UPPSALA UNIVERSITET

Informationsteknologi

Today’s class

- Security

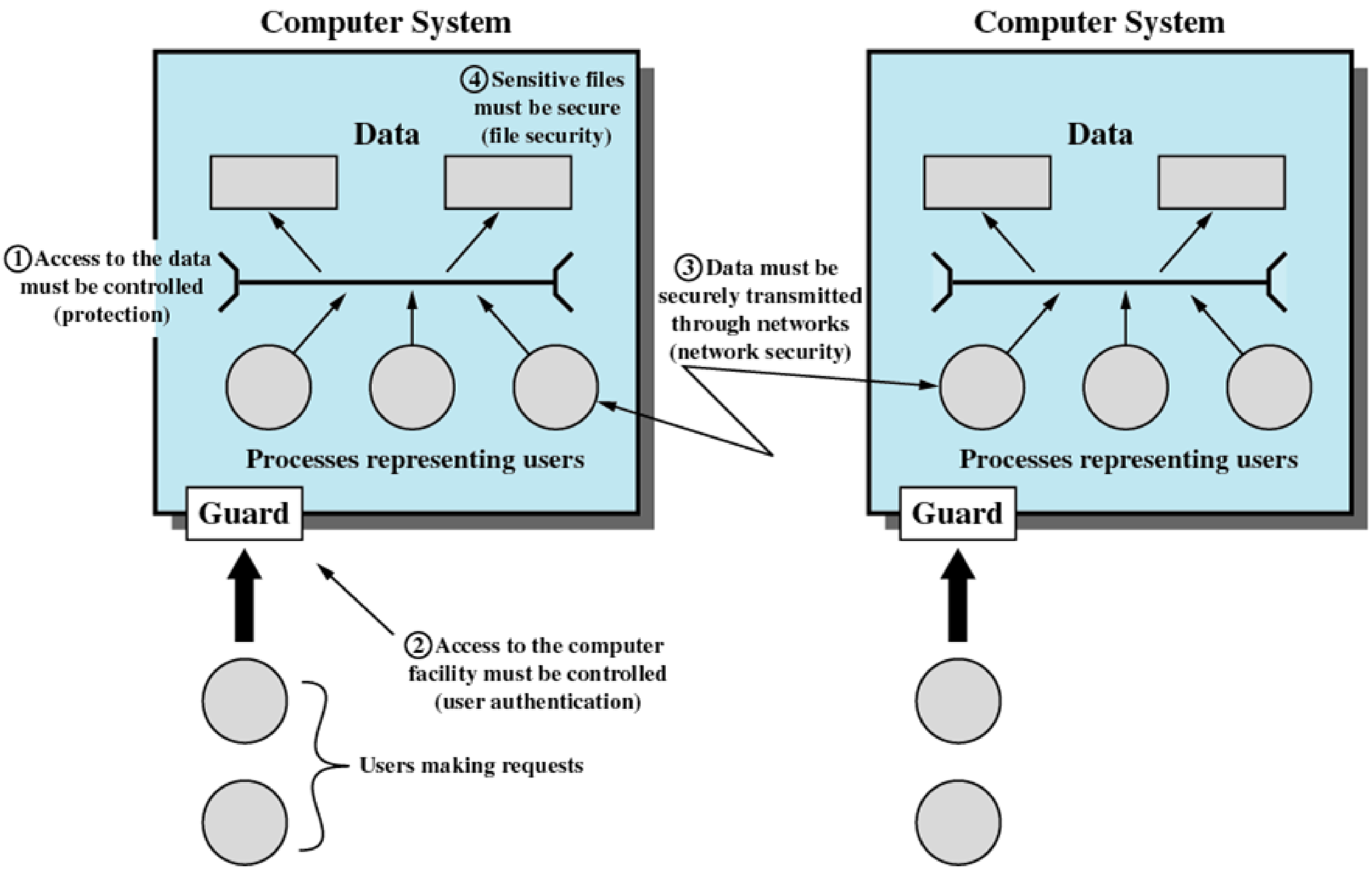
Security Requirements

- Confidentiality
- Integrity
- Availability
- Authenticity

UPPSALA UNIVERSITET

Informationsteknologi

Scope of System Security


Computer System
Computer System
④ Sensitive files must be secure (file security)
Data
Data
① Access to the data must be controlled (protection)
③ Data must be securely transmitted through networks (network security)
Processes representing users
Processes representing users
Guard
Guard
② Access to the computer facility must be controlled (user authentication)
Users making requests

Types of Threats

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

Types of Threats

- Interception
  - An unauthorized party (person, program, or computer) gains access to an asset
  - Attack on confidentiality
  - Examples:
    - Wiretapping to capture data in a network
    - Illicit copying of files or programs

