Image Authentication System using PassMatrix

Mane Komal[1], Lagad Sagar[2], Bhise Krushna[3], Hirave Kanifnath[4]

[1-4]Dept. of Computer Engineering, H.S.B.P.V.T College of Engineering, Kashti

---***---

Abstract: *Passwords are commonly used to provide security. Users normally choose a passwords is either short or meaningful for easy memorization. With a web applications and mobile apps are increasing nowadays people can access these applications anytime and anywhere with various devices. This evolution leads to great convenience but also increases the probability of exposing passwords to shoulder surfing attacks. Attackers can observe directly or use external recording devices to collect user's credentials. To overcome this problem, PassMatrix authentication system based on graphical passwords is used to resist shoulder surfing attacks. With a one -time valid login indicator and circulative horizontal and vertical bars covering the entire scope of pass-images. The prototype of PassMatrix system is also implemented on android to carry out the experimental result. Experimental result shows better resistance to shoulder surfing attack while maintaining usability.*

Keywords: Authentication, Graphical passwords, Security, Shoulder Surfing Attack, Accuracy.

I. INTRODUCTION

Textual password is a common method for authentication. It consists of upper- case, lowercase letters, numbers and special characters, though, a strong textual password is hard to memorize and recollect. Therefore, users always choose meaningful and short passwords rather than random alphanumeric strings. According to an article in Computer world, a security team at a large company ran a network password cracker and surprisingly cracked approximately 80 percent of the employee's passwords within 30 seconds. Textual passwords are often insecure due to the difficulty of maintaining strong ones. Textual passwords are often insecure due to the difficulty of maintaining strong ones. Humans have a better ability to memorize images with long-term memory (LTM) than verbal representations [22].

Different graphical password authentication schemes [2], [4], [5] were developed to address the problems and weaknesses associated with textual passwords. 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 onetime login indicators [1]. A login indicator is randomly generated for each pass-image and will be useless after the session terminates. Image based passwords were proved to be easier to recollect in several user studies [2] [18] [21]. 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 some ones shoulder or applies video capturing techniques to get passwords, PINs, or other sensitive personal information.

1.1 Goals and Objective

- To perform authentication in public using PassMatrix, to reduce shoulder surfing attack
- To efficiently perform graphical password authentication scheme applicable to all devices.

1.2 Motivation

In 2006, Wiedenbeck et al. proposed PassPoints in which the user picks up several points (2 to 4) in an image during the password creation phase and re- enters each of these preselected clickpoints in a correct order within its tolerant square during the login phase. Comparing to traditional PIN and textual passwords, the PassPoints scheme substantially increases the password space and enhances password memorability. Unfortunately, this graphical authentication scheme is vulnerable to shoulder surfing attacks. Hence, based on the PassPoints, the idea of using onetime session passwords and distractors is used to develop PassMatrix authentication system that is resistant to shoulder surfing attacks.

II. REVIEW OF LITERATURE

In 2004, Roth et al. [23] represented an approach for PIN entry against shoulder surfing attacks by increasing the noise to observers. In their approach, the PIN digits are displayed in either black or white randomly in each round. The user must respond to the system by identifying the color for each password digit. After the user has made a series of binary choices (black or white), the system can figure out the PIN number the user intended to enter by intersecting the user's choices. This approach could confuse the observers if they just watch the screen without any help of video capturing devices. However, if observers are able to capture the whole authentication process, the passwords can be cracked easily.

In 2005, Susan Wiedenbeck introduced a graphical authentication scheme PassPoints, and at that time, handheld devices could already show high resolution color pictures. In addition to graphical authentication schemes, there was some research on the extension of conventional personal identification number (PIN) entry authentication systems [24]. PassBYOP is a new graphical authentication system,in which user presents image to a system camera and then enter their password as a sequence of selections on live video of the token. Highly distinctive optical features are extracted from these selections and used as the password. They present three feasibility studies of PassBYOP examining its reliability, usability, and security shoulder surfing attack [2].

The SpyResistant Keyboard, a novel interface that allows users to enter private text without revealing it to an observer. The keyboard looks like an on screen keyboard. A user study has been conducted, based on the study, user requires more time to enter the password but prevent from observation attack [3].

