RESEARCH ARTICLE OPEN ACCESS

An Overview on Authentication Approaches and Their Usability in Conjunction with Internet and Mobile Applications

Sangare Mamoudou, Wajdi Al-Khateeb
Department of Electrical & Computer Engineering International Islamic University Malaysia
Department of Electrical & Computer Engineering International Islamic University Malaysia

ABSTRACT
The usage of sensitive online services and applications such as online banking, e-commerce etc is increasing day by day. These technologies have tremendously improved making our daily life easier. However, these developments have been accompanied by E-piracy where attackers try to get access to services illegally. As sensitive information flow through Internet, they need support for security properties such as authentication, authorization, data confidentiality. Perhaps static password (User ID & password) is the most common and widely accepted authentication method. Online applications need strong password such as a combination of alphanumeric with special characters. In general, having one password for a single service may be easy to remember, but controlling many passwords for different services poses a tedious task on users online applications . Usually users try to use same password for different services or make slight changes in the password which can be easy for attacker to guess adding increased security threat. In order to overcome this, stronger authentication solutions need to be suggested and adapted for services based network.

Keywords: Authentication, Authorization, Access control, Single and Multiple factor authentication, Authentication usability, One Time Password

I. INTRODUCTION

With the rapid growth of wireless technologies in the sectors like finance, military, aviation etc, which use online communication rather than traditional forms, there is a need to determine the authenticity of genuine users. The process during which the identity of an entity is established is known as authentication. For online transactions, currently most of the network services like financial institutions, health care insurance and mobile applications rely on user ID and password in order to authenticate their customers. However, adequate security is not provided by just usernames and passwords authentication system. This is because users have tendency to use same password for difference sensitive services or by using another version of their old password. In addition to that, users tend to create password easy to remember and therefore easy to be guessed. They also write down their password on stick note which can be easily lost or stolen. In this case , there is lack of security. Based on that, some financial institutions or in general business based networks are moving to implement authentication combining multifactor for their web and mobile applications.

This paper aims to provide an overview of different types of authentication with their usability where we discuss our contribution and evaluate on those types of authentication method of Internet and mobile applications in order to allow online based organizations to choose suitable authentication technique for their institutions. Our discuss will be focused on multi-factor authentication (MFA) with applications and mobile phone, where more than factor is considered.

II. AUTHENTICATION

Authentication is the process of establishing a level of confidence in the correctness of a claim. In a specific way, there are basically two variety of authentication based on their nature : Identity authentication and data origin authentication. The process of validating the claimed identity of an entity is called identity authentication. Whereas data origin authentication provides assurance that the source of a message is as claimed [1]. Generally speaking, the types of authentication can be classified into :

- something that the user knows
- something that the user has
- something identifying who the user is
- something where the user is located

2.1 Authentication based on what user knows :

Is a method that refers to the use of static password or PIN (Personal Identification Number). It has a the problem that there is no guarantee of password transferred, due to different types of crack tools [2]. Even though this authentication mechanism does not provide high level of security for stationary computers and mobile devices, it is easy for implementation, and user is usually free to choose password that is simple for him/her to remember.

Usability: Authentication using passwords is very popular and most widely accepted even though it provides by low level of security. This is because of the high usability and easy implementation. Also for user side , it is easy to remember passwords without complicated demands for authentication process and privacy issues.

2.2Authentication based on what user has :

This a method based on what the user has such as smart card and token, compared to password authentication based on what the user knows , it provides stronger authentication. However it has some problems of loss and theft [3-4].

Usability: There are two kind of devices used (Taken that stands alone and mobile phone used as token). Authentication process is simple and easy for the user if the process uses mobile phone. This is because he/she does not have to carry an additional device. In addition, sometime with the stand alone token, user may forget to carry it with him frequently where in this case he/she may be unable to use the service at the moment of authentication.

2.3 Authentication based on who the user is :

This method of authentication is based on the user's physical information such as fingerprint, face recognition, etc which is known as biometric. This method is stronger than the two previous ones. However, it requires high cost equipment necessity for it with the use for applications and also since the user physical information is used , it can cause the user to feel offended along with [2] .

Usability: Since it is based on physical properties , the use of biometrics can be quick and effective because it is almost impossible to loose or forget it. However, the use of biometric may not be possible by disabled people. For example the solution based on walk patterns may not be used by a user in a wheelchair or a person with a broken arm will have trouble with maintaining the typing pattern he or she would have with both hands available.

