A Survey on Shoulder Surfing Resistant Using Graphical Authentication Systems

Amale Chetashri[1], Jadhav Sneha[1], Jagdale Sushma[1], Sake Pradnya[1], Prof. Nirmal S. Suvarna[2]

B.E Student, Department of Computer Engineering, PREC, Loni, Ahmednagar, Maharashtra, India[1]

Asst. Professor, Department of Computer Engineering, PREC, Loni, Ahmednagar, Maharashtra, India[2]

ABSTRACT: Authentication based on passwords is used largely in applications for computer security and privacy. However, human actions such a choosing wrong passwords and inputted passwords in not secure way are regarded as" the weakest connection" in the authentication chain. Rather than arbitrary alphanumeric character, users tend to select a password either short or his name related for easy memorization. With web site applications and mobile phone apps charging up, peoples can get access these type of application anytime and anywhere with multiple devices. This evolution brings good convenience but also improves the probability of exposing passwords to shoulder surfingattacks. Attackers can observe directly or use external recording devices to collect users' credentials. To come this problem, we proposed a novel authentication system Pass Matrix, based on graphical passwords to resist shoulder surfing attacks. Many authentications methods are presented, but users are familiar with textual password method. Textual password methods are vulnerable to shoulder surfing andkey loggers. To come this problem many other authentication system like token based authentication, biometric bases authentication systems, graphical password methods have been proposed. However biometric bases authentication systems are costly and graphical password systems are not that secure and efficient.

KEYWORDS: Graphical Passwords, Authentication, Shoulder Surfing Attack.

I. INTRODUCTION

Shoulder surfing technique of gathering information such as usernames and passwords by watching over a person's shoulder while he/she logs into the system, by helping attackers to gain a access to the system. Key logging is the practice of noting the keys struck on keyboard, typically in manner so that person using the system keyboard is unaware that such action is monitored. There are two types of keyloggers viz. software key logger and hardware keylogger. Software keylogger are installed on the computer systems which usually are located between the OS and the keyboard hardware, and every keystroke is recorded.

Textual passwords have been the most widely used authentication method for decades. Comprised of numbers and upper- case and lower-case Alphabets, textual passwords are considered strong enough to resist against brute force attacks. However, a strong textual password is hard to memorize and recollect [1]. Therefore, users tend to choose passwords that are either short or from the dictionary, rather than random alphanumeric strings. Even worse, it is not a rare case that users may use only one username and password for multiple accounts [2]. According to an article in Computer world, a security team at a large company ran a network password cracker and surprisingly cracked approximately 80% of the employees' passwords within 30 seconds [3]. Textual passwords are often insecure due to the difficulty of maintaining strong ones. Various graphical password authentication schemes were developed to address the problems and weaknesses associated with textual passwords. Based on some studies such as those in, humans have a better ability to memorize images with long-term memory (LTM) than verbal representations. Image-based passwords were proved to be easier to recollect in several user studies. As a result, users can set up a complex authentication password and are capable of recollecting it after a long time even if the memory is not activated periodically. However, most of these image-based passwords are vulnerable to shoulder surfing attacks (SSAs). This type of attack either uses direct observation, such as watching over someone's shoulder or applies video capturing techniques to get passwords, PINs, or other sensitive personal information. The human actions such as choosing wrong passwords for new accounts and entering passwords in an not secure way for later logins are regarded as the weakest link in the authentication chain [4]. Therefore, an authentication scheme should be designed to overcome these

vulnerabilities. In this project, we purposed a secure graphical authentication system named PassMatrix that protects users from becoming victims of shoulder surfing attacks when inputting passwords in public through the usage of one-time login indicators. A login indicator is randomly generated for each pass-image and will be useless after the session terminates. The login indicator provides better security against shoulder surfing attacks, since users use a dynamic pointer to point out the position of their passwords rather than clicking on the password object directly.

