**Al- Mustaqbal University**

**College of Sciences**

**Department of Cybersecurity**

**Principles of Cyber Security**

**First stage**

**Lecture 3**

 **2025-2024 Lectuer : Muntather AL-Mousawi**

 **Overview**

This lecture deals with authentication and the secure management

of user accounts that enforces authentication credentials and then

goes on to explain single sign-on systems and the advanced

management of credentials needed for such systems.

**Lecture Objectives**

**3.1** Describe the different types of authentication credentials.

**3.2** Explain the different attacks on authentication.

**OB.3.1: Describe the different types of authentication credentials**

**3.1 Authentication Credentials**

1. Theauthentication can be based on where a user is (geolocation),

what a user has (like a token or a card), what a user is (biometrics),

what a user knows (such as a password), and what a user does

(cognitive and behavioral biometrics).

**3.1.1 What You Know: Passwords**

1. We can define the password as a secret combination of letters,

 numbers, and/or characters that only the user should know.

2. Note that passwords are the most common type of authentication

 today.

3. Emphasize that despite their widespread use, passwords provide

 only weak protection.

4. The weakness of passwords centers on human memory.

5. The challenges that passwords present to the human memory.

**(1)**

 a. Long and complex passwords can be difficult to memorize.

 b. There are many different passwords to remember because

 users have so many accounts.

 c. Security policies that mandate password expiration

 exacerbate these problems.

6. The shortcuts that people take with passwords including weak

 passwords and reusing passwords, and the predictable syntax

 often used

7. The types of attacks against password that were prevalent in the

 past: social engineering, capturing, and resetting.

8. Detail contemporary password attacks

 a. Offline hash algorithm attacks.

 b. Brute force attacks. Note the LM hash, NTLM hash, and pass

 the hash.

 c. Mask attack. Note the parameters used: password length,

 character set, language, pattern, skips.

 d. Show the steps and analysis in a rules attack

 e. The dictionary attack begins with the attacker creating

 encrypted versions of common dictionary words, and then

 comparing them against those in a stolen password file.

 f. The hybrid attack, which is a variation of the dictionary attack.

 g. Discuss how a rainbow table is used to crack a password; note

 that tables can be used repeatedly and are available on the

 internet.

 h. Point out that password collections obtained by attacks

 provided a massive number of actual passwords, plus insight

 into users’ thinking and password-creation habits.

 i. Review the common attack sequence,

**(2)**

9. Point out that protection and security of passwords is contingent

 on rigorous controls by both users and the enterprise.

 a. Users:

 i. Discuss password length and complexity. Show the

 increase in complexity based on length as displayed in

 Table 11-3.

 ii. Review password recommendations:

 1. Do not use passwords that consist of dictionary

 words or phonetic words.

 2. Do not use birthdays, family member names, pet

 names, addresses, or any personal information.

 3. Do not repeat characters (xxx) or use sequences

 (abc, 123, qwerty).

 4. Explain how to add non-keyboard characters to

 passwords to increase security.

 iii. Review the recommendations for managing passwords

 and note the rise of password management

 applications.

b. Enterprises: Review the responsibilities of organizations for

 password security, i.e., protecting digests.

1. Explain salts and their benefits.
2. Explain key stretching, specifically bcrypt and PBKDF2.

**3.1.2 What You Have: Tokens, Cards, and Cell Phones**

 1. Define multifactor authentication.

 2. Emphasize that a significant increase in the level of security of

 authentication credentials can be achieved by using a token.

 3. Explain hardware and software security tokens.

 displays a hardware token example.

 4. Discuss the advantages that tokens have over passwords:

 a. Standard passwords are static in nature while tokens produce

 dynamic passwords that change frequently. Note the two

 types of dynamic passwords: TOTP and HTOP.

 b. A user might not know if an attacker has stolen his password,

 so confidential information could be accessed without the

 user’s knowledge where if a token is stolen it is more obvious.

**(3)**

 5. Note that a smart card contains an integrated circuit chip that can

 hold information, which can then be used as part of the

 authentication process. Refer to figure 11-8 to illustrate a smart

 card. Reference the U.S. DoD common access card and the PIV

 standard.