Types of Threats

- Modification
  - An unauthorized party not only gains access but tampers with an asset
  - Attack on integrity
  - Examples:
    - 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
  - Examples:
    - 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 availability, secrecy, and integrity
  - Statistical analysis of data files 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
    - Examples:
      - Release of message contents – a telephone conversation, an electronic mail message, and a transferred file are all subject to these threats
      - Traffic analysis – Encryption masks the contents of what is transferred so even if obtained by someone, they would be unable to extract information; however the pattern of communication could be observed

UPPSALA
UNIVERSITET

Informationsteknologi

Computer System Assets

- Communication Lines and Networks
  - Active Attacks
    - Involve some modification of the data stream or the creation of a false stream
    - Four categories:
      - Masquerade
      - Replay
      - Modification of messages
      - Denial of service

UPPSALA UNIVERSITET

Informationsteknologi

Protection

- No protection
  - Sensitive procedures are run at separate times
- Isolation
  - Each process operates separately from other processes with no sharing or communication
  - Each process has its own address space and files

UPPSALA
UNIVERSITET

Informationsteknologi

Protection

- Share all or share nothing
  - Owner of an object (e.g. a file) 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

UPPSALA UNIVERSITET

Informationsteknologi

Protection of Memory

- Essential in a multiprogramming environment
- Need to insure the correct functioning of the various processes that are active
- Easily accomplished with a virtual memory scheme

