Extended Text and Color Based Session Password Security against Shoulder Surfing and Spyware

[1]Ms.Kiran P. Lokhande, [2]Ms.Vimmi Gajbhiye
[1] M.Tech(CSE) III [rd] Sem Student ,[2] Assistant Professor
[1] Department of Computer Science & Engineering
[1] AGPCE Nagpur, India

***Abstract*— Authentication is the first step in information security. It requires the user to memorize their password and remember at login time. textual passwords are the most traditional schemes that are used for providing security, but textual passwords are vulnerable to dictionary attacks, shoulder surfing, and spyware. Graphical password schemes overcome the shortcomings of textual passwords, but they were vulnerable to shoulder surfing attacks. 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. to overcome this problem text and color are combined to generate passwords for providing higher security. a new technique called extended text and color based session password security against shoulder surfing and spyware. Session password can be used every time the password is created for authentication. In the proposed system, the user can easily and efficiently login system. Proposed scheme is resistant to shoulder surfing and accidental login and spyware.**

***Keywords*—Shoulder surfing, spyware, authentication.**

I. INTRODUCTION

Today's Because of increasing threats to networked computer systems, there is great need for security innovations. Security practitioners and researchers have made strides in protecting systems and, correspondingly, individual users' digital assets. However, the problem arises that, until recently, security was treated wholly as a technical problem – the system user was not factored into the equation. Current authentication methods can be divided into three main areas: Token based authentication, Biometric based authentication and Knowledge based authentication, Knowledge based authentication. Token based techniques, such as key cards, bank cards and smart cards are widely used. Many token-based Authentication systems also use knowledge based techniques to enhance security. For example, ATM cards are generally used together with a PIN number. Biometric based authentication techniques [6.7], such as fingerprints, iris scan, or facial recognition, are not yet widely adopted. The major drawback of this approach is that such systems can be expensive, and the identification process can be slow and often unreliable. However, this type of technique provides the highest level of security. Knowledge based techniques are the most widely used authentication techniques. It divided into two categories: Recognition-based and recall-based graphical techniques. Using recognition-based techniques, a user is presented with a set of images and the user passes the authentication by recognizing and identifying the images he or she selected during the registration stage. Using recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage. These all and many graphical password schemes with different degrees of resistance to shoulder surfing have been proposed and each has its pros and cons. Text-based password schemes are ubiquitous due to ease of use, inexpensive implementation, and user familiarity. However, they have the security and usability drawback of being typically difficult to remember, and they suffer from predictability if user-choice is allowed. This is because users tend to select weak passwords. Graphical passwords have been proposed on the premise that humans are better at retaining visual information. However, it is a relatively young area of research and the studies conducted have several limitations. First, there is a lack of comparison between the different types of graphical password schemes; and similarly, there have only been a limited number of studies comparing graphical and text-based schemes. Secondly, there have been few studies conducted in the environment of use which is necessary to enable realistic evaluations of the use of graphical passwords. Let us see in brief about the terms shoulder surfing and spyware.

1.1 Shoulder surfing:

In computer security, shoulder surfing refers to using direct observation techniques, such as looking over someone's shoulder, to get information. It is commonly used to obtain passwords, PINs, security codes, and similar data. Shoulder surfing is particularly effective in crowded places because it is relatively easy to observe someone as they: Fill out a form, enter their PIN at an automated teller machine, and enter a password at a cybercafé, public and university libraries, enter a code for a rented locker in a public place such as a swimming pool or airport. Shoulder surfing can also be done at a distance using binoculars or other vision-enhancing devices. Inexpensive, miniature closed-circuit television cameras can be concealed in ceilings, walls or fixtures to observe data entry.

1.2 Spyware:

Spyware is a type of malware that is installed on a computer without the knowledge of the owner in order to collect the owner's private information. Spyware is often hidden from the user in order to gather information about internet interaction, keystrokes (also known as key logging), passwords, and other valuable data. Spyware can also negatively affect a computer's performance by installing additional software, redirecting web browser searches, changing computer settings, reducing connection speeds, changing the homepage or even completely disrupting network connection ability.