A system that mitigates the issues of shoulder surfing via a novel approach to user input. With EyePassword, a user enters sensitive input (password, PIN, etc.) by selecting from an onscreen keyboard using only the orientation of their pupils (i.e. the position of their gaze on screen), making eavesdropping by a malicious observer largely impractical. They have presented a number of design choices and discuss their effect on usability and security. They conducted user studies to evaluate the speed, accuracy and user acceptance of our Scalable Shoulder Surfing Resistant Textual Graphical Password Authentication Scheme (S3PAS), combines both graphical and textual password schemes and provides perfect resistant to shoulder surfing, hidden camera and spyware attacks. It can replace with conventional textual password systems without changing existing user password profiles. It shows significant potential bridging the gap between conventional textual password and graphical password. [5].

A new secure authentication scheme called Predicate based Authentication Service (PAS). In this scheme, for the first time, the concept of a predicate is introduced for authentication. They conduct analysis on the proposed scheme and implement its prototype system. Their analytical data and experimental data illustrate that the PAS scheme can achieve a desired level of security and user friendliness [6].

III. SYSTEM ARCHITECTURE

3.1. Registration phase:

1. The user creates an account which contains a username and a password.

2. The password consists of only one pass-square per image for a sequence of n images.

The number of images (i.e., n) is decided by the user after considering the tradeoff between security and usability of the system.

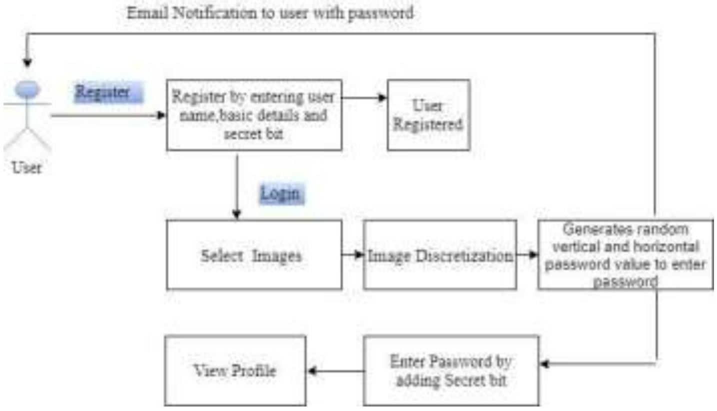
Email Notification to user with password
Register
User
Register by entering user name,basic details and secret bit
User Registered
Login
Select Images
Image Discretization
Generates random vertical and horizontal password value to enter password
View Profile
Enter Password by adding Secret bit

Fig. 1. System Architecture

3. The only purpose of the username is to give the user an imagination of having a personal account.

4. The username can be omitted if PassMatrix is applied to authentication systems like screen lock.

5. The user can either choose images from a provided list or upload images from their device as pass-images.

6. Then the user will pick a pass-square for each selected pass-image from the grid, which was divided by the image discretization module.
7. The user repeats this step until the password is set.

3.2 Authentication phase:

The user uses his/her username, password and login indicators to log into PassMatrix. The following describes all the steps in detail:

1. The user inputs his/her username which was created in the registration phase.

2. A new indicator comprised of a letter and a number is created by the login indicator generator module. The indicator will be shown when the user uses his/her hand to form a circle and then touch the screen. In this case, the indicator is conveyed to the user by visual feedback. The indicator can be delivered to user by email.

Next, the first pass-image will be shown on the display, with a horizontal bar and a vertical baron its top and left respectively. To respond to the challenge, the user flings or drags the bars to align the pre-selected pass-square of the image with the login indicator. For example, if the indicator is (E,11) and the pass-square is at (5, 7) in the grid of the image, the user shifts the character E to the 5th column on the horizontal bar and 11 to the 7th row on the vertical bar.
Repeat step 2 and step 3 for each preselected passimage.

The communication module gets user account information from the server through HttpRequest and POSTmethod.

Finally, for each image, the password verification module verifies the alignment between the passsquare and the login indicator. Only if all the alignments are correct in all images, the user is allowed to log into PassMatrix.

IV. PASS MATRIX

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. PassMatrix is composed of the following components.

- Image Discretization Module
- Horizontal and Vertical Axis Control Module
- Login Indicator generator Module
- Communication Module
- Password Verification Module
- Database
- Secret bit

4.1. Image Discretization Module:

This module divides each image into squares, from which users would choose one as the pass-square. As shown in Figure 1, an image is divided into a 7 * 11 grid. The smaller the image is discretized, the larger the password space is. However, the overly concentrated division may result in recognition problem of specific objects and increase the difficulty of user interface operations on palm-sized mobile devices

4.2 Login Indicator Generator Module:

This module generates a login indicator consisting of several distinguishable characters , such as alphabets and numbers or visual materials, such as colors and icons for users during the authentication phase. In the implementation, the characters A to G and 1 to 11 for a 7*11 grid. Both letters and numbers are generated randomly and therefore a different login indicator will be provided each time the module is called. The generated login indicator can be given to users visually or acoustically for sending this patterns on users email.

