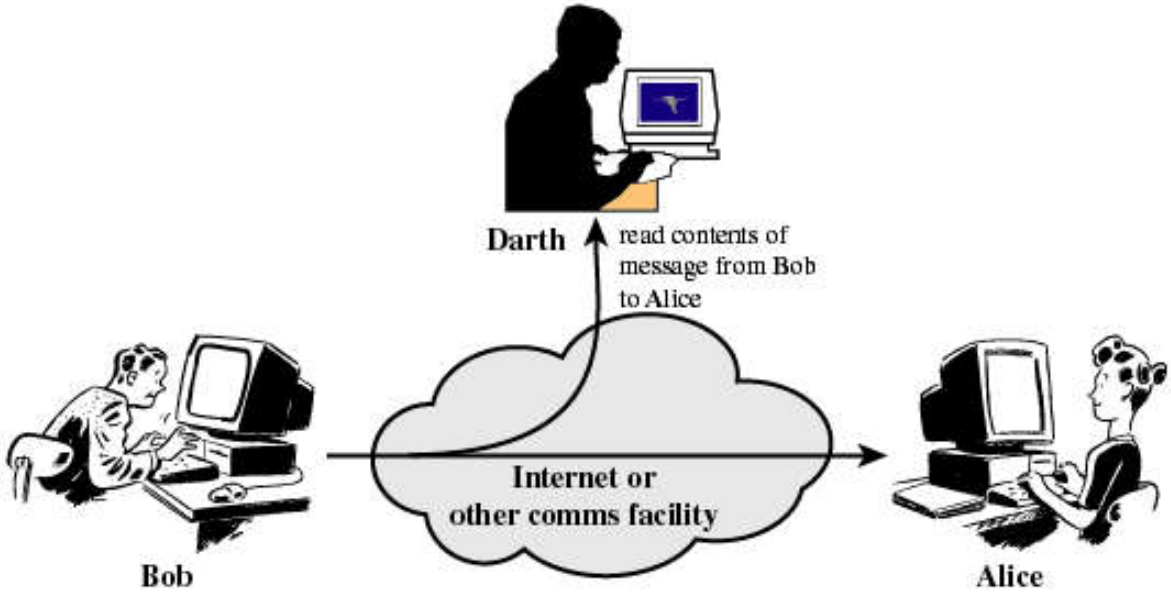
Computer System Assets

- Communication Lines and Networks – Passive Attacks
  - Learn or make use of information from the system but does not affect system resources
  - Traffic analysis
    - Encryption masks the contents of what is transferred so even if obtained by someone, they would be unable to extract information

* Passive attack: prevent rather than detect

Computer System Assets

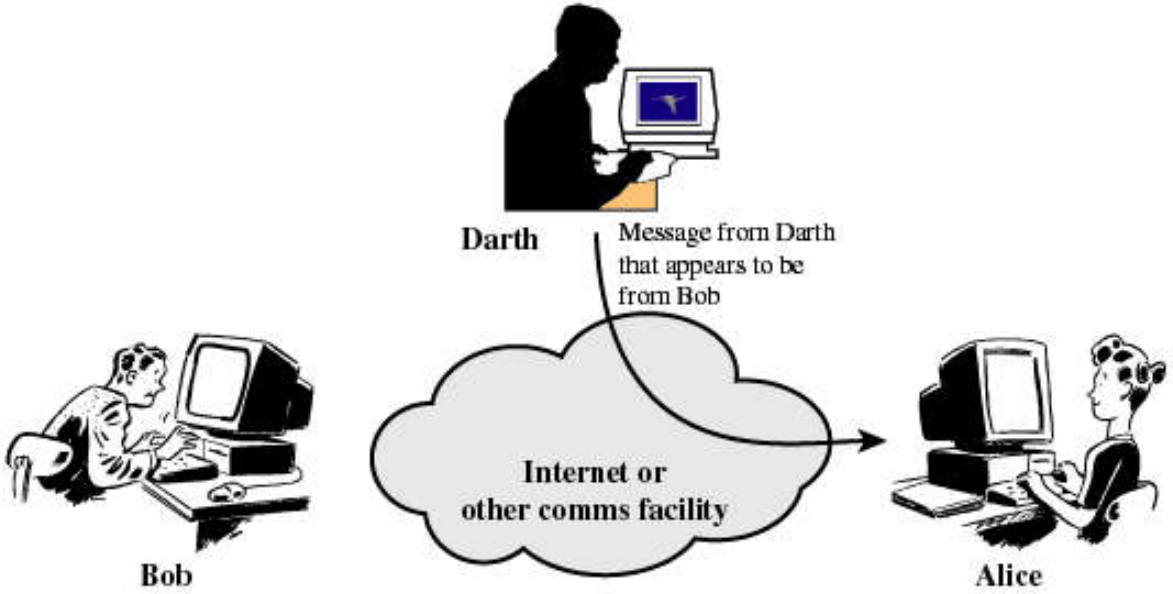
- Communication Lines and Networks – Passive Attacks
  - Release of message contents for a telephone conversion, an electronic mail message, and a transferred file are subject to these threats



(a) Release of message contents

Computer System Assets

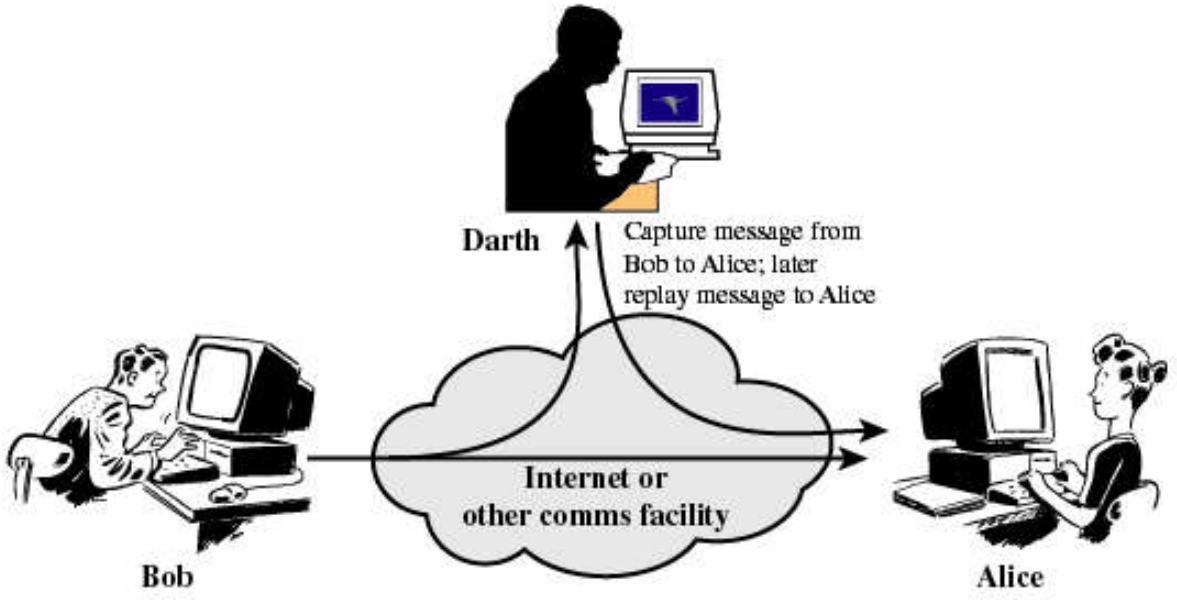
- Communication Lines and Networks – Active Attacks → alter system resources → affect their operations
  - Masquerade takes place when one entity pretends to be a different entity