User-Oriented Access Control

- Referred to 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

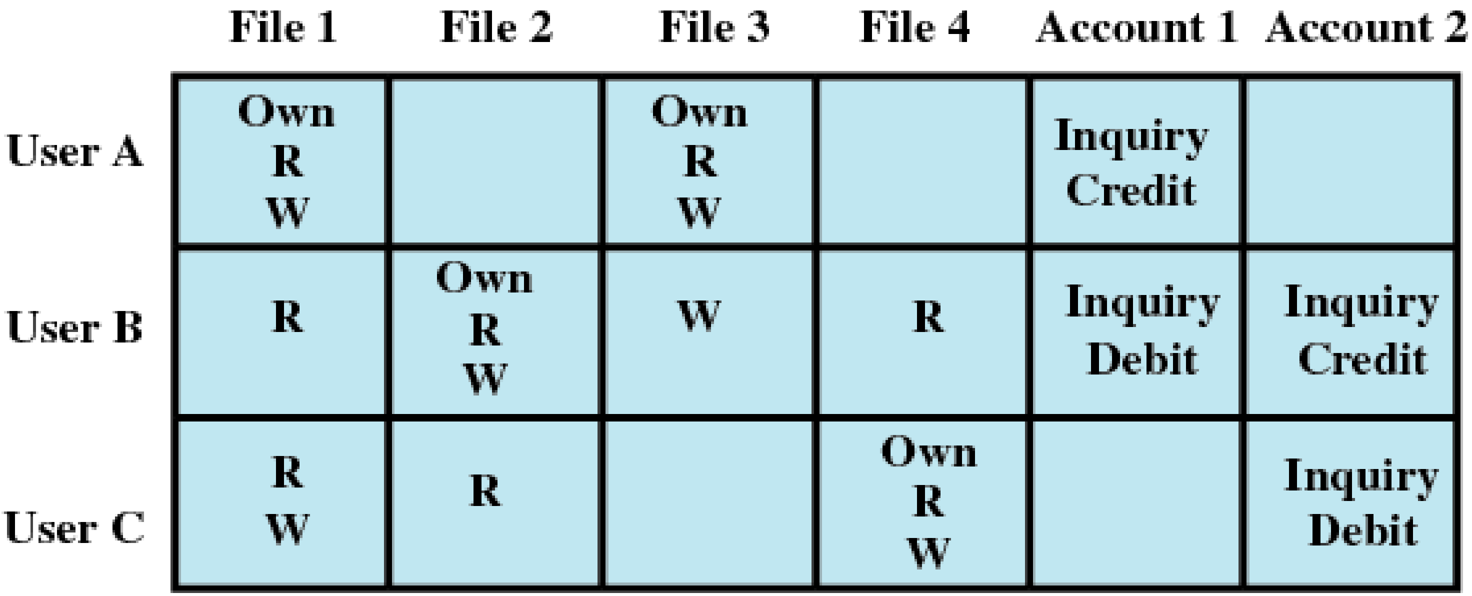
Data-Oriented Access Control

- 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



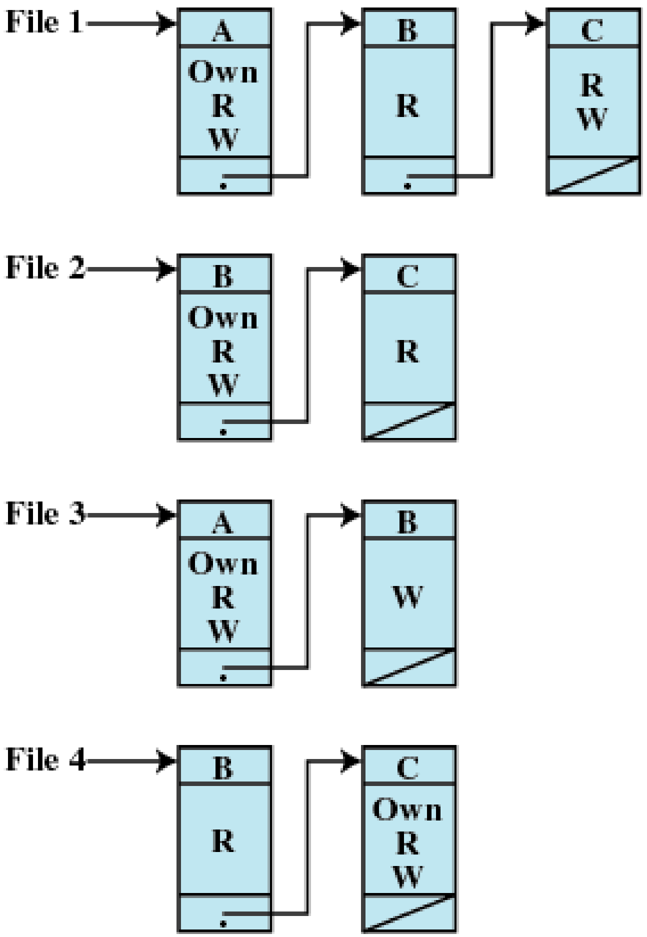
	File 1	File 2	File 3	File 4	Account 1	Account 2
User A	Own R W		Own R W		Inquiry Credit	
User B	R	Own R W	W	R	Inquiry Debit	Inquiry Credit
User C	R W	R		Own R W		Inquiry Debit

UPPSALA UNIVERSITET

Informationsteknologi

Access Control List

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

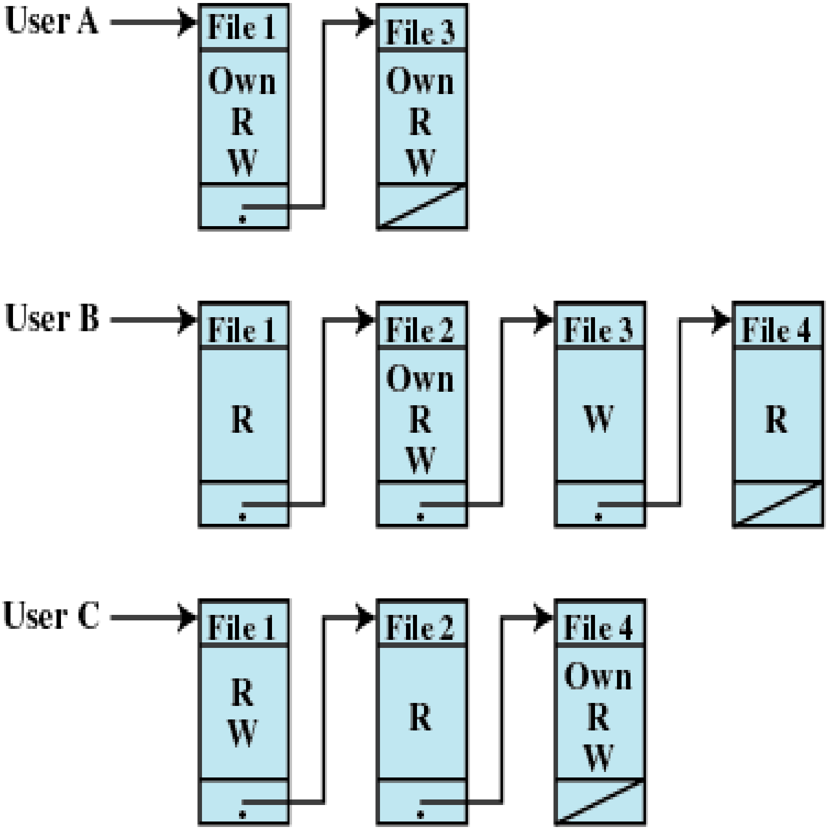


UPPSALA UNIVERSITET

Informationsteknologi

Capability Tickets

- Access matrix decomposed by rows
- Specifies authorized objects and operations for a user



