Network Security and Cryptography

Topic 4: Lecture 1

Operating System Security and Vulnerabilities

The Unit Roadmap

- Introduction to Network Security and Cryptography
- Cryptography Techniques
- **Operating System Security and Vulnerabilities**
- Software Vulnerabilities and attacks
- Network Security and Defense
- Email and Web Security
- Firewalls
- VLAN and VPN
- Wireless Security
- Information Security Management

Scope and Coverage

This topic will cover:

- Operating System Security basics
- User Authentication
- Unix Access Control

Learning Outcomes

By the end of this topic students will be able to:

- Understand the importance of securing the operating system.
- Explain the concept of user authentication and describe various authentication methods
- Comprehend Unix file permissions (read, write, execute) for users, groups, and others.

Recap on Last Topic

- Key exchange is a critical process in secure communication, ensuring the safe exchange of cryptographic keys.
- Asymmetric encryption involves public and private keys for secure data transmission and authentication.
- Message authentication code (MAC): A function of the message and a secret key that produces a fixed-length value that serves as the authenticator.
- Hash function: A function that maps a message of any length into a fixed-length hash value, which serves as the authenticator.
- Hash function is used for digital signatures.

Quiz

1. What is the primary advantage of using asymmetric cryptography over symmetric cryptography?

   a) Faster encryption and decryption

   b) Simplicity in key management

   c) Same key for both parties

   d) Secure communication without prior key exchange

   Correct Answer

Quiz

2. Which cryptographic primitive is commonly used to create a digital signature?

a) Symmetric encryption

b) Asymmetric encryption

c) Hash Function **Correct Answer**

d) MAC

Quiz

3. What is the concept of a public key infrastructure (PKI) related to in asymmetric cryptography?

a) Management of symmetric keys

b) Distribution of public keys **Correct Answer**

c) Compression of digital signatures

d) Creation of Message Authentication Codes

Quiz

4. Which property is crucial for a secure Message Authentication Code (MAC)?

a) Reversibility

b) Collision resistance **Correct Answer**

c) Compression ratio

d) Key length

Quiz

5. How does a digital signature provide non-repudiation in communication?

a) By encrypting the entire message

b) By using a one-time password

c) By binding the signature to the sender's identity

d) By compressing the message before signing

Correct Answer (c)

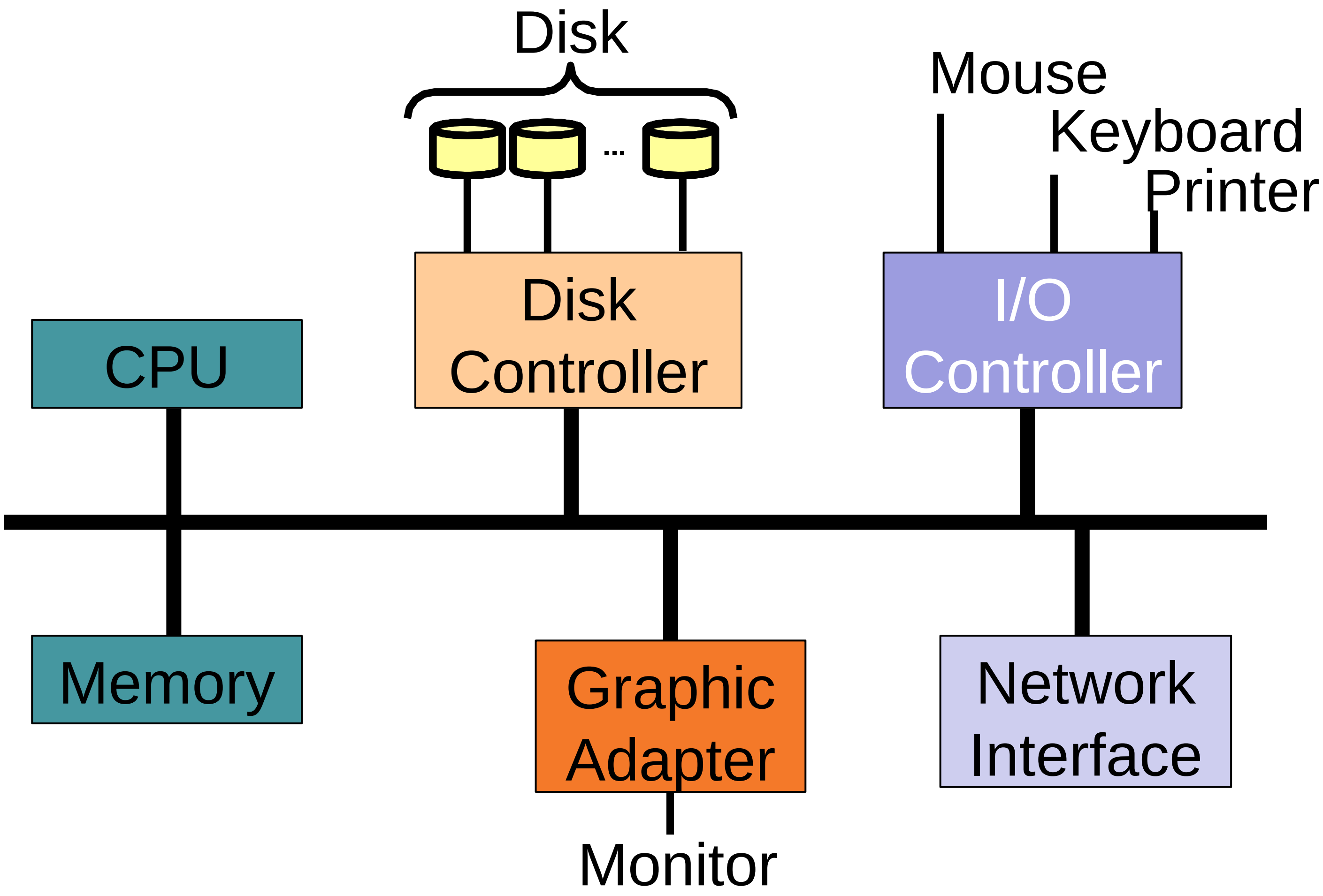
What is an Operating System?

