A Comprehensive Study on Different Authentication Factors

B. Madhuravani[1]
MLR Institute of Technology
Dundigal, Hyderabad, India

Dr. P. Bhaskara Reddy[2]
MLR Institute of Technology
Dundigal, Hyderabad, India

P. LalithSamanth Reddy[3]
Institute of Aeronautical Engineering
Dundigal, Hyderabad, India

***Abstract*—Security is the practice of defending information from unauthorized access. This paper gives the study of different authentication factors to authenticate a legitimate person to use online services securely. The usage of passwords for authentication is no longer sufficient so the stronger authentication schemes are necessary. We start with reviewing different authentication factors. Two Factor Authentication (2FA) using devices such as tokens and ATM cards avoids number of short comings that are associated with traditional passwords, but they include the cost of purchasing, issuing, and managing the Tokens or cards. Multifactor authentication makes use of different authentication mechanisms to provide strong authentication. In this paper we do a survey on different authentication factors.**

***Keywords*— Authentication, SFA(Single Factor Authentication), 2FA(Two Factor Authentication), MFA(Multifactor Authentication), OTP(One time Password), 2WAY(Mutual Authentication), KBA(Knowledge Based Authentication)**

INTRODUCTION

Authentication plays a vital role especially in online services. There are several ways through which we can authenticate users. These range from the simple systems such as a combination of the username and password to complex systems such as biometric and / or one time usage based variable tokens. As technology is changing day to day, organizations need to adapt their security systems to effectively fight against imposters, hackers, thieves, and the like. Selecting the right technologies for each organization cannot be generalized.

Authentication is the assurance that the communicating entity claims to be genuine.

According to Fermi Lab [1], authentication is a form of computer security in which the identities of networked users, clients and servers are verified without transmitting passwords over the network. Access controls exist to prevent unauthorized access. Companies should ensure that unauthorized access is not allowed and also authorized users cannot make unnecessary modifications.

There are mainly two types of password

- Static password
- Dynamic Password

Static passwords are highly susceptible to cracking, because passwords used will get cached on the hard drives. Dynamic password is a password which changes every time the user logs in. An OTP is a set of characters that can act as a form identity for one time only. Once the password is used, it is no longer used for any further authentication. Even if the attacker gets the password, it is most likely that it was already used once, as it was being transmitted, thus useless to the attacker.

I.AUTHENTICATION

Authentication is the process of identifying an individual, usually based on a username and password. In security systems, authentication is distinct from authorization ,which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access.

Authentication procedure is based on three universally recognized authentication factors.

- Something you know, e.g. Passwords.
- Something you have, e.g. One-time password tokens and Digital certificates.
- Something you are, e.g. Biometrics.

The following Table1 indicates various options used under each of the three factors.

You Know	You Have	You Are
UserName	Smartcard	FingerPrint
Password	USB thumbdrive	FaceRecognition
PIN	ATM	Hand Geometry
CVV no.	MobilePhone	IRIS

Table 1

Most of two-factor authentication solutions combine "something you know" and "something you have". They require the usage of an additional device, which demands administration from the service provider and extra care from the user. Multi-channel communication is another way to further improve the security of an authentication scheme.

II. TYPES OF AUTEHNTICATION FACTORS

a. Single Factor Authentication

Single-factor authentication (SFA) is the traditional security procedure that requires a user name and password to authenticate the user. The most recognized type of SFA method is "passwords". Although this type of authentication is used widely, they have problems such as being hard to remember, vulnerable to guessing, dictionary attack, key-logger, shoulder-surfing and social engineering [2].

b. Two Factor Authentication

Two Factor Authentication, also known as, 2FA provides an extra layer of security that requires not only a password and username but also something the user have as second factor.

c. Multi Factor Authentication

Multi Factor Authentication, also known as, MFA is an approach to authentication which requires the presentation of two or more of the three authentication factors.

III. MUTUAL AUTEHNTICATION

Mutual Authentication or Two way authentication (sometimes written as 2WAY authentication) refers to two parties authenticating each other suitably. In technology terms, it refers to a client or user authenticating themselves to a server and that server authenticating itself to the user in such a way that both parties are assured of the others' identity. When describing online authentication processes, mutual authentication is often referred to as website-to-user authentication, or site-to-user authentication.

With mutual authentication, a connection can occur only when the client trusts the server's digital certificate and the server trusts the client's certificate. The exchange of certificates is carried out by means of the Transport Layer Security (TLS) protocol. If the client's key store contains more than one certificate, the certificate with the latest timestamp is used to authenticate the client to the server. This process reduces the risk that an unsuspecting network user will inadvertently reveal security information to a malicious or insecure Web site.