The shoulder surfing attack in an attack that can beperformed by the adversary to obtain the user's passwordby watching over the user's shoulder as he enters hispassword. As conventional password schemes arevulnerable to shoulder surfing, Sobrado and Birget [1]proposed three shoulder surfing resistant graphicalpassword schemes. Since then, many graphical passwordschemes with different degrees of resistance to shouldersurfing have been proposed, e.g., [2][3]and each has its pros and cons. Seeing that most users aremore familiar with textual passwords than pure graphicalpasswords, Zhao et al. [10] proposed a text-based shouldersurfing resistant graphical password scheme, S3APS. InS3PAS, the user has to mix his textual password on thelogin screen to get the session password. However, thelogin process of Zhao et al.'s scheme is complex andtedious. And then, several textbased shoulder surfingresistant graphical password schemes have been proposed,e.g., [11]Unfortunately, none of existingtext-based shoulder surfing resistant graphical passwordschemes is both secure and efficient enough. In this paper,we will propose an improved text-based shoulder surfingresistant graphical password scheme by using colors. Theoperation of the proposed scheme is simple and easy tolearn for users familiar with textual passwords. The usercan easily and efficiently to login the system without usingany physical keyboard or on-screen keyboard.

II. LITERATURE SURVEY

In 2002, Sobrado and Birget [1] proposed three shouldersurfing resistant graphical password schemes, the Movable Frame scheme, the Intersection scheme, and the Trianglescheme. However, both the Movable Frame scheme and theIntersection scheme have high failure rate. In the Trianglescheme, the user has to choose and memorize several passionas his password. To login the system, the user has tocorrectly pass the predetermined number of challenges. Ineach challenge, the user has to find three pass-icons amonga set of randomly chosen icons displayed on the loginscreen, and then click inside the invisible triangle createdby those three pass-icons. In 2006, Wiedenbeck et al. [3]proposed the Convex Hull Click Scheme (CHC) as animproved version of the Triangle scheme with superiorsecurity and usability. To login the system, the user has tocorrectly respond several challenges. In each challenge, theuser has to find any three pass-icons displayed on the loginscreen, and then click inside the invisible convex hullformed by all the displayed pass-icons. However, the logintime of Convex-Hull Click scheme may be too long. In2009, Gao et al. [4] proposed a shoulder surfing resistantgraphical password scheme, ColorLogin, in which thebackground color is a usable factor for reducing the logintime. However, the probability of accidental login of Color Login is too high and the password space is too small.In 2009, Yamamoto et al. [9] proposed a shoulder surfing esistant graphical password scheme, TI-IBA, in whichicons are presented not only spatially but also temporally.TI-IBA is less constrained by the screen size and easier forthe user to find his pass-icons. Unfortunately, TI-IBA's resistance to accidental login is not strong. And, it may bedifficult for some users to find his pass-icons temporally displayed on the login screen. As most users are familiarwith textual passwords and conventional textual password authentication schemes have no shoulder surfing resistance,Zhao et al. [10], in 2007, proposed a text-based shoulder surfing resistant graphical password scheme, S3PAS, inwhich the user has to find his textual password and then follow a special rule to mix his textual password to get asession password to login the system. However, the login process of Zhao et al.'s scheme is complex and tedious.

Dhamija and Perrig proposed a graphical authentication scheme based on the HashVisualization technique. In their system, the user is asked to select a certain numberof images from a set of random pictures generated by a program. Later, the userwill be required to identify the preselected images in order to be authenticated. Theresults showed that 90 percentage of all participants succeeded in the authenticationusing this technique, while only 70percentage succeeded using text-based passwordsand PINS. The average log-in time, however, is longer than the traditional approach.A weakness of this system is that the server needs to store the seeds of the portfolioimages of each user in plain text. Also, the process of selecting a set of picturesfrom the picture database can be tedious and time consuming for the user.

Akula and Devisetty's algorithm [10] is similar to the technique proposed by Dhamijaand Perrig [4]. The difference is that by using hash function SHA-1, which produces a 20 byte output, the authentication is secure and require less

memory. The author's suggested a possible future improvement by providing persistent storage and thiscould be deployed on the Internet, cell phones and PDA's.

Weinshall and Kirkpatrick sketched several authentication schemes, such as picturerecognition, object recognition, and pseudo word recognition, and conducted a numberof user studies. In the picture recognition study, a user is trained to recognize a large set of images (100 to 200 images) selected from a database of 20,000 images.After one to three months, users in their study were able to recognize over 90 of theimages in the training set. This study showed that pictures are the most effectiveamong the three schemes tested. Pseudo codes can also be used, but require propersetting and training.