A program that acts as an intermediary between a user of a computer and the computer hardware.

Operating system goals:

- Execute user programs and make solving user problems easier.
- Make the computer system convenient to use.
- Use the computer hardware in an efficient manner.

A Modern Computer System

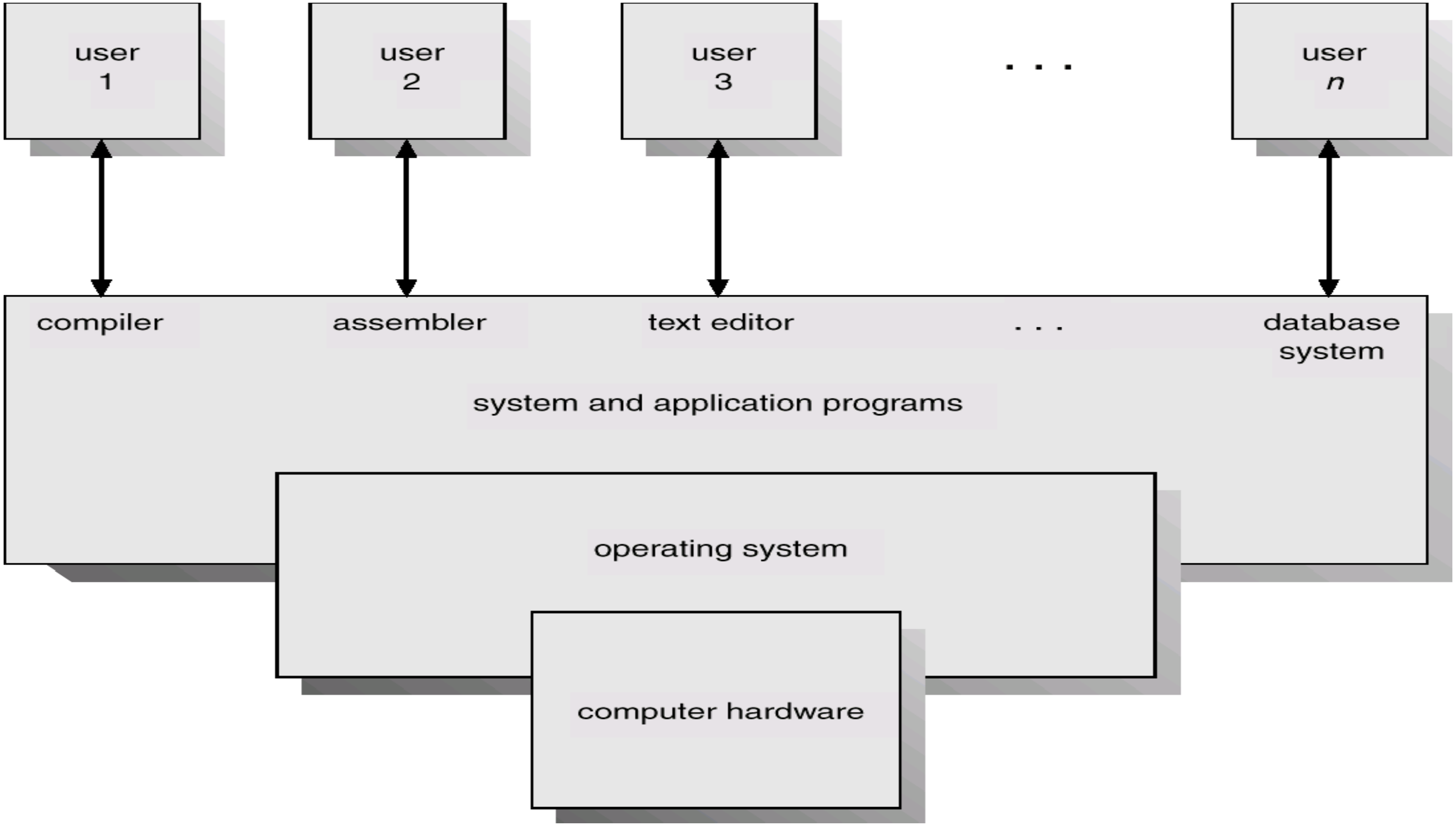


Silberschatz, A., et al. (2005) *Operating system concepts*. New York: Wiley.

Computer System Components

- Hardware
  - ✓ Provides basic computing resources (CPU, memory, I/O).
- Operating system
  - ✓ Controls and coordinates the use of the hardware among the various application programs.
- Applications programs
  - ✓ Define the ways in which the system resources are used to solve the computing problems of the users.
- Users
  - ✓ E.g., people, machines, other computers.

Abstract View of System Components



Silberschatz, A., et al. (2005) *Operating system concepts*. New York: Wiley.

Operating System Definitions

- Resource allocator – manages and allocates resources.
- Control program – controls the execution of user programs and operations of I/O devices.
- Kernel – the one program “running” at all times (all else being application programs).

What Security Goals Does Operating System Provide?

- Goal 1: enabling multiple users securely share a computer
  - ✓ Separation and sharing of processes, memory, files, devices, etc.

- What do C, I, A, mean here?

- What is the threat model?

How to Achieve the Security Goals 1?

- Memory protection
- Processor modes
- User authentication
- File access control

What Security Goals Does Operating System Provide?

- Goal 2: ensure secure operation in networked environment
- What do C, I, A, mean here?
- What is the threat model?

How to Achieve the Security Goals 2?

- Authentication
- Access Control
- Secure Communication (using cryptography)
- Logging & Auditing
- Intrusion Prevention and Detection
- Recovery

Memory Protection: Access Control to Memory

- Ensures that one user s process cannot access other's memory
  - ✓ fence
  - ✓ relocation
  - ✓ base/bounds register
  - ✓ segmentation
  - ✓ paging
  - ✓ – …
- Operating system and user processes need to have different privileges

CPU Modes (a.k.a. Processor Modes or Privilege

System mode (privileged mode, master mode, supervisor mode, kernel mode)

- Can execute any instruction,
- Can access any memory locations, e.g., accessing hardware devices,
- Can enable and disable interrupts,
- Can change privileged processor state,
- Can access memory management units,
- Can modify registers for various descriptor tables

Reading: http://en.wikipedia.org/wiki/CPU_modes

User Mode

- Access to memory is limited,
- Cannot execute some instructions,
- Cannot disable interrupts,
- Cannot change arbitrary processor state,
- Cannot access memory management units,
- Transition from user mode to system mode must be done through well defined call gates (system calls).

