OPEN ACCESS INTERNATIONAL JOURNAL OF SCIENCE & ENGINEERING

A SURVEY ON SHOULDER SURFING RESISTANT GRAPHICAL AUTHENTICATION SYSTEMS

Mr. Shanteshwar Bhagwan Khankare[1], Prof. Manisha Singh[2]

PG Students Department of Computer Engineering, Dhole Patil College of Engineering, Wagholi, Near Eon IT park, Pune-412207, Maharashtra, India[1]

Assistant Professor, Department of Computer Engineering, Dhole Patil College of Engineering, Wagholi, Near Eon IT park., Pune-412207, Maharashtra, India[2]

Abstract: Authentication dependent on passwords is utilized generally in applications for PC security and protection. In any case, human activities such a picking incorrectly passwords and inputted passwords in not secure way are viewed as" the weakest connection" in the validation chain. Otherwise self-assertive alphanumeric character, clients have a tendency to choose a secret word either short or his name related for simple memorization. With site applications and cell phone applications energizing, people groups can get to these kind of use whenever and anyplace with numerous gadgets. This advancement brings great accommodation yet in addition enhances the probability of presenting passwords to shoulder surfing attacks. Attackers can watch specifically or utilize outer account gadgets to gather clients' credentials. To come this issue, This paper presents a novel authentication framework Pass Matrix, based on graphical passwords to oppose shoulder surfing attacks. Numerous authentication strategies are displayed, however clients know about textual password technique. Textual password techniques are powerless against shoulder surfing and key loggers. To come this issue numerous other authentication framework like token based authentication, biometric bases authentication frameworks, graphical password strategies have been presented. Anyway biometric bases authentication frameworks are expensive and graphical password frameworks are not excessively secure and proficient.

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 key loggers viz. software key logger and hardware key logger. Software key logger 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, 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.

II LITERATURE SURVEY

2.1 In 2013, Ahmed Al-Haiqi, Mahamod Ismail, Rosdiadee Nordin[3] takes further steps along the path of exploring the aspects of the new threat, addressing the question of which available sensors can perform best in the context of the inference attack. Design and implement a benchmark experiment, against which the performances of several commodity smartphone-sensors are compared, in terms of inference accuracy. All available Android motion sensors are considered through different settings provided by the OS, and we add the option of fusing several sensors input into a single dataset, to examine the amount/lack of improvement in the attack accuracy. The results indicate an outstanding performance of the gyroscope sensor, and the potential improvement obtained out of sensors data fusion. On the other hand, it seems that sensors with magnetometer component or the accelerometer alone have less benefit in the adverted attack.

2.2 In 2009, Gao et al. [4] proposed a shoulder surfing resistant graphical password scheme, Color Login, in which the background color is a usable factor for reducing the login time. However, the probability of accidental login of Color Login is too high and the password space is too small.

2.3 In 2009, Yamamoto et al. [9] proposed a shoulder surfing resistant graphical password scheme, TI-IBA, in which icons are presented not only spatially but also temporally. TI-IBA is less constrained by the screen size and easier for the user to find his pass-icons. Unfortunately, TI-IBA's resistance to accidental login is not strong. And, it may be difficult for some users to find his pass-icons temporally displayed on the login screen. As most users are familiar with textual passwords and conventional textual password authentication schemes have no shoulder surfing resistance,

2.4 Zhao et al. [10], in 2007, proposed a text-based shoulder surfing resistant graphical password scheme, S3PAS, in which the user has to find his textual password and then follow a special rule to mix his textual password to get a session password to login the system. However, the login process of Zhao et al.'s scheme is complex and tedious.

2.5 Akula and Devisetty's algorithm [10] is similar to the technique proposed by Dhamija and 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 this could be deployed on the Internet, cell phones and PDA's.

2.6 Weinshall and Kirkpatrick sketched several authentication schemes, such as picture recognition, object recognition, and pseudo word recognition, and conducted a number of 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 the images in the training set. This study showed that pictures are the most effective among the three schemes tested. Pseudo codes can also be used, but require proper setting and training.

2.7 Sobra do and Bir get 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, So bra do and Birget suggested using 1000 objects, which makes 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. 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 log in process can be slow.

2.8 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 consists of thumbnail photos and then registers a sequence of images as a password. During the authentication, the user must enter the registered images in the corrects sequence. 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 numerical password. The result showed that the image sequence length was generally shorter than the textural password length. To address this problem, two pictures can be combined to compose a new alphabet element, thus expanding the image alphabet size. 10. Takada and Koike discussed a similar graphical password technique for mobile devices. This technique allows users to use their favourite image for authentication.

III TECHNIQUES USED

3.1 "Pass face" is a technique developed by Real User Corporation. 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 have shown that Pass faces are very memorable over long intervals. Comparative studies conducted by Brosto and Sasse showed that Pass face shad 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 useless frequently by users. However the effectiveness of this method is still uncertain. Paper 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.

3.2 “PassMatrix”, users choose one square per image for a sequence of n images rather than n squares in one image as that in the Pass Points 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.