4.3. Horizontal and Vertical Axis Control Module:

There are two scroll bars: a horizontal bar with a sequence of letters and a vertical bar with a sequence of numbers.

4.4. Communication Module:

This module is in charge of all the information transmitted between the client devices and the authentication server. Any communication is protected by SSL (Secure Socket Layer) protocol and thus, is safe from being eavesdropped and intercepted.

4.5 Password Verification Module:

This module verifies the user password during the authentication phase. A pass Horizontal scroll bar and vertical bar square acts similar to a password digit in the text-based password system. The user is authenticated only if each pass-square in each pass-image is correctly aligned with the login indicator.

4.6 Database:

The database server contains several tables that store user accounts, passwords (positions of pass-squares), and the time duration. PassMatrix has all the required privileges to perform operations like insert, modify, delete and search.

4.7 Secret bit:

This is single digit number which is choosen by user while registering this number is not displayed anywhere to user it stored by system internally to recognize the user. User needs to remember the secret bit and add that secret bit to his existing system generated password.

V. RESULTS

Questionnaire responses scores are 1 to 5

Questions	Mean	Median
Some information is exposed when authenticating in public.	4.5	4
I would have serious loss if my passwords were cracked.	4.5	4
PassMatrix can protect my passwords from beinga ttacked by SSA.	4.4	4
Compared to text passwords and PIN, PassMatrix is more secure.	4.5	4
PassMatrix is secure and trustable.	4.5	4
It's easy and fast to create an account in Pass- Matrix.	4.5	4
In general, PassMatrix is a user-friendly system and is easy to use.	4.5	4
The time consumed for using PassMatrix is acceptable.	4.3	4
I tend to choose squares that are eye- catching.	3	3
I tend to choose squares that areobtrusive.	2	2

Table 1: Questionnaires

Table 1 shows all the questions with their mean and median scores. As the result shows, participants felt it is insecure to use traditional text passwords or PIN methods, and they believed that using PassMatrix to log in can protect their passwords from being shoulder surfing attacked. For the user experience on PassMatrix, the mean scores of the series of questions are high, ranging from 3 to 4.5. All participants agreed that PassMatrix is easy to use and the majority of them (95.00%) considered the time spent (or in other words, complexity) for the PassMatrix's login process is acceptable. For an in-depth investigation at the number of pass-images users may accept in different authentication scenarios, see Figure 2, we found out that users tended to set only one pass-image as their password for screen lock in their mobile phones, 2 to 3 for OS user login and e-mail service login, and 3 to 5 for bank accounts.

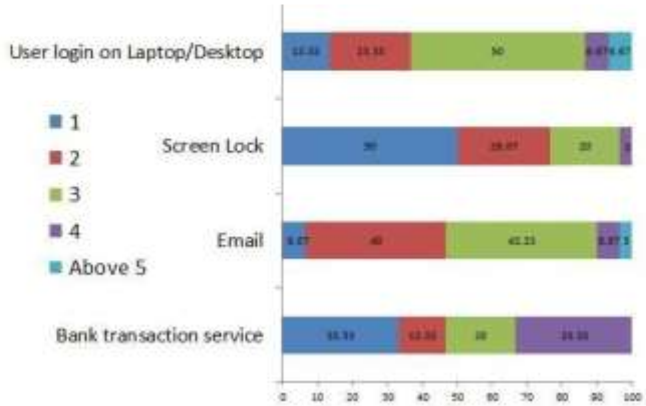

Fig.2 Number of Pass Images Selected for Different Authentication Scenario.

There are two parameters to evaluate effectiveness of proposed system : Accuracy and Usability

5.1 Accuracy

$$\text{First Accuracy (FA)} = \frac{\textit{Successful attempts in first try}}{\textit{total attempts}}$$

$$\text{Total Accuracy (TA)} = \frac{\textit{Successful attempts}}{\textit{Total attempts}}$$

- Successful attempts in first try = 3

- Total attempts = 5

- Successful attempts = 4

- Total attempts = 5

- FA = 3 / 5 = 0.60

- TA = 4/ 5 = 0.80

5.2 Usability – Time required to login to the system.

The total time required to log into PassMatrix with an average of 2-3 pass-images is between 30 and 50 seconds.

