A Survey on Identity and Access Management

[1]Shreyas Kanna, [2]C. Umarani

Abstract

Identity and access management (IAM) is a technological framework for business that enables the creation, maintenance, and use of digital identity — ensuring that the right people gain access to the right materials and records at the right time. This paper presents a technical survey on Identity and Access Management.

Keywords: Identification, authentication, authorization.

Introduction

Identification, authentication, &authorization:

To be able to access a set of data or a resource, a subject has to be Identified, Authenticated, &authorized.

Identification – describes a method of securing that a subject such as user , program , or process is a real entity as it claim it to be.Ex- username,acc.number etc.

Authentication – Testing of evidence of a user's identity.Ex – password.

Authorization- granting access to an object after subject has been properly identified and authenticated.

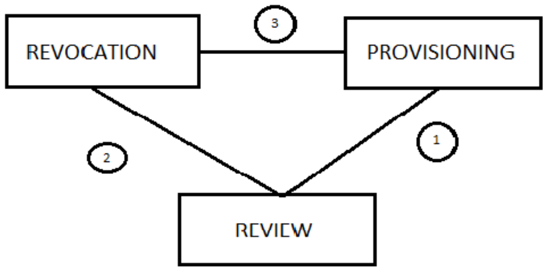
Identity Management:

Identity management is the use of different products to identify , authenticate & authorize the users through automated means.

It describes the management of individual identities, their authentication and privileges or permissions within or the system and enterprise boundaries.

The goal is to increase the security and productivity while decreasing the cost, downtime, and repetitive tasks.

Identity and access provisioning lifecycle:



1. Provisioning
- create new accounts
- provision them with appropriate rights and privileges.

2. Review –
- check accounts periodically
- disable in-active accounts
- check for excessive and creeping privileges

3. revocation
- disable an account as soon as employee leaves
- set account expiry date for temporary accounts
- delete an expired account as per organization's policy

To ensure an application is authorized to make requests to potentially sensitive resources, the system can use digital identification, such as certificate or one-time password.

Guidelines for user identification

1. Uniqueness– identification must be unique
2. Non-descriptive – the role or job function should not be exposed by ID
3. Secure assurance – Id issuing process must be well secure and documented.

Verifying Identification Information

The function of identification is to map a known quantity to an unknown entity to make it known .
There are 3 general factors that can be used for verifying identification:
1. Something you know- password, PIN
2. Something you have – key, swipe cards, access cards, badges
3. Something you are –Biometrics

Password:

Password is a sequence of character that is known by the authentic users and is used to authenticate himself.

Biometrics types :

1. Physiological - voice, DNA, fingerprint
2. Behavioral – typing rhythm, gait, signature analysis etc.

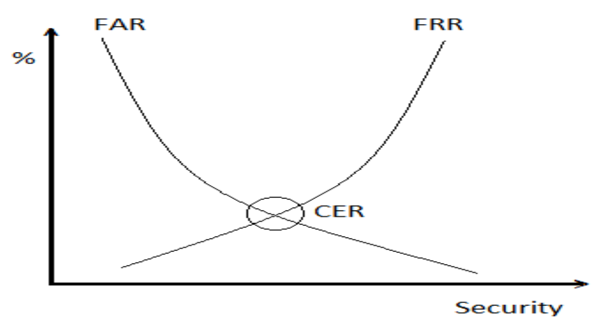
Biometrics characteristics:

1. Acceptance- refers to user acceptance of biometric system.Depends on privacy intrusiveness and physical discomfort.
2. Throughput rate– also called as biometric system response time (time taken to process the authentication). (avg time -6-10sec).
3. Enrollment time – time taken by biometric system to register and create an account for the first time. (avg-less than 2 mins).

Types of biometrics:

1. Finger print
2. Hand geometry
3. Iris scan
4. Retina scan
5. Voice print
6. Keyboard dynamics
7. Signature
8. Facial scan (bone struct, nose ridges, eye widths, chin size).

Accuracy of biometric



FRR (False rejection Rate) – rejects an authorized individuals from being authenticated. It is also called as type1 error.

FAR(False Acceptance Rate) - when an un-authorized person whom should be rejected is accepted. It is also called as type 2 error.