(a) Masquerade

Computer System Assets

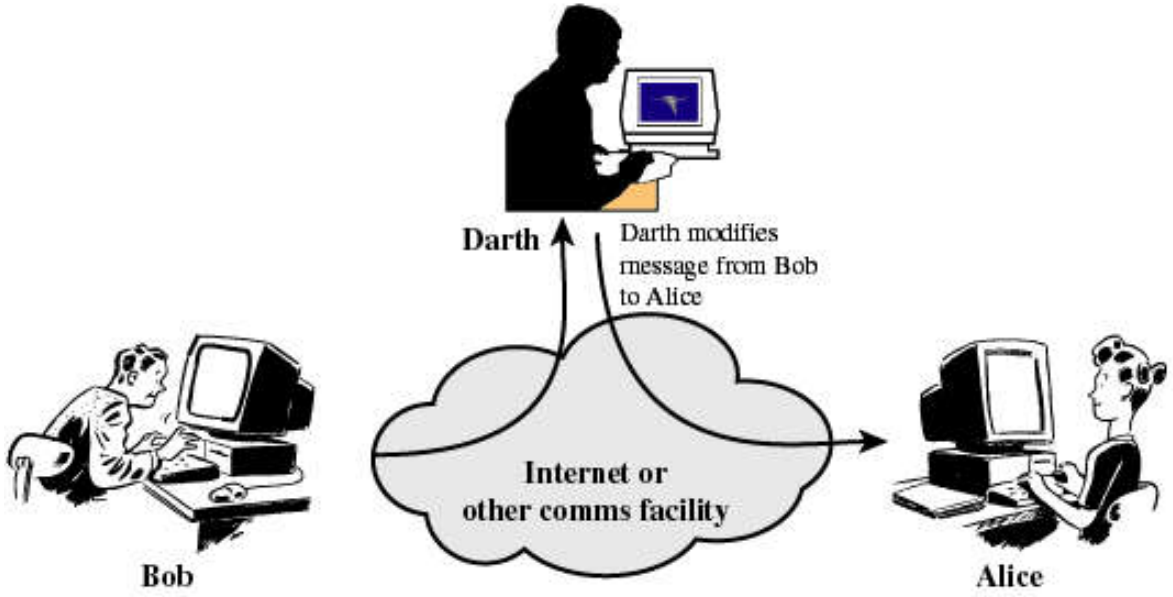
- Communication Lines and Networks – Active Attacks
  - Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect



(b) Replay

Computer System Assets

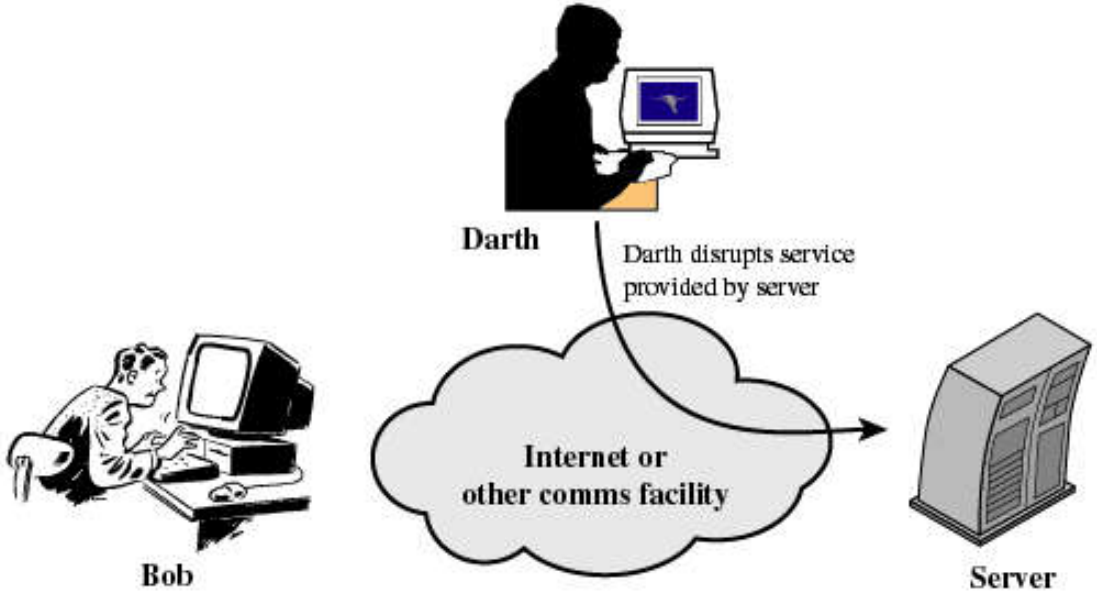
- Communication Lines and Networks – Active Attack
  - Modification of messages means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect



(c) Modification of messages

Computer System Assets

- Communication Lines and Networks – Active Attacks
  - Denial of service prevents or inhibits the normal use or management of communications facilities
    - Disable network or overload it with messages



(d) Denial of service

Protection

- No protection
  - Sensitive procedures are run at separate times
- Isolation
  - Each process operates separately from other processes with no sharing or communication

Protection

- Share all or share nothing
  - Owner of an object declares it public or private
- Share via access limitation
  - Operating system checks the permissibility of each access by a specific user to a specific object
  - Operating system acts as the guard

Protection

- Share via dynamic capabilities
  - Dynamic creation of sharing rights for objects
- Limit use of an object
  - Limit not just access to an object but also the use to which that object may be put
  - Example: a user may be able to derive statistical summaries but not to determine specific data values

User-Oriented Access Control

- Referred as authentication
- Log on
  - Requires both a user identifier (ID) and a password
  - System only allows users to log on if the ID is known to the system and password associated with the ID is correct
  - Users can reveal their password to others either intentionally or accidentally
  - Hackers are skillful at guessing passwords
  - ID/password file can be obtained

Data-Oriented Access Control

- Associated with each user, there can be a profile that specifies permissible operations and file accesses
- Operating system enforces these rules
- Database management system controls access to specific records or portions of records

Access Matrix

- Subject
  - An entity capable of accessing objects
- Object
  - Anything to which access is controlled
- Access rights
  - The way in which an object is accessed by a subject

