# Study Guide for Chapter 4 Access Control

March 1, 2025

# 1 Access Control Principles

## 1.1 Access Control Context

Access control is a fundamental aspect of computer security, ensuring that only authorized entities can access specific resources. It involves:

- **Authentication**: Verifying the credentials of a user or system entity.
- **Authorization**: Granting rights or permissions to access resources.
- **Audit**: Reviewing system records to ensure compliance and detect security breaches.

## 1.2 Access Control Policies

Access control policies dictate who or what can access specific resources and the type of access permitted. Policies are categorized into:

- **Discretionary Access Control (DAC)**: Access is based on the identity of the requestor and access rules.
- **Mandatory Access Control (MAC)**: Access is based on security labels and clearances.
- **Role-Based Access Control (RBAC)**: Access is based on user roles within the system.
- **Attribute-Based Access Control (ABAC)**: Access is based on attributes of the user, resource, and environment.

# 2 Subjects, Objects, and Access Rights

## 2.1 Subjects

A **subject** is an entity capable of accessing objects, typically equated with a process. Subjects are categorized into:

- **Owner**: Creator or administrator of a resource.
- **Group**: Named group of users with specific access rights.
- **World**: Users not included in owner or group categories.

### 2.2 Objects

An **object** is a resource to which access is controlled, such as files, directories, or devices.

### 2.3 Access Rights

Access rights describe how a subject may access an object, including:

- **Read**: View information.
- **Write**: Modify or delete data.
- **Execute**: Run programs.
- **Delete**: Remove resources.
- **Create**: Generate new resources.
- **Search**: List or search directories.

## 3 Discretionary Access Control (DAC)

### 3.1 Access Control Model

DAC allows entities to grant access rights to others. It is implemented using:

- **Access Control Lists (ACLs)**: Lists users and their permitted access rights for each object.
- **Capability Tickets**: Specify authorized objects and operations for a user.

### 3.2 Protection Domains

A **protection domain** is a set of objects with access rights. Domains can be static or dynamic, allowing processes to have different access rights at different times.

# 4 Example: Unix File Access Control

## 4.1 Traditional UNIX File Access Control

UNIX uses a hierarchical file system with permissions for owner, group, and others. Special permissions include:

- **SetUID**: Temporarily grants the user the rights of the file owner.
- **SetGID**: Temporarily grants the user the rights of the file group.
- **Sticky Bit**: Restricts file deletion to the owner.

## 4.2 Access Control Lists in UNIX

Modern UNIX systems support extended ACLs, allowing more flexible access control by assigning permissions to named users and groups.

# 5 Role-Based Access Control (RBAC)

## 5.1 RBAC Reference Models

RBAC assigns access rights to roles rather than individual users. The NIST RBAC standard defines four models:

- $\mathbf{RBAC}_0$: Base model with users, roles, permissions, and sessions.
- $\mathbf{RBAC}_1$: Adds role hierarchies.
- $\mathbf{RBAC}_2$: Adds constraints.
- $\mathbf{RBAC}_3$: Combines $\mathrm{RBAC}_1$ and $\mathrm{RBAC}_2$.

## 5.2 Role Hierarchies

Role hierarchies allow roles to inherit permissions from subordinate roles, reflecting organizational structures.

## 5.3 Constraints

Constraints restrict role assignments and permissions, such as mutually exclusive roles and cardinality limits.

# 6 Attribute-Based Access Control (ABAC)

## 6.1 Attributes

ABAC uses attributes of subjects, objects, and the environment to make access control decisions. Attributes include:

- **Subject Attributes**: Characteristics of the user or process.
- **Object Attributes**: Characteristics of the resource.
- **Environment Attributes**: Contextual information like time or location.

### 6.2 ABAC Logical Architecture

ABAC evaluates access requests based on predefined rules and attributes, providing fine-grained access control.

### 6.3 ABAC Policies

Policies define rules for access based on attributes, allowing for flexible and dynamic access control.

## 7 Identity, Credential, and Access Management (ICAM)

### 7.1 Identity Management

ICAM manages digital identities and attributes, ensuring trustworthy identities across applications.

### 7.2 Credential Management

Credentials bind identities to tokens, such as smart cards or digital certificates, and are managed throughout their lifecycle.

### 7.3 Access Management

Access management ensures that entities are granted appropriate access to resources based on their identity and attributes.