Sobrado and Birget developed a graphical password technique that deals with theshoulder surfing problem. In the first scheme, the system will display a number ofpass-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 allthe pass-objects. In order to make the password hard to guess, Sobrado and Birgetsuggested using 1000 objects, which makes the display very crowded and the objectsalmost indistinguishable, but using fewer objects may lead to a smaller passwordspace, since the resulting convex hull can be large. In their second algorithm, a usermoves a frame (and the objects within it) until the pass object on the frame linesup with the other two pass objects. The authors also suggest repeating the processa few more times to minimize the likelihood of logging in by randomly clicking orrotating. The main drawback of these algorithms is that the log in process can be slow.

"Passface" is a technique developed by Real User Corporation. The basic idea isas follows. The user will be asked to choose four images of human faces from a facedatabase as their future password. In the authentication stage, the user sees a gridof nine faces, consisting of one face previously chosen by the user and eight decoyfaces. The user recognizes and clicks anywhere on the known face. This procedure is

epeated for several rounds. The user is authenticated if he/she correctly identifiesthe four faces. The technique is based on the assumption that people can recallhuman faces easier than other pictures.

User studies by Valentine have shown that Passfaces are very memorable over longintervals. Comparative studies conducted by Brosto and Sasse showed that Passfaceshad only a third of the login failure rate of text-based passwords, despitehaving 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 usedless frequently by users. However the effectiveness of this method is still uncertain.

Paper studied the graphical passwords created using the Passface technique andfound obvious patterns among these passwords. For example, most users tendto choose faces of people from the same race. This makes the Passface passwordsomewhat predictable. This problem may be alleviated by arbitrarily assigning facesto users, but doing so would make it hard for people to remember the password. Jansen et al. [3,4] proposed a graphical password mechanism for mobile devices.During the enrolment stage, a user selects a theme (e.g. sea, cat, etc.) which consistsof thumbnail photos and then registers a sequence of images as a password.During the authentication, the user must enter the registered images in the correctsequence. One drawback of this technique is that since the number of thumb nail mages is limited to 30, the password space is small. Each thumbnail image is assigned a numerical value, and the sequence of selection will generate a numericalpassword. The result showed that the image sequence length was generally shorterthan the textural password length. To address this problem, two pictures can becombined to compose a new alphabet element, thus expanding the image alphabetsize. 10. Takada and Koike discussed a similar graphical password technique formobile devices. This technique allows users to use their favourite image for authentication.

III. **PORPOSED SYSTEM**

In PassMatrix, users choose one square per image for a sequence of n images rather than n squares in one image as that in the PassPoints scheme. Based on the user study of Cued Click Points. However, aiming at alleviating shoulder surfing attacks, we do not recommend this approach since the feedback that is given to users might also be obtained by attackers. Due to the fact that people do not register a new account or set up a new screen lock frequently, we assume that these setup events can be done in a safe environment rather than in public places. Thus, users can pick up pass-squares by simple touching at or clicking on them during the registration phase.
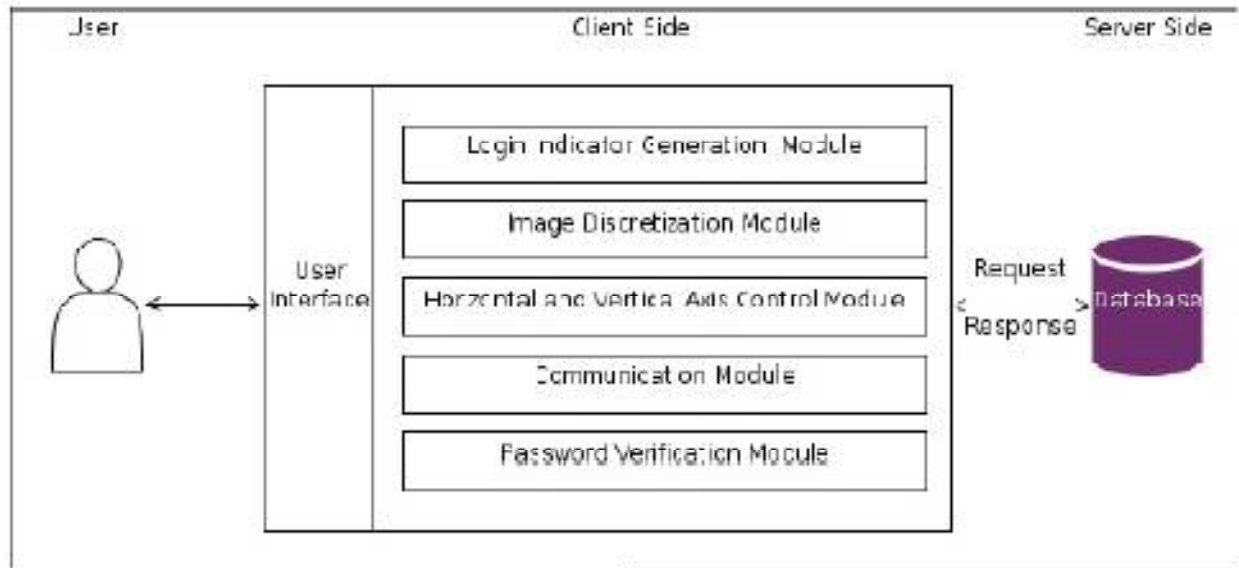
Fig. 1 System Architecture

