ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 4, April 2015

3D SECURE PASSWORD

Ashwini Sakpal, Kalpana Lande[1], Pooja Yeole, Prafull Kalokhe, Shrikant Sanas[2]

IT Department, Mumbai University, India[1]

Padmabhushan Vasantdada Patil Pratishthan's College of Engineering Sion, Chunabhatti, Mumbai, India[2]

Abstract: 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. In this paper, a technique is proposed to generate session passwords using colors which are resistant to shoulder surfing. This method is suitable for Personal Digital Assistants.

Keywords: Authentication, session passwords, shoulder surfing.

I. INTRODUCTION

Authentication is the first step in information security in today's world; there are many techniques for protecting the passwords. These techniques are vulnerable to different attacks such as shoulder surfing, eves dropping, dictionary attack, spyware etc. Graphical passwords have their own disadvantages. Complicated passwords are difficult to remember. We are using color password for which session passwords are created. For every login user input is different password. The password is generated using text and color rating which are resistant to various attacks. It can be used where security is of main purpose such as net banking, trade transactions, server-side etc.

Authentication technique consists of 3 phases: registration phase, login phase and verification Phase.

During registration, user rates the colors. 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. In these schemes First it will be checked that the user is already registered or not. If yes, then it will go for the step of login, but if user is not registered then first he will go through registration and then to the login step. Then at the time of transaction the color pairs and grid will be shown and from that the user will enter the session password. This password will be verified at the verification phase. If the user wants another session then a new session will be generated and the grid and color pair will be shown to the user again.

II. RELETED 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.

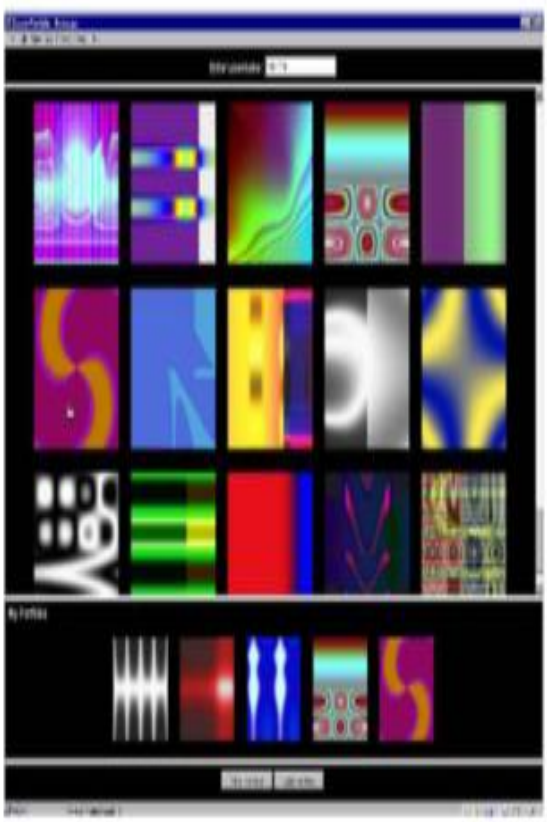

Figure 1: Random images used by Dhamija and Perrig

Pass face [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.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 4, April 2015

Figure 2: Example of Pass faces

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.

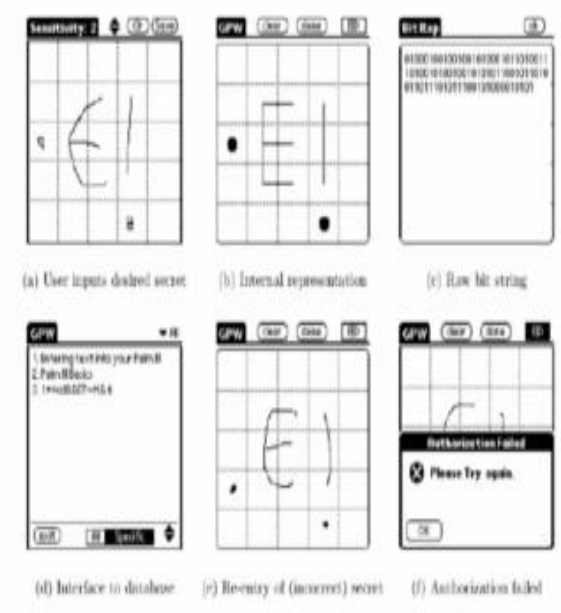

Figure 3: DAS technique by Jermyn

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.