### 7.4 Identity Federation

Identity federation allows organizations to trust digital identities and attributes from external sources, facilitating collaboration.

## 8 Trust Frameworks

### 8.1 Traditional Identity Exchange Approach

Traditional identity exchange involves agreements between identity service providers and relying parties, ensuring trust in shared identity information.

### 8.2 Open Identity Trust Framework (OITF)

OITF provides a standardized approach to identity and attribute exchange, ensuring trust and security in digital transactions.

## 9 Case Study: RBAC System for a Bank

The Dresdner Bank implemented an RBAC system to manage access to various applications. Roles were defined by job function and position, with access rights assigned based on roles. The system improved security and reduced administrative overhead.

## 10 Recommended Reading

Key references for further study include:

- [**DOWN85**]: Basic elements of DAC.
- [**SAND96**]: Comprehensive overview of RBAC.
- [**HU13**]: Overview of ABAC models.
- [**CIOC11**]: Introduction to ICAM.
- [**RUND10**]: Overview of OITF.

## 11 Key Terms

Key terms include:

- **Access Control List (ACL)**: A list of permissions attached to an object.
- **Role-Based Access Control (RBAC)**: Access control based on user roles.
- **Attribute-Based Access Control (ABAC)**: Access control based on attributes.
- **Identity Federation**: Trusting digital identities from external organizations.
- **Protection Domain**: A set of objects with associated access rights.

# Multiple Choice Questions

## Section 1: Electronic User Authentication Principles

1. **What is the primary purpose of user authentication?**

   a) To encrypt data

   b) To verify the identity of a user

   c) To store passwords securely

   d) To generate random numbers

2. **Which of the following is NOT a means of authenticating a users identity?**

   a) Something the individual knows

   b) Something the individual possesses

   c) Something the individual thinks

   d) Something the individual is

3. **What is the role of a Registration Authority (RA) in user authentication?**

   a) To issue electronic credentials

   b) To establish and vouch for the identity of an applicant

   c) To verify the identity of a claimant

   d) To store hashed passwords

4. **Which assurance level is appropriate for accessing restricted services of very high value?**

   a) Level 1

   b) Level 2

   c) Level 3

   d) Level 4

5. **What is the potential impact of an authentication error classified as "High"?**

   a) Minor financial loss

   b) Significant degradation in mission capability

   c) Severe or catastrophic adverse effect

   d) Limited adverse effect

## Section 2: Password-Based Authentication

6. **What is the primary vulnerability of password-based authentication?**

   a) Passwords are always encrypted

   b) Passwords can be easily guessed or stolen

   c) Passwords are stored in plaintext

   d) Passwords are never changed

7. **What is the purpose of a salt value in password hashing?**

   a) To encrypt the password

   b) To prevent duplicate passwords from being visible

   c) To reduce the length of the password

   d) To make passwords easier to remember

8. **Which of the following is a countermeasure to offline dictionary attacks?**

   a) Using a salt value

   b) Storing passwords in plaintext

   c) Allowing unlimited login attempts

   d) Using short passwords

9. **What is a rainbow table used for?**

   a) To store hashed passwords

   b) To precompute potential hash values for password cracking

   c) To generate random passwords

   d) To encrypt passwords

10. **What is the main drawback of computer-generated passwords?**

    a) They are too easy to guess

    b) Users may have difficulty remembering them

    c) They are always short

    d) They are not secure

11. **What is the purpose of a Bloom filter in password management?**

    a) To store passwords securely
    b) To efficiently check if a password is in a list of disallowed passwords
    c) To generate random passwords
    d) To encrypt passwords

12. **Which of the following is a characteristic of a strong password?**

    a) It is easy to remember
    b) It is short and simple
    c) It includes a mix of uppercase, lowercase, numbers, and symbols
    d) It is based on a dictionary word

## Section 3: Token-Based Authentication

13. **What is a memory card?**

    a) A card that stores and processes data
    b) A card that stores data but does not process it
    c) A card that generates random numbers
    d) A card that encrypts data

14. **Which of the following is a drawback of memory cards?**

    a) They are difficult to use
    b) They require special readers
    c) They are immune to theft
    d) They do not require a PIN

15. **What is a smart card?**

    a) A card that stores data but does not process it
    b) A card with an embedded microprocessor
    c) A card that only works with magnetic stripes
    d) A card that cannot be used for authentication

