Authentication schemes for session password

VAISHNAVI PANCHAL*, CHANDAN P. PATIL*

*Department of Computer Engineering, PVPIT, Pune .

Abstract

The increase in the usage of automated systems has brought an increase in the amount of personal information in the electronic form; and as a result there is a need for confidentiality. The most common method for authentication is textual passwords. But textual passwords are vulnerable to shoulder surfing, social engineering, dictionary attacks and eves dropping. Most of the graphical passwords are vulnerable to shoulder surfing. To address this problem, text can be combined with colors to generate session passwords for authentication. Session passwords are one time passwords which are used only once and for every login a new session password is generated. The session passwords provide better security as password changes for every session. Therefore, we propose an authentication scheme using text and colors for generating session passwords.

Keywords: *Session passwords, Pair-based Authentication Scheme, Hybrid Authentication scheme.*

Introduction:

The most common method used for authentication is textual password. The vulnerabilities of this method like eves dropping, dictionary attack, social engineering and shoulder surfing are well known. Random and lengthy passwords can make the system secure. But the main problem is the difficulty of remembering those passwords. Studies have shown that users tend to pick short password or passwords that are easy to remember. Unfortunately, these passwords can be easily guessed or cracked.

The alternative techniques are graphical passwords and biometrics. But these two techniques have their own disadvantages. Biometrics, such as finger prints, iris scan or facial recognition have been introduced but not yet widely adopted. The major drawback of this approach is that such systems can be expensive and the identification process can be slow. There are many graphical password schemes that are proposed in the last decade. But most of them suffer from shoulder surfing which is becoming quite a big problem. There are graphical password schemes that have been proposed which are resistant to shoulder-surfing but they have their own drawbacks like usability issues or taking more time for user to login or having tolerance levels. In this paper, we use two authentication schemes namely Pair-based authentication scheme and Hybrid Textual authentication scheme.

Literature Survey:

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.

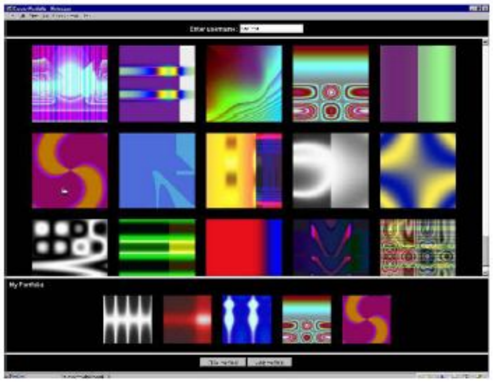


Figure 1: Random images used by Dhamija and Perrig

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.

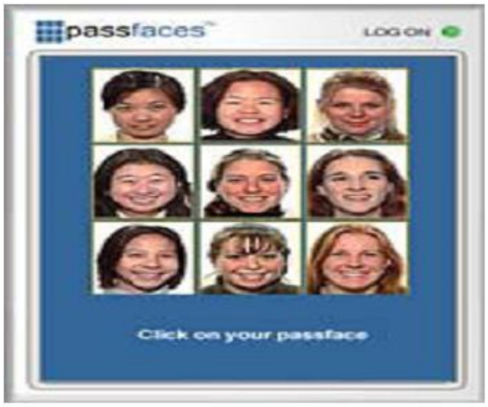
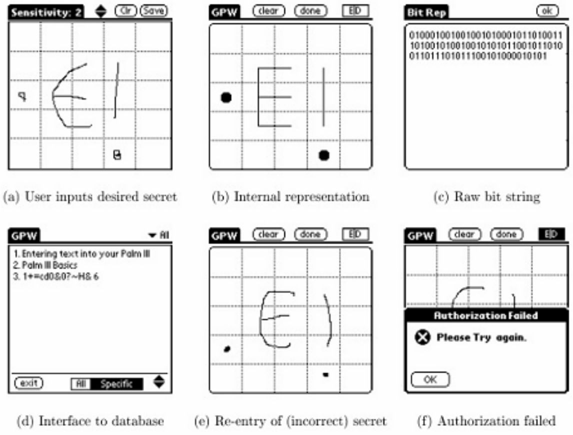


Figure 2: Example of Passfaces

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.



010001001001001010001011010011
101001010010010101011001011010
0110111010111001010000010101

1. Entering text into your Palm III
2. Palm III Basics
3. 1+=cd0&0?~H& 6

Please Try again.

(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

Figure 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.