In the propose system extended text and color based session password security is provide against shoulder surfing and spyware, Here we apply a wheel base structure to combine the enter password and the enhance work is to provide color combination with each character. the user is authenticated using session password. Session password is the password that is provided to authenticate the user for a session. and it will send via text message on his/her registered mobile number. Session password consists of two items, user text password and its color combination code. Session passwords are used only once.Everytime the users enters a session he has to input different password. Once the session is over that password becomes is of no use for next session and the current session gets terminated. Session password provide more security as every time the session start a new password is created and they are not prone to dictionary attacks ,brute force attacks and shoulder surfing attacks. Because of using wheel based structure, the user can easily and efficiently to login the system without using any physical keyboard or on-screen keyboard. It can be resistant to the key logger and mouse tracker spyware. The operation of the proposed scheme is simple and easy to learn for users familiar with textual passwords. The user can easily and efficiently to login the system.

II. LITERATURE SURVEY

Dhamija and Perrig [1] proposed a graphical authentication scheme based on the Hash Visualization technique In their system, the user is asked to select a certain number of images from a set of random pictures generated by a program. Later, the user will be required to identify the preselected Images in order to be authenticated. A weakness of this system is that the server needs to store the seeds of the portfolio images of each user in plain text. Also, the process of selecting a set of pictures from the picture database can be tedious and time consuming for the user.

Sobrado and Birget [2] developed a graphical password technique that deals with the shoulder surfing problem. In the first scheme, the system will display a number of pass-objects (pre-selected by user) among many other objects. To be authenticated, 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, Sobrado and Birget suggested using 1000 objects, which makes the display very crowded and the objects almost In distinguishable, but using fewer objects may lead to a smaller password space, since the resulting convex hull can be large. In their second algorithm, a user moves a frame (and the objects within it) until the pass object on the frame lines up with the other two pass objects. The authors also suggest repeating the process a few more times to minimize the likelihood of logging in by randomly clicking or rotating. The main drawback of these algorithms is that the login process can be slow.

Man, et al. [3] proposed another shoulder-surfing resistant algorithm. In this algorithm, a user selects a number of pictures as pass-objects. Each pass-object has several variants and each variant is assigned a unique code. During authentication, the user is challenged with several scenes. Each scene contains several pass-objects (each in the form of a randomly chosen variant) and many decoy-objects. The user has to type in a string with the unique codes corresponding to the pass-object variants present in the scene as well as a code indicating the relative location of the pass objects with reference to a pair of eyes. The argument is that it is very hard to crack this kind of password even if the whole authentication process is recorded on video because where is no mouse click to give away the pass-object information. However, this method still requires users to memorize the alphanumeric code for each pass-object variant. Hong, et al. [4] later extended this approach to allow the user to assign their own codes to pass-object variants. However, this method still forces the user to memorize many text strings and therefore suffer from the many drawbacks of text-based passwords.

Pass face is a technique developed by Real User Corporation [5]. The basic idea is as follows. The user will be asked to choose four images of human faces from a face database as their future password. In the authentication stage, the user sees a grid of nine faces, consisting of one face previously chosen by the user and eight decoy faces. The user recognizes and clicks anywhere on the known face. This procedure is repeated for several rounds. The user is authenticated if he/she correctly identifies the four faces. The technique is based on the assumption that people can recall human faces easier than other pictures. User studies by Valentine [8, 9] have shown that Pass faces are very memorable over long intervals. Comparative studies conducted by Brostoff and Sasses showed that Pass faces had only a third of the login failure rate of text-based passwords despite having about a third the frequency of use. Their study also showed that the Pass face-based log– in process took longer than text passwords and therefore was used less frequently by users. However the effectiveness of this method is still uncertain. Davis, et al. studied the graphical passwords created using the Pass face technique and found obvious patterns among these passwords. For example, most users tend to choose faces of people from the same race. This makes the Pass face password somewhat predictable. This problem may be alleviated by arbitrarily assigning faces to users, but doing so would make it hard for people to remember the password.

Jermyn, et al. [10] proposed a technique, called "Draw - a - secret (DAS)", which allows the user to draw their unique password. A user is asked to draw a simple picture on a 2D grid. The coordinates of the grids occupied by the picture are stored in the order of the drawing. During authentication, the user is asked to re-draw the picture. If the drawing touches the same grids in

the same sequence, then the user is authenticated. Jermyn, et al. suggested that given reasonable-length passwords in a 5 X 5 grid, the full password space of DAS is larger than that of the full text password space.

Sreelatha et al. [12] was introduced new a text-based shoulder surfing resistant graphical password scheme by using colors. In this 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. 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. Consider the ratings and 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. 3. The same method is followed for other pairs of colors. For figure 10 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. as the user has to additionally memorize the order of several colors, the memory burden of the user is high.