Access Matrix

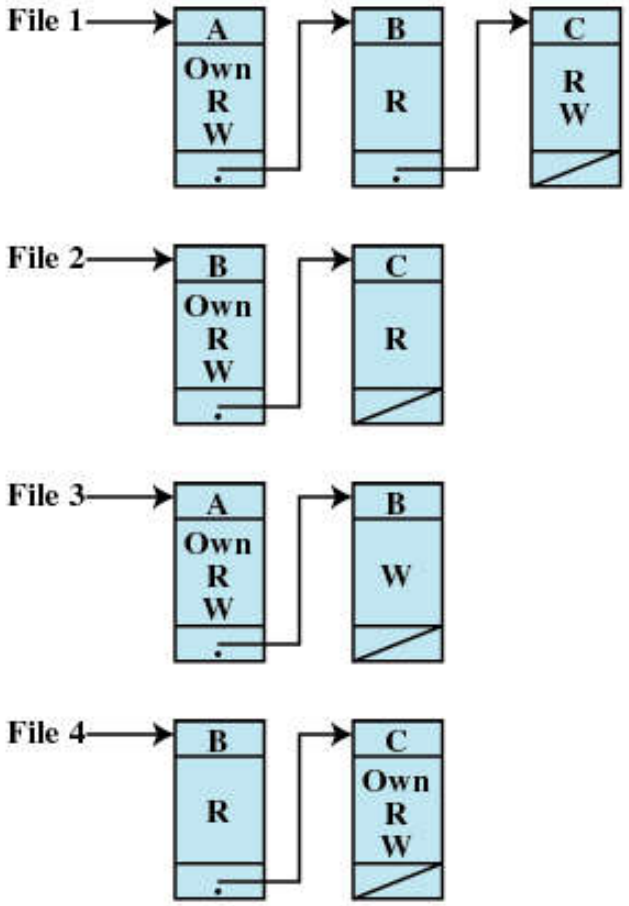
	File 1	File 2	File 3	File 4	Account 1	Account 2
User A	Own R W		Own R W		Inquiry Credit	
User B	R	Own R W	W	R	Inquiry Debit	Inquiry Credit
User C	R W	R		Own R W		Inquiry Debit

(a) Access matrix

Access Control List

- Matrix decomposed by columns
- For each object, an access control list gives users and their permitted access rights

Access Control List

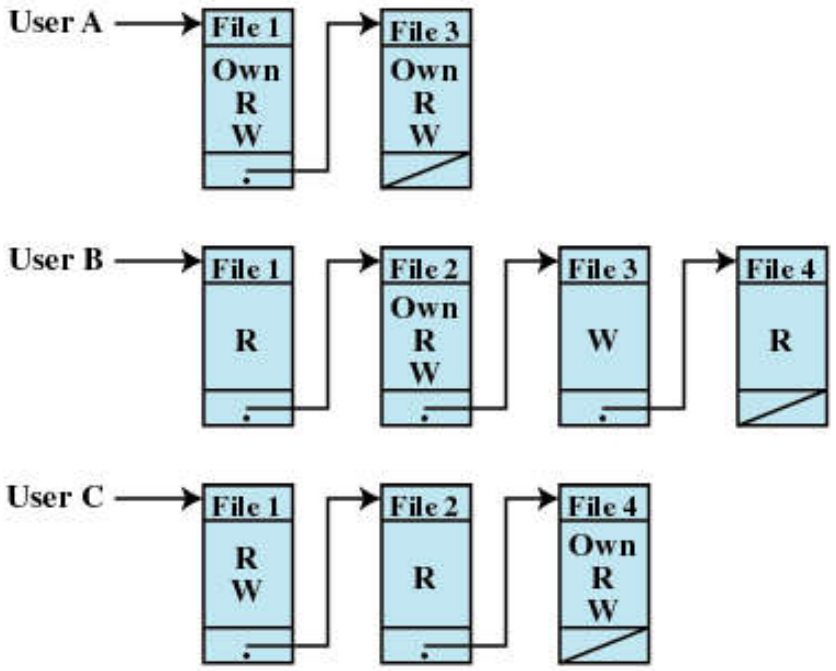


(b) Access control lists for files of part (a)

Capability Tickets

- Decomposition of access matrix by rows
- Specifies authorized objects and operations for a user

Capability Tickets



(c) Capability lists for files of part (a)

Intrusion Techniques

- Objective of intruder is the gain access to the system or to increase the range of privileges accessible on a system
- Protected information that an intruder acquires is a password

Techniques for Learning Passwords

- Try default password used with standard accounts shipped with system
- Exhaustively try all short passwords
- Try words in dictionary or a list of likely passwords
- Collect information about users and use these items as passwords

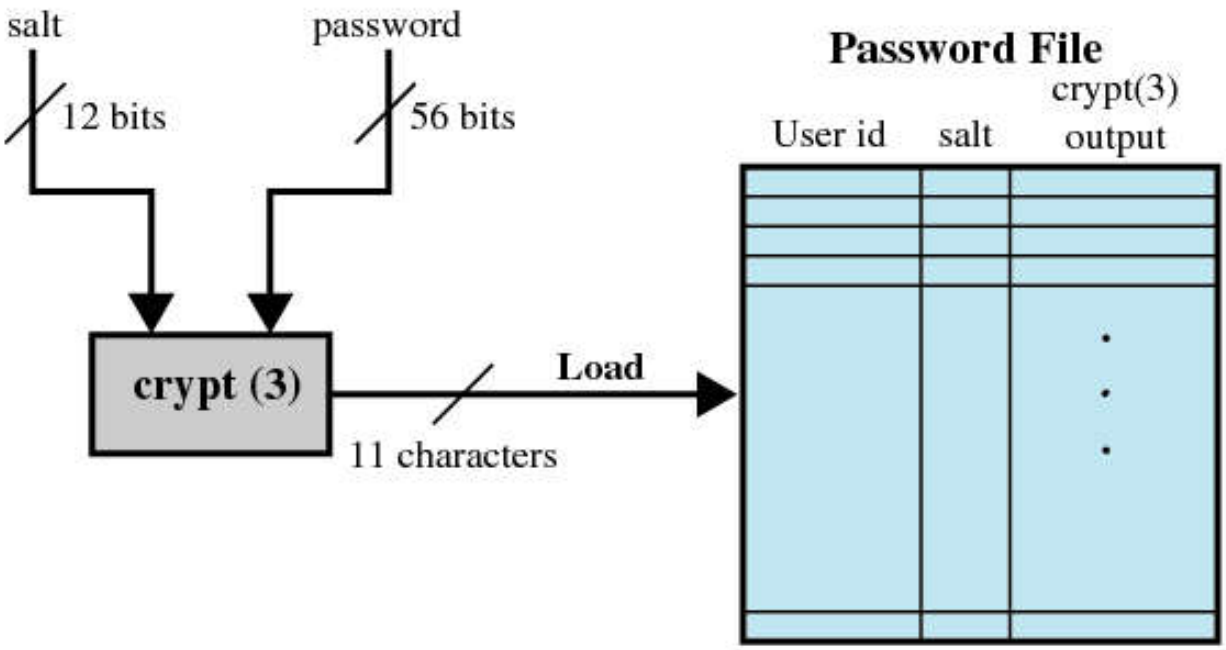
Techniques for Learning Passwords

- Try users' phone numbers, social security numbers, and room numbers
- Try all legitimate license plate numbers for this state
- Use a Trojan horse to bypass restrictions on access
- Tap the line between a remote user and the host system

