Volume 3, No. 11, November 2012
Journal of Global Research in Computer Science
ISSN-2229-371X
REVIEW ARTICLE
Available Online at www.jgrcs.info

AN APPROACH FOR USER AUTHENTICATION ONE TIME PASSWORD (NUMERIC AND GRAPHICAL) SCHEME

Brajesh Kumar Kushwaha
MTech(4th sem),CSE Department,
Mewar University, Chittorgarh (Rajasthan) India.
brajesh_kumar82@yahoo.com

Abstract **-** Day by day number of Internet users increasing. Now people are using different online services provided by Banks, College/Schools, Hospitals, online utility bill payment and online shopping sites. To access online services Text-based authentication system is in use. The text-based authentication scheme faces some drawbacks with usability and security issues that bring troubles to users. For example, if the user is not very intelligently constructed the password with extra security measures, it is very easy to hack for an expert hacker. On the contrary, if a password is hard to guess, then it is often hard to remember. A person has to memorize as many password as many different websites he/she is using. So he/she gets confused and/or forgets the correct userId/password combinations. We should have an alternative system to overcome these problems. To deal with these drawbacks, authentication scheme that use a combination of images as password is proposed. Graphical passwords consist of clicking or dragging activities on the pictures rather than typing textual characters, might be the option to overcome the problems that arises from the Text-based password system. In this paper, a comprehensive study of the existing graphical password schemes and shoulder surfing problem is performed. The best way in asynchronous mode user/password validation and One Time Password authentication is proposed for enhancement in security and privacy.

Keywords- Graphical Passwords, One Time Password (OTP), Recognition-Based Graphical User Authentication, Recall-Based Graphical User Authentication, Pure Recall-Based Authentication, Cued Recall-Based Authentication, Usability, Security. Shoulder Surfing.

INTRODUCTION

With the increased use of different online services available, the need to develop a secure system is very important. The system should be able to authenticate a correct user and provide the online transactions in terms of high security, privacy and reliability. Many user authentication schemes are available these days. But out of these entire how many are truly secure? To answer it lets go through the background of text-based and graphical passwords. The most common computer authentication method is for a user to submit a user name and a text password. The vulnerabilities of this method have been well known. One of the main problems is the difficulty of remembering passwords. Studies have shown that users tend to pick short passwords or passwords that are easy to remember [1]. Unfortunately, these passwords can also be easily guessed or broken. The graphical passwords schemes act as a possible alternative to text-based schemes, which are proposed mainly by the fact that humans can remember pictures better than text [2]. It is very easy to remember and recognize Images/Pictures based password than text-based password. Psychology studies have revealed that the human brain is better at recognizing and recalling images than text [3]. One more advantage is that Graphical passwords is harder to guess or broken by brute force.

In this paper One Time Password based login system is designed and explained to avoid shoulder surfing in combination of graphical/text password authentication scheme using asynchronous technique.

METHODS OF AUTHENTICATIONS

The following are main methods of authentications [14]

a. Token based authentication.
b. Biometrics based authentication.
c. Knowledge based authentication.

Token-based techniques, such as key cards, bank cards and smart cards are widely used. Many token-based authentication systems also use knowledge-based techniques to enhance security. For example, ATM cards are generally used together with a PIN number.

Biometric based authentication techniques, such as fingerprints, iris scans, or facial recognition has been developed due to uniqueness properties of biometrics. These systems are very secure. The major drawback of this approach is that such systems can be expensive, and the identification process can be slow and often unreliable.

Knowledge based techniques are the most widely used authentication techniques and include both text-based and picture-based passwords. The picture-based techniques can be further divided into two categories: recognition -based and recall-based graphical techniques. Using recognition-based techniques, a user is presented with a set of images and the user passes the authentication by recognizing and identifying the images he or she selected during the registration stage. Using recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage.

GRAPHICAL PASSWORD: AN ALTERNATE TO TEXT-BASED PASSWORD

Graphical passwords were originally described by Blonder [4]. In his description, an image would appear on the screen, and the user would click on a few chosen regions of it. If the correct regions were clicked in, the user would be authenticated.

Jensen et al. [5] proposed a graphical password scheme based on "picture -password " designed especially for mobile devices such as PDAs. Throughout the password creation, the user has to select the theme first (e.g. sea and shore, cat and dog and etc) which consists of thumbnail photos. The user then selects and registers a sequence of the selected thumbnail photo to form a password (Fig.1). The user needs to recognize and identify the previously seen photos and touch it in the correct sequence using a stylus in order to be authenticated. However, as the numbers of thumbnail photos are limited only to 30, the size of the password space is considered small. A numerical value is assigned for each thumbnail photo and the sequence of selection will produce a numerical password. This numerical password is shorter than the length of textual password. To over-come this problem a user can select one or two thumbnail photos as one single action in order to create and enlarge the size of the password space. However, this will make the memorability of the created password become more complex and difficult.

