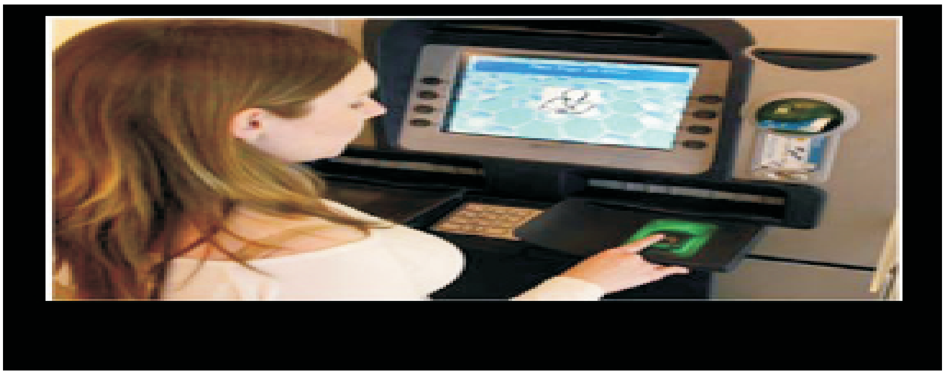
IndustrialScience
ISSN No : 2347-5420
Impact Factor : 1.5015 (UIF) 2014

ISSN: 2347-5420 Impact Factor : 1.5015(UIF) Volume - 2 | Issue - 3 | Feb - 2016



Uday Gobbur

COMPARATIVE STUDY ABOUT PASSWORD AUTHENTICATION SCHEMES FOR DATA SECURITY

Uday Gobbur[1] and Suhas Raut[2]
[1]Master of Engineering student, Department of Computer science & Engineering
NK Orchid College of Engineering & Technology, Solapur, Maharashtra, India.
[2]Ph.D. Professor, Department of Computer science & Engineering
NK Orchid College of Engineering & Technology, Solapur, Maharashtra, India.

ABSTRACT

Textual passwords are the most common methods 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, To start with user login with permanent password and then 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, two techniques are proposed to generate session passwords using text and colors which are resistant to shoulder surfing. These methods are suitable for Personal Digital Assistants.

KEY WORDS: Authentication, session passwords, Circular password scheme.

1. 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 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.

This paper is organized as follows: in section 2. Related work is discussed; in section 3. Proposed Authentication schemes introduced; conclusion is proposed in section 4.

2. 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.

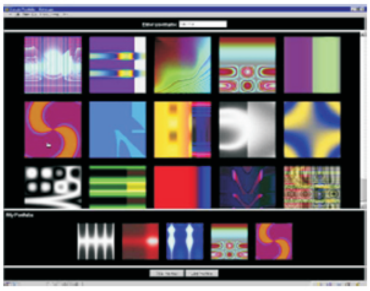


Figure 1: Random images used by Dhamija and Perrig

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.

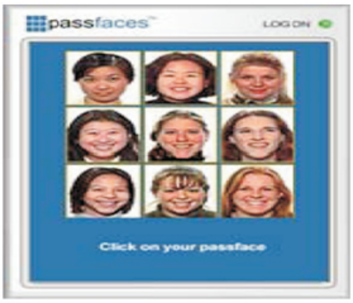


Figure 2: Example of Passfaces

Haichang et al [7] proposed a new shoulder-surfing resistant scheme as shown in figure 3 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.

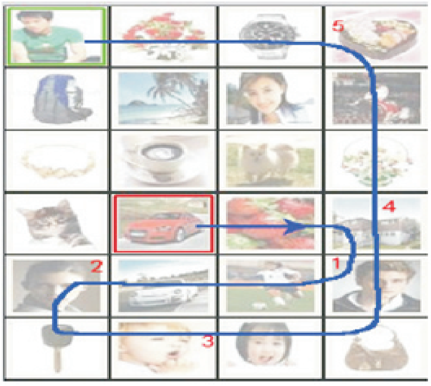


Figure 3: Haichang's shoulder-surfing technique

Wiedenback et al [8] describes a graphical password entry scheme using convex hull method towards Shoulder Surfing attacks as shown in figure 4. 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.

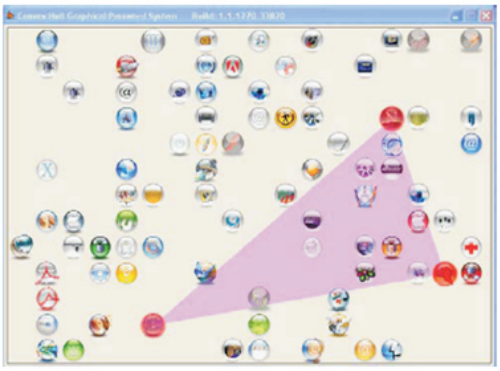


Figure 4: Example of a convex hull

3. PROPOSED AUTHENTICATION SCHEMES

In proposed system, we give the secure password by making combination of text, image Circular Password for data security. Text based password nothing but regular textual username and password scheme. For ex. In system login Username is Admin, Password is also Admin. In image based password 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. In circular password scheme, we provide anticlockwise and clockwise selection of alphabets. Selection of alphabets based on degree of rotation in anticlockwise or clockwise direction. In this scheme we give degree of rotation as an Input.

In existing systems passwords are very difficult to remember and time consuming. But proposed system we will give secure circular graphical password for our system which is simple to remember and difficult to guess for unauthorized users.

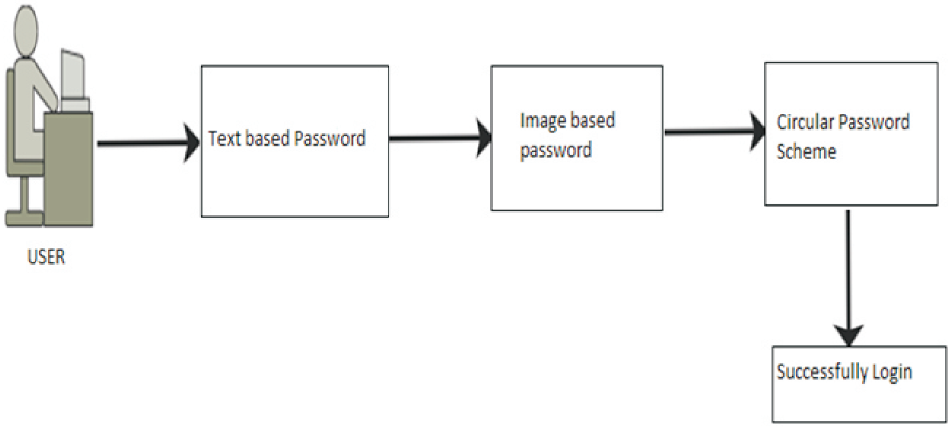


Figure 5: Proposed Architecture

4. CONCLUSION:

By referring base papers, in existing systems passwords are very difficult to remember and time consuming. But we focused on design a system which Resistant the shoulder surfing attack. The user can easily and efficiently login the system without using any physical keyboard or on-screen keyboard. We will give secure circular graphical password for our system which is simple to remember and difficult to guess for unauthorized users.

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.