ID Provides Security

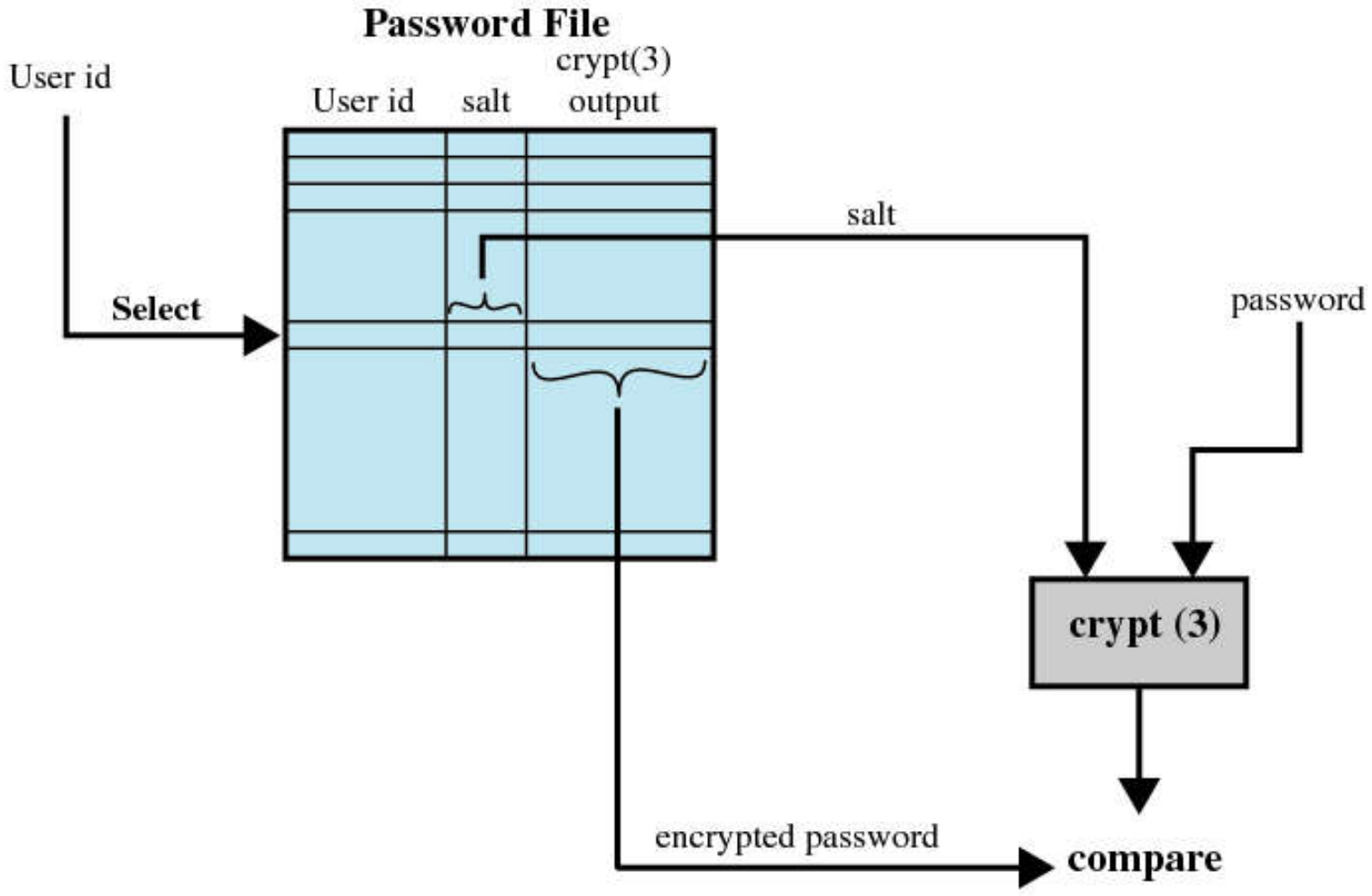
- Determines whether the user is authorized to gain access to a system
- Determines the privileges accorded to the user
  - Superuser enables file access protected by the operating system
  - Guest or anonymous accounts have more limited privileges than others
- ID is used for discretionary access control
  - A user may grant permission to files to others by ID

UNIX Password Scheme



(a) Loading a new password

UNIX Password Scheme



(b) Verifying a password

Password Selection Strategies

- Computer generated passwords
  - Users have difficulty remembering them
  - Need to write it down
  - Have history of poor acceptance

Password Selection Strategies

- Reactive password checking strategy
  - System periodically runs its own password cracker to find guessable passwords
  - System cancels passwords that are guessed and notifies user
  - Consumes resources to do this
  - Hacker can use this on their own machine with a copy of the password file

Password Selection Strategies

- Proactive password checker
  - The system checks at the time of selection if the password is allowable
  - With guidance from the system users can select memorable passwords that are difficult to guess

* A loose interpretation of intruder behavior ⇒ catch more intruders
* A tight interpretation of intruder behavior ⇒ intruders not identified as intruders