A convenient authentication method might not be valued by some people as their privacy is more concerned. Another concern is if their information is somehow compromised, the users will not be able to change it, thing that they could do with their password [6].

2.4 Location based authentication:

The process of identifying someone by detecting simply their presence at certain location and authenticity, is location based authentication. A special combination of objects is required in order to enable location based authentication:

- A sign of identity has to be present from an individual that applies for being identified and authenticated
- At least one human authentication factor has to be carried by the individual that may be recognized on the distinct location.
- The distinct location must be equipped with a resident means that is capable to determine the coincidence of individual at this distinct location [5-12].

Usability: When it comes to the usability, location based authentication is not an obstacle, this is because it can be transparent for the user. However, considering the low degree of usage and today's support, one can think that location based authentication processes would be dependent on third party applications. These applications may not integrate well with the devices, and then exclude certain group of users. So in this case, there may some challenges when it comes to use some knowledge that only exists at the location.

It is important to point out that password method is the most widely used among authentication protocols mentioned above, for the reason that it is easy to remember password and it is also simple and inexpensive. However, since users tend to use information related to themselves like birthday and pet names, etc as password, this method can be easily guessed and cracked by software like PWDUMP & John the Ripper [13-14]. Additionally, password can be vulnerable to wire tapping in case it is transferred in plain text [2].

III. SINGLE AND MULTI- FACTOR AUTHENTICATION

Different types of authentication depend on their factors. If there is more than one factor then it will be more difficult to compromise than single-factor techniques.

In the point of view of different enterprises, authentication techniques may vary. That variety can be based on the ease of use, cost and robustness against attacks. Perhaps password solution for authentication is most widely used and accepted. For certain web sites or mobiles applications, it might be cost effective and appropriate solution for authenticating but it does stand alone for accessing [7] . For the web-based E-mail account, biometric solution might be too expensive since it provides basic security for authentication. When applications deal with sensitive information of users, appropriate authentication is required. So when we discuss about authentication in this paper we recommends to enterprises to choose better level of authentication to secure their web and mobile applications.

For determining the authenticity of a person or device or system, there are many factors. In general, the more factors that are used in the authentication process, the more robust the security process will be. We refer to multi-factor authentication when two or more factors are used in the process. In this section we will describe different types of authentication based on the different factors which will include their pros and cons of the authentication techniques.

3.1. Single-Factor Authentication (SFA) or Traditional Authentication.

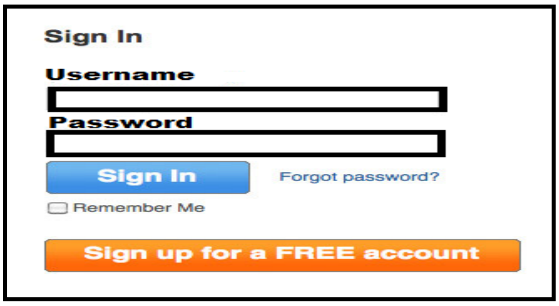


Figure 1. Web mail page with single-factor authentication [17].

As from the Figure 1 above, SFA is a traditional security requirement that requires a user ID and password to get access into the web or mobile application or system. Here, the security hinges with the diligence of the end user . This means that an additional precaution should be taken by a user [7] for instance, a strong password should be created by a user which should contains alphanumeric and special characters, in order to ensure that it could be difficult to get access by guessing it. In this case, it may be advisable for networks based businesses to implement more complex system, such as multiple factor authentication if their services include sensitive data.

Based on the figure 2 below, SFA works as follows. It is required from a user to enter his ID or username and Password which will be checked in the database. If the ID and password displayed match with the ones existing in the database of the server, authentication process will succeed. If not , user will be asked to provide correct ID or Password.

