Two Level Authentication Schema

Rupesh Tapkir[#1], Shubhangi Khalate[#2], Priyanka Sarade[#3], Shital Bukan[#4], Shwetal Patil[*5]
#Student, Department of Computer Engineering, University of Pune, MMIT, Lohgaon Pune, Maharashtra, India

[*]*Lecturer, Department of Computer Engineering, University Of Pune, MMIT, Lohgaon, Pune, Maharashtra, India*

Abstract:
Authentication is basic step of information security. Textual password and graphical passwords are the methods used for authentication. Textual passwords are prone to eves dropping, dictionary attacks, social engineering and shoulder surfing. Graphical passwords are believed to be more secure than textual passwords, but the authentications are usually complicated and time consuming for users. To solve this problem, text can be combined with images or colors to generate session passwords for authentication. Session passwords are unique that can be used only once and every time a new password is generated.

Keywords: **Authentication, OTP, session password**

1. INTRODUCTION

The nature of today's web threats over internet is changing day by day; current attacks are much more aggressive than they were in the past. This made web, network and application security extremely difficult and major issue. It is of top concern for personal as well as corporate to protect their confidential data.

An authentication factor is a piece of information and process used to certify or verify the identity of a person or other entity requesting access to various resources. User validation for most web sites and services today is undertaken using a password. Where a higher level of security is required (e.g. for access to on online banking service), a second factor is typically used in addition to the password therefore "two level authentication schema".

Existing authentication methods can be divided into three main categories:

- Token based authentication
- Biometric based authentication
- Knowledge based authentication

Token based techniques, such as key cards, bank cards and smart cards are widely used. Many token-based authentication systems also collaboratively use knowledge based techniques to improve security. For example, ATM cards are generally used in combination with a PIN number. Biometric based authentication techniques, such as fingerprints, iris scan, or facial recognition, are not yet widely adopted. The major drawback of this approach is that such systems can be expensive, and the identification process can be slow and often unreliable. However, this type of technique provides the highest level of security. Knowledge based techniques are the most widely used authentication techniques and include both text-based and picture-based passwords [1][6][9].

2. RELATED WORK

Dhamija and Perrig [3] proposed a graphical authentication scheme. In the system developed by them user has to select a certain number of images from the set of random pictures at a time of registration. The set of random pictures are generated by some program. Later, during login the user has to identify the images that pre-selected at a time of registration for authentication from a set of images. This system is vulnerable to shoulder surfing.

Figure 1: Random images used by Dhamija and Perrig

Jermyn [7] proposed a new authentication technique called "Draw_a_Secret" (DAS).In this technique user has to draw the picture on a 2D grid at a time of registration. During login phase use is required to re_draw the pre_defined picture on a 2D grid. For successful authentication drawing must be touches the same grids in the same sequence. If the drawing touches the same grid in the same sequence, then the user is authenticated .This system is vulnerable to shoulder surfing.

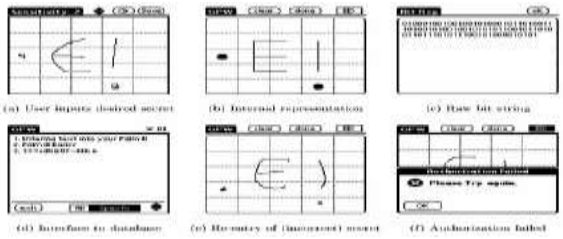

Figure 2: DAS technique by Jermyn

Syukri [4] developed a new authentication technique. In this authentication technique user drawing the signature using mouse. Basically this authentication technique included two stages, registration and verification. At the time of registration stage the user draw his signature with a mouse. After drawing signature system extracts the signature area. In second stage it takes the user signature as input and after that it then extracts the parameters of the signature which is draw at a time of registration stage.

Disadvantages of this authentication technique

1) Technique is the forgery of signatures.
2) Drawing with mouse is not familiar to many people.
3) It is difficult to draw the signature in the same perimeters at the time of registration.

