Simple Authentication Technique for Session Management Using Odd and Even Pair of Random Text and Color Password in Cloud Computing

P.Kalimuthu and A.Justin Diraviam
Department of Computer Science and Engineering, Sardar Raja College of Engineering, Tamil Nadu, India
kalimuthucharless@gmail.com, jusma@rediffmail.com

***Abstract* - While some legal challenges in cyberspace have started to become clearer, the use of cloud computing and hosted applications adds a new dimension of legal risk. Compliance, privacy, and security problems are compounded by the use of remote, distributed services operated by third parties. Businesses employing these new technologies must look a new at their online risk, and learn how to assess and manage it. Authentication is the first line of defense against compromising confidentiality and integrity. Though traditional login/password based schemes are easy to implement, they have been subjected to several attacks. Textual-based password authentication scheme tends to be more vulnerable to attacks such as shoulder surfing and hidden camera. To overcome the vulnerabilities of traditional methods, visual or graphical password schemes have been developed as possible alternative solutions to text-based password schemes. Because simply adopting graphical password authentication also has some drawbacks, schemes using graphic and text have been developed. In this paper, we propose a hybrid password authentication scheme based on equal number of Random color and text. It uses color and text on the grid as the origin passwords and allows users to login with text passwords via traditional input devices. The method provides strong resistant to hidden-camera and shoulder-surfing. Moreover, the scheme has high scalability and flexibility to enhance the authentication process security. The analysis of the security level of this approach is also discussed.**

***Keywords* - Authentication, session passwords, shoulder surfing**

I. Introduction

Traditionally, alphanumeric passwords have been used for user authentication. While today other methods including biometrics and smart cards are possible alternatives, passwords are likely to remain dominant for some time because of concerns about reliability, privacy, security, and ease of use of other technologies [2]. However, in the use of passwords dilemmas often arise in the tradeoff between security and usability. The dilemma, as formulated by Birget in [21, p. 104], arises because passwords are expected to comply with two fundamentally conflicting Requirements:

(1) Passwords should be easy to remember, and the user authentication protocol should be executable quickly and easily by humans.

(2) Passwords should be secure, i.e., they should look random and should be hard to guess; they should be changed frequently, and should be different on different accounts of the same user; they should not be written down or stored in plain text. Because it is difficult for humans to remember random strings, users tend to ignore requirements for secure passwords. This leads to poor password practices, including short, simple passwords that are easy to break either by a dictionary attack or personal knowledge of the password owner, use of the same password over months or years, reuse of identical or nearly identical passwords on multiple systems, and propensity to write down passwords and store them insecurely, e.g., a text file containing the user's passwords stored on insecure computers or PDAs, Post-Its notes stuck on or near the computer monitor or inside a desk drawer [1,3, 10, 11].

In an effort to improve password security by making passwords easier to remember, researchers have developed graphical passwords. In a typical graphical password scheme a user chooses several images to be his or her password. When logging in, the user must click on the password images among a larger group of distracter images. If the user clicks on the correct images, he or she is authenticated. Users' memory for a graphical password may be better than for an alphanumeric password. Secure alphanumeric passwords (i.e., random strings) are based on pure recall from memory, a skill that is notoriously difficult for humans. By contrast, graphical passwords are based on recognition of previously known images, a skill at which humans are proficient. Indeed, image-based passwords have shown good memorability in user testing [2, 5, 6, 8, 9]. However, the problem of shoulder-surfing is a recognized drawback of graphical passwords. Shoulder-surfing refers to someone watching over the user's shoulder as the user enters a password, thereby capturing the password. While alphanumeric passwords systems are vulnerable to shoulder-surfing if the attacker can see the keyboard, graphical password systems may be more vulnerable in certain settings. For example, clicking on images on a large, vertical display screen may make users' actions easier to capture.

In this paper, two new authentication schemes are proposed for Cloud computing. These schemes authenticate the user by session passwords. Session passwords are passwords that are used only once. Once the session is terminated, the session password is no longer useful. For every login process, users input different passwords. The session passwords provide better security against dictionary and brute force

attacks as password changes for every session. The proposed authentication schemes use text and colors for generating session passwords.

This paper is organized as follows: in section 2 related works is discussed; in section 3 the new authentication schemes are introduced; security analysis is done in section 4; conclusion is proposed in section 5.

II. Related Work

Dhamija and Perrig[1] proposed a graphical authentication scheme where the user has to identify the pre-defined images to prove user's authenticity. In this system, the user selects a certain number of images from a set of random pictures during registration. Later, during login the user has to identify the pre selected images for authentication from a set of images as shown in figure 1. This system is vulnerable to shoulder-surfing.