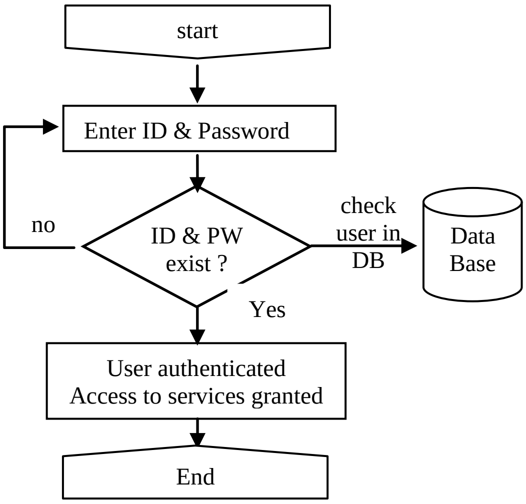


Figure 2. Flow chart of single factor authentication

3.2 Two Factor Authentication (2FA)

Is a mechanism which implements two forms of authentication and it is therefore considered to be stronger and more secure than the traditionally implemented one [9]. In 2FA, the end user is required to provide something in his possession such as smart card or unique key generator and something memorized such as password or PIN or security code. Withdrawing money from an ATM machine utilizes two factor authentication; the user must possess the ATM card, i.e. what you have, and must know a unique personal identification number (PIN), i.e. what you know.

According to the recent studies, getting only password would no longer be enough to give access to an attacker since he/she needs additional item to get access to the victim's account. Therefore 2FA can reduce the risk of many online fraud or attacks. However by using 2FA , there is no guarantee of preventing online fraud.

The cost of purchasing, issuing, and managing the tokens or cards are some of the main issues of 2FA. Using more than one factor requires carrying multiple tokens/cards which are likely to get lost or stolen, from the customer’s point of view [11].

Another issue with 2FA is standardization process to implement authentication. Because interoperability is an issue. Since there are various implementation of it, it is recommended to take into consideration in picking, emerging, testing, implementing and maintaining when it comes to an end-to-end secure authentication system.

3.3 Multi-Factor Authentication (MFA)

Multi-Factor Authentication (MFA) or strong authentication is a mechanism that contains multi-level implementation for application security to identify and verify the oneness of the claim. More specifically MFA is an approach to authentication which requires the presentation of two or more authentication factors such as combining a *knowledge* factor ("something only the user *knows*"), a *possession* factor ("something only the user *has*"), and an *inherence* factor ("something only the user is"). In addition, specifically in financial institutions, MFA is characterized by the use of different controls at different points in a transaction process. So that a weakness in one control can be generally compensated by the strength of another one [10]. Therefore, MFA can substantially strengthen the overall security of Internet-based services. In addition to that it can be effective in protecting sensitive customer information by preventing identity theft, and reducing account takeovers and the resulting financial losses.

Unlike SFA that involves only a user ID and Password, 2FA that requires an additional item such as typical token; MFA includes biometric such as finger print, facial and iris recognition which make authentication process stronger and difficult to be hacked. However, generally speaking, although some high-security applications may require the combination of the three most used factors in authentication (knowledge base, possession factor and inherence factor), it has not been widely applied [16] .

In the simplest form, nowadays most financial institutions use MFA by combining graphical image where the process is illustrated in Figure 3 below. As it can been seen that in Figure 3 MFA involves 3 steps of authentication which are grouped into two steps. The first step requires user to enter his ID. This is followed by asking the user to confirm his secure access image which has been chosen by him during enrolment and message to login. And finally he/she is required to provide the password.

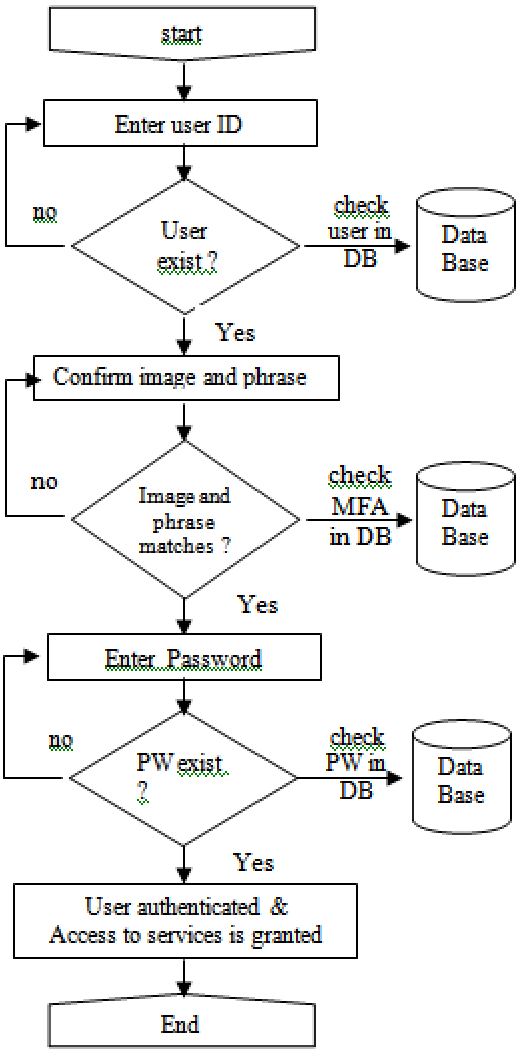
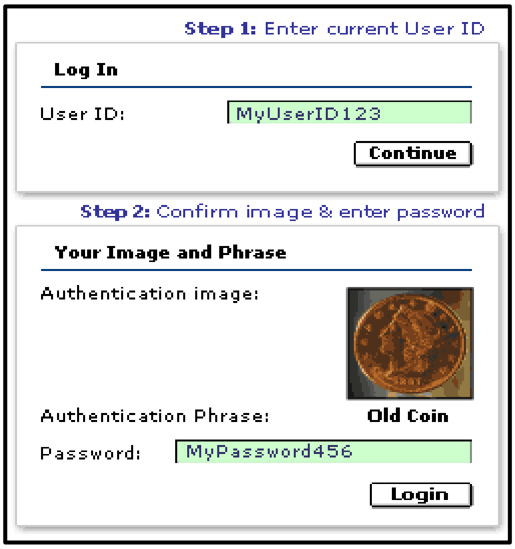