false negatives

false positives

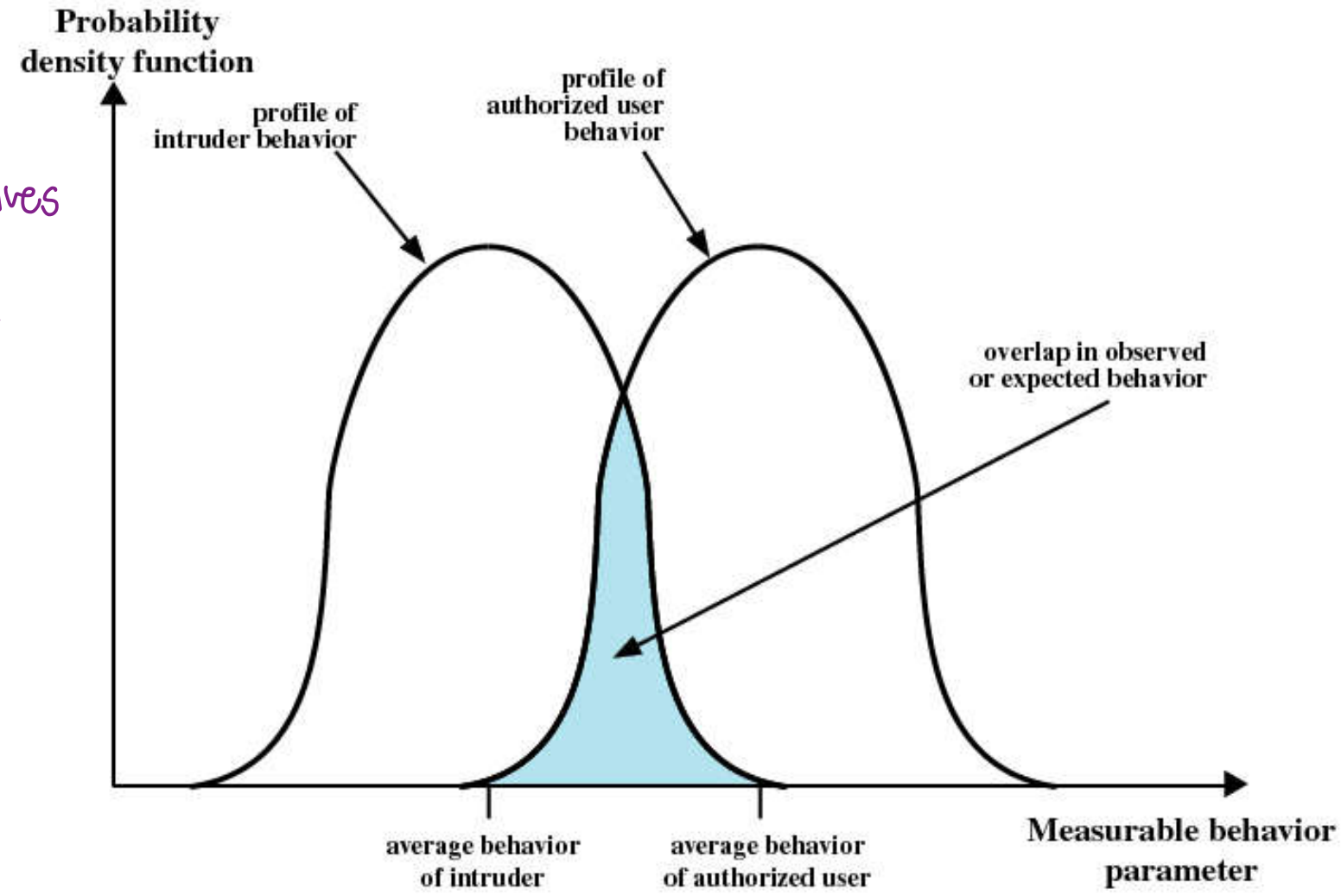


Figure 16.7 Profiles of Behavior of Intruders and Authorized Users

* Detecting a misfeasor is more difficult !!
(legitimate users performing unauthorized fashion)

Intrusion Detection

- Assume the behavior of the intruder differs from the legitimate user
- Statistical anomaly detection
  - Collect data related to the behavior of legitimate users over a period of time
  - Statistical tests are used to determine if the behavior is not legitimate behavior

Intrusion Detection

- Rule-based detection
  - Rules are developed to detect deviation from previous usage pattern
  - Expert system searches for suspicious behavior

Intrusion Detection

- Audit record
  - Native audit records
    - All operating systems include accounting software that collects information on user activity
  - Detection-specific audit records
    - Collection facility can be implemented that generates audit records containing only that information required by the intrusion detection system

Malicious Programs

- Those that need a host program
  - Fragments of programs that cannot exist independently of some application program, utility, or system program
- Independent
  - Self-contained programs that can be scheduled and run by the operating system

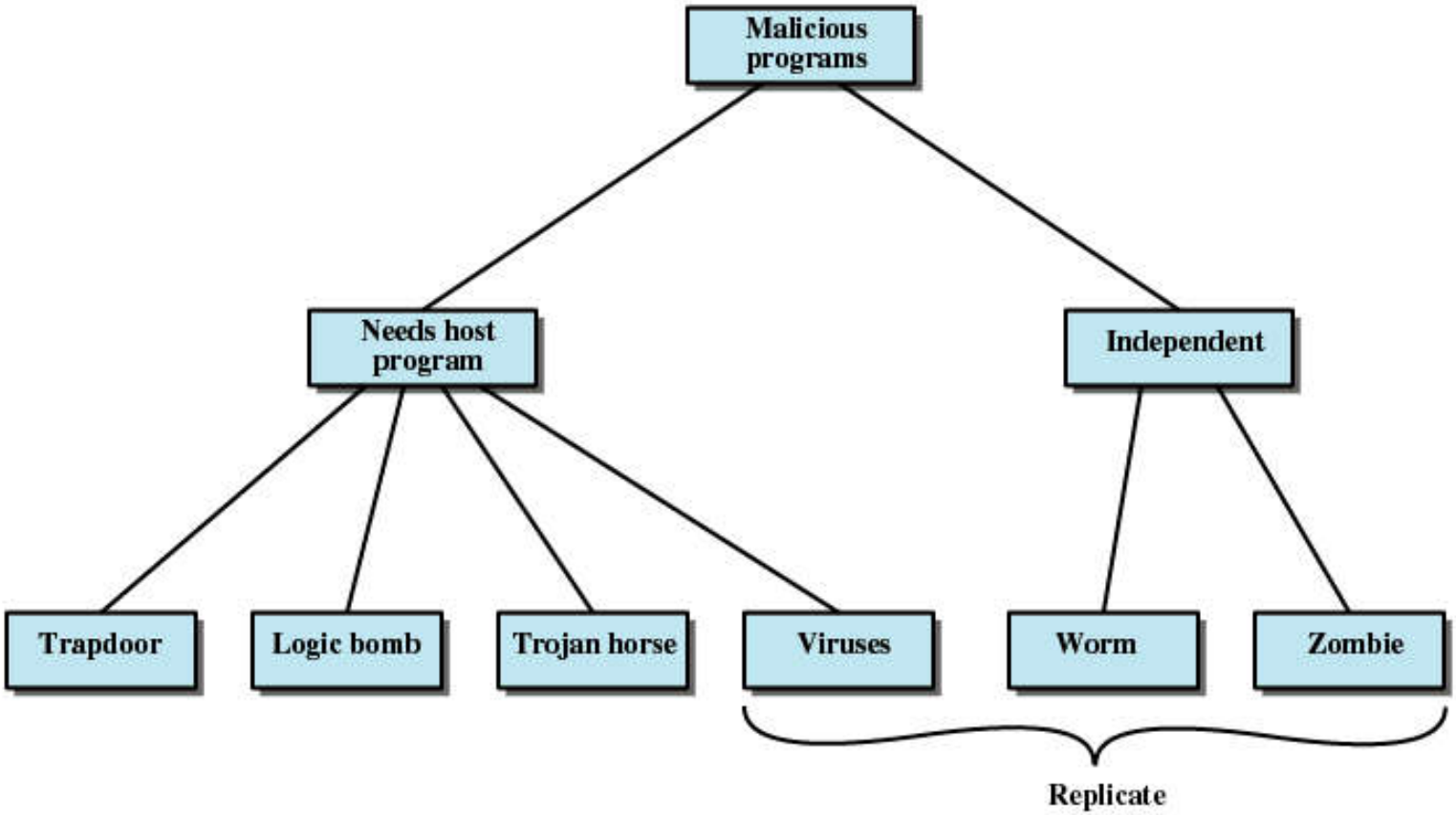


Figure 16.8 Taxonomy of Malicious Programs

Trapdoor: mechanisms bypassing normal security check

Zombie: program actived on infected machine to launch attacks on other machines

Logic bomb: program triggers an unthorized act when predefined cond^{n} is met

Trapdoor

- Entry point into a program that allows someone who is aware of trapdoor to gain access
- Used by programmers to debug and test programs
  - Avoids necessary setup and authentication
  - Method to activate program if something wrong with authentication procedure