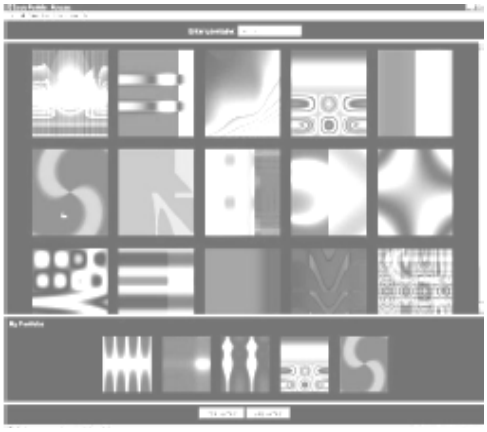
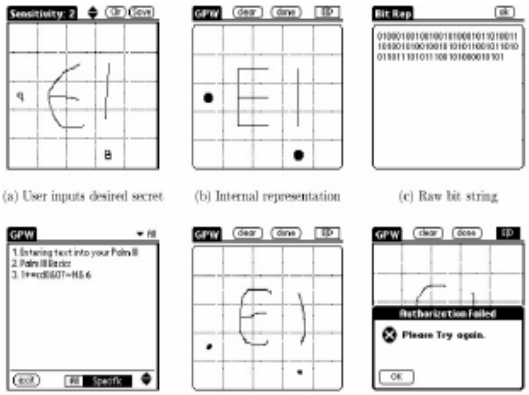


Fig. 1 Random images used by dhamija and perrig

Passface [2] is a technique where the user sees a grid of nine faces and selects one face previously chosen by the user as shown in figure 2. Here, the user chooses four images of human faces as their password and the users have to select their pass image from eight other decoy images. Since there are four user selected images it is done for four times.

Fig. 2 Example of passfaces

Jermyn, et al. [3] proposed a new technique called "Draw-a-Secret" (DAS) as shown in figure 3 where the user is required to re-draw the pre-defined picture on a 2D grid. If the drawing touches the same grids in the same sequence, then the user is authenticated. This authentication scheme is vulnerable to shoulder surfing.



(a) User inputs desired secret (b) Internal representation (c) Raw bit string

(d) Interface to database (e) Re-entry of (incorrect) secret (f) Authorization failed

Fig. 3 DAS technique by Jermyn

Syukri [4] developed a technique where authentication is done by drawing user signature using a mouse as shown in figure 4. This technique included two stages, registration and verification. At the time of registration stage the user draws his signature with a mouse, after that the system extracts the signature area. In the verification stage it takes the user signature as input and does the normalization and then extracts the parameters of the signature.

The disadvantage of this technique is the forgery of signatures. Drawing with mouse is not familiar to many people, it is difficult to draw the signature in the same perimeters at the time of registration.

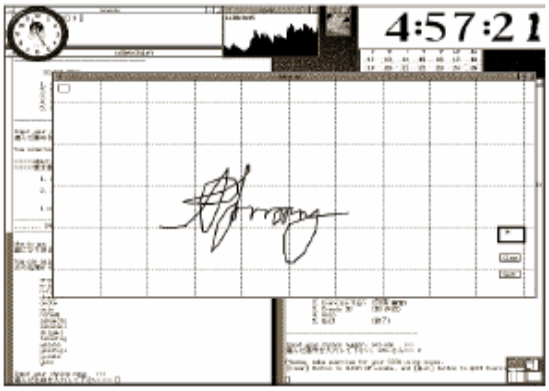


Fig. 4 Signature technique by Syukri

Blonder [5] designed a graphical password scheme where the user must click on the approximate areas of pre-defined locations. Passlogix [6] extended this scheme by allowing the user to click on various items in correct sequence to prove their authenticity.

Haichang et al [7] proposed a new shoulder-surfing resistant scheme as shown in figure 5 where the user is required to draw a curve across their password images orderly rather than

clicking on them directly. This graphical scheme combines DAS and Story schemes to provide authenticity to the user.