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

UPPSALA
UNIVERSITET

Informationsteknologi

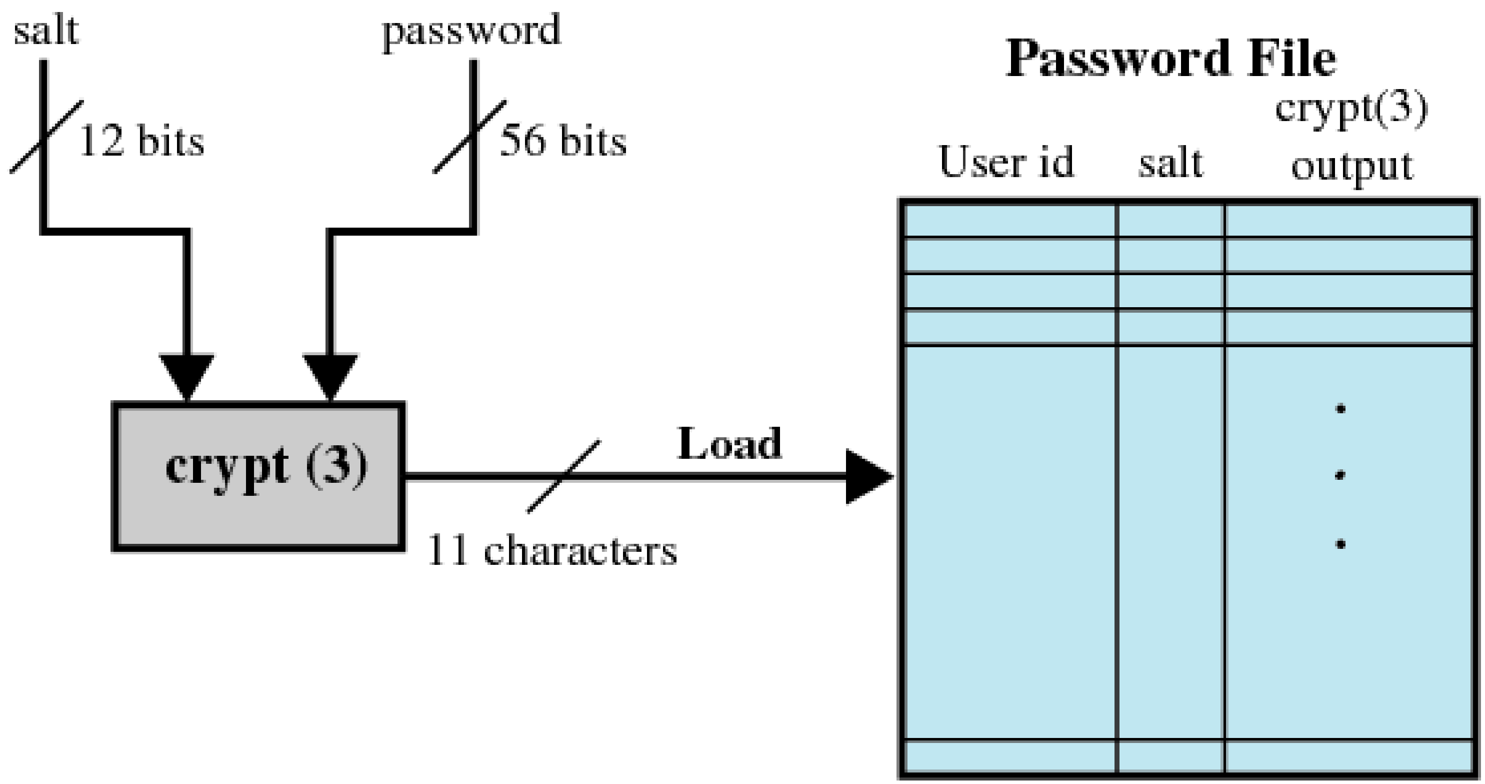
Techniques for Learning Passwords

- Try users’ phone numbers, social security or person numbers, and room numbers
- Try all legitimate license plate numbers for location where the person is living
- 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



UPPSALA UNIVERSITET

Informationsteknologi

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

Intrusion Detection

- Assume the behavior of the intruder differs from the legitimate user in ways that can be quantified
- 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