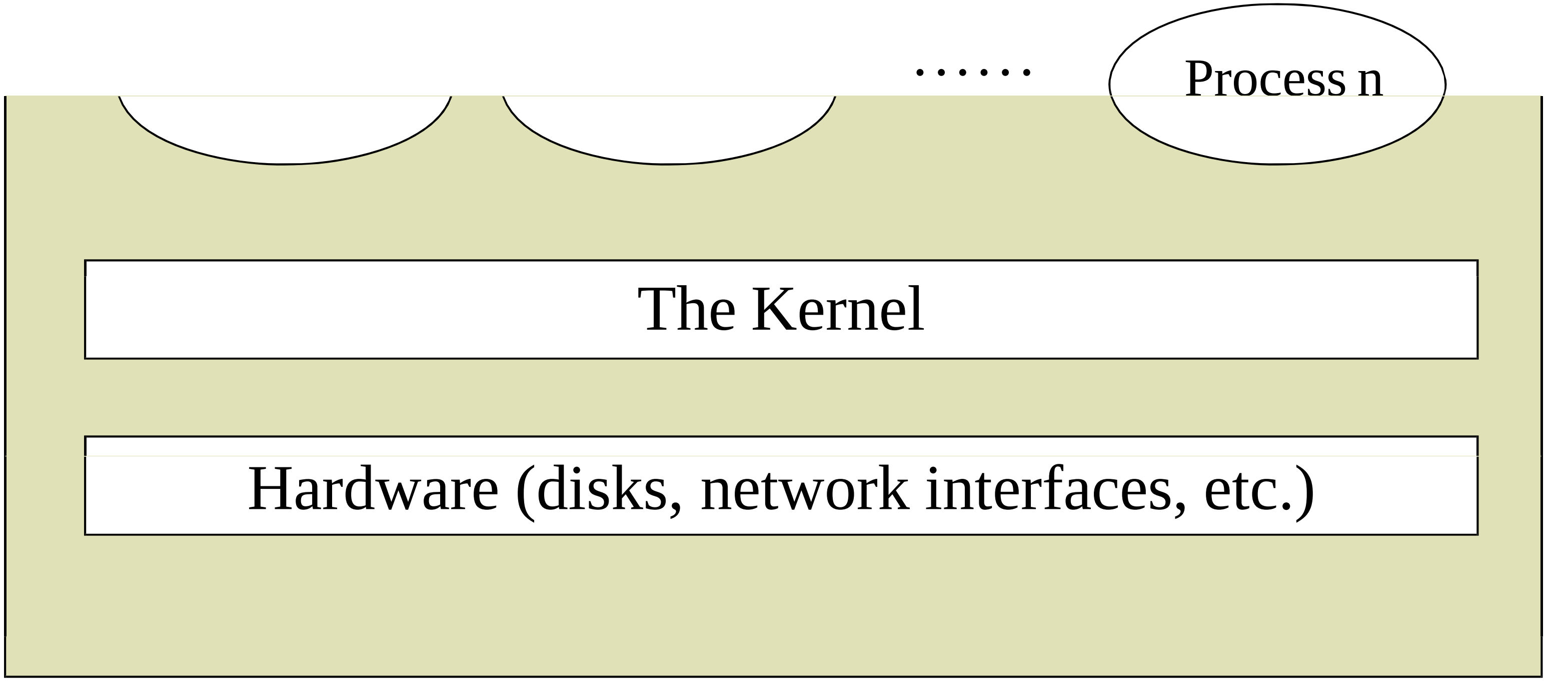
System Calls

- Guarded gates from user mode (space, land) into kernel mode (space, land).
- Use a special CPU instruction (often an interruption), transfers control to predefined entry point in more privileged code; allows the more privileged code to specify where it will be entered as well as important processor state at the time of entry.
- The higher privileged code, by examining processor state set by the less privileged code and/or its stack, determines what is being requested and whether to allow it.

Kernel Space vs User Space

- Part of the OS runs in the kernel model
  - ✓ known as the OS kernel
- Other parts of the OS run in the user mode, including service programs (daemon programs), user applications, etc.
  - ✓ they run as processes
  - ✓ they form the user space (or the user land)
- Difference between kernel mode and processes running as root (or superuser, administrator)

High-level View of Kernel Space vs. User Space



User Authentication

Using a method to validate users who attempt to access a computer system or resources, to ensure they are authorized.

Types of user authentication:

- Something you know
  - ✓ User accounts with passwords
- Something you have
  - ✓ Smart cards or other security tokens
- Something you are
  - ✓ Biometrics

Scenarios Requiring Authentication

Scenarios

- Logging into a local computer
- Logging into a computer remotely
- Access web sites

Potential vulnerabilities to consider when client authenticating server

- channel between the client and the server
- server compromise
- client compromise
- weak passwords

What are some threats?

Common User Authentication Breaches

- Password-based Attacks
- Credential Stuffing
- Phishing
- Keylogging
- Man in the Middle
- Biometric Spoofing
- Insider Attack

Threats to Passwords

- Online guessing attempts
- Offline dictionary attacks
- Login spoofing
- Shoulder surfing
- Social engineering
  - ✓ e.g., pretexting: creating and using an invented scenario (the pretext) to persuade a target to release information or perform an action and is usually done over the telephone

Storing Passwords (UNIX Case Study)

Old UNIX

- The file /etc/passwd stores H(password) together with each user’s login name, user id, home directory, login shell, etc.
- file must be world readable
- Brute force attacks possible even if H is one-way
  - how to brute-force when trying to obtain password of any account on a system with many accounts?

New UNIX

- H(password) stored in /etc/shadow, readable only by root

Dictionary Attack

- A type of brute-force attack used by hackers to gain unauthorized access to a computer system or online account, such as an email or a user account on a website.

- The attacker attempts to guess the correct password for the target account by systematically trying a large number of possible passwords from a predefined list, often called a "dictionary."

