A RESEARCH OF AUTHENTICATION AND AUTHORIZATION METHODS

1

2

Abstract: **Authentication is a process of granting a user access to an information system. there are three main types of authentication mechanisms, password entry, smartcard and biometric. And then authorization is the process of giving someone permission to do or have something. Every access control has four processes Identification, Authentication, Authorization and Accountability. Particularly MFA is expected to be utilized for human to – everything interactions by enabling fast, user – friendly and reliable authentication when accessing a service. In this paper we review of authentication, authorization and examples of MFA systems and cryptography.**

Keywords: **Authentication - Authorization - Techniques - Multifactor authentication (MFA) – Cryptography.**

1. INTRODUCTION

Today almost everything is digitalized and automated, where business, academic , scientific and economic world revolve around the exchange of information. That's where authentication comes into place. authentication is a process of validating the user's identity. Users are identified using different authentication mechanism. In a security systems the authentication process checks the information provided by the user with the database. The authorization process is handled three ways authorization is performed for authenticated user, authorization is performed for members of the group, authorization is performed access the multiple systems and accountability is a process keeping system logs. System logs keep track of successful and unsuccessful logins.

There are three universal authentication factors.

a) Something you know, such as a username and a password.

b) Something you have, such as a smartcard.

c) Something you are, such as a fingerprint.

the paper will help the readers in better understanding of different techniques and explore the field.

2. AUTHENTICATON

Verifies you are who you say you are methods.

a) Login form

b) HTTP authentication

c) HTTP digest

d) X.509 certificates

e) Custom authentication method.

3. AUTHORIZATION

Decide if you have permission to access a resource methods.

f) Access controls for URLs.

g) Secure object and methods

h) Access control lists (ACLs)

4. DIFFERENCE BETWEEN AUTHENTICATION AND AUTHORIZATION

Authentication is the process of verifying who you are. **Authorization** is the process of verifying what you have access to.

5. AUTHENTICATION MECHANISMS

Authentication mechanisms it specifies a challenge – response protocol in which data is exchanged between the client and the server for the purpose of authentication and establishment of a security layer on which to carry out subsequent communication.

- Password based authentication
- Token based authentication
- Biometric based authentication

5.1. Password Based Authentication:

The server maintains a list of names and passwords,if a particular name is on the list,and if the user types the correct password,the server grants access. Certificate based authentication. Client authentication based on certificates is part of the SSL protocol.

5.2. Token based Authentication:

Token based authentication is a security technique that authenticates the user who attempt to login to a server,a network,or some other secure system,using a seurity token provided by the server. The service validates the security token and process the user request.

5.3. Biometric based Authentication:

Biometric based authentication is a security process that relies on the unique biological characteristics of an individual to verify that be is who is says be is... typically, biometric authentication is used to manage access to physical and digital resources such as buildings,rooms and computing devices.

6. THE GENERAL FORMS OF AUTHENTICATION

- Identity – confirming credentials.
- Typically categorized by knowledge.
- Inherence and location factors.

Four – factor authentication is a newer security para diagram then two factors or three factors authentication.

7. CRYPTOGRAPHY

The conversion of data in to a secret code for transmission overa public network. Today,most cryptography is digital,and the original text “Plain Text” is turned into a coded equivalent called “Cipher Text” via an encryption algorithm.

Its denote simply the original informations to transmitted by the meaning less formation.

7.1. The Basic Principles:

7.1.1. Encryption

In a simplest form, encyption is to convert the data in some and unreadable form. This helps in protecting the privacy while sending the data from sender to receiver

7.1.2. Authentication

This is another important principle of cryptography. In a authentication ensures that the message was originated from the originator claimed in the message.

7.1.3. Integrity

Now, one problem that a communication system can face is the loss of integrity of message being send from sender to receiver. This means that cryptography should ensure that the messages that are received by the receiver are not allotted anywhere on the communication path. This canbe achieved by using the concept of cryptographic hash.

7.1.4 Non- Repudiation

Cryptography should prevent the originator or sender to act this way. One popular way to achieve this is through the use of digital signatures.

7.2. Types of Cryptography:

There are three types of cryptography techniques:

a) Secret- key cryptography

b) Public- key cryptography

c) Hash function

7.2.1. Secret - Key Crptography:

This type of cryptography technique uses just a single key. The sender applies a key to encrypt a message while the receiver applies the same key to decrypt the message. Since only single key is used so we say that this is a symmetric encryption.

The biggest problem with this technique is the distribution of key as this algorithm makes use of single key for encryption or decryption.

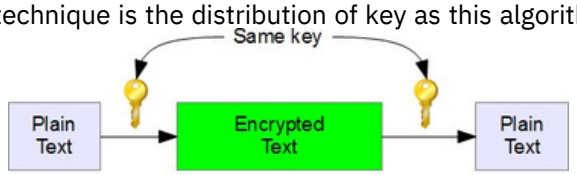


Fig 1: Secret – Key Cryptography

7.2.2. Public - Key Cryptography: This type of crptography technique involves two key crypto system in which a secure communication can take place between receiver and sender over insecure communication channel. Since a pair of keys is applied here so this technique is also known as symmetric encryption. In this method, each party has a private key and a public key. The private is secret and is not revealed while the public key is shared with all those whom you want to communicate with.