 6. Point out that cell phones are increasingly used to communicate

 OTPs

**3.1.3 What You Are: Biometrics**

 1. Note that biometrics authentication involves standard biometrics

 and cognitive biometrics.

 a. Explain that standard biometrics uses a person’s unique

 physical characteristics for authentication.

 b. The most common uses are fingerprints and eye scans via

 retinal scanners and fingerprint scanners

 c. Mention the use of voice recognition and the reasons it would

 prove difficult for a hacker to emulate.

 d. Note that additional biometric authentication may come from

 iris scanners.

 2. Review disadvantages of standard biometrics:

 a. Costs of specialized scanners

 b. The technology is not yet foolproof. Note the terms FAR, FRR,

 and CER.

 c. Researchers have proven that the technology can be tricked.

 3. Note that cognitive biometrics is related to the perception, thought

 process, and understanding of the user.

 4. Explain that cognitive biometrics is considered to be much easier

 for the user to remember because it is based on the user’s life

 experience and it is very difficult for an attacker to imitate.

**3.1.4 What You Do: Behavioral Biometrics**

 1. Explain that behavioral biometrics authenticates by normal actions

 that the user performs.

 2. Detail one of the most promising fields of behavioral biometrics,

 keystroke dynamics. Keystroke dynamics use the unique typing

 cadence of each user to create a template, which is then used to

 authenticate a user

**(4)**

**3.1.5 Where You Are: Geolocation**

 1. Introduce geolocation as an authentication method, which can

 associate a geographic location, ISP, and even days and times to an

 IP address.

**Quick Quiz 1**

1. A(n) \_\_\_\_ is a secret combination of letters, numbers, and/or

characters that only the user should know.

2. The \_\_\_\_ attack conducts statistical analysis on stolen passwords.

3. True or False: A token is typically a small device (usually one that

can be affixed to a keychain) with a window display.

4. True or False: Cognitive biometrics is considered to be much more

difficult for the user to remember.

5. Authentication that interprets a user’s physical whereabouts is

known as \_\_\_\_\_\_\_\_\_\_.

**OB.3.2: Explain the Different Attacks on Authentication.**

**3.2.1 Different Attacks on Authentication**

**Brute Force Attacks:**

In a brute force attack, an adversary systematically tries all possible

combinations of usernames and passwords until the correct one is

found. This method relies on the assumption that weak or easily

guessable passwords can be discovered through exhaustive trial

and error.

**Phishing Attacks:**

Phishing involves tricking individuals into revealing their

authentication credentials by posing as a trustworthy entity.

Attackers often send deceptive emails or messages that appear

legitimate, prompting users to enter their usernames and

passwords on fraudulent websites.

**Man-in-the-Middle (MitM) Attacks:**

MitM attacks involve intercepting and manipulating communication

between two parties, such as a user and a server. Attackers can

capture authentication credentials during transmission, enabling

them to impersonate the legitimate user.

**(5)**

**Keylogging:**

Keyloggers are malicious programs or devices that record

keystrokes on a user's computer. By capturing the keystrokes

related to authentication, attackers can obtain usernames,

passwords, and other sensitive information without the user's

knowledge.

**Biometric Spoofing:**

Biometric authentication, such as fingerprint or facial recognition,

can be compromised through spoofing techniques. Attackers may

use artificial fingerprints or facial images to deceive biometric

systems and gain unauthorized access.

**Rainbow Table Attacks:**

Rainbow tables are precomputed tables of hash values for different

possible passwords. In a rainbow table attack, attackers use these

tables to quickly find the original password from a stored hash,

especially if the password is weak and easily guessed.

1. **Password Spraying:**

Password spraying is a technique where attackers try a few

commonly used passwords across many user accounts to avoid

detection by account lockout policies. This method aims to bypass

defenses that lock accounts after multiple failed login attempts.

**Additional Resources**

1. Security Tip (ST05-012), Supplementing Passwords from US-CERT,

the United States Computer Emergency Readiness Team:

**https://www.us-cert.gov/ncas/tips/ST05-012**

2. OAuth

**http://oauth.net/**

**(6)**