To illustrate, suppose an unsuspecting online bank customer or retail consumer is directed to a Web site created for the purpose of phishing. In that situation, mechanisms will prevent the input of critical data such as PINs (personal identification numbers), passwords or Social Security numbers unless a trusted connection has been established to the satisfaction of both the user's computer and the network server. A well-designed mutual authentication solution also protects against other forms of online fraud such as man in the middle attacks, shoulder surfing, Trojan horses, and key loggers. Mutual authentication should not be confused with two-factor authentication, a security process in which the client provides two means of identification to the server, such as a physical token and a password. For optimum security, mutual authentication can be used in conjunction with this and other countermeasures such as firewalls, antivirus software and anti-spyware programs.

Challenge –Response mechanism can be implemented for the high value transactions which exceed some threshold.

IV. MULTI FACTOR AUTHENTICATION

Multifactor authentication (MFA) is a security system in which more than one form of authentication is implemented to verify the legitimacy of a transaction. In contrast, single factor authentication (SFA) involves only a user ID and password. In two-factor authentication, the user provides dual means of identification, one of which is typically a physical token, such as a card, and the other of which is typically something memorized, such as a security code. Additional authentication methods that can be used in MFA include verification such as finger scanning, iris recognition, facial recognition and voice ID. It is based on “something you are [3]”. The major problem of biometric as an authentication scheme is the high cost of additional devices needed for identification process [4]. In addition to these methods, smart cards and other electronic devices can be used along with the traditional user ID and password.

V. KNOWLEDGE BASED AUTHENTICATION

Knowledge based techniques are the most extensively used authentication techniques and include both text based and picture based passwords [5]. Knowledge-based authentication (KBA) is based on “Something You Know” to identify you For Example a Personal Identification Number (PIN), password or pass phrase. It is an authentication scheme in which the user is asked to answer at least one "secret" question . KBA is often used as a component in multifactor authentication (MFA) and for self-service password retrieval. Knowledge based authentication (KBA) offers several advantages to traditional (conventional) forms of e-authentication like passwords, PKI and biometrics .

The picture-based techniques can be further sub divided into four main categories: First is Recognition based Systems which are also known as Cognometric Systems or Searchmetric Systems. Recognition based techniques involve identifying whether one has seen an image before. The user must only be able to recognize previously seen images, not generate them unaided from memory. Second is Pure Recall based systems which are also known as Drwanmetric Systems. In pure recall-based methods the user has to reproduce something that he or she created or selected earlier during the registration stage. Third is Cued Recall based systems which are also called Iconmetric Systems. In cued recall-based methods, a user is provided with a hint so that he or she can recall his his/her password. Fourth is Hybrid systems which are typically the combination of two or more schemes. Like recognition and recall based or textual with graphical password schemes.

VI. STORAGE OF IDENTIFIABLE PICTURES

Identifiable pictures (images) are one of the authentication factors that can be used to provide website authentication. These identifiable pictures act as an extra layer of authentication to prevent unauthorized access to the accounts and assure that the customer is at the valid online banking site. Identifiable pictures used for web authentication can be stored in three different ways[6].

They are

1. Images stored at server side (web server),
2. Images stored at client side, and
3. Images can be divided into two shares, storing one share at server side and the other share at client side and merging the two shares using visual cryptography.

Images stored at server side: System displays set of identifiable pictures from which the user selects their desired images. While logging in if the system displays the picture which was selected by the user then, the user can be assured that he is not using the fake web site.

Images stored at client side: Identifiable pictures can also be stored at client side computer for assuring the user that he is on the real site and not on a phishing site. In this, the user himself provides some images and the server randomly takes some parts of the images and displays the image and then the user enters the password.

Authentication using Visual cryptography: Naor and Shamir [7] introduced the visual cryptography scheme (VCS) as a simple and secure way to allow the secret sharing of images without any cryptographic computations. Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes a mechanical operation that does not require a computer [8]. The picture is divided into two shares and one share can be stored at server and the other share can be stored at client side. The customer is already provided with one share image and when he/she logs in, the server provides the other secret shared image and by using visual cryptographic technique, the two transparencies are overlaid and display the decrypted image. It is not possible to retrieve the secret information from one of the shares

