ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 6, June 2017

Resisting Shoulder Surfing Attacks Using Secured Graphical Pass Matrix Authentication Scheme

[1] Rashmi B.K, [2] Manisha Singh, [3] Mranali Gupta, [4] Surya R, [5] Sushmitha Narayan
[1] Asst. Prof. Dept. of CSE, RRIT, B'lore-90, Karnataka
[2][3][4][5] UG Students, Dept. of CSE, RRIT, B'lore-90, Karnataka

***Abstract*— Authentication based on passwords is used largely in applications for computer security and privacy. However, human actions such as choosing bad passwords and inputting passwords in an insecure way are regarded as "the weakest link" in the authentication chain. Rather than arbitrary alphanumeric strings, users tend to choose passwords either short or meaningful for easy memorization. With web applications and mobile apps piling up, people can access these applications anytime and anywhere with various devices. This evolution brings great convenience but also increases the probability of exposing passwords to shoulder surfingattacks. Attackers can observe directly or use external recording devices to collect users' credentials. To overcome this problem, we proposed a novel authentication system PassMatrix, based on graphical passwords 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, PassMatrix offers no hint for attackers to figure out or narrow down the password even they conduct multiple camera-based attacks. We also implemented a PassMatrix prototype on Android and carried out real user experiments to evaluate its memorability and usability. From the experimental result, the proposed system achieves better resistance to shoulder surfing attacks while maintaining usability.**

I. INTRODUCTION
II.

Textual passwords have been the most widely used authentication method for decades. Comprised of numbers and upper- and lower-case letters, 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 [4], [5], [6], [7] were developed to address the problems and weaknesses associated with textual passwords. Based on some studies such as those in [8], [9], 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 [10], [11], [12]. 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 [13], [14], [15].The human actions such as choosing bad passwords for new accounts and inputting passwords in an insecure way for later logins are regarded as the weakest link in the authentication chain [16]. Therefore, an authentication scheme should be designed to overcome these vulnerabilities. In this paper, we present 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.

1.1Motivation

As the mobile marketing statistics compilation by Danyl, the mobile shipments had overtaken PC shipments in 2011, and the number of mobile users also overtaken desktop users at 2014, which closed to 2 billion [17]. However, shoulder surfing attacks have posed a great threat to users' privacy

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 6, June 2017

and confidentiality as mobile devices are becoming indispensable
in modern life. People may log into web services and apps in public to access their personal accounts with their smart phones, tablets or public devices, like bank ATM. Shoulder-surfing attackers can observe how the passwords were entered with the help of reflecting glass windows, or let alone monitors hanging everywhere in public places. Passwords are exposed to risky environments, even if the passwords themselves are complex and secure. A secure authentication system should be able to defend against shoulder surfing attacks and should be applicable to all kinds of devices. Authentication schemes in the literature such as those in [6], [18], [19], [20], [21], [22], [23], [24],[25] are resistant to shoulder-surfing, but they have either usability limitations or small password space. Some of them are not suitable to be applied in mobile devices and most of them can be easily compromised to shoulder surfing attacks if attackers use video capturing techniques like Google Glass [15], [26]. The limitations of usability include issues such as taking more time to log in, passwords being too difficult to recall after a period of time, and the authentication method being too complicated for users without proper education
and practice.In 2006, Wiedenbeck et al. proposed PassPoints [7] in which the user picks up several points (3 to 5) in an image during the password creation phase and re-enters each of these pre-selected click-points in a correct order within its tolerant square during the login phase. Comparing to traditional PIN and textual passwords, the Pass-Points 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, we add the idea of using one-time session passwords and distracters to develop our PassMatrix authentication system that is resistant to shoulder surfing attacks.

1.2 Organization

This paper is organized as follows. Section 2 provides the backgrounds of related techniques about graphical authentication schemes and Section 3 describes attack models. The proposed PassMatrix is presented in Section 4. The user study and its results are available in Section 5 and Section 6 respectively. A security analysis is discussed in Section 7. And we conclude the paper.

III. PROBLEM STATEMENT

2.1 Problem Statement

With the increasing amount of mobile devices and web services, users can access their personal accounts to send confidential business emails, upload photos to albums in the cloud or remit money from their e-bank account anytime and anywhere. While logging into these services in public, they may expose their passwords to unknown parties unconsciously. People with malicious intent could watch the whole authentication procedure through omnipresent video cameras and surveillance equipment, or even a reflected image on a window [37]. Once the attacker obtains the password, they could access personal accounts and that would definitely pose a great threat to one's assets. Shoulder surfing attacks have gained more and more attention in the past decade. The following lists the research problems we would like to address in this study:

1) The problem of how to perform authentication in public so that shoulder surfing attacks can be alleviated.
2) The problem of how to increase password space than that of the traditional PIN.
3) The problem of how to efficiently search exact password objects during the authentication phase.
4) The problem of requiring users to memorize extra information or to perform extra computation during authentication.
5) The problem of limited usability of authentication schemes that can be applied to some devices only.