Password Salts

- A random piece of data is added to the password before it runs through the hashing algorithm, making it unique and harder to crack.
- When using both hashing and salting, even if two users choose the same password, salting adds random characters to each password when the users enter them.
- Benefits:
  - Dictionary attacks much more difficult.
  - If two users happen to choose the same password, it doesn’t immediately show.

Mechanisms to Defend Against Dictionary and Guessing Attacks

- Protect stored passwords (use both cryptography & access control)

- Disable accounts with multiple failed attempts

Mechanisms to Avoid Weak Passwords

- Allow long passphrases
- Randomly generate passwords
- Check the quality of user-selected passwords
  - ✓ use a number of rules
  - ✓ run dictionary attack tools
- Give user suggestions/guidelines in choosing passwords
  - ✓ e.g., think of a sentence and select letters from it, “It’s 12 noon and I am hungry” => “I’S12&IAH”
  - ✓ Using both letter, numbers, and special characters
- Mandate password expiration
- Things to remember: Usability issues

Login Spoofing

- A technique used to steal a user's password.
- A user is presented with a normal login prompt to enter a username and password, but this is actually a malicious program.
- Once a username and password is entered, this information is logged or otherwise passed to an attacker to compromise security.

Defend Against Login Spoofing: Trusted Path

- Trusted Path is a concept in computer security that refers to the assurance that the communication between a user and a computer system is secure and has not been tampered with.

- This helps protect against login spoofing and other attacks by ensuring that the user is interacting with the actual, trusted system and not an imposter.

Defending Against Other Threats

Use ideas from recent research:

- Graphical passwords,
- Combine with typing

Go beyond passwords

- Security tokens
- Biometrics
- Face lock

2 or multi-factor authentication

- Banks are required to use 2-factor authentication from 2006 for online banking

Using Passwords Over Insecure Channel

One-time passwords

- Each password is used only once
- Defend against passive adversaries who eavesdrop and later attempt to impersonate

Challenge response

- Send a response related to both the password and a challenge

Zero knowledge proof of knowledge

How to do One-Time Password

- Time-synchronized OTP
- Shared lists of one-time passwords
- Using a hash chain (Lamport)
  - ✓ h(s), h(h(s), h(h(h(s))), …, h1000(s)
  - ✓ use these values as passwords in reverse order

Lamport’s One-Time Password

- Lamport's one-time password (OTP) scheme is a cryptographic method used for authentication and password security.

- It was introduced by Leslie Lamport in the late 1980s and is a simple yet effective approach for enhancing the security of password-based authentication systems, particularly against brute-force attacks.

Lamport's One-Time Password

Preparation

- Initially, both the user and the authentication system generate a large table of one-time passwords.
  - Each password is generated using a cryptographic hash function, such as SHA-256.
- These passwords are typically stored securely on both the user's device (e.g., a smartphone or security token) and the authentication server.

Lamport’s One-Time Password

Authentication

- When a user attempts to log in, they provide the system with the next one-time password in their sequence.
  - This password is marked as used after the authentication attempt.

- The authentication system verifies the submitted OTP by comparing it with the expected value generated on its side.
  - If they match, the user is granted access.

Lamport’s One-Time Password

One-Time

- Each password can only be used once. Once a password is used for authentication, it is no longer valid.
- The next time the user logs in, they provide the next OTP in the sequence.

Lamport's OTP scheme is robust against password guessing attacks because the attacker can only guess a single password from the user's sequence, and it becomes invalid once used.

However, one of the drawbacks of Lamport's scheme is that the user and the authentication system must stay synchronized.

Issues to Consider in Password Systems

- Which types of attacks to defend against?
  - ✓ targeted attack on one account
  - ✓ attempt to penetrate any account on a system
  - ✓ attempt to penetrate any account on any system
  - ✓ service denial attack
- Whether to protect users against each other?
- Can users be trained? Will they follow the suggestions?
- Will the passwords be used in other systems?
- Whether the passwords will be used in a controlled environment?

Checkpoint Summary

- Operating system (OS) is a program that acts as an intermediary between a user of a computer and the computer hardware.
- OS security goal is enabling multiple users securely share a computer and ensure secure operation in networked environment.
- OS uses user authentication methods to achieve these goals such as passwords.
- Multiple methods to have secure passwords such as password salt, one time password, etc.

Awarding
Great British
Qualifications

Network Security and Cryptography

Topic 4: Operating System Security and Vulnerabilities

Lecture 2

Unix Access Control

Access Control

ITU-T Recommendation X.800 defines access control as follows:

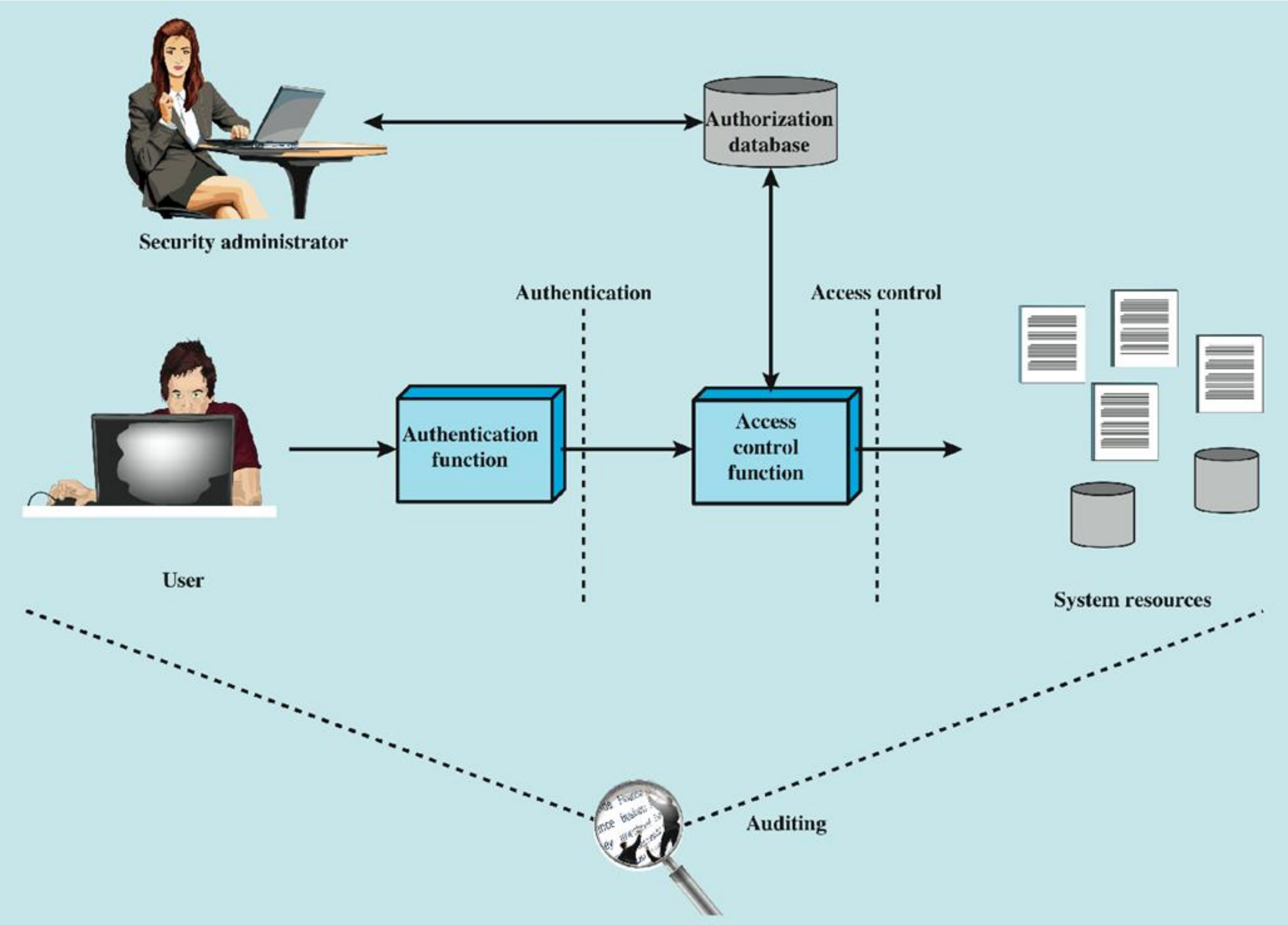
“The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.”

Access Control Principles

RFC 2828 defines computer security as:

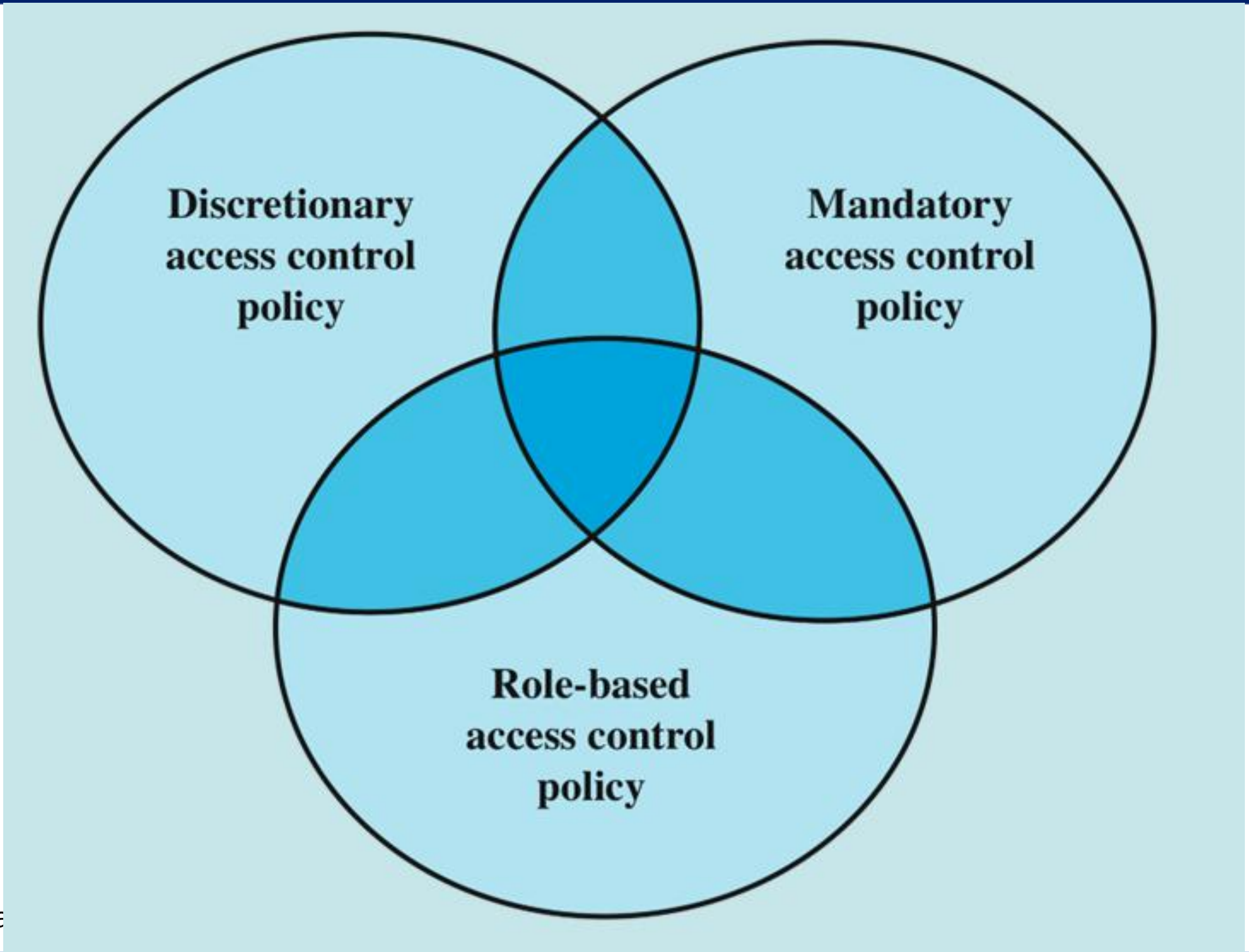
> **“Measures that implement and assure security services in a computer system, particularly those that assure access control service”.**

Relationship Among Access Control and Other Security Functions



Stallin

Access Control Policies


Discretionary access control policy
Mandatory access control policy
Role-based access control policy

Sta

Discretionary Access Control (DAC)

Owner Control:

- Resource owners determine who can access their resources and set access permissions.