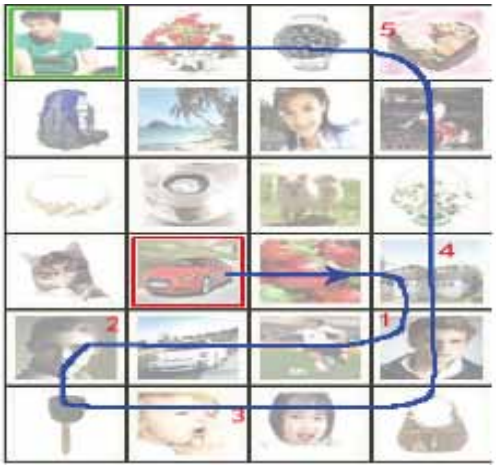


Fig. 5 Haichang's shoulder-surfing technique

Wiedenback et al [8] describes a graphical password entry scheme using convex hull method towards Shoulder Surfing attacks as shown in figure 6. A user needs to recognize pass-objects and click inside the convex hull formed by all the pass-objects. In order to make the password hard to guess large number of objects can be used but it will make the display very crowded and the objects almost indistinguishable, but using fewer objects may lead to a smaller password space, since the resulting convex hull can be large.

Fig. 6 Example of a convex hull

Jansen [9, 10] proposed a graphical password scheme for mobile devices. During password creation, a user selects a theme consisting of photos in thumbnail size and set a sequence of pictures as a password. During authentication, user must recognize the images in the correct order. Each thumb nail image is assigned a numerical value, thus the sequence of the chosen images will create a numerical password. As the no. of images is limited to 30, the password space of this scheme is not large. We inshall and Kirkpatrick [11] proposed several authentication schemes such as picture recognition, object recognition and pseudo word recognition and conducted user studies on these. The results declared that pictures are most effective than the other two proposed schemes. Goldberg [12] designed a technique known as "passdoodle". This is a graphical password authentication scheme using handwritten design or text usually drawn with a stylus onto a touch sensitive screen.

To overcome the shoulder-surfing problem, many techniques are proposed. Zhao and Li proposed a shoulder-surfing resistant scheme"S3PAS". The main idea of the scheme is as follows. In the login stage, they must find their original text passwords in the login image and click inside the invisible triangle region. The system integrates both graphical and textual password scheme and has high level security. Man, et al proposed another shoulder-surfing resistant technique. In this scheme, a user chooses many images as the pass-objects. The pass-objects have variants and each of them is assigned to a unique code. In the authentication stage, the user must type the unique codes of the pass objects variants in the scenes provided by the system. Although the scheme shows perfect results in resisting hidden camera, it requires the user to remember code with the pass-object variants. More graphical password schemes have been summarized in a recent survey paper. Zheng et al designed a hybrid password scheme based on shape and text. The basic concept is mapping shape to text with strokes of the shape and a grid with text.

III. New Authentication Schemes

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.

A. Odd and Even 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. 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.

Figure 7 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. The first letter in the pair is used to select the row and the Next odd letter is used to select the column. The intersection letter is part of the session password. And again the second letter in the pair is used to select the row and the Next even letter is used to select the column.

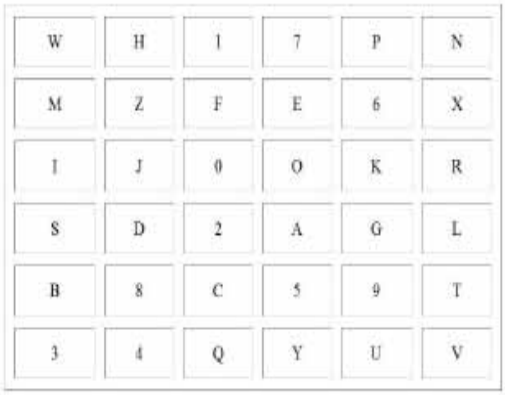


Fig. 7 Login interface

Fig. 8 Intersection letter for the pair AN

This is repeated for all pairs of secret pass. And the 6 secret pass characters are merged. Fig 8 shows that L is the intersection symbol for the pair "AN". The password entered by the user is verified by the server to authenticate the user. If the password is correct, the user is allowed to enter in to the system. The grid size can be increased to include special characters in the password.

B. Hybrid Textual Authentication Scheme

During registration, user should rate colors as shown in figure 9. The User should rate colors from 1 to 8 and he can remember it as "RLYOBGIP". Same rating can be given to different colors. 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 10. The color grid consists of 4 Odd and even pairs of colors. Each Odd and Even pair of color represents the row and the column of the grid.

Figure 10 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.