Figure 3. Flowchart of multi-factor authentication procedure



Step 1: Enter current User ID

Log In

User ID: MyUserID123

Step 2: Confirm image & enter password

Your Image and Phrase

Authentication image:

Authentication Phrase: **Old Coin**

Password: MyPassword456

Fig. 4: Step 1 and Step 2 of online banking page with MFA questions

3.4 One Time Password (OTP)

One time password (OTP) is a password in which passwords are used only once. This means that each time a user will be authenticated with a new password key [8]. A number of shortcoming associated with static passwords are avoided by OTPs. It provides much more stronger security level because even if a key of a user is compromised, the hacker will gain access just for that specific session. If an OTP that has been already used to log into a service is recorded by a potential hacker , he/she will not be able to use it again , since it will be no longer valid. Therefore OTP can resists against replay attack because of the life short time. However, since OTP are difficult to be remembered by human being, they require additional framework or an electronic device in order to work properly.

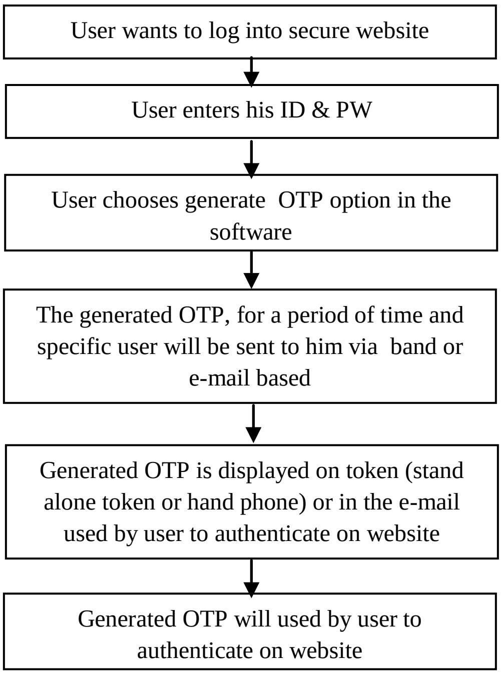

User wants to log into secure website
User enters his ID & PW
User chooses generate OTP option in the software
The generated OTP, for a period of time and specific user will be sent to him via band or e-mail based
Generated OTP is displayed on token (stand alone token or hand phone) or in the e-mail used by user to authenticate on website
Generated OTP will used by user to authenticate on website

Figure 5. Generation of OTP to secure login or secure transaction

As illustrated in Figure 5, OTP generation consists of the following steps. First, a user decides to login into secure website. After that user will be required to enter his ID and password. And then he/she will choose the generate password option in the software and that will be displayed in a given period of time, for instance in ten minute. And then the generated OTP is sent to user via out of band to his token or phone or via e-mail based. Finally the generated OTP will be used by user to authenticate on website.

In this paper, all the authentication procedure that have been described can be implemented, tested and integrated with mobile applications as well as iOS, Android, Blackberry and Windows based smart phone applications in order to prevent different kind of attacks by providing strong security schemes [15].

