ISSN:0975-9646

Design and Analysis of User Identification for Graphical Password System

Devika S[#], Backiyalakshmi R[*]

[#]M.Tech Student , [*]Assistant professor
Department of Computer Science and Engineering,
PRIST University Pondicherry, India.

Abstract - **Authentication is necessary in multi-user systems. User name and password are used to authenticate a user. Textual passwords are the most common method used for authentication. But textual passwords are vulnerable to eves dropping, dictionary attacks, social engineering and shoulder surfing. Graphical passwords are introduced as alternative techniques to textual passwords. Most of the graphical schemes are vulnerable to shoulder surfing. To address this problem, text can be combined with images or colors to generate session passwords for authentication. Session passwords can be used only once and every time a new password is generated. This project proposes two techniques to generate session passwords using text and colors which are resistant to shoulder surfing. These methods are suitable for Personal Digital Assistants.**

Keywords— **Authentication, session passwords, shoulder surfing.**

I. INTRODUCTION

A *password* is a secret word or string of characters that is used for authentication, to prove identity or gain access to a resource (example: an access code is a type of password). The password should be kept secret from those not allowed access. The use of passwords is known to be ancient. Sentries would challenge those wishing to enter an area or approaching it to supply a password or watchword. Sentries would only allow a person or group to pass if they knew the password. In modern times, user names and passwords are commonly used by people during a log in process that controls access to protected computer operating systems, mobile phones, cable TV decoders, automated teller machines (ATMs), etc. A typical computer user may require passwords for many purposes: logging in to computer accounts, retrieving e-mail from servers, accessing programs, databases, networks, web sites, and even reading the morning newspaper online. Despite the name, there is no need for passwords to be actual words; indeed passwords which are not actual words may be harder to guess, a desirable property. Some passwords are formed from multiple words and may more accurately be called a passphrase. The term *passcode* is sometimes used when the secret information is purely numeric, such as the personal identification number (PIN) commonly used for ATM access. Passwords are generally short enough to be easily memorized and typed.

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. Some studies have shown that users tend to pick short passwords 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 passwords 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. Personal Digital Assistants are being used by the people to store their personal and confidential information like passwords and PIN numbers. Authentication should be provided for the usage of these devices. In this project, two new authentication schemes are proposed for PDAs. 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.

II. RELATED WORK

A. *User Study Using Images For Authentication:*

It 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. This system is vulnerable to shoulder-surfing.

Passface 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[2].

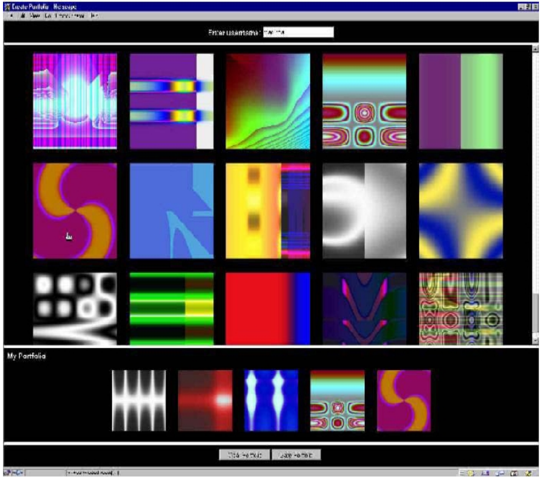


Fig. 2.1 Random images used by Dhamija and Perrig Passfaces

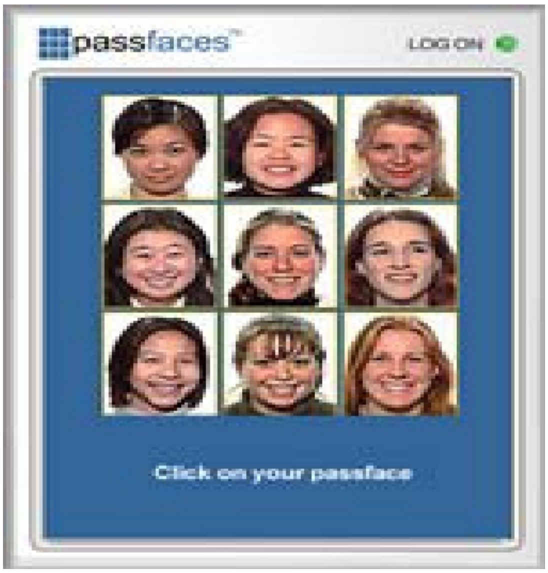
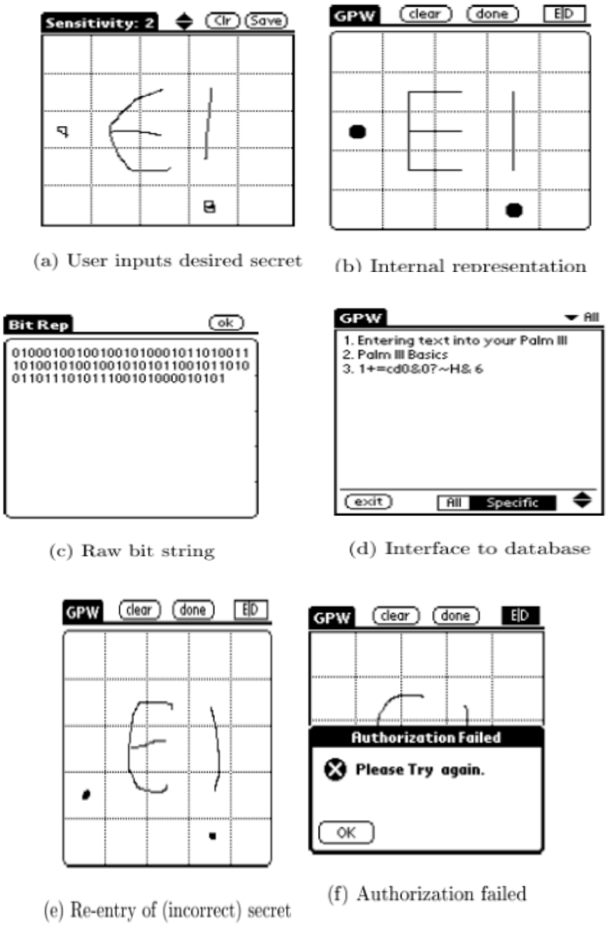