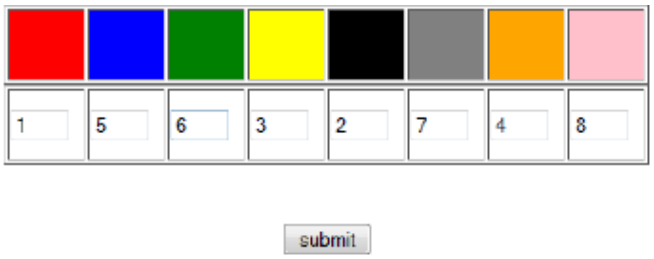


Fig. 9 Rating of colors by the user

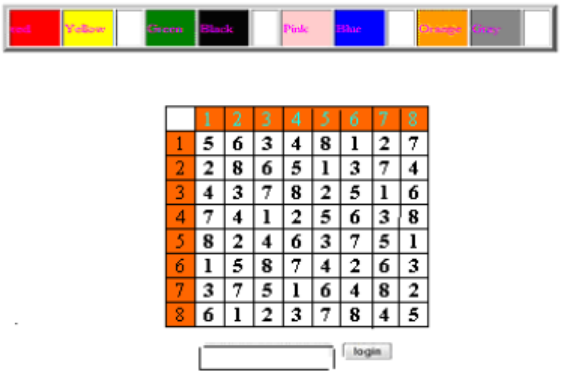


Fig. 10 Login interface

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 figure 9 ratings and figure 10 login interfaces for demonstration. The first pair has red and yellow colors. The red color rating is 1 and yellow color rating is 3. So the first letter of session password is 1st row and 3rd column intersecting element i.e 3. The same method is followed for other pairs of colors. For figure 10 the password is " 3573 ". 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.

IV. Security Analysis

As the interface changes every time, the session password changes. This technique is resistant to shoulder surfing. Due to dynamic passwords, dictionary attack is not applicable. Hidden camera attacks are not applicable to Cloud because it is difficult to capture the interface in the Cloud.

1). 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.

2). Shoulder Surfing: These techniques are Shoulder Surfing Resistant. In Odd and Even 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 84 .So these are resistant to shoulder surfing.

3). Guessing: Guessing can't be a threat to the pair based because it is hard to guess secret pass and it is 36. The hybrid textual scheme is dependent on user selection of the colors and the ratings. If the general order is followed for the colors by the user, then there is a possibility of breaking the system.

4). 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.

5). 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 368. 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 88.

A. User Study

We conducted the user study of the proposed techniques with 10 participants for each technique. As the techniques are new, first the participants were briefed about the techniques. They were given demonstrations for better understanding purpose. Then each user was requested to login. After that, the usability study was conducted with the students in two sessions. The sessions were conducted in time frame of one week.

Table 1 shows the registration time for each technique. Table 2 shows the log-in time for each technique for the first session of user study. Table 3 shows the log-in time for the second session which was taken after one week of first session.

TABLE I REGISTRATION TIME FOR PASSWORDS

Technique	Avg	Min	Max
Hybrid Textual Authentication	58	48.8	78.4

For Pair-based Authentication, registration is similar to existing Authentication.

TABLE II LOGIN TIME FOR CORRECT PASSWORDS AT SESSION 1

Technique	Avg	Min	Max
Pair based Authentication	29.95	24.6	43.26
Hybrid Textual Authentication	47.2	28.5	72

TABLE III LOGIN TIME FOR CORRECT PASSWORDS AT SESSION 2

Technique	Avg	Min	Max
Pair based Authentication	26.25	18	40.4
Hybrid Textual Authentication	39.16	26.4	63.5

It is observed that, as the user gets practised over, he is able to login without any problem. If the user is able to remember the password or ratings of colors, the schemes are resistant to shoulder surfing. The easiest way to remember ratings for colors is to use some concept or story and this leads to successful login in the Hybrid Textual Authentication.

V. CONCLUSION

In this paper, two authentication techniques based on text and colors are proposed for Cloud Computing. These techniques generate session passwords and are resistant to dictionary attack, brute force attack and shoulder-surfing. Both the techniques use grid for session passwords generation. Pair based technique requires no special type of registration; during login time based on the grid displayed a session password is generated. For hybrid textual scheme, ratings should be given to colors, based on these ratings and the grid displayed during login, session passwords are generated. However these schemes are completely new to the users and the proposed authentication techniques should be verified extensively for usability and effectiveness.

REFERENCES

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

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

[3] 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.

[4] 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-

[5] Verlag Lecture Notes in Computer Science (1438), 1998, pp. 403-441.

[6] G. E. Blonder, "Graphical passwords," in Lucent Technologies, Inc., Murray Hill, NJ, U. S. Patent, Ed. United States, 1996.

[7] Passlogix, site http://www.passlogix.com.

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

[9] S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy, N. Memon, "Design and longitudinal evaluation of a graphical password system". *International J. of Human-Computer Studies* 63 (2005) 102-127.

[10] W. Jansen, "Authenticating Mobile Device User through Image Selection," in *Data Security,* 2004.

[11] W. Jansen, "Authenticating Users on Handheld Devices "in *Proceedings of Canadian Information Technology Security Symposium,* 2003.