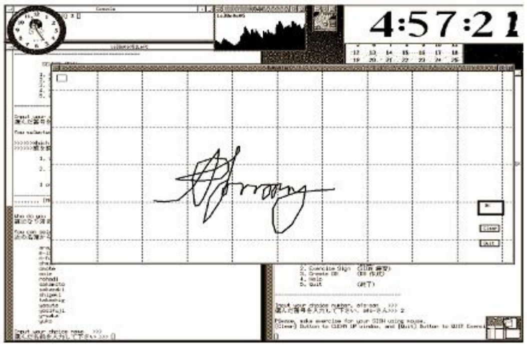


Figure 4: Signature technique by Syukri

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.

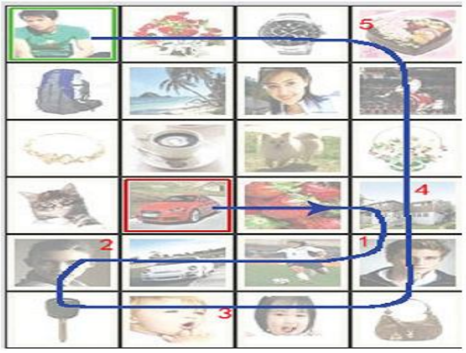


Figure 5: Haichang's shoulder-surfing technique

Jansen [8,9] 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. Weinshall and Kirkpatrick [10] 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 [11] 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.

Proposed work:

The proposed system uses two modes of authentication namely the Normal mode and the Safe mode. Further the proposed system uses Authentication technique consisting of 3 phases: registration phase, login phase and verification phase. During registration, user enters his password in first method 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.

Normal Mode

The Normal mode comprises of the Pair based Authentication scheme and Hybrid Textual Authentication scheme.

Safe Mode

The Safe mode comprises of the Pair based Authentication scheme and the One-Time-Password technique. The user can login either through the Normal mode or the Safe mode as per his requirement.

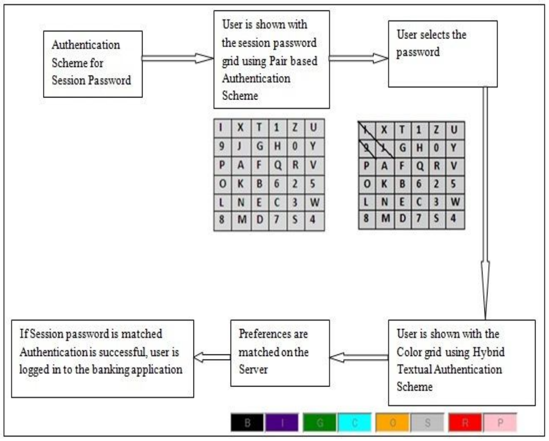
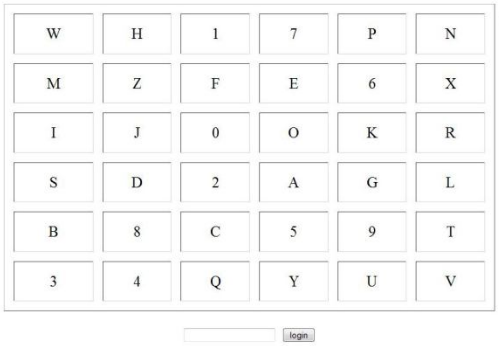

Authentication Scheme for Session Password
User is shown with the session password grid using Pair based Authentication Scheme
User selects the password
I X T 1 Z U
9 J G H 0 Y
P A F Q R V
O K B 6 2 5
L N E C 3 W
8 M D 7 S 4
I X T 1 Z U
9 J G H 0 Y
P A F Q R V
O K B 6 2 5
L N E C 3 W
8 M D 7 S 4
If Session password is matched Authentication is successful, user is logged in to the banking application
Preferences are matched on the Server
User is shown with the Color grid using Hybrid Textual Authentication Scheme
B
I
G
C
O
S
R
P

Fig. 6: Architecture of the proposed system

Pair-based Authentication scheme

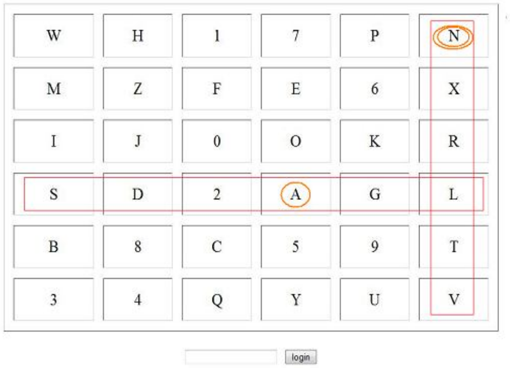
During registration user submits his password. Minimum length of the password is 8 and it can be called as secret pass. The secret pass should contain even number of characters. Session passwords are generated based on this secret pass. During the login phase, when the user enters his username an interface 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.