UPPSALA UNIVERSITET

Informationsteknologi

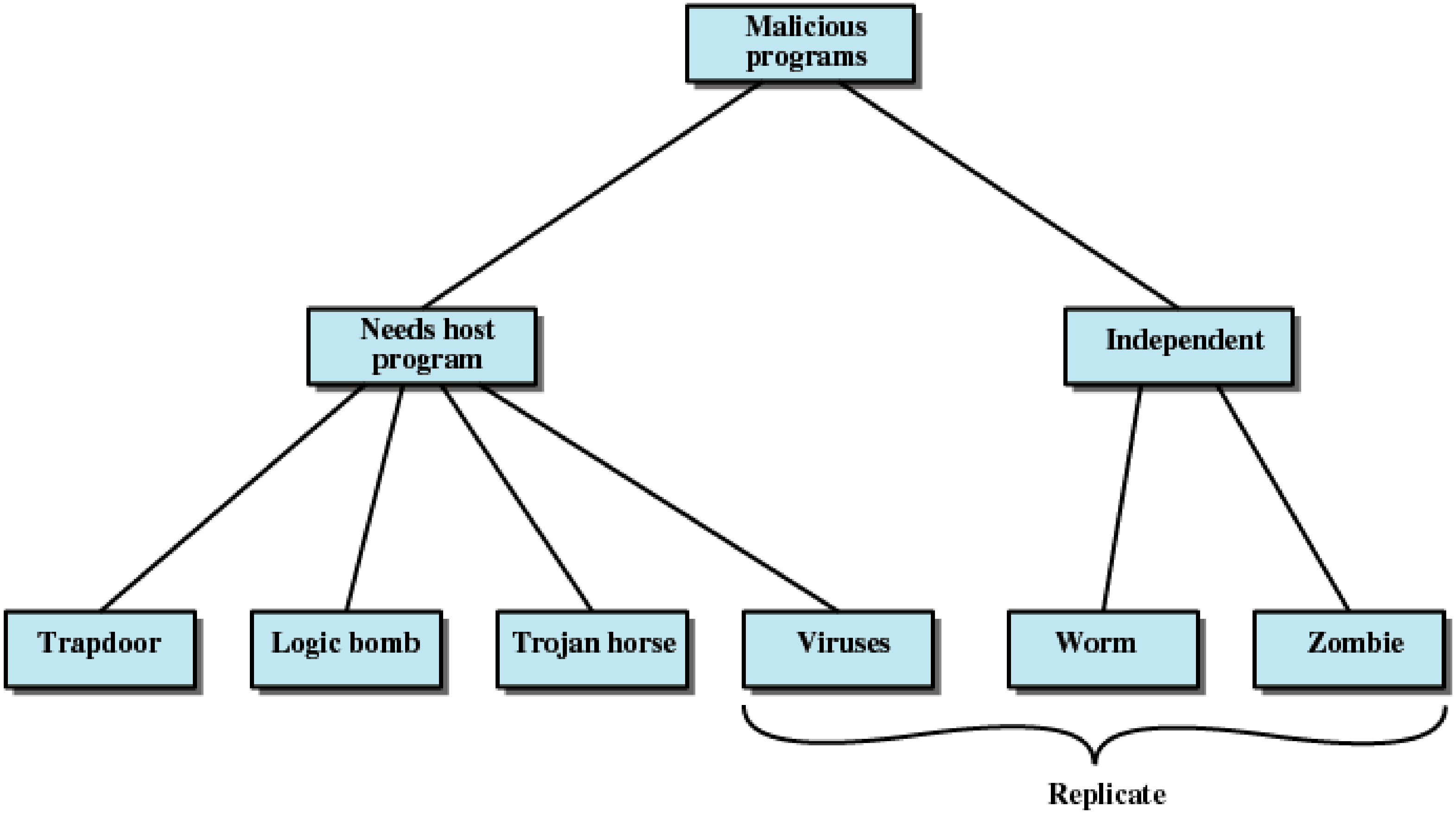
Intrusion Detection

- Audit record
  - Fundamental tool for intrusion detection
  - 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

Taxonomy of Malicious Programs



Trap Door

- Entry point into a program that allows someone who is aware of the trap door 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

UPPSALA UNIVERSITET

Informationsteknologi

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 a copy of the 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

