Principles of Cyber Security_Lecture 04: Authentication Solutions

Contents

Lecture 04: Authentication Solutions

Outline

- Overview
- Objectives
- Quick Quizzes
- Class Discussion Topics
- Additional Resources

Lecture Notes

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

4.1 Describe how to implement authentication security solutions

4.2 Explain What Single Sign-On Can Do

4.3 List the account management procedures for securing passwords

OB.4.1: Describe how to implement authentication security solutions

4.1.1 Implement Authentication Security Solutions

In the dynamic landscape of cybersecurity, establishing robust authentication security solutions is paramount for safeguarding digital assets and sensitive information. Authentication serves as the primary line of defense against unauthorized access, ensuring that only legitimate users gain entry to systems, networks, and data repositories. This introduction will provide a foundational overview of key considerations and steps involved in implementing effective authentication security measures.

Authentication, at its core, verifies the identity of users seeking access to a system or application. As the digital realm becomes increasingly interconnected, the importance of implementing sophisticated authentication security solutions cannot be overstated. Threat actors continually evolve their tactics, making it imperative for organizations to fortify their defenses and stay ahead of potential vulnerabilities.

To embark on a successful implementation of authentication security solutions, several fundamental steps and best practices should be considered. These encompass multi-factor authentication (MFA) to add layers of verification, enforcing strong password policies, employing account lockout mechanisms to thwart brute force attacks, and ensuring secure transmission of credentials over networks. Moreover, the integration of biometric authentication, such as fingerprint or facial recognition, adds an extra dimension of security.

Regular security audits and monitoring, coupled with user education initiatives, contribute to an organization's resilience against evolving threats. Implementing single sign-on (SSO) solutions streamlines user access while maintaining stringent security protocols. Role-based access controls (RBAC) tailor permissions based on user roles, and time-based access controls restrict entry during specified hours.

OB.4.2: Explain What Single Sign-On Can Do

4.2.1 Single Sign-On

1. One of the problems facing users today is the fact that they have multiple accounts across multiple platforms that all ideally use a unique username and password.
2. The idea behind identity management is to have one username and password to gain access to all accounts so that the user only has one username and password to remember.
3. Note that when networks are owned by different organizations, it is called federated identity management (FIM).
4. Discus single sign-on (SSO), which is one application of FIM.
5. Review some of the current federation systems, referencing Table 11-4.

OB.4.3: Account Management Procedures for Securing Passwords

4.3.1 Account Management

1. Note that managing the passwords in user accounts can be accomplished by setting restrictions regarding the creation and use of passwords.
2. Discuss the six common domain password policy settings, which are called Microsoft setting objects.
3. Refer to Table 11-5 to discuss the password policy settings for Windows Group Policy.
4. Discuss the Account Lockout Policy, which is an Active Directory Domain Services (AD DS) security feature.
5. Refer to Table 11-6 for a list of the account lockout policy settings in Windows Active Directory.

Quick Quiz 1

1. SSO is an application of _____?

2. Which of the following is not a password setting in Microsoft Windows group policy?
   - Password length
   - Password History
   - Password alias
   - Password complexity
   - Password encryption

3. All of the following are federation systems, except _____?
   a. Shibboleth
   b. Open ID Connect
   c. OAuth
   d. OpenFed

4. The Active Directory Domain Service policy that can block a login after a specified number of failed logins over a specified time period is named: _____.

   Answer: Account Lockout Policy

Class Discussion Topics

1. Discuss the use of distributed (federated) authentication systems in use at your institution. If no such system is in use, have students research how certain systems integrate with the identity system at your institution.
2. Discuss personal experiences with password management. How do they manage their own various accounts? Do they have experiences in data centers with password problems related to management or user indifference?

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/**