IV. CONCLUSION

In this paper we have studied different methods for graphical password authentication scheme. we proposed a shoulder surfing resistant authentication system based on graphical passwords, named PassMatrix. Using a one-time login indicator per image, users can point out the location of their pass-square without directly clicking or touching it, which is an action vulnerable to shoulder surfing attacks. Because of the design of the horizontal and vertical bars that cover the entire pass-image, it offers no clue for attackers to narrow down the password space even if they have more than one login records of that account. Furthermore, we will implement a PassMatrix prototype on windows and carried out user experiments to evaluate the memorability and usability

REFERENCES

1. Xiaoyuan Suo, Ying Zhu G. Scott. Owen 2005, 'Graphical passwords: a survey',21st Annual Computer Security Applications Conference.
2. Zhi Li , Qibin Sun , Yong Lian , and D. D. Giusto , 2005, 'An Association –BasedGraphical Password Design Resistant to Shoulder-Surfing Attack', IEEE InternationalConference on Multimedia and Expo (ICME).
3. Julie Thrope, P. C. van Oorschot, Anil Somayaji, 2005, 'Pass - thoughts: authenticatingwith our minds', Proceedings of the 2005 workshop on New security paradigms,ACM.
4. Susan Wiedenbeck, Jim Waters, Leonardo Sobrado, Jean -Camille Birget, 2006,'Design and Evaluation of a Shoulder -Surfing Resistant Graphical PasswordScheme',Proceedings of Advanced Visual Interfaces (AVI2006).
5. Furkan, Tari, A. Ant Ozok, Stephen H. Holden, 2006, 'A comparison of perceived and real shoulder -surfing risks between alphanumeric and graphical passwords', Proceedingsof the second symposium on Usable privacy and security, ACM.
6. Di Lin, Paul Dunphy, Patrick Olivier, JeYan, 2007, 'Graphical password s & qualitativespatial relations',Proceedings of the 3rd symposium on Usable privacy andsecurity, ACM.
7. Manu Kumar, Tal Garnkel, Dan Boneh, Terry Winograd, 2007, 'Reducing shoulder surfing by using gaze -based password entry',Proceedings of the 3rd s ymposiumonUsable privacy and security, ACM.
8. Cheryl, Hinds and Chinedu Ekwueme, 2007, 'Increasing security and usability ofcomputer systems with graphical passwords',Proceedings of the 45th annual southeastregional conference, ACM.
9. Huanyu Zhao a nd Xiaolin Li , 2007, 'S3PAS: A Scalable Shoulder - Surfing ResistantTextual -Graphical Password Authentication Scheme', 21st International Conferenceon Advanced Information Networking and Applications Workshops (AINAW).
10. Saranga Komanduri and Dugald R. Hutchings, 2008, 'Order and entropy in picturepasswords', Proceedings of graphics interface, Canadian Information ProcessingSociety.
11. Paul Dunphy, James Nicholson, Patrick Oliver,2008, 'Securing passfaces for description',Proceedings of the 4th symp osium on Usable and security, ACM.