International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org
Volume 4, Issue 10, October 2015 **ISSN 2319 - 4847**

A Theoretical Approach to Simple 4-D Authentication Scheme Resistant to Shoulder Surfing Attack

[1]Ms. ShraddhaGajare, [2]Mrs. VaishaliLondhe, [3]Mrs. NilimaNikam

[1]Department of Computer Engineering, M. E Student,YadavraoTasgaokar Instituteof Engineering and Technology

[2]M. E, Department of Computer Engineering, YadavraoTasgaokar Instituteof Engineering and Technology.

[3]M. E, Department of Computer Engineering, YadavraoTasgaokar Instituteof Engineering and Technology.

ABSTRACT

Since conventional password schemes are vulnerable to shoulder surfing, many shoulder surfing resistant graphical password schemes have been proposed. However, as most users are more familiar with textual passwords than pure graphical passwords, text-based graphical password schemes have been proposed. Unfortunately, none of existing text-based shoulder surfing resistant graphical password schemes is both secure and efficient enough. Here, we propose 4-D Password scheme to make the existing scheme even more robust and powerful. We propose to different authentication scheme to one system, and this will lend more stability and make the attacks on user privacy even more difficult to succeed in. We proposed a system with graphical password scheme, Color code authentication, OTP based authentication, and Time Elapse Authentication scheme composed as a 4-D Authentication system.

1.INTRODUCTION

Today, although the password authentication is used widely, since users write their password directly on screen and tend to make their password easy to remember, they may be vulnerable to several attacks such as brute-force, guessing, replay, and shoulder surfing. Although many authentication schemes were proposed to improve the usability and security, they are still vulnerable to the shoulder surfing attack. In this project, we propose a 4-D pattern-based authentication scheme which is secure against this attack. Also, we analyse the usability, deplorability, and security of the proposed authentication scheme, compared to the other authentication schemes. Devising a user authentication scheme based on several identification schemes that is both secure and practically usable is a challenging problem. The greatest difficulty lies with the susceptibility of the entry process to direct observational attacks, such as human shoulder-surfing and camera-based recording. This project starts with an examination of a previous attempt at solving the entry problem, which was based on several authentication schemes like Authentication using a Rotating wheel with 8 sectors, Color Code Authentication, OTP Authentication and Time Elapse Authentication schemes. Even though the method required uncomfortably many user inputs, it had the merit of being easy to understand and use. Our analysis that takes both the experimental and theoretical approaches reveals multiple serious shortcomings of the previous method, including round redundancy, unbalanced key presses, highly frequent system errors, and insufficient resilience to recording attacks. The lessons learned through our analysis are then used to improve the authentication scheme. The new scheme has the remarkable property of resisting camera-based recording attacks over an unlimited number of authentication sessions without leaking any passwords.

2.RELATED WORK

Literature Survey shows existing anti-shoulder surfing mechanism is usually applicable for graphical password scheme for common security applications only, hence there is a need to increase the complexity of This is why, in this paper, we are trying to improve the security of graphical password for mobile devices, by proposing an anti-shoulder surfing mechanism called 4D Graphical Password Authentication.

Existing System:

Today, password is the most popular way to authenticate a user to login to computer systems. However, we all know that traditional text-based password systems are vulnerable to the shoulder-surfing attack. Through this paper we use the word "shoulder-surfing" in the following sense: A shoulder-surfing attack consists of a user being filmed during his/her login.

Some of the Authentication schemes are as follow:
1. A graphical authentication scheme where the user has to identify the pre-defined images to prove user's authenticity

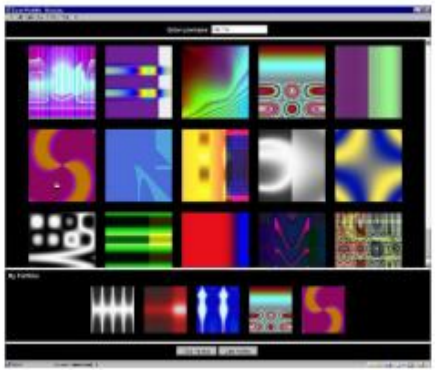


Figure 1: Existing System-1- Graphical Authentication Scheme

2. A "**Passface**" technique where the user sees a grid of nine faces and selects one face previously chosen by the user as shown in figure. 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: Existing System 2 – Passface

3. A new shoulder-surfing resistant scheme as shown in figure 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: existing System 3 - Graphical Story Scheme

3.PROBLEM DEFINITION

Information and computer security is supported largely by passwords which are the principle part of the authentication process. The most common computer authentication method is to use alphanumerical username and password which has significant drawbacks. To overcome the vulnerabilities of traditional methods, visual or graphical password

schemes have been developed as possible alternative solutions to text based scheme. A potential drawback of graphical password schemes is that they are more vulnerable to shoulder surfing than conventional alphanumeric text passwords. When users input their passwords in a public place, they may be at risk of attackers stealing their password. An attacker can capture a password by direct observation or by recording the individual's authentication session.