Access Rights:

- Permissions, such as read, write, and execute, are assigned to users or groups.

Flexible but Risky:

- DAC provides flexibility but relies on resource owners to manage access, which can lead to security risks.

Resource-Centric:

- DAC focuses on controlling access to specific resources rather than controlling access by role or job function.

Mandatory Access Control (MAC)

Strict Security Labels:

- MAC enforces access control through security labels, which specify who can access resources and at what security level.

Government and Military Use:

- MAC is commonly used in environments where the strictest security is required.

Limited Flexibility:

- MAC restricts users' ability to change access controls, and access decisions are typically made by security administrators.

Data Confidentiality:

- MAC enforces data confidentiality and integrity by classifying and labeling data based on its sensitivity.

Role-Based Access Control (RBAC)

Access by Roles:

- RBAC organizes users into roles and grants access permissions to those roles rather than individual users.

Simplified Administration:

- RBAC simplifies access control management by associating permissions with roles.

Role Hierarchies:

- RBAC may include role hierarchies, where roles inherit permissions from higher-level roles.

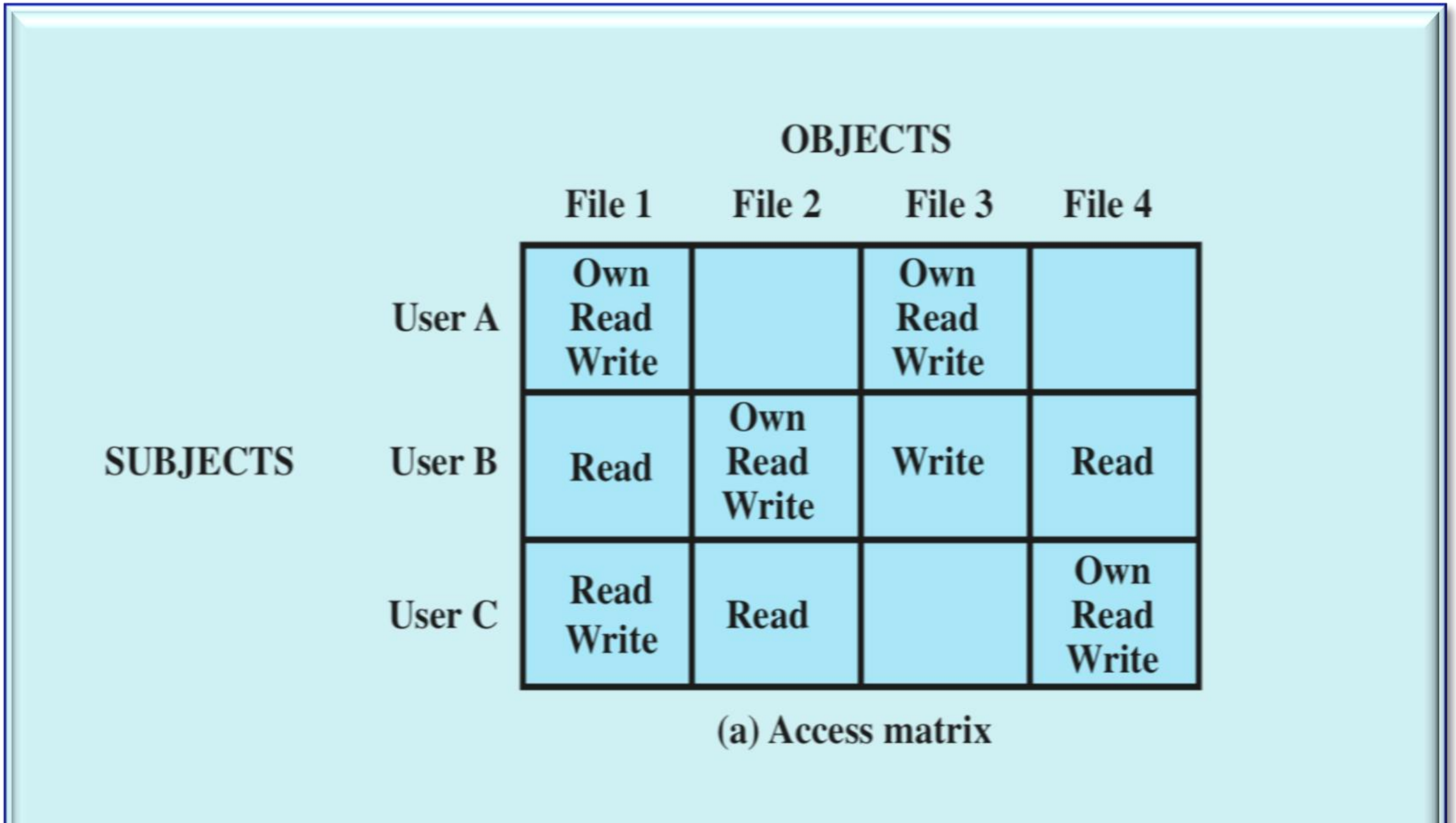
Used in Many Environments:

- RBAC is widely used in various settings, including business, healthcare, and online services, to efficiently manage access and security.

Access Control Requirements

- reliable input
- support for fine and coarse specifications
- least privilege
- separation of duty
- open and closed policies
- policy combinations and conflict resolution
- administrative policies
- dual control

Access Matrix Model



		OBJECTS			
		File 1	File 2	File 3	File 4
SUBJECTS	User A	Own Read Write		Own Read Write	
	User B	Read	Own Read Write	Write	Read
	User C	Read Write	Read		Own Read Write

(a) Access matrix

Stallings W, Brown L. Computer security: principles and practice. Pearson; 2012.

Access Matrix Model

Basic Abstractions

- ✓ Subjects
- ✓ Objects
- ✓ Rights

The rights in a cell specify the access of the subject (row) to the object (column).