W	H	1	7	P	N
M	Z	F	E	6	X
I	J	0	O	K	R
S	D	2	A	G	L
B	8	C	5	9	T
3	4	Q	Y	U	V

Fig. 7: Login Interface

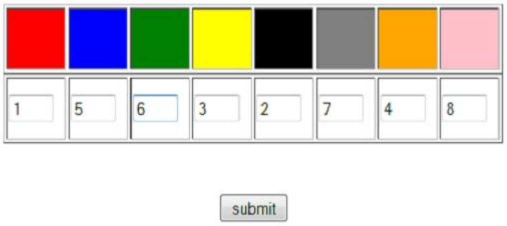
User enters the password depending upon the secret pass. User considers his secret pass in terms of pairs. The session password consists of alphabets and digits. The first letter in the pair is used to select the row and the second letter is used to select the column. The intersection letter is part of the session password. This is repeated for all pairs of secret pass. 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.



W	H	1	7	P	N
M	Z	F	E	6	X
I	J	0	O	K	R
S	D	2	A	G	L
B	8	C	5	9	T
3	4	Q	Y	U	V

Fig. 8: Intersection letter for the pair AN

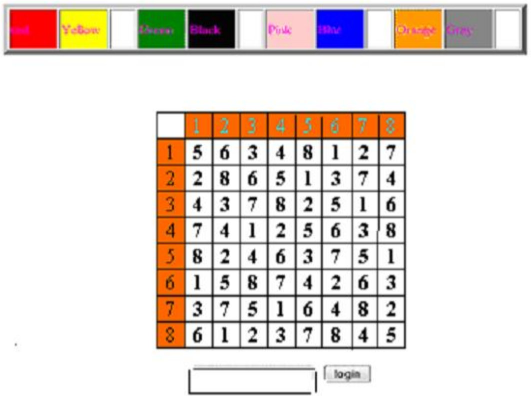
Hybrid Textual Authentication Scheme



🟥	🟦	🟩	🟨	⬛	▨	🟧	▨
1	5	6	3	2	7	4	8

Fig. 9: Color Rating

During registration, user should rate colors as shown in figure. The User should rate colors from 1 to 8 and he can remember it as “BIGCROPS”. Same rating can be given to different colors. During the login phase, 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. The color grid consists of 8 pairs of colors. Each pair of color represents the row and the column of the grid.



	1	2	3	4	5	6	7	8
1	5	6	3	4	8	1	2	7
2	2	8	6	5	1	3	7	4
3	4	3	7	8	2	5	1	6
4	7	4	1	2	5	6	3	8
5	8	2	4	6	3	7	5	1
6	1	5	8	7	4	2	6	3
7	3	7	5	1	6	4	8	2
8	6	1	2	3	7	8	4	5

Fig.10: Color Rating Intersection Interface

One Time Password Technique

This technique is used if the user wants to login through the Safe mode. Initially in the Safe mode, after the user authenticates the Pair based Authentication scheme, a code is sent to his/her mobile phone. This code has to be entered by the user in the next level of authentication. The code entered by the user is matched and the user is authenticated.

Registration

This module is used to register user details in three parts. They are namely Authentication Password, Color Priority Password and Other details. First, user is going to enter the normal password but it using capital A-Z letters and 0-9 Numbers. Second the user will put the color priority in eight colors.

Conclusion :

The proposed system allows the user to login through two modes, the Normal mode and the Safe mode. For some users it can be difficult to remember the ratings given to the colors during registration, so the user can use the Safe mode authentication where the user do not have to rate the colors instead he/she would have to enter the code sent to the mobile phone. Thus, it makes the system to be user friendly as per the user's choice.

This system aims at reducing the risks from the different malicious activities to a great extent thereby increasing the security and efficiency proving it to be very advantageous in today's world where the confidential data security has become so essential due to the increasing cyber thefts and hacks, etc. Our system aims to be extremely robust and secured to the malicious activities, therefore providing user the freedom to have complete security while handling his or her confidential data and security essential systems from anywhere.

Future Scope:

The proposed system is completely new to the users and should be verified extensively for the usability and effectiveness. This system can also be developed as windows application folder locker or as an external gateway authentication to connect the application to a database or an external embedded device.

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

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

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

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

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

[10] D. Weinshall and S. Kirkpatrick, "Passwords You’ll Never Forget, but Can’t Recall," in Proceedings of Conference on Human Factors in Computing Systems (CHI). Vienna, Austria: ACM, 2004, pp. 1399-1402.

[11] J. Goldberg, J. Hagman, V. Sazawal, "Doodling Our Way to Better Authentication", CHI '02 extended abstracts on Human Factors in Computer Systems, 2002.