16. **Which authentication protocol involves generating a unique password periodically?**

    a) Static protocol
    b) Dynamic password generator
    c) Challenge-response protocol
    d) Memory protocol

17. **What is the purpose of the eID function in an electronic identity card?**

    a) To store a digital representation of the cardholders identity
    b) To provide general-purpose identity verification
    c) To generate digital signatures
    d) To encrypt data

## Section 4: Biometric Authentication

18. **Which of the following is a static biometric characteristic?**

    a) Voice pattern
    b) Typing rhythm
    c) Fingerprint
    d) Handwriting

19. **What is the purpose of enrollment in a biometric system?**

    a) To verify the users identity
    b) To create a template of the users biometric characteristic
    c) To generate random numbers
    d) To encrypt biometric data

20. **What is the false match rate in biometric systems?**

    a) The frequency with which samples from the same source are erroneously assessed as different
    b) The frequency with which samples from different sources are erroneously assessed as the same
    c) The frequency of correct matches
    d) The frequency of system failures

21. **Which biometric characteristic is considered the most accurate?**

    a) Voice
    b) Fingerprint
    c) Iris
    d) Signature

22. **What is the main challenge in dynamic biometric authentication?**

    a) Capturing static features
    b) Dealing with variations in the biometric sample
    c) Storing large amounts of data
    d) Encrypting biometric templates

## Section 5: Remote User Authentication

23. **What is a nonce in a challenge-response protocol?**

    a) A random number used to prevent replay attacks

    b) A hash function

    c) A password

    d) A biometric template

24. **Which of the following is a countermeasure to replay attacks?**

    a) Using a nonce

    b) Storing passwords in plaintext

    c) Using short passwords

    d) Allowing unlimited login attempts

25. **What is the primary purpose of a challenge-response protocol?**

    a) To encrypt data

    b) To verify the identity of a user

    c) To store passwords securely

    d) To generate random numbers

## Section 6: Security Issues for User Authentication

26. **Which of the following is a client attack?**

    a) Password guessing

    b) Password file theft

    c) Eavesdropping

    d) Replay attack

27. **What is a Trojan horse attack in the context of user authentication?**

    a) An attack where the adversary floods the service with authentication attempts

    b) An attack where a malicious application masquerades as an authentic one

    c) An attack where the adversary replays a captured authentication sequence

    d) An attack where the adversary guesses the password

28. **Which of the following is a countermeasure to denial-of-service attacks?**

    a) Using multifactor authentication

    b) Allowing unlimited login attempts

    c) Storing passwords in plaintext

    d) Using short passwords

## Section 7: Practical Applications and Case Studies

29. **What is the primary purpose of the UAE iris biometric system?**

    a) To encrypt data

    b) To identify expelled individuals attempting to re-enter the country

    c) To store passwords securely

    d) To generate random numbers

30. **What is the main vulnerability in ATM systems discussed in the case study?**

    a) Lack of encryption for sensitive data

    b) Use of strong passwords

    c) Use of multifactor authentication

    d) Use of biometric authentication

# Answer Key

1. b) To verify the identity of a user
2. c) Something the individual thinks
3. b) To establish and vouch for the identity of an applicant
4. d) Level 4
5. c) Severe or catastrophic adverse effect
6. b) Passwords can be easily guessed or stolen
7. b) To prevent duplicate passwords from being visible
8. a) Using a salt value
9. b) To precompute potential hash values for password cracking
10. b) Users may have difficulty remembering them
11. b) To efficiently check if a password is in a list of disallowed passwords
12. c) It includes a mix of uppercase, lowercase, numbers, and symbols
13. b) A card that stores data but does not process it
14. b) They require special readers
15. b) A card with an embedded microprocessor
16. b) Dynamic password generator
17. b) To provide general-purpose identity verification
18. c) Fingerprint
19. b) To create a template of the users biometric characteristic
20. b) The frequency with which samples from different sources are erroneously assessed as the same
21. c) Iris
22. b) Dealing with variations in the biometric sample
23. a) A random number used to prevent replay attacks
24. a) Using a nonce
25. b) To verify the identity of a user
26. a) Password guessing

27. b) An attack where a malicious application masquerades as an authentic one

28. a) Using multifactor authentication

29. b) To identify expelled individuals attempting to re-enter the country

30. a) Lack of encryption for sensitive data