CER (Cross-over Error Rate)– describes where the FRR and FAR are equal. It is also called as Equal error rate(ERR).

High Accuracy = high FAR & low FRR.

Lower CER = high accuracy.

Tokens:

Steps to authenticate user using asynchronous based token:

1. challenge number is displayed on workstation
2. user enters challenge number and pin permanently associated with pad
3. response is read from the pad
4. user enters response from the handheld device
5. authentication server verifies the response

Memory cards and smart cards:

1. memory card:
   - ❖ holds user information however not process the information
   - ❖ user Id and pin is entered and compared to the memory card information to authenticate the user
2. smart card: they can they and also process the information as they have necessary software , microprocessor and integrated circuit(IC).
   2 types of smart cards are:
   i. contact cards: with gold sealed module contacts and chips
   ii. contactless cards: with antenna ,chip and IC

AUTHORIZATION:

Authorization is based on the following concepts:
- ❖ Need to know principle: depending on the subject's duty and requirements, the subject is given access to a specific information.
- ❖ Authorization creep: when employee moved from one department to another, change the privileges and remove previous permissions to maintain least privilege.
- ❖ Access Control List (ACL): specifies the subjects which are granted access and the operations allowed on subjects.
- ❖ Default to zero: access controls should always start with zero access. Admin can then allow various access based on the organization's security policy.

Access :A gateway which allows legitimate users to use the resources which he/she is allow to use.Access Criteria: an organization should grant access privileges to subjects based on its level of trust and need to know to know policy.

Access criteria are based on :

- ❖ Role- Access granted depending on role or job function in the organization
- ❖ Groups- Creating user groups and assigning rights and privileges to the group.
- ❖ Location- Access given based on the location of the user
- ❖ Time- Access is granted based on the time
- ❖ Transaction/command- Granted based on the user privileges to carry out certain commands and functions on the dat**a**

Access control types based on security layer:

1. Administrative control: broad set of policies , procedure and standards . It is also called as Directive control.
2. Technical control: It is also called as logical controls. It is implemented using software, hardware and firmware.

Ex- protocols, encryption and system access .

3. Physical control: manages physical access to information such as application servers and network devices .

Ex- logs , fences, security guards.

Access control types based on functionality:

1. Preventive: Avoid problems before they occur
2. Detective : Detect a problem that is happening
3. Corrective: Correct the problem that has happened
4. Deterrent: Discourages someone from doing an act
5. Recovery: restore a resource from an event that has occurred
6. Compensation: Provides alternative controls to other controls

Access control models:

The way in which a subject will access an object is guided by access control model. A model must be chosen to fulfill the directive of the security policy

1. Discretionary Access Control (DAC) model:

Discretionary access control (DAC) is a type of security access control that grants or restricts object access via an access policy determined by an object's owner group and/or subjects. DAC mechanism controls are defined by user identification with supplied credentials during authentication, such as username and password. DACs are discretionary because the subject (owner) can transfer authenticated objects or information access to other users. In other words, the owner determines the object access privilege.

2. Mandatory Access Control (MAC) model:
3. Role Based Access Control (RBAC):

Identity management technologies:

1. Password management:

It is the common practice for validating a user's identity during the authentication process. A process governing user password should consider following:

2. Directory management:

Corporate directory is a comprehensive database that contains information pertaining to the company's network resources and users

3. Account management:

Involves creating user accounts on every system; modifying the account privileges when required; and decommissioning the accounts when they are no more required

4. Profile management:

Collection of information associated with a particular user identity or group

5. Web Access Management:

WAM makes use of software controls to control what users can access from web-based enterprise assets using their web browser

6. Single Sign-On (SSO):

User needs to enter credentials only once to get access to all the corporate resources which are entitled to user

Conclusion: A Survey on Identity Access Management reveals that Multifactor Authentication Is highly secure in most of the cases. But in some applications, Single sign-on ,Single factor Authentication also seems to be good. Selection is Purely based on the application.

References

Information Security-Nina Godbole.

Author's details

[1]MCA-ISMS Student, Jain University, Bangalore

[2]Professor,Jain University,Bangalore