Figure 3: Signature technique by Syukri

Haichang [5] proposed a new authentication technique. In this proposed scheme keeps most of the advantage of story and achieves stronger security. This technique is depends on users drawing a curve across their password images in order, Instead of direct input. In this authentication scheme user uses a set of images. This set of images gathered from http://images.google.com. To create a password, a user orderly chooses several images from the set as his/her pass_images. The user can remember the connection between the pass_images by mentally constructing a story. For conformation, the user should draw a curve to cross his/her pass_images in right ordered without lifting the stylus from the drawing surface. While drawing a curve across their password images orderly user does not clicking on the image directly. This graphical scheme combines DAS and Story schemes to provide authenticity to the user. During the authentication phase, user must recognize his/her pass_images and draw a curve to orderly cross them. The curve thus passes through both pass_images and other random images used to confuse the attacker.

Figure 4: Haichang's shoulder-surfing technique

3. PROPOSED SYSTEM

Authentication technique consists of 3 phases: registration phase, login phase and verification phase. During registration, user enters his password in first method or rates the colors in the second method. During login phase, the user has to enter the password based on the interface displayed on the screen. The system verifies the password entered by comparing with content of the password generated during registration.

3.1 Pair-based Authentication scheme

During registration user submits his password. Minimum length of the password is 8 and it can be called as secret pass [2][8]. The secret pass should contain even number of characters. Session passwords are generated based on this secret pass. During the login phase, when the user enters his username an interface consisting of a grid is displayed. The grid is of size 6 x 6 and it consists of alphabets and numbers. These are randomly placed on the grid and the interface changes every time.

Registration Module:

In this system we can use the 2 levels for password authentication. Firstly we use the textual password and then secondly we use the color password. We can also use the one time password (OTP). Now, In Registration phase users have to create the account. When user wants to create a new account, he must have to enter all the details. User also must have to give one password that is textual password. This password is the user's actual password. The password should contain only characters and numbers, no special character is allowed. This textual password can be called as

secret pass. The secret pass should contain even number of characters. Session passwords are generated based on this secret pass.

After entering the textual password, user have to enter the color password. In the color password registration,

One 1x8 grid is displayed. In this grid total 8 colors are placed in order of **BIGCROPS**. The colors in the grid are blue, indigo, green, cyan, red, orange, pink, silver. User has to rate the colors using numbers 1 to 8 as shown in figure 5. User has to remember this rating. User can assign same rating to different colors. Then user has to submit the form.

Figure 5: Color rating

Login Module:

During the login phase, when the user enters his username and interface consisting of a grid is displayed. The grid is of size 6 x 6 consisting of alphanumeric characters. These are randomly placed on the grid and the grid shuffles every time when you login or refresh.

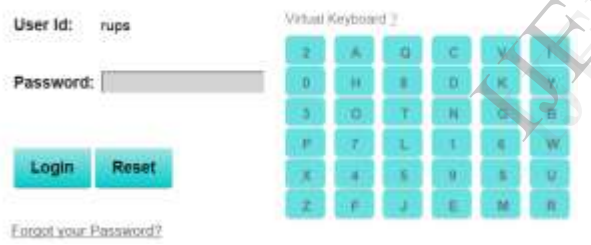

Figure 6: Login interface

Figure 6 shows the login interface. User has to enter the password depending upon the secret pass. User has to consider his secret pass in terms of pairs. The session password consists of alphabets and digits.

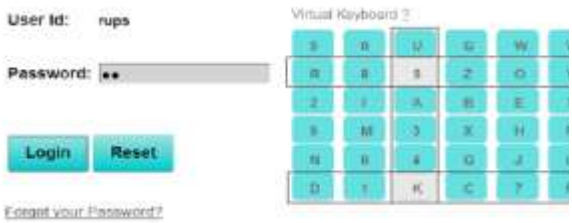

Figure 7: Textual login interface

In figure 7, consider that the password is 'rups'. There are two pairs 'ru' and 'ps'. For first pair 'ru', select the row of 'r' and column of 'u', the intersection letter is 's'. Therefore the first character of session password is 's'. For second pair 'ps', select the row of p and column of 's', the intersection letter is 'k'. Therefore the second character of session password is 'k'. Hence session password for current login becomes '**sk**' this password will be different for each login.

3.2 Hybrid Textual Authentication Scheme

During the login phase, when the user enters his username an interface is displayed based on the colors selected by the user. The login interface consists of grid of size 8×8. This grid contains digits 1-8 placed randomly in grid cells. The interface also contains strips of colors as shown in figure 8. The color grid consists of 4 pairs of colors. Each pair of color represents the row and the column of the grid [2].