Logic Bomb

- Code embedded in a legitimate program that is set to “explode” when certain conditions are met
  - Presence or absence of certain files
  - Particular day of the week
  - Particular user running application

Trojan Horse

- Useful program that contains hidden code that when invoked performs some unwanted or harmful function
- Can be used to accomplish functions indirectly that an unauthorized user could not accomplish directly
  - User may set file permission so everyone has access

Virus

- Program that can “infect” other programs by modifying them
  - Modification includes copy of virus program
  - The infected program can infect other programs

Worms

- Use network connections to spread form system to system
- Electronic mail facility
  - A worm mails a copy of itself to other systems
- Remote execution capability
  - A worm executes a copy of itself on another system
- Remote log-in capability
  - A worm logs on to a remote system as a user and then uses commands to copy itself from one system to the other

Zombie

- Program that secretly takes over another Internet-attached computer
- It uses that computer to launch attacks that are difficult to trace to the zombie's creator

Trusted Systems

- Multilevel security
  - Information organized into levels
  - No read up
    - Only read objects of a less or equal security level
  - No write down
    - Only write objects of greater or equal security level

Rules about how info can flow

* No information can leak out from a higher security level to a lower one

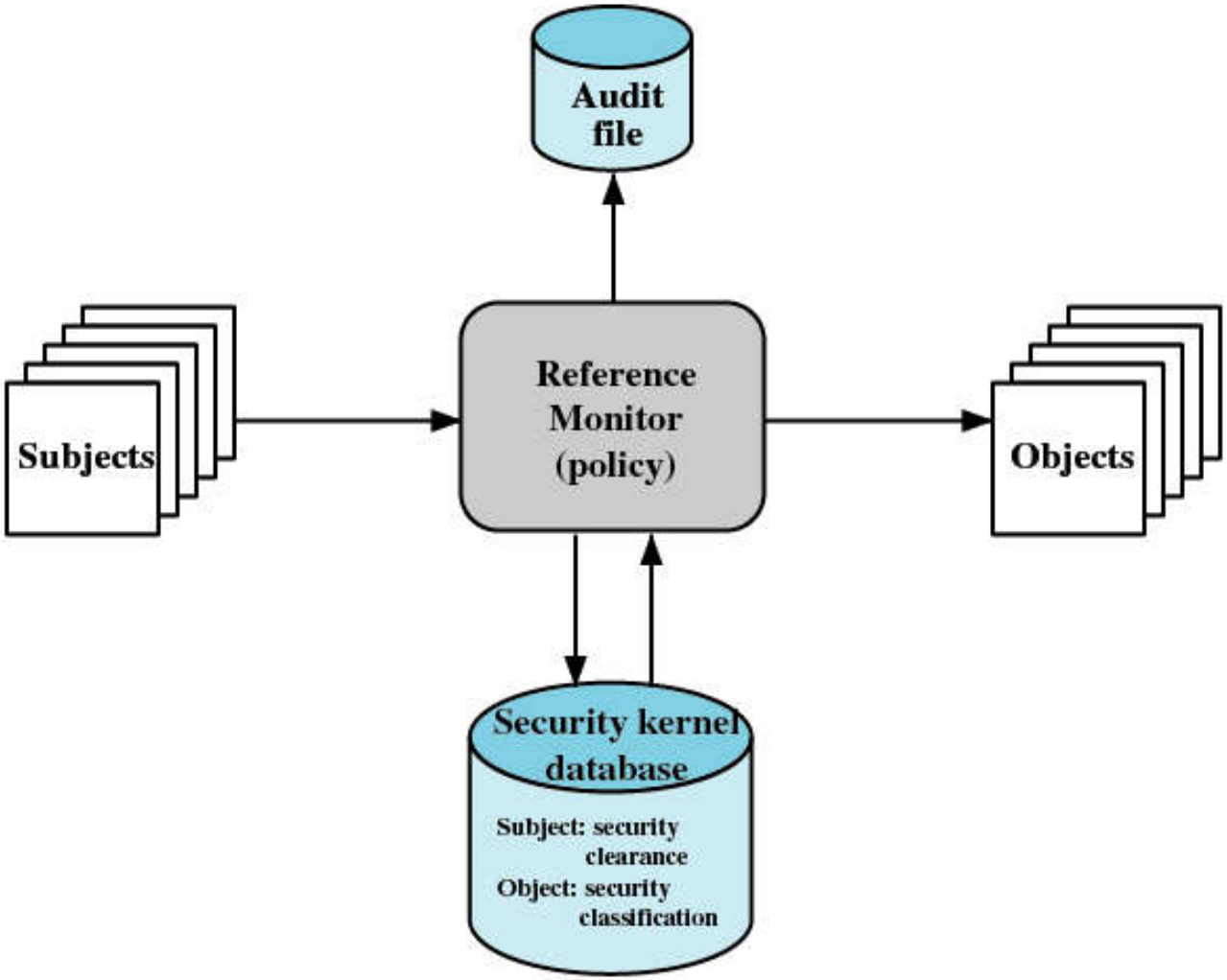
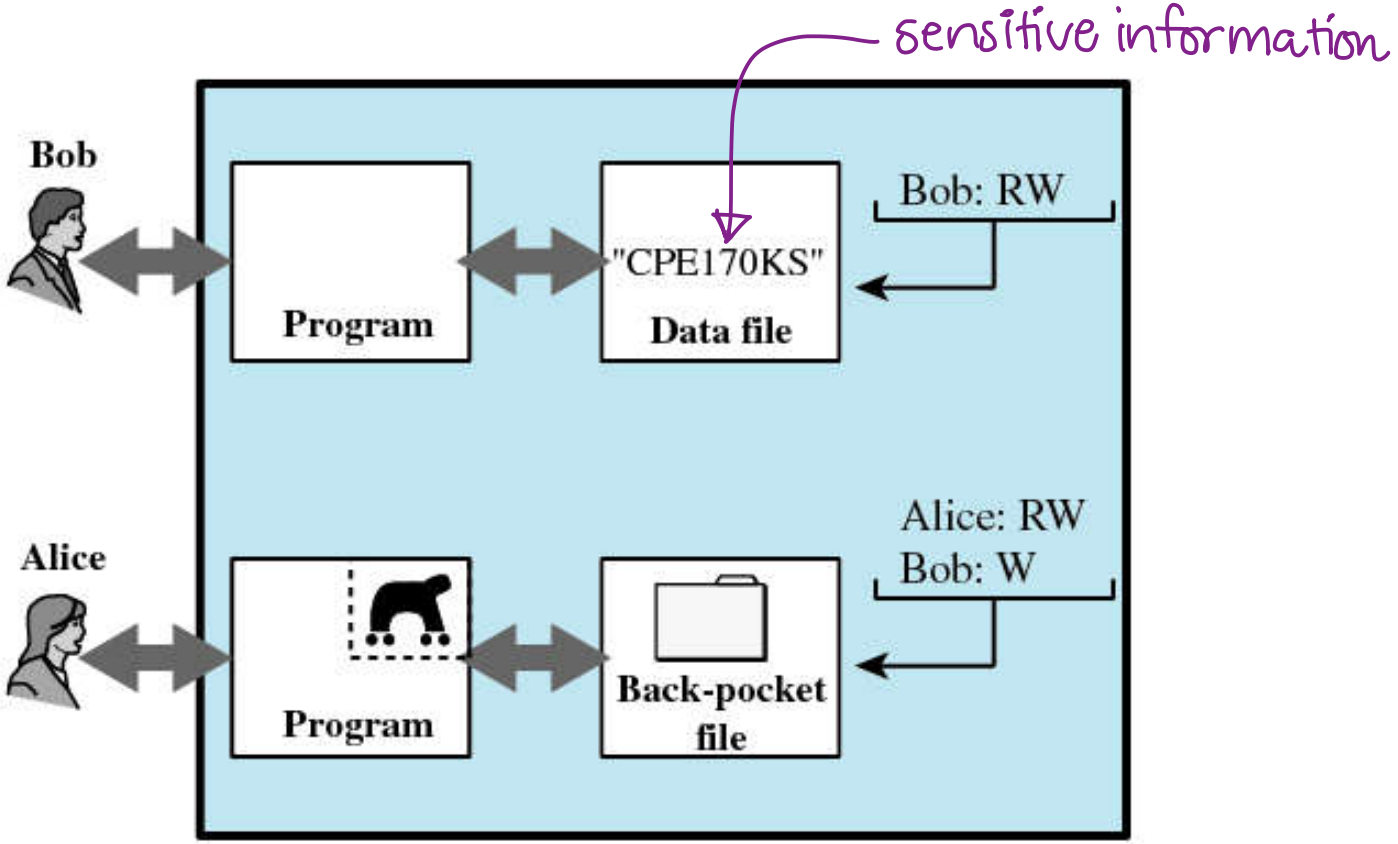


