Protecting Information Assets
- Week 10 -

Identity Management and Access Control

MIS5206 Week 10

- Team Presentation
- Identity Management and Access Control
- Test Taking Tip
- Quiz

Team Presentation

This week's subject is Public Key Encryption and Digital Signatures

The team is:

Business focus: Rinku Patel

Technical focus: Mustafa Al Shalchi

Risk Assessment/Mitigation focus: Ziwei Zhu

Identity Management and Access Control

Business owners and managers are constantly identifying areas of security risk and taking steps to mitigate that risk. In an IT environment, risk takes the form of access.

What do we mean by “Access Control”

- Access is the ability to create a flow of information between user and system

- Access Controls are security features that control how users and systems communicate and interact with one another

Access Control Principles

Three main security principles apply to access control:

Confidentiality
Integrity
Availability

What's the difference between Identification, Authentication and Authorization?

Identification, Authentication and Authorization are distinct functions

Identification: Who you say you are

Authentication: Confirmation that you are who you say you are

Authentication: What privileges you are allowed based on who you are

Identification

Identification

Method of establishing the subject's (user, program, process) identity

- Use of user name or other public information
- Know identification component requirements

Authentication

- Authentication
  - Method of proving the identity.
    - Something a person is, has, or does.
    - Use of biometrics, passwords, passphrase, token, or other private information.

Authentication

- Biometrics
  - Verifies an identity by analyzing a unique person attribute or behavior
- Most expensive way to prove identity, also has difficulties with user acceptance
- Many different types of biometric systems

Authentication

Most common biometric systems:

- Fingerprint
- Palm Scan
- Hand Geometry
- Iris Scan
- Signature Dynamics
- Keyboard Dynamics
- Voice Print
- Facial Scan
- Hand Topography

Authentication

- Biometric systems can be hard to compare
- Type I Error: False rejection rate
- Type II Error: False acceptance rate
  - This is an important error to avoid

Authentication

Passwords

- User name + password most common identification, authentication scheme
- Weak security mechanism, must implement strong password protections

Authentication

Techniques to attack passwords

- Electronic monitoring
- Access the password file
- Brute Force Attacks
- Dictionary Attacks
- Social Engineering

Authentication

Passphrase

- Is a sequence of characters that is longer than a password
- Takes the place of a password
- Can be more secure than a password because it is more complex

Authentication

Token Devices

- Synchronous
  - Time Based
  - Counter Synchronization
- Asynchronous

Authentication

Hashing & Encryption

- Hash or encrypting a password to ensure that passwords are not sent in clear text (means extra security)
- Salts: Random values added to encryption process for additional complexity.

Authentication

- Cryptographic Keys
  - Use of private keys or digital signatures to prove identity
- Private Key
- Digital Signature
  - Beware digital signature vs. digitized signature.

Authorization

Authorization

– Determines that the proven identity has some set of characteristics associated with it that gives it the right to access the requested resources

Authorization

Access Criteria can be based on:

- Roles
- Groups
- Location
- Time
- Transaction Types

Authorization

Authorization Concepts

- Authorization Creep
- Default to Zero
- Need to Know Principle
- Access Control Lists

Authorization

Complexity leads to problems in controlling access:

- Different levels of users with different levels of access
- Resources may be classified differently
- Diverse identity data
- Corporate environments keep changing

Authorization

Advantages of centralized administration and single sign on:

- User provisioning
- Password synchronization and reset
- Self service
- Centralized auditing and reporting
- Integrated workflow (increase in productivity)
- Regulatory compliance

Authorization

- Single Sign On Capabilities
  - Allow user credentials to be entered one time and the user is then able to access all resources in primary and secondary network domains
- SSO technologies include:
  - Kerberos
  - Sesame
  - Security Domains
  - Directory Services

Access Control Models

Access Control Models:

- Discretionary
- Mandatory
- Role Based

Access Control Models

- Discretionary Access Control (DAC)
  - A system that uses discretionary access control allows the owner of the resource to specify which subjects can access which resources.
  - Access control is at the discretion of the owner.

Access Control Models

Mandatory Access Control (MAC)

- Access control is based on a security labeling system. Users have security clearances and resources have security labels that contain data classifications.
- This model is used in environments where information classification and confidentiality is very important (e.g., the military).

Access Control Models

- Role Based Access Control Models
  - Role Based Access Control (RBAC) uses a centrally administered set of controls to determine how subjects and objects interact.
  - Is the best system for an organization that has high turnover.

Access Control Techniques

Different access controls and technologies available to support the different models

- Rule Based Access Control
- Constrained User Interfaces
- Access Control Matrix
- Content Dependent Access Control
- Context Dependent Access Control

Access Control Techniques

Types of Centralized Access Control

- Radius - Remote Authentication Dial In User Service
- TACACS -Terminal access controller access control system
- Diameter - name is a pun on the RADIUS protocol

Test Taking Tip

Look at the facts and ask yourself, so what?

- The issue that jumps out is likely to be the issue that the correct response addresses.
- Non-relevant answers can be eliminated more readily.
- Especially useful in questions that ask for the “Best” answer.

Quiz