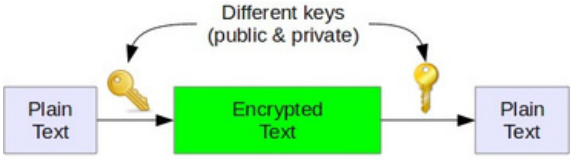


Fig 2: Public – Key Cryptography

7.2.3. Hash Functions:

This technique does not involve any key. Rather it uses a fixed length hash value that is computed on the basis of the plain text message. Hash functions are used to check the integrity of the message to ensure that the message has not be altere compromised or affected by virus.

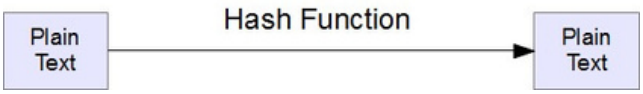


Fig 3: Hash Function

8. COMPARISON

The following compares different techniques of authentication

Table 1: - Comparison

	Secret - Key Cypto Systems	Public – Key Crypto Systems	Bio metric Systems
Speed	High	Low	High
Memory Requirement	64 Bits of Secret Key	400 – 500 Bits of Secret Key	9 Bits to Mega Bytes Depends on the Application
Reliability	Good	Very Good	Good
Security Level	High	High	Reasonable
Convenience	Convenient	Export Restrictions	Not in all Applications
Availability	Export Restrictions		Available

9. MULTIFACTOR AUTHENTICATION (MFA)

MFA is a security system that requires more than one method of authentication from independent categories of credentials to verify the user's for a login or other transaction.

Multi-factor authentication can be used in any scenario (internal or external) where an additional layer of protection and security against compromised credentials is required one of the most important application of multi- factor authentication is its use for accessing and managing network environment remotely.

Today, digitalization decisively penetrates all the sides of the modern society. One of the key enablers to maintain this process secure is authentication. It covers many different areas of a hyper – connected world, including online payments , communications , access right management, etc. this work sheds light on the evolution of authentication systems towards multi- factor authentication (MFA) starting from single – factor authentication (SFA) and through.

9.1. AWS

MFA addsextra security because it requires users to provide unique authentication from an AWS supported MFA mechanism in addition to their regular sign-in credentials when they access AWS websites or services virtual MFA device.

9.2. IAM users

To configure and enable a virtual MFA device for use with your root user(console)

1. Sign in to the AWS Management console.
2. Do one of the following....
3. choose mange MFA or active MFA,depending on which option you chose in the preceding step.
4. In the wizard,choose virtual MFA deviceand then choose continue.

9.3. Types of MFA

Multi-factor authentication is a method of logon verification where at least two different factors of proof are required.There are generaliy three recognized types of authentication factors:

Type1-something You Know-includes password,PINs,combination,code words,or secret handshakes.Anything that you can remember and then type,say,do,performo or otherwise recall when needed falls into this category.

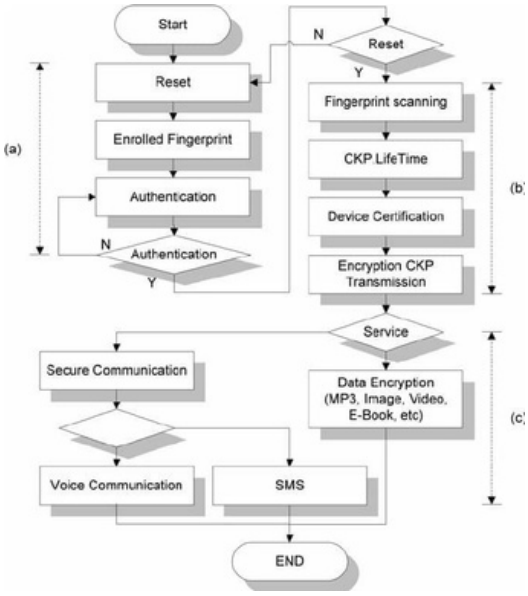
Type2-Something You Have-includes all items are physical objects,such as keys,smartphones,smart carts,USB drives and token devices(A token device produces a time-based PIN or can computed a response from a challenge number issued by the sever).

Type3-Something You Are-includes any part of the human body that can be offerd for verification,such as fingerprints,palm scanning ,facial recognition,retina scans,iris scans,and voice verification

9.4. MFA Code:

AWS multi- factor authentication (MFA) is the practice or requiring two or more forms of authentication to protect AWS Resources. It is an added security features available through Identity and Access Management (IAM) that strengthens user name and passwords credentials.

10. FLOW CHART



11.1. Authentication:

 There are numerous advantages of authentication systems which are used to identify the user of a home,ATM or a security clearance computer system

 The main purpose of these systems is to validatethe users rightto access the system and information,and protect against identity theft and fraud.

11.2. Authorization:

 Authorization lists simplify managing authorities

 One operation can be used to give a user authority to all the objects on the list

 Authorization lists reduce the number of private authorities on the system.

12. CONCLUSION

In this paper, we presented a review of authentication and authorization methods. Computer industries has created a array of identification and authentication technologies like User ID, Password, OTP, LWDAD, Secure Socket Layer, SMAL and Security Requirements. Cyper Criminals think in the world they try to look for weakness in authentication system to illegaly access other users accounts and enjoy previleges and services others paid for it. Thus, strong and effective authentication approches are imperative for successful digital transaction because it is very simple, practica scalable and easy to implement the username and password method is still the most widely used. This paper is estab in required to modelling authentication and authorization mechanisms.