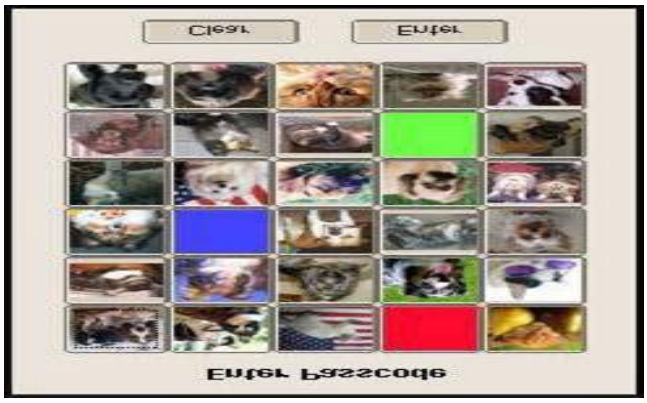

Figure. 1- Cats and dogs photos [5][13]

Based on humane recalling ability Real User Corporation has developed their own commercial product named Passfaces TM [6][13][14]. Basically, Passfaces works as follows, users are required to select the previously seen human face from a grid of nine faces one of which is known while the rest are decoys (Fig. 2). This step is continuously repeated until all the four faces are identified.

Figure. 2- Passfaces TM

The Passfaces password is easier to remember compared to textual passwords (study conducted by Brostoff and Sasse [7]). It is observed that Passfaces took a much longer login time than textual passwords. Empirical and comparative studies by Davis et al. [8] showed that, in Passfaces the user's choice is highly affected by race, the gender of the user and the attractiveness of the faces. This will make the Passfaces password somewhat predictable.

Dhamija and Perrig [9][13][14] proposed a scheme using a hash visualization technique on the abstract images. The scheme is called "Déjà vu" (Fig.6). According to their studies, the result showed that it took more time to create a graphical password compared to traditional approach. Besides that, 90% of the authentication using Déjà vu succeeded compared to 70% using the traditional approach. However, due to the larger amount of pictures stored on the server side, the authentication process can be slow due to network traffic delay. Even though the size of the password space of Déjà vu is much smaller compared to text-based password, it cannot be concluded that Déjà vu scheme is easy to remember.

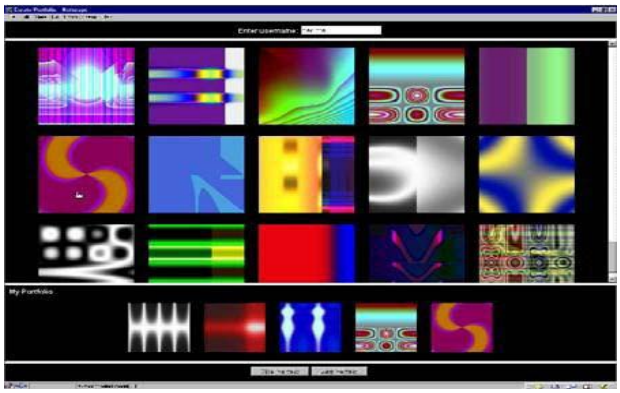

Figure. 6- Déjà vu scheme [9][13][14]

Draw-A-Secret technique [10], Grid selection [4], and Passdoodle [6] are some examples of pure recall -based techniques.
Jermyn et al [11] proposed a scheme, known as "Draw -A-Secret (DAS)".

POSSIBLE ATTACK ON TEXT-BASED PASSWORD AND GRAPHICAL PASSWORD TECHNIQUES [13]

Brute Force Attack-The main defense against brute force attack is to have a sufficiently large password space. Text-based passwords have a password space of 94 N where N is the length of the password, 94 is the number of printable characters excluding SPACE. In some graphical password techniques password space is similar to or larger than that of text-based passwords. Recognition based graphical passwords tend to have smaller password spaces than the recall based methods. A brute force attack is difficult to carry against graphical passwords than text-based passwords. Automatically generated accurate mouse movement is required in brute force attack to reproduce human input, which is mostly difficult in case of recall based graphical passwords.

Dictionary Attacks- Since recognition based graphical passwords involve mouse input instead of keyboard input, it will be impractical to carry out dictionary attacks against this type of graphical passwords. For some recall -based graphical passwords, it is possible to use a dictionary attack but an automated dictionary attack will be much more difficult than a text based dictionary attack. Overall, graphical passwords are less vulnerable to dictionary attacks than text-based passwords.

Guessing- Like a serious problem usually associated with text-based passwords, graphical passwords are also tending to predict. For example, studies on the Passface technique have shown that people often choose weak and predictable graphical passwords. Similar predictability is found among the graphical passwords created with the DAS technique.