Principals And Subjects

- A subject is a program (application) executing on behalf of some principal(s)
- A principal may at any time be idle, or have one or more subjects executing on its behalf

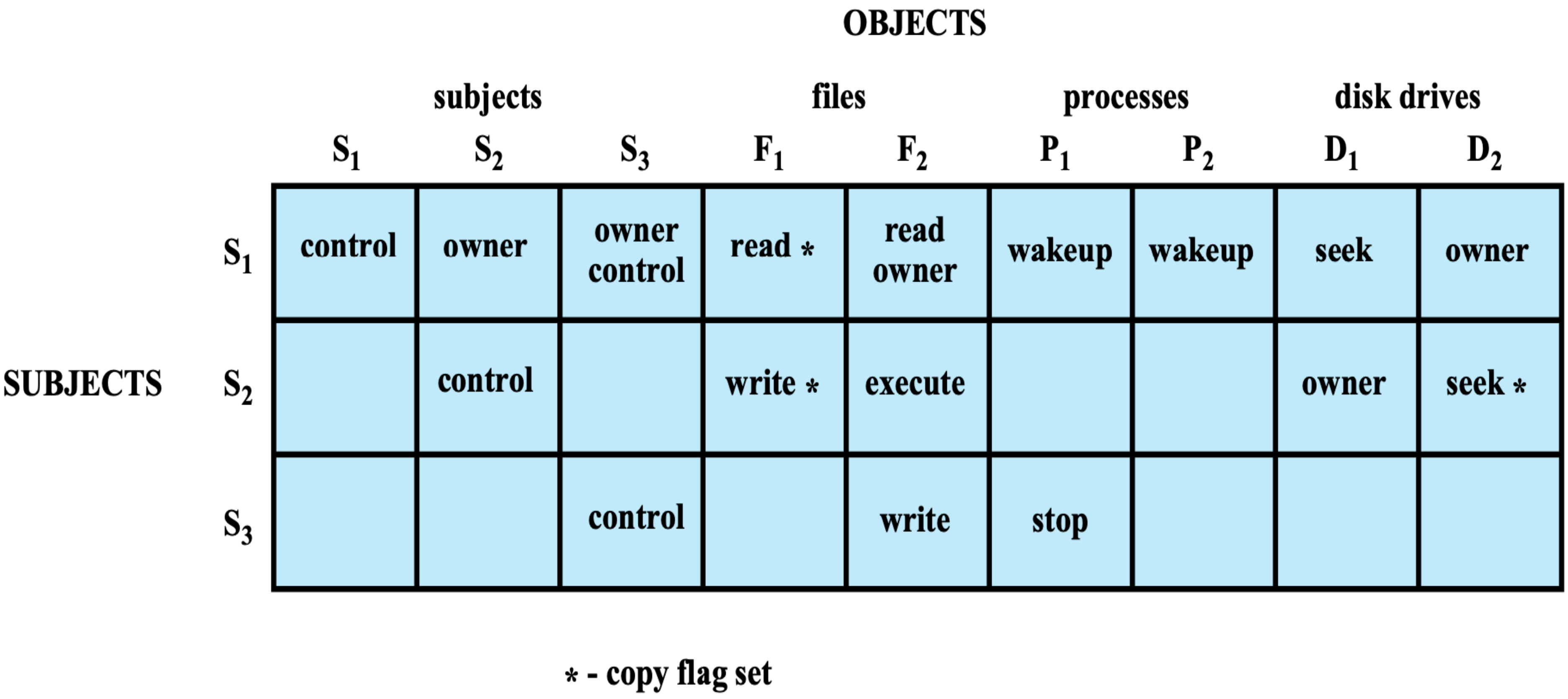
What are subjects in UNIX?

What are principals in UNIX?

Objects

- *Anything on which a subject can perform operations (mediated by rights)*
  - ✓ Usually objects are passive, for example:
  - ✓ File
  - ✓ Directory (or Folder)
  - ✓ Memory segment
- *But subjects can also be objects, with operations*
  - ✓ kill
  - ✓ suspend
  - ✓ resume

Extended Access Matrix Model



		OBJECTS								
		subjects			files		processes		disk drives	
		S_1	S_2	S_3	F_1	F_2	P_1	P_2	D_1	D_2
	S_1	control	owner	owner control	read *	read owner	wakeup	wakeup	seek	owner
SUBJECTS	S_2		control		write *	execute			owner	seek *
	S_3			control		write	stop			

* - copy flag set

Stallings W, Brown L. Computer security: principles and practice. Pearson; 2012.

UNIX Access Control

UNIX files are administered using inodes (index nodes)

- control structures with key information needed for a particular file
- several file names may be associated with a single inode
- an active inode is associated with exactly one file
- file attributes, permissions and control information are sorted in the inode
- on the disk there is an inode table, or inode list, that contains the inodes of all the files in the file system
- when a file is opened its inode is brought into main memory and stored in a memory resident inode table

