Study Guide: User Authentication

Contents

1 Introduction

This study guide covers the material from Chapter 3 of the provided PDF, focusing on User Authentication. The guide is structured to follow the chapter's content, providing detailed explanations, key concepts, and important terms.

2 Electronic User Authentication Principles

2.1 A Model for Electronic User Authentication

- **Registration Authority (RA)**: Trusted entity that establishes and vouches for the identity of an applicant.
- **Credential Service Provider (CSP)**: Issues electronic credentials to subscribers.
- **Subscriber/Claimant**: The user who is to be authenticated.
- **Verifier**: Verifies the identity of the claimant.
- **Relying Party (RP)**: Uses the authenticated information to make access control or authorization decisions.

2.2 Means of Authentication

- **Something the individual knows**: Passwords, PINs, answers to prearranged questions.
- **Something the individual possesses**: Tokens like keycards, smart cards.
- **Something the individual is (static biometrics)**: Fingerprints, retina, face.
- **Something the individual does (dynamic biometrics)**: Voice pattern, handwriting, typing rhythm.

2.3 Risk Assessment for User Authentication

- **Assurance Levels**: Levels 1 to 4, indicating the degree of confidence in the asserted identity.
- **Potential Impact**: Low, Moderate, High - the impact of an authentication error.
- **Areas of Risk**: Mapping potential impact to assurance levels.

3 Password-Based Authentication

3.1 The Vulnerability of Passwords

- **Offline Dictionary Attack**: Attacker gains access to the password file and compares hashes.
- **Specific Account Attack**: Attacker targets a specific account and submits password guesses.
- **Popular Password Attack**: Attacker uses common passwords against a wide range of user IDs.
- **Password Guessing Against Single User**: Attacker uses knowledge about the account holder to guess the password.
- **Workstation Hijacking**: Attacker waits until a logged-in workstation is unattended.
- **Exploiting User Mistakes**: Users may write down passwords or share them.
- **Exploiting Multiple Password Use**: Different devices share the same or similar passwords.
- **Electronic Monitoring**: Passwords communicated over a network are vulnerable to eavesdropping.

3.2 The Use of Hashed Passwords

- **Hashed Passwords**: Passwords are stored as hash codes to prevent plaintext storage.
- **Salt Value**: A random value added to the password before hashing to prevent duplicate passwords and increase security.
- **UNIX Password Scheme**: Uses a slow hash function and salt to secure passwords.

3.3 Password Cracking of User-Chosen Passwords

- **Traditional Approaches**: Dictionary attacks, rainbow tables.
- **Modern Approaches**: Improved processing capacity and sophisticated algorithms.

3.4 Password File Access Control

- **Shadow Password File**: Hashed passwords are kept in a separate file to protect them.
- **Vulnerabilities**: Unanticipated break-ins, accidental protection failures, lack of physical security.

3.5 Password Selection Strategies

- **User Education**: Guidelines for selecting strong passwords.
- **Computer-Generated Passwords**: Randomly generated passwords.
- **Reactive Password Checking**: System periodically runs its own password cracker.
- **Complex Password Policy**: System checks passwords at the time of selection.

4 Token-Based Authentication

4.1 Memory Cards

- **Memory Cards**: Store but do not process data, used with a PIN or password.
- **Drawbacks**: Requires special readers, token loss, user dissatisfaction.

4.2 Smart Cards

- **Smart Cards**: Contain a microprocessor, used for authentication.
- **Authentication Protocols**: Static, dynamic password generator, challenge-response.

4.3 Electronic Identity Cards

- **eID Cards**: National identity cards with electronic functions.
- **Functions**: ePass, eID, eSign.

5 Biometric Authentication

5.1 Physical Characteristics Used in Biometric Applications

- **Facial Characteristics**: Relative location and shape of key facial features.
- **Fingerprints**: Pattern of ridges and furrows on the fingertip.
- **Hand Geometry**: Shape and lengths of fingers.
- **Retinal Pattern**: Pattern formed by veins beneath the retinal surface.
- **Iris**: Detailed structure of the iris.
- **Signature**: Unique style of handwriting.
- **Voice**: Physical and anatomical characteristics of the speaker.