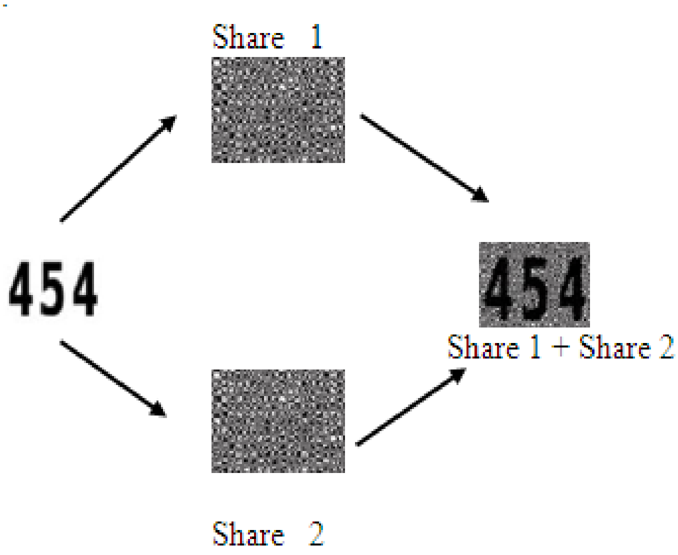

Fig: Decryption using visual cryptography

The Table2 indicates advantages and disadvantages of different picture based authentication methods

Authentication	Advantage	Disadvantage
Image Stored at Server side	Reduces phishing attack.	Does not attack Man In The Middle attack
Image Stored at Client side	Reduces brute force attack.	Does not solve phishing problem when log in from other system.
Visual Cryptography	Reduces phishing attack to some extent.	Does not solve phishing problem when log in from other system.

Table 2

VIII. CONCLUSION

Currently many authentication methods and techniques are available but each with its own advantages and limitations. Today, Single factor authentication is no longer considered secure in the internet and banking world. Passwords are known to be one of the easiest targets of hackers. While tokens provide a much safer environment for users, but it can be very costly for organizations. Biometrics is known to be very secure, but they are not used much in online transactions given the expensive hardware that is needed to identify the subject and the maintenance costs, etc. This paper describes various authentication factors in online communication. There is a growing interest in using pictures as passwords rather than text passwords. In this paper we explained the three ways of storing these pictures and analyzed their advantages and disadvantages.

ACKNOWLEDGEMENT
We thank Department of Science & Technology DST, New Delhi in funding the project under WOS-A scheme and this publication is under DST funding.

REFERENCES

[1] Fermi National Accelerator Laboratory, Office of science / U.S Department of Energy. Strong authentication at Fermilab, Sep 2006.

[2] Sabzevar, A.P. & Stavros, A., 2008," Universal Multi-Factor Authentication Using Graphical Passwords", IEEE International Conference on Signal Image Technology and Internet Based Systems (SITIS).

[3] HAFIZ, M. D., ABDULLAH, A. H., ITHNIN, N. & MAMMI, H. K., 2008, „Towards Identifying Usability and Security Features of Graphical Password in Knowledge Based Authentication Technique‟, Second Asia International Conference on Modeling & Simulation (AICMS).

[4] Haichang, G., L. Xiyang, et al. (2009). "Design and Analysis of a Graphical Password Scheme", Innovative Computing, Information and Control (ICICIC), 2009 Fourth International Conference on Graphical Passwords.

[5] I. Jermyn, A. Mayer, F. Monrose, M.K. Reiter, and A. Rubin. The Design and Analysis of Graphical Passwords. In Proc. of the 8th USENIX Security Symposium, August 23-26 1999.

[6] M V N K Prasad and S Ganesh Kumar, Authentication factors for Internet banking, IDRBT.

[7] M. Naor and A. Shamir, "Visual cryptography," in Proc EUROCRYPT,1994, pp. 1–12.

[8] Visual cryptography. Wikipedia http://en.wikipedia.org/wiki/visual_cryptography6.

B. Madhuravani, Department of CSE, MLR Institute of Technology, Dundigal, Hyderabad. She is doing Ph. D in Computer Science & Engineering, JNTUH. Her research interests include Information Security, Computer Networks, Distributed Systems and Data Structures.

Dr. P. Bhaskara Reddy, B.E.(ECE), M.Tech., Ph.D., F.I.S.E.E., MCSI, MISTE, the Director MLR Institute of Technology is a young and dynamic professor of ECE, has 25 years of Teaching, Research and Administrative experience in Reputed Engineering Colleges and Industry. Recipient of Bharath Jyothi award in 2003 and Rastraprathiba award in 2004, has acquired various positions from Asst.Professor to Principal and published 9 Laboratory Manuals, 52 Research papers at National and International Level on Education, Electronics Communication, I.T., Computer Networks, E-Commerce etc. Guided 5 Research Scholars for their Doctorates, about 40 M.Tech and B.Tech projects and Conducted 10 National Level Technical Symposiums on various topics in Electronics & Communications, Computers etc.

P.LalithSamanthReddy, currently pursuing his B.Tech final year in Computer Science & Engineering, Institute of Aeronautical Engineering, Dundigal, Hyderabad. His current research interests include Network Security and Information Security, Computer Networks.