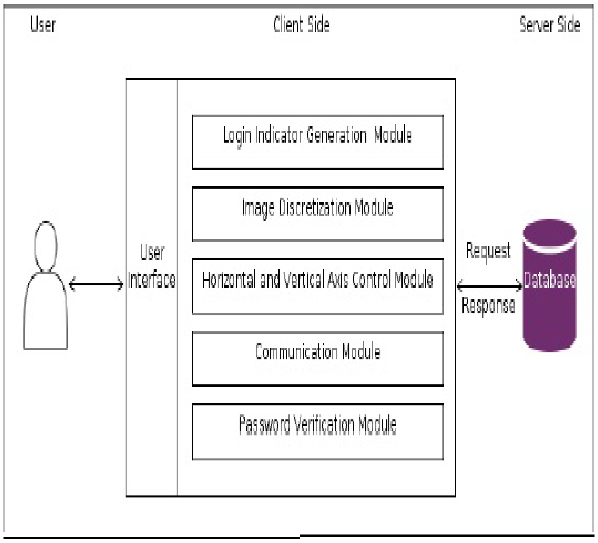
User
Client Side
Server Side
Login Indicator Generation Module
Image Discretization Module
Horizontal and Vertical Axis Control Module
Communication Module
Password Verification Module
User Interface
Request
Response
Database

Figure 1 System Architecture

IV RESULTS

This paper analysed the collected data from experiments and surveys to evaluate the effectiveness of the presented system. The results are presented in two perspectives: accuracy and usability. The accuracy perspective focuses on the successful login rates in both sessions, including the practice logins. The usability perspective is measured by the amount of time users spent in each PassMatrix phase. The results of these two analyses strongly suggested that PassMatrix is practical to use. Also the statistics of the survey data from participants about their personal background and user experience on smart phones and PassMatrix are presented.

4.1 Accuracy

In the practice phase of the first session, participants practiced the login process on an average of 4 times ranging from 1 to 14 (excluding one outlier) and then moved onto the authentication (login) phase. As defined, participants can keep trying to log in to their account until they have failed six times. In other words, a successful attempt means that a user, in less than or equal to six tries, is able to pass the authentication with a correct password. If all six tries failed, this attempt will be marked as failure. Below, define two terms First Accuracy and

Total Accuracy that were used in experiment:

$$\text{First Accuracy} \quad \frac{= Successful\ attempts\ in\ first\ Tr}{Total\ attempts} \quad ....(I)$$

$$\text{Total Accuracy} = \quad \frac{Successful\ attemp}{Total\ attempts} \quad ....(II)$$

	First session		Second Session	
	First	Total	First	Total
Practice Phase	60.00%	100%	-	-
Login Phase	86.67%	100%	66.67%	93.33%

Table 1. The accuracy of practice/authentication(login) in two sessions

4.2 Usability

In this paper counted the number of shifts and the elapsed time per pass-image in experiment to measure the usability of our PassMatrix in practice.

	Registration(1st)		
	Mean	Median	S.D
Total Time(s)	106.6	90.5	55.58

Table 2. The mean, median and standard deviation of total time in the registration phase

CONCLUSION

In this paper studied different methods for graphical password authentication scheme. It presented 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, system 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 –Based Graphical Password Design Resistant to Shoulder-Surfing Attack', IEEE International Conference on Multimedia and Expo (ICME).
3. Ahmed Al-Haiqi, Mahamod Ismail, Rosdiadee Nordin, ‘On the Best Sensor for Keystrokes Inference Attack on Android’, The 4th International Conference on Electrical Engineering and Informatics (ICEEI 2013).
4. Julie Thrope, P. C. van Oorschot, Anil Somayaji, 2005, 'Pass - thoughts: authenticating with our minds', Proceedings of the 2005 workshop on New security paradigms, ACM.
5. Susan Wieden beck, Jim Waters, Leonardo So brado, Jean - Camille Birget, 2006, 'Design and Evaluation of a Shoulder -Surfing Resistant Graphical Password Scheme', Proceedings of Advanced Visual Interfaces (AVI2006).
6. Furkan, Tari, A. Ant Ozok, Stephen H. Holden, 2006, 'A comparison of perceived and real shoulder -surfing risks between alphanumeric and graphical passwords', Proceedings of the second symposium on Usable privacy and security, ACM.
7. Di Lin, Paul Dunphy, Patrick Olivier, JeYan, 2007, 'Graphical password s & qualitative spatial relations', Proceedings of the 3rd symposium on Usable privacy and security, ACM.
8. Manu Kumar, Tal Garnkel, Dan Boneh, Terry Winog rad, 2007, 'Reducing shoulder surfing by using gaze -based password entry', Proceedings of the 3rd symposium on Usable privacy and security, ACM.
9. Cheryl, Hinds and Chinedu Ekwueme, 2007, 'Increasing security and usability of computer systems with graphical passwords', Proceedings of the 45th annual south east regional conference, ACM.
10. Huanyu Zhao a nd Xiaolin Li , 2007, 'S3PAS: A Scalable Shoulder - Surfing Resistant Textual -Graphical Password Authentication Scheme', 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW).
11. Saranga Komanduri and Dugald R. Hutchings, 2008, 'Order and entropy in picture passwords', Proceedings of graphics interface, Canadian Information Processing Society.
12. Paul Dunphy, James Nicholson, Patrick Oliver,2008, 'Securing pass faces for description', Proceedings of the 4th symposium on Usable and security, ACM.