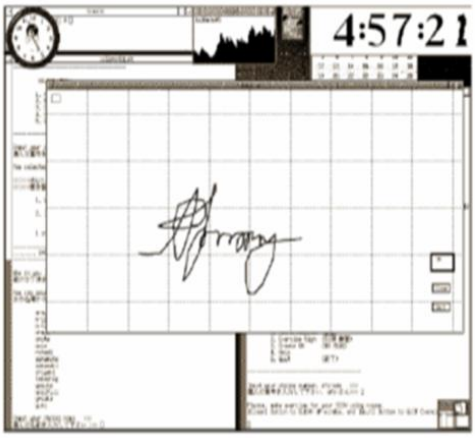

Figure 4: Signature technique by Syukri

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.

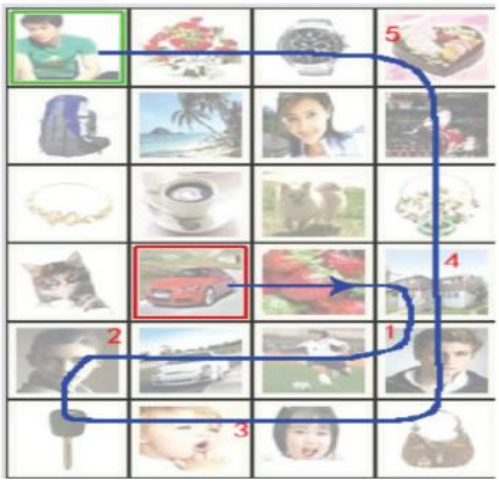

Figure 5: Haichang's shoulder-surfing technique

III. PROPOSED SYSTEM

A. Rating of Colors at the Time of Registration

During registration, user should rate colors as shown in figure 4. The User should rate colors from 1 to 8 and he can remember it as "YRGBOIMP". Same rating can be given to different colors.

Figure 6: Rating of color

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 4, April 2015

B. 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 as shown in figure 4. The color grid consists of 4 pairs of colors. Each pair of color represents the row and the column of the grid.

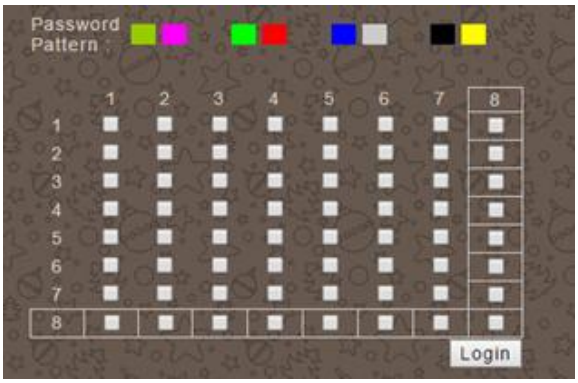

Figure 7: Grid of Number

IV. CONCLUSION

These techniques generate session passwords and are resistant to dictionary attack, brute force attack and shoulder-surfing .This technique use grid for session passwords generation. Ratings should be given to colors, based on these ratings and the grid displayed during login, session passwords are generated. However this scheme is completely new to the users and the proposed authentication techniques should be verified extensive for usability and effectiveness. It is not vulnerable to shoulder surfing, eaves dropping, and brute force attack. More sites, more passwords, more forgetting, more repeated credentials increased exposure to hacking and cloning. It is more securable as compared to the existing system.

FUTURE SCOPE

This technique can be used to develop any windows application or external authentication to connect the application to database.

ACKNOWLEDGMENT

I would like to thank Information Technology Department, P.V.P.P. Engineering College, Sion, Mumbai-22 and Faculty members for providing me all the facilities in making this project possible.

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: Pass faces. 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]. J. Goldberg, J. Hagman, V. Sazawal, "Doodling Our Way to Better Authentication", CHI '02 extended abstracts on Human Factors in Computer Systems, 2002.
[9]. 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.
[10]. 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.