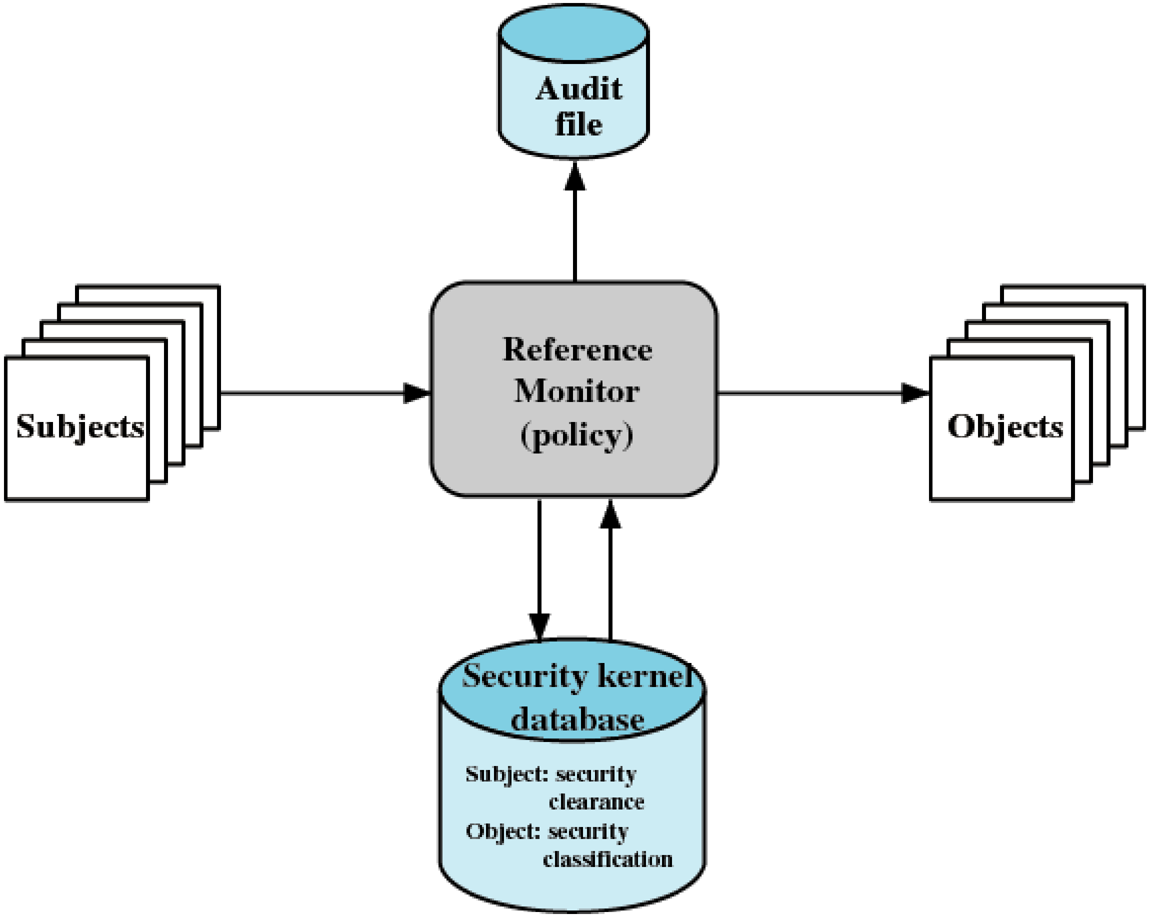
Zombie

- 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

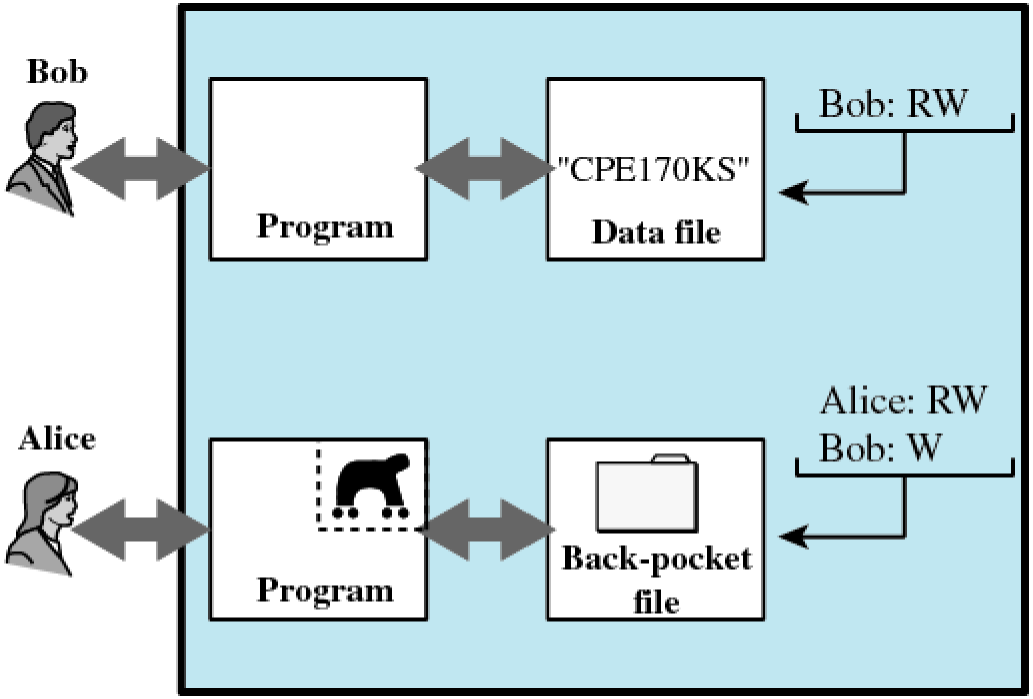
Reference Monitor


Audit file
Subjects
Reference Monitor (policy)
Objects
Security kernel database
Subject: security clearance
Object: security classification