Yi-Lun Chen, Wei-Chi Ku*, Yu-Chang Yeh, and Dun-Min Liao el.al [13] propose an improved text-based shoulder surfing resistant graphical password scheme by using colors..This scheme used a circle composed of 8 equally sized sectors. The colors of the arcs of the 8 sectors are different The alphabet used in the propose scheme contains 64 characters, including 26 upper case letters, 26 lower case letters, 10 decimal digits, and symbols "." and "/". the circle was use for login instead of using physical or onscreen keyboard. This scheme was secure but complicated and tedidious.

III. OUR PROPOSAL

The graphical password is not widely deployed in real systems due to the problem of shoulder surfing and spyware. The other vulnerabilities of graphical passwords are still not fully understood. In this paper, we have suggested, a new technique called extended text and color based session password security against shoulder surfing and spyware .Here we apply a wheel base structure to combine the enter password and the enhance work is to provide color combination with each character. Wheel is divided into 8 sector containing 64 characters placed averagely and randomly among these 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. The alphabets used in the propose scheme contains 64 characters, including 26 upper case letters, 26 lower case letters, 10 decimal digits, and symbols "." and "_". The user is authenticated using session password. Session password is the password that is provided to authenticate the user for a session. And it will send via text message on his/her registered mobile number. Session password consists of two elements, user text password and its color combination code. Session passwords are used only once. Every time the user enters a session he has to input different password. Once the session is over that password becomes is of no use for next session and the current session gets terminated. Session password provide more security as every time the session start a new password is created and they are not prone to dictionary attacks ,brute force attacks and shoulder surfing attacks. Because of using wheel based structure, the user can easily and efficiently to login the system without using any physical keyboard or on-screen keyboard. It can be resistant to the key logger and mouse tracker spyware. The operation of the proposed scheme is simple and easy to learn for users familiar with textual passwords. The user can easily and efficiently to login the system. The proposed scheme involves two phases:

A. Registration Phase.
B. Login Phase.

A. Registration Phase.

During registration phase user register him/her self with credential like name, number, address, and password in provide manually with keyboard. User can be entering their textual password of fixed length i.e. six. And choose one color as his pass-color from 8 colors assigned by the system. The remaining 7 colors not chosen by the user are his decoy- colors. After registration successfully the randomly color combination sequence is generated as per textual password and it will send to the user via text massage and it will be use only one time login.

B. Login Phase.

During login phase the user requests to login the system, and the system displays a circle composed of 8 equally sized sectors initially, 64 characters with different color combination are placed averagely and randomly among these sectors. All the displayed characters and character colors can be simultaneously rotated into either the adjacent sector clockwise by clicking the "clockwise" button once or the adjacent sector anticlockwise by clicking the anticlockwise button once and the rotation operations can also be performed by scrolling the mouse wheel. User selects its password with color combination according to the text message they have received during registration. By rotating the circle clockwise or anticlockwise. If color and character matches then user will successfully login the system. If user enters wrong color character continuously three times then session will expire automatically. And get new password to user.