Fig. 2.2 Example of Passfaces

B. *The design and analysis of graphical passwords*

This paper had proposed and evaluated new graphical password schemes that exploit features of graphical input displays to achieve better security than text based passwords. Graphical input devices enable the user to decouple the position of inputs from the temporal order in which those inputs occur, and it showed that this decoupling can be used to generate password schemes with substantially larger (memorable) password spaces. In order to evaluate the security of schemes, it devised a novel way to capture a subset of the memorable passwords[3].

This paper had explored an approach to user authentication that generalizes the notion of a textual password and that, in many cases, improves the security of user authentication over that provided by textual passwords. It designed and analyzed graphical passwords, which can be input by the user to any device with a graphical input interface. A graphical password serves the same purpose as a textual password, but can consist, for example, of handwritten designs (drawings), possibly in addition to text. The devices are personal digital assistants" (PDAs) such as the Palm PilotTM, Apple NewtonTM, Casio Cassiopeia E-10TM, and others, which allow users to provide graphics input to the device via a stylus. More generally, graphical passwords can be used whenever a graphical input device, such as a mouse, is available.



01000100100100101000101101001 1
10100101001001010101100101101 0
01101110101110010100001010 1

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

(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. 2.3 Graphical passwords

Syukri 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.

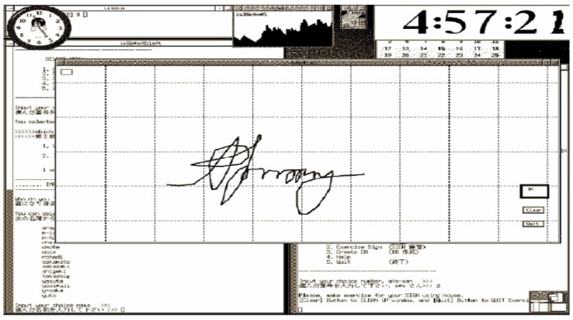


Fig 2.4 Signature technique by Syukri

C. *Graphical and password passlogix*

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

D. *A New Graphical PassworScheme Resistant Shoulder-Surfing*

Haichang et al 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.

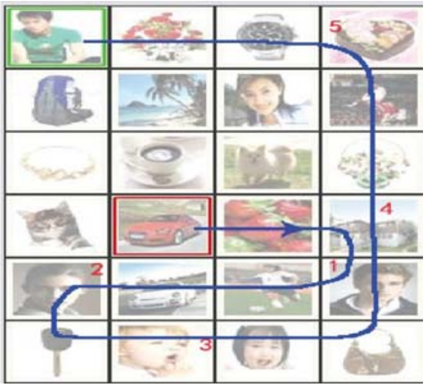


Fig 2.5 Haichang's shoulder-surfing technique

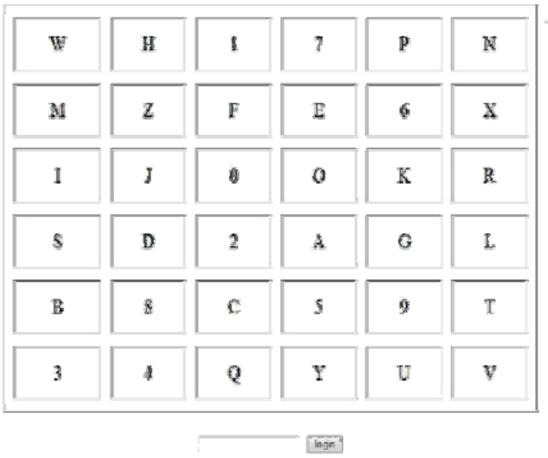
III. NEW AUTHENTICATION SCHEMES

Authentication techniques consist of three phases login, registration, verification. 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.