UPPSALA UNIVERSITET

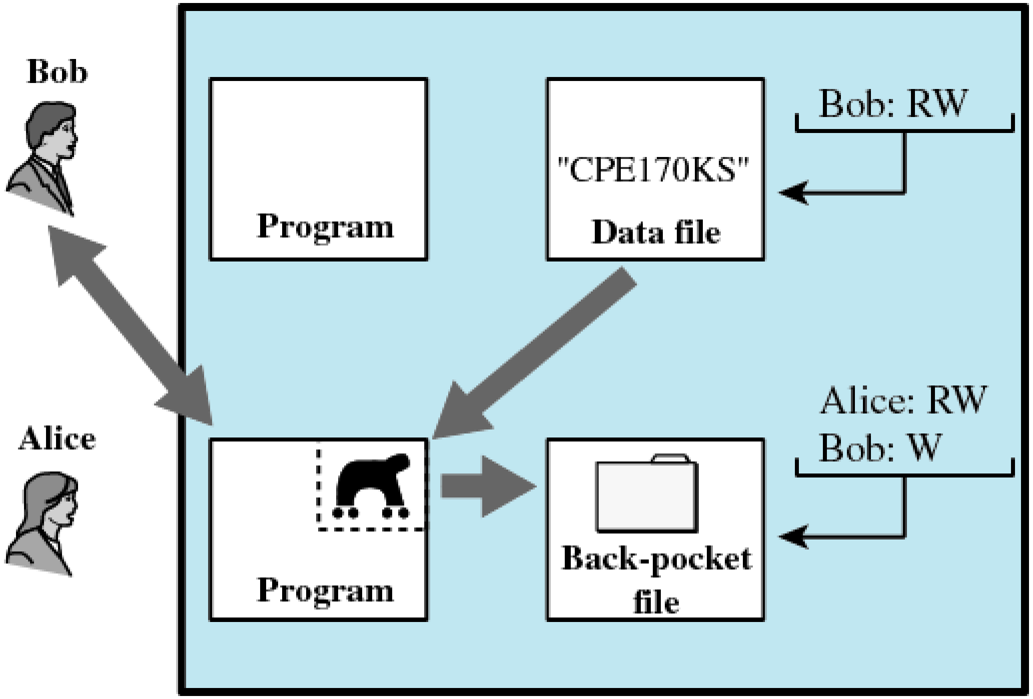
Informationsteknologi

Trojan Horse Defense



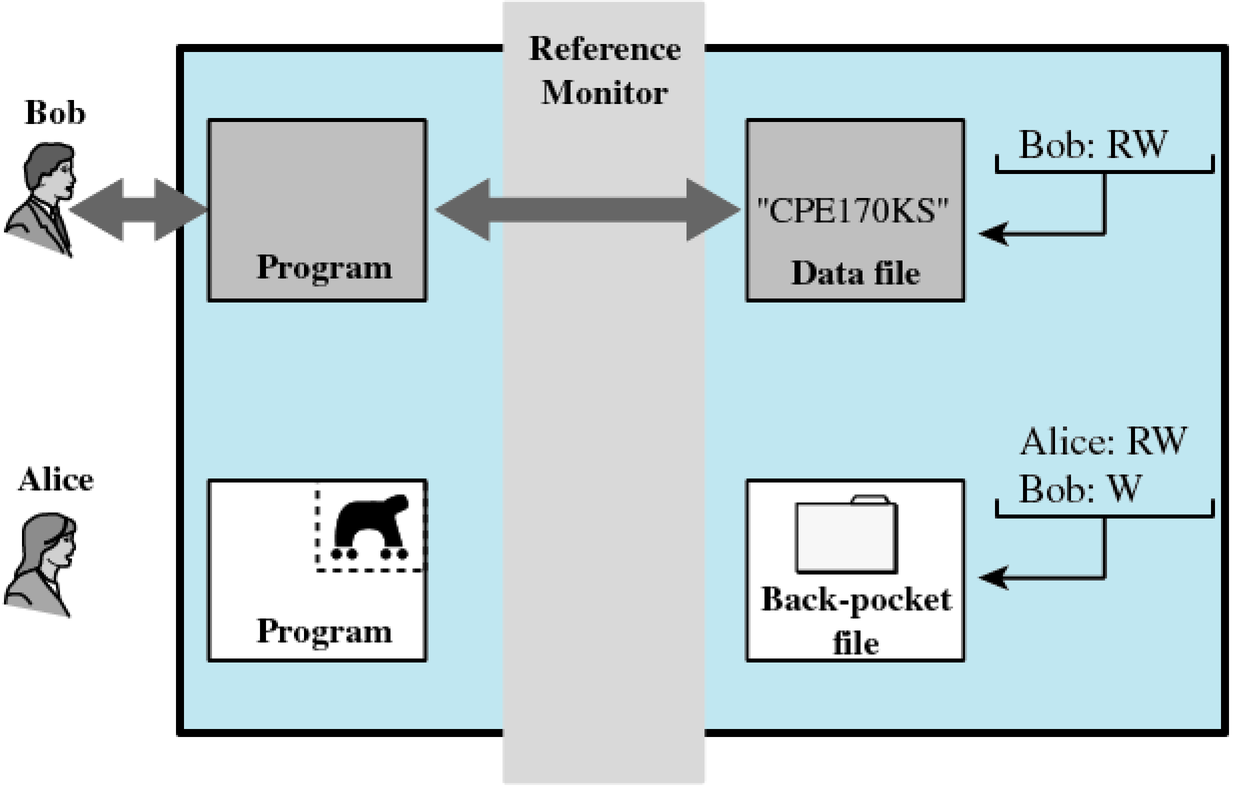
(a)