Figure 8: Color login

Figure 8 shows the login interface having the color grid and number grid of 8 x 8 having numbers 1 to 8 randomly placed in the grid. Depending on the ratings given to colors, we get the session password. As discussed above, the first color of every pair in color grid represents row and second represents column of the number grid. The number in the intersection of the row and column of the grid is part of the session password. Consider the rating of BIGCROPS is **73244866** which is given at registration time. In figure 8 the first pair has indigo and green colors. The indigo color rating is 3 and green color rating is 2. So the first letter of session password is 3rd row and 2nd column intersecting element i.e. 3. The same method is followed for other pairs of colors. Hence the password is "**3526"**. Instead of digits, alphabets can be used. For every login, both the number grid and the color grid get randomizes so the session password changes for every session.

4. SECURITY ANALYSIS

As the interface changes every time, the session password changes [2]. This technique is resistant to shoulder surfing. Due to dynamic passwords, dictionary attack is not applicable. Even key logger or mouse pointer tracker won't work because of its dynamic nature.

***Dictionary Attack*:** These are attacks directed towards textual passwords. Here in this attack, hacker uses the set of dictionary words and authenticate by trying one word after one. The Dictionary attacks fails towards our authentication

systems because session passwords are used for every login.

***Shoulder Surfing*:** These techniques are Shoulder Surfing Resistant. In Pair based scheme, resistance is provided by the fact that secret pass created during registration phase remains hidden so the session password can't be enough to find secret pass in one session. In hybrid textual scheme, the randomized colors hide the password. In this scheme, the ratings decide the session password. But with session password you can't find the ratings of colors. Even by knowing session password, the complexity is 8^4. So these are resistant to shoulder surfing.

Brute force attack: These techniques are particularly resistant to brute force due to use of the session passwords. The use of these will take out the traditional brute force attack out of the possibility.

Complexity: The Complexity for Pair-Based Authentication Scheme is to be carried over the secret pass. For a secret pass of length 8, the complexity is 36^8. In the case of the Hybrid Textual Authentication Scheme the complexity depends on colors and ratings. The complexity is 8! if ratings are unique ,otherwise it is 8^8.

5. CONCLUSION

In this paper, new authentication techniques based on textual and colors are proposed which if used in combination can prove highly beneficial. Both of these techniques use grid for session passwords generation which is unique all the times whenever you enter it and are resistant to dictionary attack, brute force attack and shoulder-surfing. However these schemes are completely new to the users and the proposed authentication techniques should be verified extensively for usability and effectiveness.

6. FUTURE SCOPE

These techniques can be developed as any windows application or an external gateway authentication to connect the application to a database or an external embedded device. It can also be used as complementary for Operating System login.

References:

[1] Real User Corporation: Passfaces. www.passfaces.com.

[2] M Sreelatha, M Shashi, M Anirudh, MD Sultan Ahamer, V Manoj Kumar "*Authentication Schemes for Session Passwords using Color and Images*", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.3, May2011.

[3] R. Dhamija, and A. Perrig. "*Déjà Vu: A User Study Using Images for Authentication*". In 9th USENIX Security Symposium, 2000.

[4] A. F. Syukri, E. Okamoto, and M. Mambo, "*A User Identification System Using Signature Written with Mouse*," in *Third Australasian Conference on Information Security and Privacy (ACISP)*: Springer-Verlag Lecture Notes in Computer Science (1438), 1998, pp. 403-441.

[5] Haichang Gao, Zhongjie Ren, Xiuling Chang, Xiyang Liu Uwe Aickelin, "*A New Graphical Password Scheme Resistant to Shoulder-Surfing*".

[6] X. Suo, Y. Zhu and G. Owen, "*Graphical Passwords: A Survey*". In Proc. ACSAC'05.

[7] Jermyn, I., Mayer A., Monrose, F., Reiter, M., and Rubin., "*The design and analysis of graphical passwords*" in Proceedings of USENIX Security Symposium, August 1999.

[8] S.Balaji, Lakshmi.A, V.Revanth, M.Saragini, V.Venkateswara Reddy "*Authentication Techniques For Engendering Session Passwords With Colors And Text*" Advances in Information Technology and Management Vol. 1, No. 2, 2012.

[9] Gajbhiye S.K., Ulhe P. "*Authentication Schemes For Session Passwords Using Color And Gray-Scale Images*" Journal of Signal and Image Processing Volume 3, Issue 1, 2012, pp.-68-70.