Figure 16.10 Reference Monitor Concept

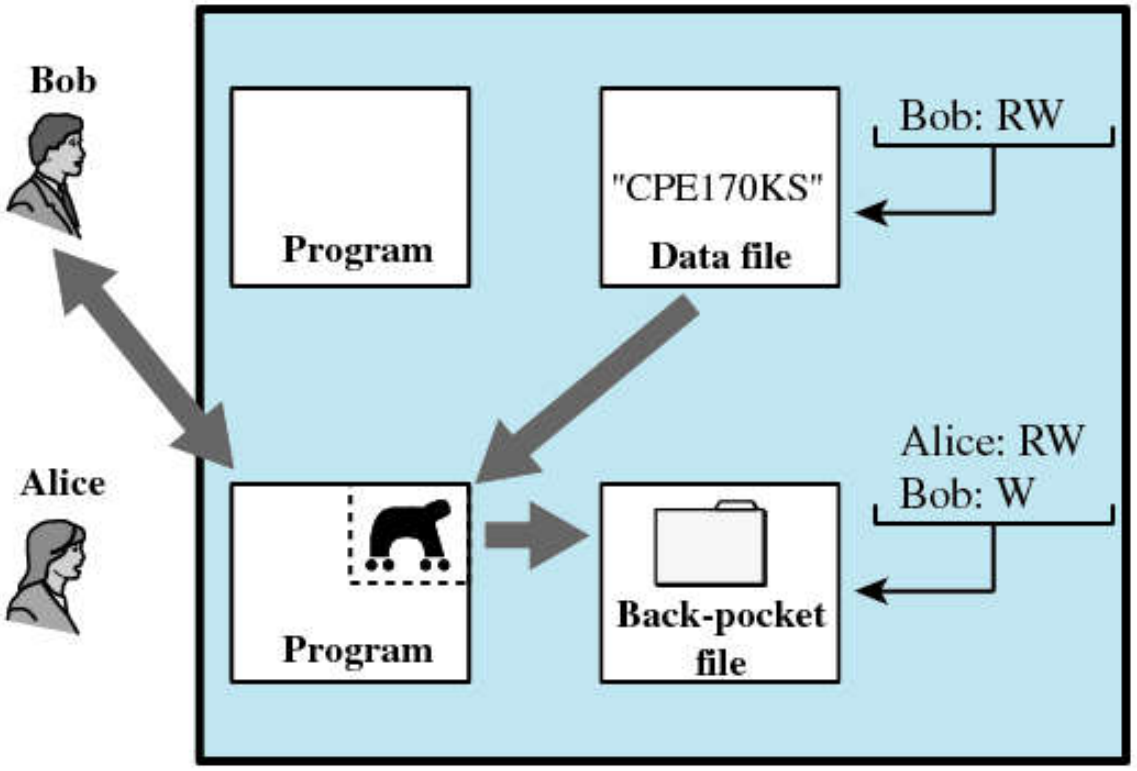
Reference monitor: enforces access-validation and audit-generation rules