Trojan Horse Defense



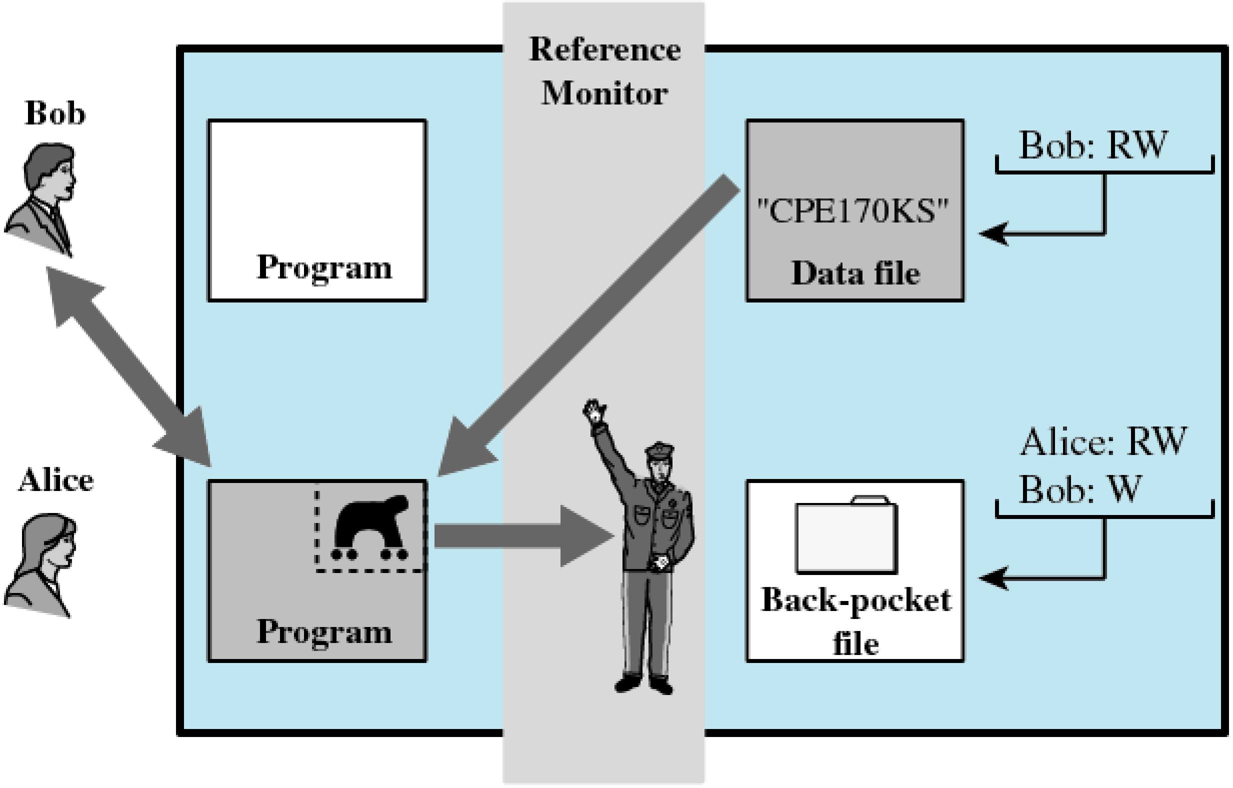
(b)

Trojan Horse Defense



(c)

Trojan Horse Defense



(d)