Problem 1: The most common computer authentication method is to use alphanumerical usernames and passwords. This method has been shown to have significant drawbacks. For example, users tend to pick passwords that can be easily guessed. On the other hand, if a password is hard to guess, then it is often hard to remember.

Problem 2: To overcome the shoulder-surfing attack issue without adding any extra complexity into the authentication procedure.

Problem 3: The advantages of pass-thought over many of the existing authentication technologies include changeability, shoulder surfing resistance, and protection against theft and user non-compliance. Disadvantages of Pass-thought authentication include the requirement for a new hardware component (including electrodes) to record The user's brain signals and the associated performance. For this reason, a pass-thought system may not be accepted for widespread use, but perhaps for high-value or high-importance applications or environments (e.g. within banks and governments)

Problem 4: An attacker can capture a password by direct observation or by recording the individual's authentication session while inserting passwords in public. This is referred to as shoulder-surfing.

Problem 5: Previous research has found graphical passwords to be more memorable than non-dictionary or "strong" alphanumeric passwords. Participants in a prior study expressed concerns that this increase in memorability could also lead to an increased susceptibility of graphical passwords to shoulder-surfing. The seminal question still remains: Can we have both usable and secure authentication systems? In particular, are graphical passwords the leading candidates to address this long-standing challenge, or do the very characteristics that make graphical passwords more memorable and usable lead to increased security vulnerabilities like shoulder-surfing?

Problem 6: A potential drawback of graphical password schemes is that they are more vulnerable to shoulder surfing than conventional alphanumeric text passwords

Problem 7: Shoulder-surfing is a problem that has been difficult to overcome

Problem 8: To gain access to computer systems, users are required to be authenticated. This is usually accomplished by having the user enter an alphanumeric username and password. Users are usually required to remember multiple passwords for different systems and this poses such problems as usability, memorability and security. Passwords are usually difficult to remember and users have developed their own methods some of which are not secure of selecting passwords which are easy to remember. The main weakness of graphical password systems is shoulder surfing.

Problem 9: Textual password is vulnerable to shoulder surfing, hidden-camera and spyware attacks. Graphical password schemes have been proposed as a possible alternative to text-based scheme. However, they are mostly vulnerable to shoulder-surfing as well.

Problem 10: Previous efforts involving picture-based passwords have not focused on maintaining a measurably high level of entropy. Since password systems usually allow user selection of passwords, their true entropy remains unknown.

Problem 11: One common practice in relation to alphanumeric passwords is to write them down or share them with a trusted friend or colleague. Graphical password schemes often claim the advantage that they are significantly more secure with respect to both verbal disclosure and writing down. In this paper they investigated the reality of this claim in relation to the Pass faces graphical password scheme.

Problem 12: User authentication is one of the important topics in information security. Traditional strong password schemes could provide with certain degree of security; however, the fact that strong passwords being difficult to memorize often leads their owners to write them down on papers or even save them in a computer file. As a result, security becomes greatly compromised.

Problem 13: Alphanumeric passwords are widely used in computer and network authentication to protect user's privacy. However, it is well known that long, text-based passwords are hard for people to remember, while shorter ones are susceptible to attack.

Problem 14: Threats such as key-loggers, weak password, and shoulder surfing, forcing the user to memorize different passwords or carrying around different tokens, "familiarization" or a lengthy "password setup" process are today's drawbacks of authentication systems.

4.PROPOSED SYSTEM

We propose an improved text-based shoulder surfing resistant graphical password scheme by using colors. In the proposed scheme, the user can easily and efficiently login system. Next, we analyze the security and usability of the proposed scheme, and show the resistance of the proposed scheme to shoulder surfing and accidental login.

We have divided our proposed work in 4 phases which are as under:

Phase 1:
The user requests to login the system, and the system displays a circle composed of 8 equally sized sectors. The colors of the arcs of the 8 sectors are different, and each sector is identified by the color of its arc, e.g., the red sector is the sector of red arc. Initially, 80 characters are placed averagely and randomly among these sectors. The user has to set his textual password K of length L(6) characters, and choose one color as his pass color from 8 colors assigned by the system.