5.3 Security Analysis

	Login	Login(After 2 weeks)
Time(Seconds)	30 Seconds	40-50 seconds

Table 2: Time required to login

To evaluate the security of the proposed authentication system against three types of attacks: random guess attack, shoulder surfing attack, and smudge attack.

5.3.1 Random Guess attack

To perform a random guess attack, the attacker randomly tries each square as a possible pass-square for each passimage until a successful login occurs. The key security determinants of the system are the number of pass-images and the degree of discretization of each image. To quantify the security of PassMatrix against random guess attacks, the entropy of a password space as in equation. Table 3 defines the notations used in the equation. If the entropy of a password space is k bits, there will be 2k possible passwords in that space

Entropy-

$$\log_2(Dx \ \times Dy)i)^{\wedge}n$$

Notation	Definition
Dx	The number of partitions in x-direction
Dy	The number of partitions in y-direction
i=1	Obtain login indicators by email OTP
i=2	Obtain login indicators by predefined images
N	The number of pass-images set by user

Table 3: Notations use in Entropy

Table 4: Entropy bits of PassMatrix vs.text passwords and PIN from 1 to 5 pass-images(1-5 click points)

n: No.of Pass Images			1	2	3	4	5
PassMatrix		Type1	6.27	12.53	18.80	25.07	31.33
		Type2	12.53	25.07	37.60	50.13	62.67
	32	Type1	9.32	18.64	27.97	37.29	46.61
		Type2	18.64	37.29	55.93	74.58	93.22
Text Passwords			6.57	13.14	19.71	26.28	32.85
PIN			3.32	6.64	9.97	13.29	16.61

5.3.2 Shoulder Surfing Attack

The shoulder surfing attack is harmful to authentication systems with either textual or graphical passwords, many novel authentication schemes were proposed to protect systems from this attack. Unfortunately, most of them were unsuccessful to alleviate the threat if the shoulder-surfing attack is camera-based. Some of the examples are PIN-entry method and spy-resistant keyboard [3] were designed based on the difficulties of short-term memory. Camera-based shoulder surfing attacks can easily crack the passwords of these schemes.

The password spaces of other schemes such as those in CAPTCHA-based method [8], Pass-icons[18] and Color-rings can be narrowed down by camera-based shoulder surfing attacks. The proposed authentication system PassMatrix takes full advantage of adding extra information to complicate the login process, using an approach to point out the locations of pass- squares implicitly instead of typing or clicking on password objects directly. The password space will not be narrowed down even if the whole authentication process is recorded by attackers. The login indicator for each pass-image is different. Thus, no pattern can be extracted from a set of pass-images in an authentication trial, neither from multiple login processes. With the above security features, PassMatrix should be strong enough to resist shoulder surfing attacks, even if the attacks are camera- equipped.

5.3.3 Smudge Attack

The smudge attack relies on detecting the oily smudges left behind by the user's fingers when operating the device using simple cameras and image processing software. Under proper lighting and camera settings, the finger smudges can be easily detected, and the heaviest smudges can be used to infer the most frequent user input pattern (the password), but in the PassMatrix system both the horizontal and vertical bars are easily shuffled and each time the pass value is different from previous one. Therefore proposed system is protected from smudge attack.

VI. Conclusion

A shoulder surfing resistant authentication system based on graphical passwords named as PassMatrix. Using a one-time login indicator per image from the set of images, users can easily point out the location of their pass-square without directly clicking or touching it. Because of the design of the horizontal and vertical bars that cover the entire pass-image, it offers no clue for attackers to write down the password space even if they have more than one login records of that account. Adding a single digit number which is choosen by user while registering provides more security, if attacker hacks user's mail and get the login indicator value, he/she doesn't know that user is adding a secret number to original value.

Acknowledgement

I wish to thank all the people who gave us an unending support right from the idea was conceived. I express my sincere and profound thanks to my Guide Prof.Hirave Kanifnath and Head of the Department Prof.Hiranwale S.B for their guidance and motivation for completing my work, and I am also thankful to all those who directly or indirectly guided and helped me in preparation of this paper.