A. *Pair Based Authentication*

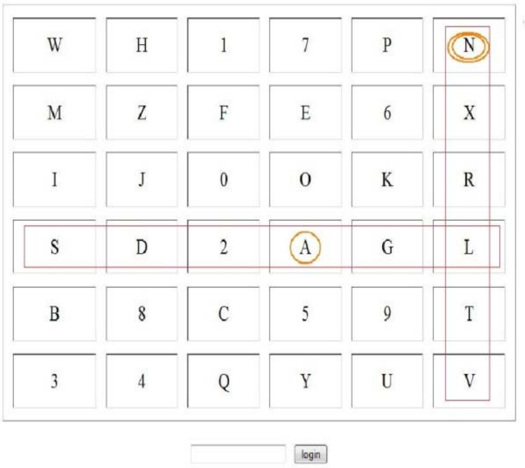
During registration user submits his password. Minimum length of the password is 8 and it can be called as secret pass. The secret pass should contain even number of characters. Session passwords are generated based on this secret pass. During the login phase, when the user enters his username an interface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

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. 3.1 Login interface

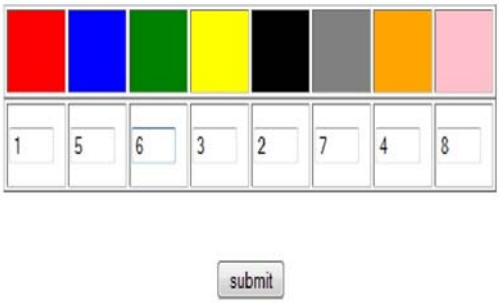


W	H	1	7	P	N
M	Z	F	E	6	X
I	J	0	O	K	R
S	D	2	A	G	L
B	8	C	5	9	T
3	4	Q	Y	U	V

Fig. 3.2 Intersection letter for the pair AN

B. *Hybrid Textual Authentication Scheme*

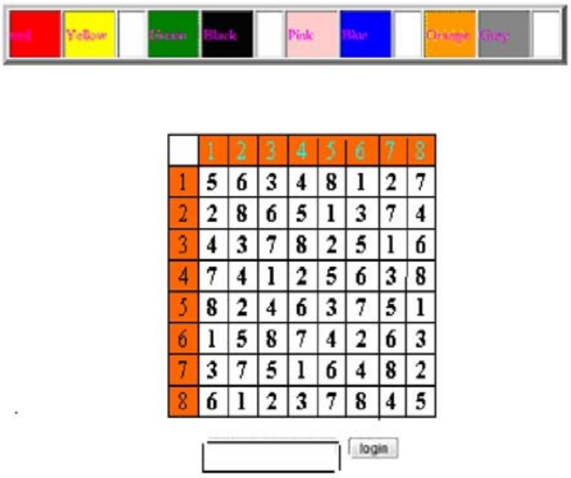
During registration, user should rate colors .The User should rate colors from 1 to 8 and he can remember it as "RLYOBGIP". Same rating can be given to different colors.



🟥	🟦	🟩	🟨	⬛	▨	🟧	🟪
1	5	6	3	2	7	4	8

Fig. 3.3 Rating of colors by the user

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. The color grid consists of 4 pairs of colors. Each pair of color represents the row and the column of the grid. The number in the intersection of the row and column of the grid is part of the session password. For every login, both the number grid and the color grid get randomizes so the session password changes for every session.



	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. 3.4 Login interface

The system verifies the password entered by comparing with content of the password generated during registration. The authentication techniques should be verified extensively for usability and effectiveness.

IV. CONCLUSION

In this project, two authentication techniques based on text and colors are proposed for PDAs. 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.

V.FUTURE ENHANCEMENTS

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 PDAs because it is difficult to capture the interface in the PDAs.The two new authentication schemes proposed in this project can be used in email services. Instead of colors normal images and pictures can be used. Interface grid structure can be changed according to the application level.

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] 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.

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

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

[11] 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.

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

[13] H. Zhao and X. Li, "S3PAS: A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme," in 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW 07), vol. 2. Canada, 2007, pp. 467-472.

[14] S. Man, D. Hong, and M. Mathews, "A shoulder surfing resistant graphical password scheme," in Proceedings of International conference on security and management. Las Vegas, NV, 2003.

[15] X. Suo, Y. Zhu and G. Owen, “Graphical Passwords: A Survey”. In Proc. ACSAC'05.

[16] Z. Zheng, X. Liu, L. Yin, Z. Liu “A Hybrid password authentication scheme based on shape and text” Journal of Computers, vol.5, no.5 May 2010.

AUTHOR PROFILE

Mrs.Devika S, Received The B.Tech (Information Technology) From Sri Andal Alagar College of Engg, Anna University, Chennai, Tamil Nadu, India and Presently Pursuing Final Year M.TECH CSE, In PRIST University, Pondicherry Campus, Pondicherry, India in 2012 and 2014.

Ms. R.Backiyalakshmi Received The M.Tech In Computer Science And Engineering. Presently she is a Working Assistant Professor in Computer Science and Engineering at PRIST University, Pondicherry Campus, and Pondicherry, India.