Trojan Horse Defense



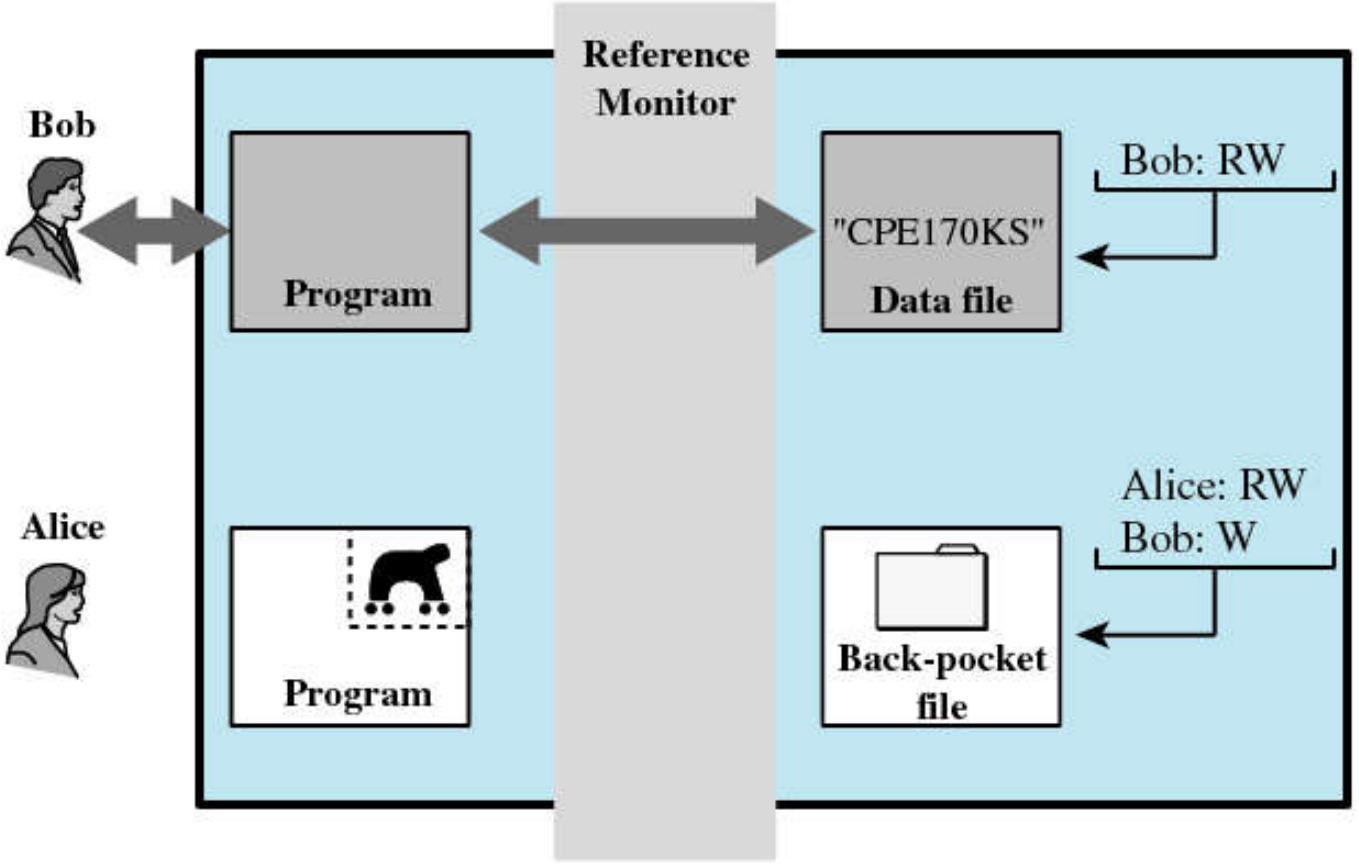
(a)

Trojan Horse Defense



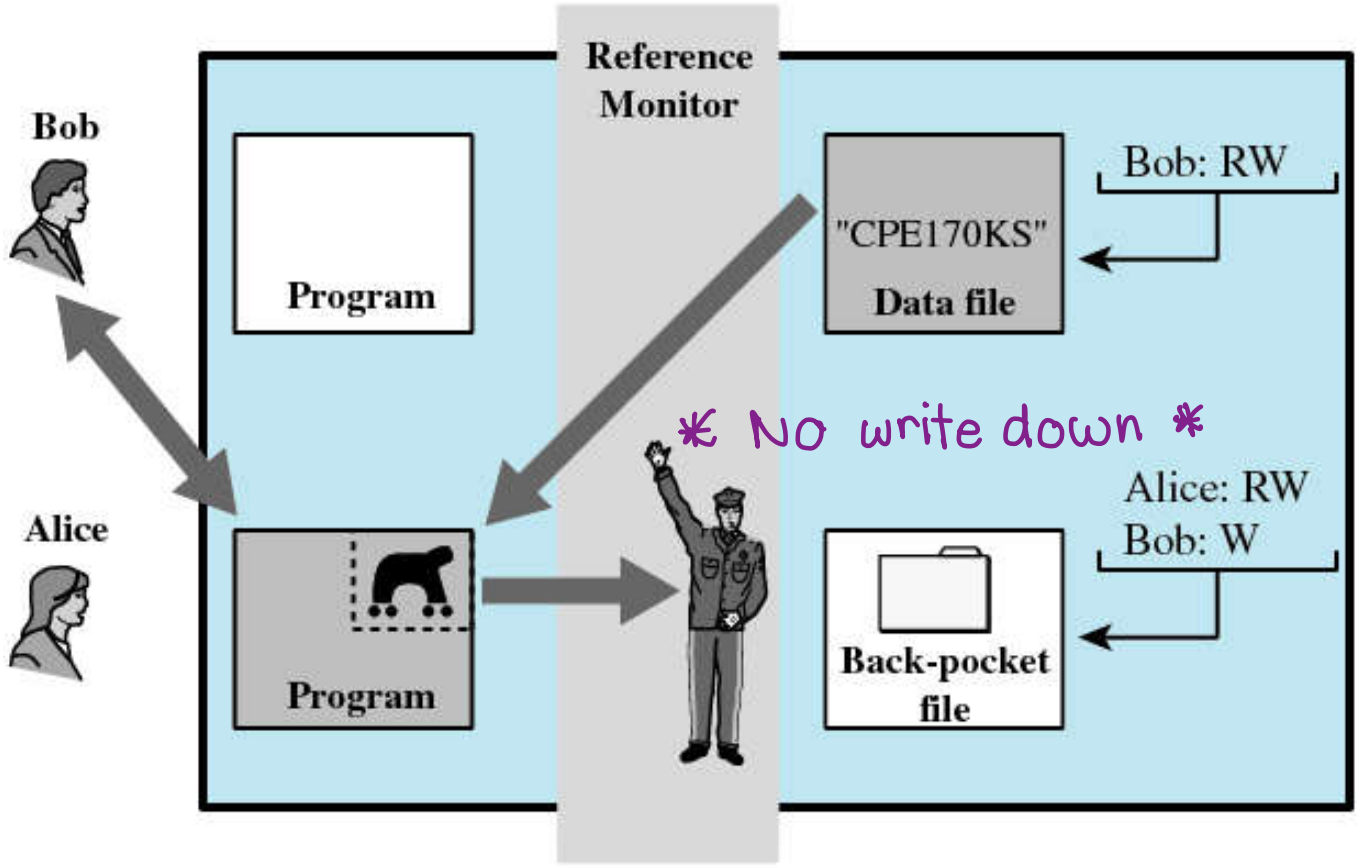
(b)

Trojan Horse Defense



(c)

Trojan Horse Defense



(d)

open a file

Reference monitor accepts all system calls involving security ⇒ decide to process or not

⇒ no possibity to bypass this decision