Spyware Attack- Excluding a few exceptions, key logging or key listening spyware cannot be used to break graphical passwords. It is not clear whether "mouse tracking " spyware will be an effective tool against graphical passwords or not. However, mouse motion alone is not enough to break graphical passwords. Such information has to be associated with application information, such as position and size of window, as well as time information. Shoulder surfing: Most of the graphical passwords are vulnerable to shoulder surfing like text-based passwords. A few recognition-based techniques are designed to resist shoulder surfing. Not any of the recall-based based techniques are resistant to should-surfing attack.

Social Engineering- To give away graphical passwords to another person is difficult as compared to text-based password. For example, it is very difficult to give away graphical passwords over the phone. Setting up a phishing web site to obtain graphical passwords would be more time consuming.

Shoulder Surfing- A potential drawback of graphical password schemes is that they are more vulnerable to shoulder surfing than conventional alphanumeric text passwords. When users input their passwords in a public place, they may be at risk of attackers stealing their password. An attacker can capture a password by direct observation or by recording the individual's authentication session. This is referred to as shoulder surfing and is a known risk, of special concern when authenticating in public places.

OUR SCHEME

A study of existing graphical password techniques suggests that graphical password scheme is much better than the text-based password scheme. But we should take care of "shoulder surfing" in implementing graphical password authentication system. One Time Password scheme is implemented in the authentication system to avoid shoulder surfing.

How it works:

a. The first time a user registers with the website, application or service, they will go through a first time user registration process. The user will have to select a few **authentication categories** image they can easily remember – such as dogs, house, flowers and cars etc.
b. Any time authentication is required; the user will enter his/her User_ID/Login_ID (a unique identity to be allocated). Then he clicks a validate user button. For a valid user a Secure **One-Time Password (numeric)** will be sent to his/her registered Mobile/E-mail.
c. The user is also presented with a randomly generated grid of images. The pictures that appear are **different every time**, but the user will always look for their same categories. Each picture **is randomly paired with a different alphanumeric character**. In this way, system generates a unique, one-time password every time. Yet, the user only needs to remember their few categories.[12]
d. The user authenticates by identifying which images on the grid fit their secret authentication categories. They can simply click on the appropriate images, or type the alphanumeric characters that appear on the correct images to form a **one-time password (Graphical).**
e. Also the user will have to give the **One Time Password (numeric)** sent to his/her mobile/E-mail.

Secure Login:

Login ID: [ ] Validate

OTP(numeric): [ ]

OTP(Graphic):

(Source: http://www.confidenttechnologies.com/)

By creating one-time passwords, our proposed scheme of user authentication provides strong authentication that is secure against dictionary attacks, key loggers and the security breaches associated with weak passwords, stolen credentials and password re-use. This system can be used in banking, online shopping sites and other very secure sites.

ACKNOWLEDGEMENT

I express sincere gratitude to my guide for providing his valuable guidance and necessary facilities needed for the successful completion of this paper throughout. I thank my parents for their support and thank all my friends and well-wishers who were a constant source of inspiration.

REFERENCES

[1]. A. Adams and M. A. Sasse, "Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures," Communications of the ACM, vol. 42, pp. 41-46, 1999.

[2]. SFR IT-Engineering (2007) http://www.sfrsoftware.de/cms/EN/pocketpc/viskey/.

[3]. Nelson, D.L., U.S. Reed, and J.R. Walling. Picture Superiority Effect. Journal of Experimental Psychology: Human Learning and Memory 3, pp. 485-497, 1977.

[4]. Blonder G. (1996) In Lucent Technologies, Inc., Murray Hill, NJ, United States Patent 5559961.

[5]. Jansen W., Gavrila S., Korolev V., Ayers R. and Swanstrom R. (2003) NISTt NISTIR 7030.

[6]. Real User Cor por at i on (2007) Passf aces TM ,http//:www.realuser.com.

[7]. Brostoff S. and Sasse M.A. In People and Computers XIV –Usability or Else: Proceedings of HCI. Sunderland, U.K, 2000.

[8]. Davis D., Monrose F. and Reiter M.K. (2004) Proceedings ofthe 13th USENIX Security Symposium. California.

[9]. Dhamija R. and Perrig A. (2000) In Proceedings of the 9 thUSENIX Security Symposium.

[10]. Sobr ado L. and Bi r get J. (2007) ht t p: / /rutgersscholar.rutgers.edu/volume04/sobrbirg/sobrbi rg.htm.

[11]. Jermyn I., Mayer A. Monrose F., Reiter M.K. and Rubin A.D. (1999) In Proceedings of the 8th USENIX Security.

[12]. www.ConfidentTechnologies.com.

[13]. http://www.bioinfo.in/uploadfiles/13476885341_1_2_WRJ HCI.pdf

[14]. http://www.acsac.org/2005/papers/89.pdf