5.2 Operation of a Biometric Authentication System

- **Enrollment**: User presents a name and biometric characteristic to the system.
- **Verification**: User enters a PIN and uses a biometric sensor.
- **Identification**: System compares the presented template with stored templates.

5.3 Biometric Accuracy

- **False Match Rate**: Frequency with which biometric samples from different sources are erroneously assessed to be from the same source.
- **False Nonmatch Rate**: Frequency with which samples from the same source are erroneously assessed to be from different sources.
- **Threshold**: Determines the balance between false match and false nonmatch rates.

6 Remote User Authentication

6.1 Password Protocol

- **Challenge-Response Protocol**: Host generates a random number and functions, user responds with a function of the random number and password hash.

6.2 Token Protocol

- **Challenge-Response Protocol**: Similar to password protocol, but uses a token-generated passcode.

6.3 Static Biometric Protocol

- **Challenge-Response Protocol**: User presents a biometric, system compares it to stored templates.

6.4 Dynamic Biometric Protocol

- **Challenge-Response Protocol**: User presents a dynamic biometric, system compares it to stored templates.

7 Security Issues for User Authentication

7.1 Client Attacks

- **Password Guessing**: Adversary attempts to guess the password.
- **Token Theft**: Adversary must acquire the physical token.

7.2 Host Attacks

- **Password File Theft**: Adversary gains access to the password file.
- **Token Passcode Theft**: Adversary gains access to token passcodes.

7.3 Eavesdropping, Theft, and Copying

- **Password Eavesdropping**: Adversary observes the user entering the password.
- **Token Theft**: Adversary steals or copies the token.
- **Biometric Copying**: Adversary copies or imitates the biometric parameter.

7.4 Replay Attacks

- **Replay**: Adversary repeats a previously captured user response.

7.5 Trojan Horse Attacks

- **Trojan Horse**: Malicious application or device masquerades as authentic.

7.6 Denial of Service

- **Denial of Service**: Adversary floods the service with authentication attempts.

8 Practical Application: An Iris Biometric System

- **UAE Iris Biometric System**: Used for border control, identifies individuals based on iris patterns.
- **Enrollment**: Expelled foreigners are subjected to an iris scan.
- **Identity Checking**: Iris scanners at ports compare incoming passengers' iris patterns to a central database.

9 Case Study: Security Problems for ATM Systems

- **ATM Vulnerabilities**: Confidentiality and integrity issues due to lack of encryption.
- **Recommendations**: Short-term fixes like network segmentation, long-term fixes like application-level encryption.

10 Key Terms

- **Biometric**: Authentication based on physical characteristics.
- **Challenge-Response Protocol**: Protocol where the host challenges the user to prove identity.
- **Claimant**: User attempting to prove identity.
- **Credential**: Data structure binding identity to a token.
- **Credential Service Provider (CSP)**: Issues electronic credentials.
- **Dynamic Biometric**: Authentication based on dynamic physical characteristics.
- **Enroll**: Process of registering a user in a biometric system.
- **Hashed Password**: Password stored as a hash code.
- **Identification**: Process of presenting an identifier to the security system.
- **Memory Card**: Card that stores but does not process data.

- **Nonce**: Random number used in challenge-response protocols.
- **Password**: Secret word or phrase used for authentication.
- **Rainbow Table**: Precomputed table for reversing cryptographic hash functions.
- **Registration Authority (RA)**: Entity that establishes and vouches for identity.
- **Relying Party (RP)**: Entity that uses authenticated information.
- **Salt**: Random value added to a password before hashing.
- **Shadow Password File**: File storing hashed passwords separately.
- **Smart Card**: Card with an embedded microprocessor.
- **Static Biometric**: Authentication based on static physical characteristics.
- **Subscriber**: User registered with a credential service provider.
- **Token**: Object possessed by a user for authentication.
- **User Authentication**: Process of verifying a user's identity.
- **Verification**: Process of corroborating the binding between an entity and an identifier.
- **Verifier**: Entity that verifies the identity of a claimant.

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