IV. WORKFLOW OF THE PROPOSED SCHEME

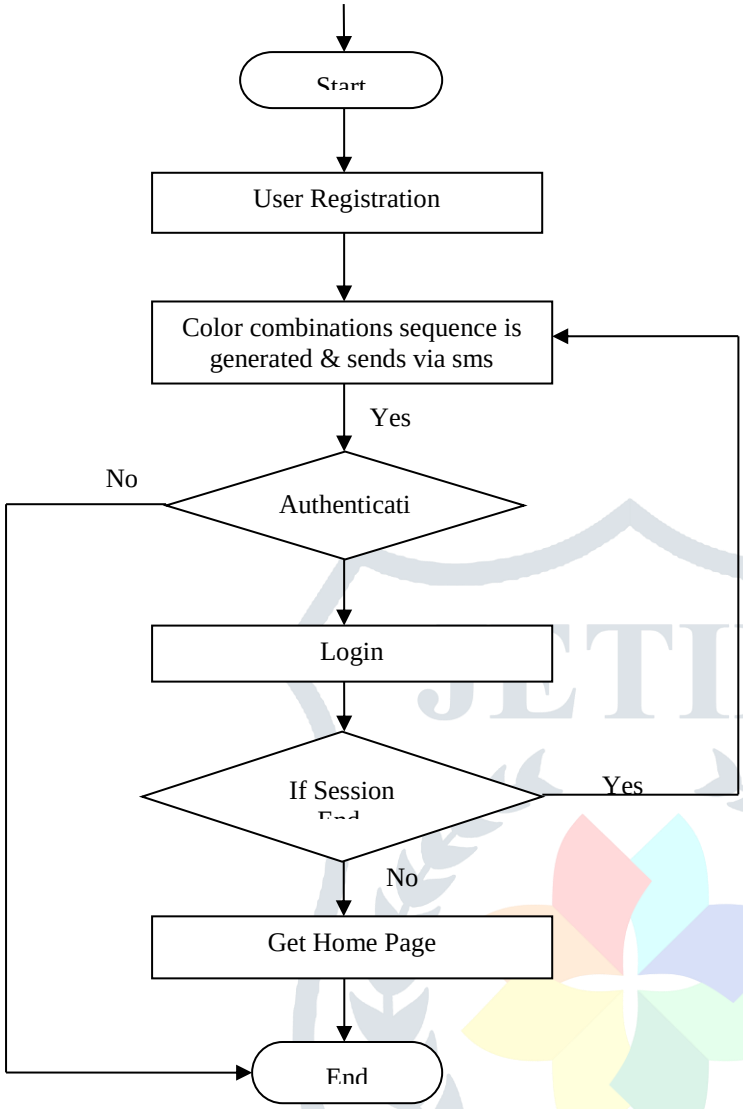

Figure. Working of Proposed scheme

V. CONCLUSION

This paper has introduced some graphical passwords techniques. The strengths and the weaknesses of either system were evaluated with special focus on the security and usability of each. One key factor that was noted in this paper is the critical need for further examination and testing of graphical password systems. This is especially important as passwords are used to secure more and more of our everyday computer systems. Security, especially cyber security is one of the major concerns of our time with access to sensitive information like personal records and banking details being secured by passwords, it is very critical that these passwords be as secure as possible whilst also being convenient for the user. Text-based passwords have been shown to have several usability challenges. It is therefore essential to develop alternatives to these passwords that can be more secure. Although the main argument for graphical passwords is that people are better at memorizing graphical passwords than text-based passwords, the existing user studies are very limited and there is not yet convincing evidence to support this argument. Our preliminary analysis suggests that it is more difficult to break graphical passwords using the traditional attack methods such as brute force search, dictionary attack, or spyware. However, since there is not yet wide deployment of graphical password systems, the vulnerabilities of graphical passwords are still not fully understood. Overall, the current graphical password techniques are still immature.

Much work can be done to improve the security of the system, and to validate its performance. to overcome the limitations in existing system this paper going to propose such a system which provide extended text and color based session password security against shoulder surfing and spyware. this system will generate session passwords and are resistant to dictionary attack, brute force attack and shoulder-surfing. Because of using wheel based structure at time of login. This will resistant to key logger and mouse tracker spyware .In the proposed system user can easily and efficiently complete the login process without worrying about shoulder surfing attacks and spyware. The operation of the proposed scheme will be simple and easy to learn for users familiar with textual passwords.

REFERENCES

[1] R. Dhamija, and A. Perrig. "Déjà Vu: A User Study Using Images for Authentication".
   a. In9th USENIX Security Symposium, 2000

[2] L. Sobrado and J.-C. Birget, "Graphical passwords, *"The Rutgers Scholar, An Electronic Bulletin for*

[3] 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. *Symposium*, 1999.

[4] D. Hong, S. Man, B. Hawes, and M. Mathews, "A password scheme strongly resistant to spyware," in *Proceedings of International conference on securitynand management*. Las Vergas, NV, 2004.

[5] Real User, "www.realuser.com," last accessed in June2005

[6] K. Gilhooly, "Biometrics: Getting Back to Business," in *Computerworld, May 09*, 2005.

[7] A. Jain, L. Hong, and S. Pankanti, "Biometric identification," *Communications of the ACM*, vol. 33,pp. 168-176, 2000.

[8] T. Valentine, "An evaluation of the Pass face personal authentication system," Technical Report, Goldsmiths College, University of London 1998.

[9] Valentine, "Memory for Pass faces after a Long Delay," Technical Report, Goldsmiths College, University of London 1999.

[10] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The Design and Analysis of Graphical Passwords," in *Proceedings of the 8th USENIX Security Symposium*, 1999.

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

[12] International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.3, May 2011

[13] IEEE 2nd International Symposium on Next-Generation Electronics (ISNE) - February 25-26 , Kaohsiung , Taiwan