References

1. Hung-Min Sun, Shiuan-Tung Chen,"A Shoulder Surfing Resistant Graphical Authentication System", 1545-5971 ,2015 IEEE.
2. Andrea Bianchi, Ian Oakley, and Hyoung shick Kim, PassBYOP: Bring Your Own Picture for Securing Graphical Passwords, 2168-2291,IEEE-2015
3. D. Tan, P. Keyani, and M. Czerwinski, Spy-resistant keyboard: Towards more secure password entry on publicly observable touch screens, in Proceedings of OZCHIComputer- Human Interaction Special Interest Group (CHISIG) of Australia. Canberra, Australia: ACM Press. Citeseer, 2005.
4. M. Kumar, T. Garfinkel, D. Boneh, and T. Winograd, Reducing shoulder-surfing by using gaze-based password entry, in Proceedings of the 3rd symposium on Usable privacy and security. ACM, 2007, pp. 1319.
5. H. Zhao and X. Li, S3pas: A scalable shoulder-surfing resistant textual-graphical password authentication scheme, in Advanced Information Networking and Applications Workshops, 2007. AINAW07. 21st International Conference on, vol. 2. IEEE, 2007, pp. 467472
6. Xiaole Bai , Wenjun Gu, PAS: Predicate-based Authentication Services Against Powerful Passive Adversaries,2008.
7. Z. Zheng, X. Liu, L. Yin, and Z. Liu, A stroke-based textual password authentication scheme, in Education Technology and Computer Science, 2009. ETCS09. First International Workshop on, vol. 3. IEEE, 2009, pp. 9095.
8. L. Wang, X. Chang, Z. Ren, H. Gao, X. Liu, and U. Aickelin, "Against spyware using captcha in graphical password scheme", in 2010 24th IEEE International Conference on Advanced Information Networking and Applications. IEEE, 2010, pp. 760767.
9. D. Kim, P. Dunphy, P. Briggs, J. Hook, J. Nicholson, J. Nicholson, and P. Olivier, Multitouch authentication on tabletops, in Proceedings of the 28th international conference on Human factors in computing systems. ACM, 2010, pp. 10931102.
10. E. von Zezschwitz, A. De Luca, and H. Hussmann, Honey, i shrunk the keys: Influences of mobile devices on password composition and authentication performance, in Proceedings of the 8th Nordic Conference on Human-Computer Interaction: Fun, Fast, Foundational, ser. NordiCHI 14. New York, NY, USA: ACM, 2014, pp. 461470.
11. A. Bianchi, I. Oakley, V. Kostakos, and D. S. Kwon, The phone lock: Audio and haptic shoulder-surfing resistant pin entry methods for mobile devices, in Proceedings of the Fifth International Conference on Tangible, Embedded, and Embodied Interaction, ser. TEI 11. New York, NY, USA: ACM, 2011, pp. 197200.
12. A. Bianchi, I. Oakley, and D. S. Kwon, The secure haptic keypad: A tactile password system, in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ser. CHI 10. New York, NY, USA: ACM, 2010, pp. 10891092.
13. S. Sood, A. Sarje, and K. Singh, Cryptanalysis of password authenti-cation schemes: Current status and key issues, in Methods and Models in Computer Science, 2009. ICM2CS 2009. Proceeding of International Conference on, Dec 2009, pp. 17.
14. S. Gurav, L. Gawade, P. Rane, and N. Khochare, Graphical password authentication: Cloud securing scheme, in Electronic Systems, Signal Processing and Computing Technologies (ICESC), 2014 International Conference on, Jan 2014, pp. 479483.
15. A. Paivio, T. Rogers, and P. Smythe, Why are pictures easier to recall than words? Psychonomic Science, 1968.
16. J. Long and K. Mitnick, No Tech Hacking: A Guide to Social Engineer-ing, Dumpster Diving, and Shoulder Surfing. Elsevier Science, 2011.
17. T. Takada, fakepointer: An authentication scheme for improving security against peeping attacks using video

cameras, in Mobile Ubiquitous Computing, Systems, Services and Technologies, 2008. UBICOMM 08. The Second International Conference on. IEEE, 2008, pp. 395400.

18. S. Wiedenbeck, J. Waters, L. Sobrado, and J.-C. Birget, Design and evaluation of a shoulder-surfing resistant graphical password scheme, in Proceedings of the working conference on Advanced visual interfaces, ser. AVI 06. New York, NY, USA: ACM, 2006, pp. 177 184.
19. B. Laxton, K. Wang, and S. Savage, Reconsidering physical key secrecy: Teleduplication via optical decoding, in Proceedings of the 15th ACM conference on Computer and communications security. ACM, 2008, pp. 469478.
20. L. Li, L. Zhong, Z. Yang, and M. Kitsuregawa, Qubic: An adaptive approach to query based recommendation, J. Intell. Inf. Syst., vol. 40, no. 3, pp. 555587, Jun. 2013.