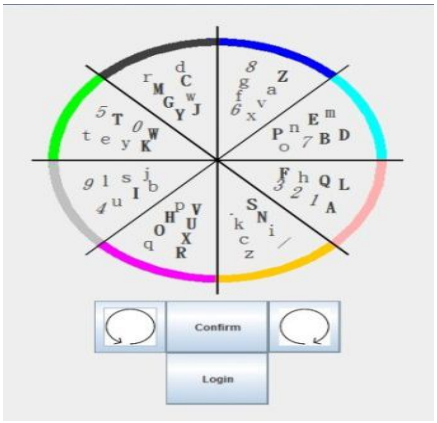


Figure 4: Proposed System - Phase 1

Phase 2:
OTP is used when user passed the above two Phases and OTP should be Verified to Navigate to next phase.
Phase 3:
During registration, user should rate colors as shown in figure. The User should rate colors from 1 to8 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. The color grid consists of 4 pairs of colors. Each pair of color represents the row and the column of the grid. Figure 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. 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.

Figure 5: Proposed System - Phase 3 Ratings

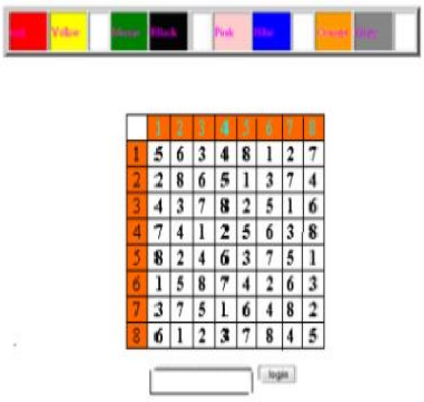
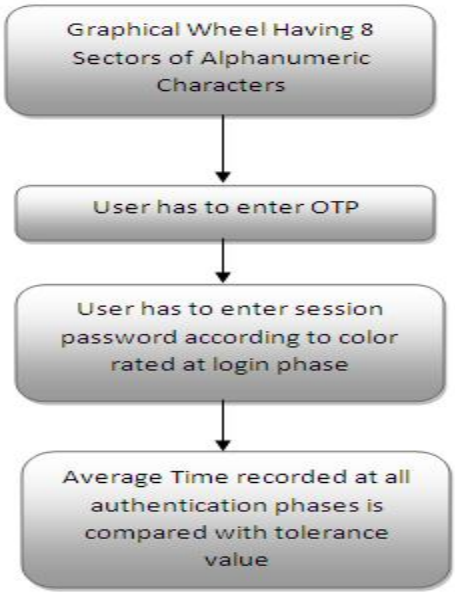


Figure 6: Proposed System - Phase 3 - Login Interface

Consider the figure (5) ratings and figure (6) login interface 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. the same method is followed for other pairs of colors. For figure (6) 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.

Phase 4:

Average Time of a user to complete all Authentication phases is recorded and it is compared with a tolerance value which is relatively small. User gets authenticated only after passing this last phase.



Block diagram for Proposed System

5.CONCLUSION:

We propose 4-D Password scheme to make the existing scheme even more robust and powerful. We proposefour different authentication schemes to one system, and this will lend more stability and make the attacks on user privacy even more difficult to succeed in. We proposed a system with graphical password scheme, Color code authentication, OTP based authentication, and Time Elapse Authentication scheme composed as a 4-D Authentication system. The scheme works onthe framework of partially observable attacker model. Fromsecurity point of view the scheme is quite robust against somepossible attacks such as shoulder surfing, guessing password,side channel attack, etc. And from usability point of view thescheme is user friendly and takes very less time for login. Alsothe scheme can be used by both math and non-math orientedpeople.

REFERENCES

[1]. Yi-Lun Chen, Wei-Chi Ku*, Yu-Chang Yeh, and Dun-Min Liao "A Simple Text-Based Shoulder Surfing Resistant Graphical Password Scheme", IEEE 2nd International Symposium on Next-Generation Electronics (ISNE) - February 25-26 , Kaohsiung , Taiwan 2013.

[2]. Nilesh Chakraborty, SamratMondal "Color Pass: An Intelligent User Interface to Resist Shoulder Surfing Attack", Proceeding of the 2014 IEEE Students' Technology Symposium.

[3]. L. Sobrado and J. C. Birget, "Graphical passwords," The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4, 2002.

[4]. L. Sobrado and J.C. Birget, "Shoulder-surfing resistant graphical passwords," Draft, 2005. (http://clam.rutgers.edu/~birget/grPssw/srgp.pdf) [3] S. Wiedenbeck, J. Waters, L. Sobrado, and J. C. Birget, "Design and evaluation of a shoulder-surfing resistant graphical password scheme," Proc. of Working Conf. on Advanced Visual Interfaces, May. 2006, pp. 177-184.

[5]. M. M. Group, "http://www.internetworldstats.com/stats.htm," June 2012.

[6]. C. Herley, P. C. Oorschot, and A. S. Patrick, "Passwords: If were so smart, why are we still using them?," in Financial Cryptography, pp. 230–237, 2009.

[7]. www.webeopdia.com/term/s/shoulder−surfing.html (last access Octeber,2013).

[8]. A. Paivio, "Mind and its evaluation: A dual coding theoretical approach,"2006.