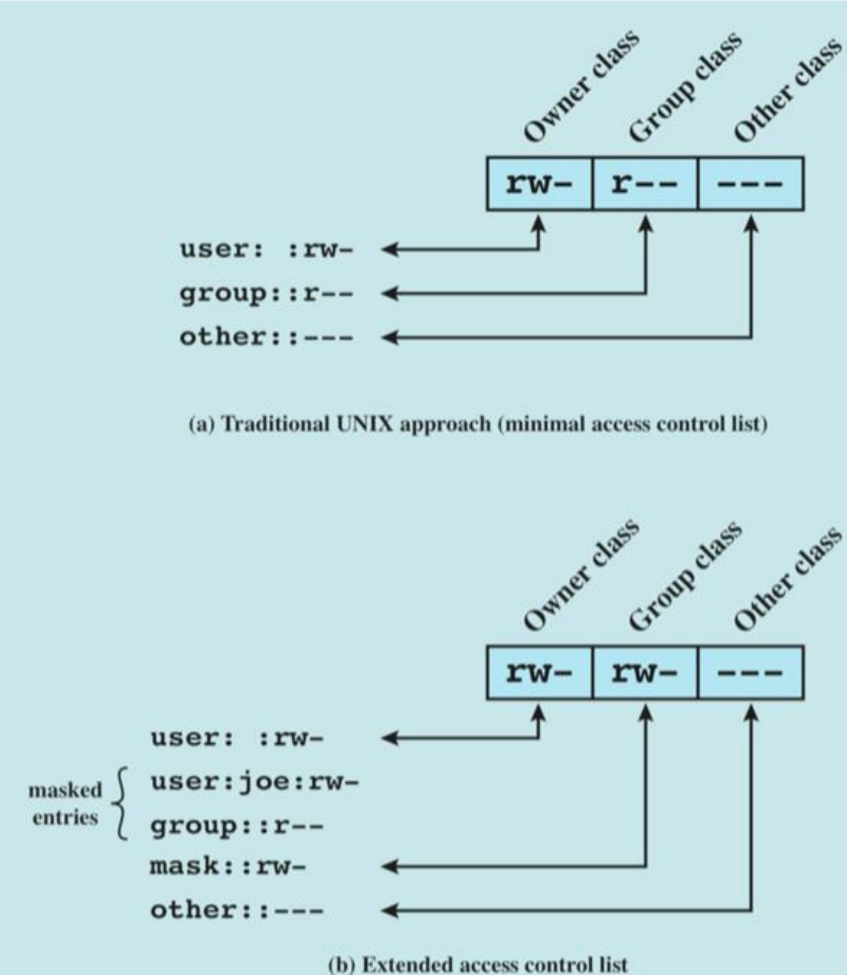
UNIX Access Control

Directories are structured in a hierarchical tree

- may contain files and/or other directories
- contains file names plus pointers to associated inodes

UNIX File Access Control

- Unique user identification number (user ID)
- Member of a primary group identified by a group ID
- Belongs to a specific group
- 12 protection bits
  - ✓ specify read, write, and execute permission for the owner of the file, members of the group and all other users
- The owner ID, group ID, and protection bits are part of the file's inode.



(a) Traditional UNIX approach (minimal access control list)

(b) Extended access control list

Stallings W, Brown L. Computer security: principles and practice. Pearson; 2012.

Access Control Lists (ACLs) in UNIX

- Modern UNIX systems support ACLs
  - ✓ FreeBSD, OpenBSD, Linux, Solaris
- FreeBSD
  - ✓ Setfacl command assigns a list of UNIX user IDs and groups
  - ✓ any number of users and groups can be associated with a file
  - ✓ read, write, execute protection bits
  - ✓ a file does not need to have an ACL
  - ✓ includes an additional protection bit that indicates whether the file has an extended ACL

Access Control Lists (ACLs) in UNIX

When a process requests access to a file system object two steps are performed:

- Step 1: selects the most appropriate ACL
  - ✓ owner, named users, owning / named groups, others
- Step 2: checks if the matching entry contains sufficient permissions

Class Activity: File Access Control in a Small Business

Explain how access control policies (DAC, MAC, RBAC) fit within the given scenario:

- Scenario 1: File Access in Small Business
- Scenario 2: Military Base Access Control
- Scenario 3: Healthcare Information Access

File Access in Small Business

DAC: Each employee can decide who can access the files they create. They set permissions on their files and folders, allowing specific colleagues to read, write, or delete them.

MAC: The company follows strict government regulations. Access to sensitive files is determined by labels that indicate the security classification. Employees don't have control over changing the labels; access is determined by security administrators and government requirements.

RBAC: The company uses a role-based system. Employees are assigned roles like "Accountant," "Sales," and "HR." Each role has predefined permissions. For example, the Accountant role can access financial files, while the Sales role can access sales data. Access rights are assigned based on roles, not individual users.

Military Base Access Control

DAC: Soldiers are allowed to control the access to their personal lockers. They set permissions for their lockers, deciding who can open them and what can be stored inside.

MAC: The base employs strict security clearances. Access to different areas and information is determined by a person's clearance level. Only those with the appropriate clearance can access specific locations or documents. Soldiers have no control over this; it's decided by higher authorities.

RBAC: The military uses role-based access control. There are roles such as "Soldier," "Officer," and "Commander." Each role has predefined access to different areas of the base and information. Soldiers are assigned roles based on their rank and responsibilities.

Healthcare Information Access

DAC: Doctors, nurses, and other healthcare professionals control access to their patient records. They can set permissions for their records, allowing selected colleagues to view or modify them.

MAC: Healthcare data is highly sensitive. Access to patient records is determined by the patients' confidentiality level and the healthcare providers' role. Only authorized personnel with the necessary clearance and role can access specific patient records.

RBAC: The healthcare facility employs role-based access control. There are roles like "Physician," "Nurse," and "Administrator." Each role has predefined access rights to various types of patient data. Access is granted based on job responsibilities, not individual requests.

Topic Summary

- Operating system (OS) is a program that acts as an intermediary between a user of a computer and the computer hardware.
- OS uses user authentication methods to achieve these goals such as passwords.
- Multiple methods to have secure passwords such as password salt, one time password, etc.
- OS uses access control for the prevention of unauthorized use of a resource.

Next Topic 5: Software Vulnerabilities and Attacks

- Software vulnerabilities
- Malwares
- Worms

References

- CHARLES J. B., Christopher G., Philip C., Donald S. 2018. Cybersecurity Essentials, John Wiley & Sons, Inc.
- CIAMPA, M. (2012). Security+ guide to network security fundamentals. Cengage Learning.
- HOFFMAN, A. 2020. Web Application Security: Exploitation and Countermeasures for Modern Web Applications, O'Reilly.
- OZKAYA, E. 2019. Cybersecurity: The Beginner's Guide. Packet Publishing Ltd.
- SILBERSCHATZ, A., PETER B. G. AND GAGNE, G. (2010). Operating system concepts. Hoboken: John Wiley & Sons.
- STALLINGS, W. 2022. Cryptography and Network Security: Principles and Practice, Global Edition, 8th edition, Pearson.
- TANENBAUM, A. AND BOS, H. (2023). Modern Operating Systems, Global Edition. Pearson.

NCC education® Awarding Great British Qualifications

Topic 4 – Operating System Security and Vulnerabilities

Any Questions?