IV. CONCLUSION

In this paper different authentication systems have been investigated and discussed From that, it can be seen that, in performing user authentication, there are many approaches (both for mobile and stationary devices). It can said that there is no unique solution appropriate to every situation. So it can be pointed out that in order to select an authentication method, various factors need to be taken into consideration such as usability, security, specific functionality of the application/service, privacy, user requirements. Therefore, finding the right balance between these factors and selecting an authentication technique that is suitable for the specific service and accepted by users is the most challenging issue.

Today's traditional password based authentication is no longer considered secure in the Internet especially in network based services. Since they can be easily guessed. In order to meet organizations demand and provide stronger authentication, 2FA and MFA have been introduced . Nowadays, we got MFA and it is very difficult to break it. The above authentication techniques have been successfully implemented, tested, and widely accepted and have shown to be strong and secure. An online service will be difficult to be hacked if it has numerous factors of authentication **.**

REFERENCES

[1] M. Alzomai , " *Identity Management : Strengthening One Time Password Authentication Through Usability* ". *PhD thesis May 2011.*

[2] H.C. Kim, H.W. Lee, K.S.Lee , M.S. Jun, " *Design of One-Time Password Mechanism using Public Key Infrastructure* ".978-0-7695-3322-3/08 © 2008 IEEE DOI 10.1109/NCM.2008.77.

[3] ISO 7816-3 *Electronic signals and transmission protocols*.

[4] ISO 7816-1 Physical characteristics.

[5] http://en.wikipedia.org/wiki/Location-based_authentication.

[6] Z. Zareh Hosseini, E. Barkhordari " *Enhancement of security with the help of real time authentication and one time password in e-commerce transactions* ". *2013 5th Conference on Information and Knowledge Technology. 978-1-4673-6490-4/13/2013 IEEE.*

[7] A. S. Yeole VES, B. B. Meshram " *Improving Security of E- Commerce application by using Multifactor Authentication ". 2nd International Conference and workshop on Emerging Trends in Technology (ICWET) 2011. Proceedings published by International Journal of Computer Applications® (IJCA).*

[8] Y.S. Lee, H.T. Lirn, H.J. Lee, " *A Study on Efficient OTP Generation using Stream Cipher with Random Digit ". ISBN 978-89-5519-146-2 Feb. 7-10, 2010 ICACT2010.*

[9] F. Aloul, S. Zahidi, W. El-Hajj " *Two Factor Authentication Using Mobile Phones ". 978-1-4244-3806-8/09/© 2009 IEEE.*

[10] M.M. Mohammed, Dr. M. Elsadig, " *A Multi-layer of Multi Factors Authentication Model for Online Banking Services" . 2013International Conference on Computing and Electronic Engineering (ICCEEE) .978-1-4673-6232-0/13/2013 IEEE.*

[11] K.P. Thooyamani, R. Udayakumar and V.Khanaa. " *Extra Authentication in ATM Using Bluetooth ". World Applied Sciences Journal 29 (Computer Sciences, Engineering and Its Applications):* 155-159, 2014 ISSN 1818-4952 ©IDOSI Publications, 2014 DOI: 10.5829/idosi.wasj.2014.29.csea.2250.

[12] S. D. Ghogare, S. P. Jadhav, A. R. Chadha, Hima C. Patil "Location Based Authentication: " *A New Approach toward providing Security " InternationalJournal of Scientific and Research Publications, Volume 2, Issue 4, April 2012 1 ISSN 2250-3153*

[13] http://en.wikipedia.org/wiki/Pwdump

[14] B. Ewaida, *Pass-the-hash: Tools and Mitigation, SANS Institute InfoSec Reading Room*. *GIAC (GCIH) Gold Certification.* January 21st 2010

[15] S. Chaudhari, S.S. Tomar, Anil Rawat Design, *Implementation and Analysis of Multi Layer*, Multi Factor Authentication (MFA) Setup for webmail Access in Multi trust Networks, 978-1-4577-0240-2/11©2011 IEEE.

[16] LAWRENCE O'GORMAN, *FELLOW, IEEE. Comparing Passwords*, Tokens, and Biometrics for User Authentication, ROCEEDINGS OF THE IEEE, VOL. 91, NO. 12, DECEMBER 2003.

[17] http://www.hongkiat.com/blog/how-to-ruin-good-user-experience/