2.2 Attack Model

2.2.1 Shoulder Surfing Attacks

Based on previous research [20], [21], [25], [34], [35], users' actions such as typing from their keyboard, or clicking on the pass-images or pass-points in public may reveal their passwords to people with bad intention. In this paper, based on the means the attackers use, we

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 6, June 2017

categorize shouldersurfing attacks into three types as below:

1) Type-I: Naked eyes.

2) Type-II: Video captures the entire authentication process only once

3) Type-III:Video captures the entire authentication process more than once.

The latter types of attacks require more effort and techniques from attackers. Thus, if an authentication scheme is able to resist against these attacks, it is also secure against previous types of attacks. Some of the proposed authentication schemes [4], [5], [6], [7], [25], [38], including traditional text-password and PIN, are vulnerable to shoulder surfing Type-I attacks and thus are also subject to Type-II and Type- III attacks. These schemes reveal passwords to attackers as soon as users enter their passwords by directly pressing or clicking on specific items on the screen. Other schemes such as those in [19], [34] can resist against Type-I but are vulnerable to Type-II and Type-III attacks since the attackers can crack passwords by intersecting their video captures from multiple steps of the entire authentication process.

IV. PASSMATRIX

To overcome (1) the security weakness of the traditional PIN method, (2) the easiness of obtaining passwords by observers in public, and (3) the compatibility issues to devices, we introduced a graphical authentication system called PassMatrix. In PassMatrix, a password consists of only one pass-square per pass-image for a sequence of n images. The number of images (i.e., n) is user-defined.Figure 5 demonstrates the proposed scheme, in which the first pass-square is located at (4, 8) in the first image, the second pass-square is on the top of the smoke in the second image at (7, 2), and the last pass-square is at (7, 10) in the third image.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 [7] scheme. Based on the user study of Cued Click Points (CCP) [40] proposed by Chiasson et al.,

Fig. 5. A password contains three images (n=3) with a pass square in
each. The pass squares are shown as the orange-filled area in each image.the CCP method does a good job in helping users recollect and remember their passwords. If the user clicks on an incorrect region within the image, a different image will be shown to give the user a warning feedback. 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 simply touching at or clicking on them during the registration phase.

3.1 Overview

PassMatrix is composed of the following components (see Fig6):
_ Image Discretization Module
_ Horizontal and Vertical Axis Control Module
_ Login Indicator generator Module
_ Communication Module
_ Password Verification Module
_ Database

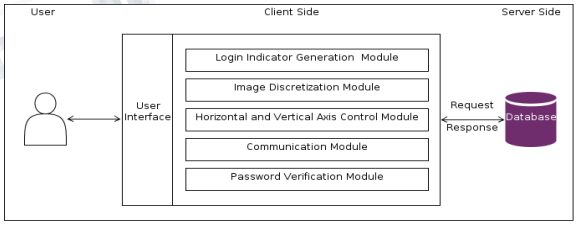


Fig. 6. Overview of the PassMatrix system.

a) ***Image Discretization Module.*** This module divides each image into squares, from which users would choose one as the pass-square. As shown in Figure 5, 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. Hence, in our

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 6, June 2017

implementation, a division was set at 60-pixel intervals in both horizontal and vertical directions, since 60 pixels2 is the best size to accurately select specific objects on touch screens.

b) ***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 our implementation, we used 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 the former case, the indicator could be shown on the display (see Figure 7(a)) directly or through another predefined image. If using a predefined image, for instance, if the user chooses the square (5, 9) in the image as in Figure 7(b), then the login indicator will be (E, 11). For the acoustical delivery, the indicator can be received by an audio signal through the ear buds or Bluetooth. One principle is to keep the indicators secret from people other than the user, since the password (the sequence of passsquares) can be reconstructed easily if the indicators are known.

Fig. 7. (a) Obtain the login indicator (E,11) directly. (b) Obtain the login indicator through a predefined image.

c) ***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. This control module provides **drag** and **fling** functions for users to control both bars. Users can fling either bar using their finger to shift one alphanumeric at a time. They can also shift several checks at a time by dragging the bar for a distance. Both bars are circulative, i.e., if the user shifts the horizontal bar in Figure 8(c) to left by three checks, it will become the bar shown in Figure 8(d). The bars are used to implicitly point out (or in other words, align the login indicator to) the location of the user's pass-square.

d) ***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 [41] and thus, is safe from being eavesdropped and intercepted.

e) ***Password Verification Module.*** This module verifies the user password during the authentication phase.

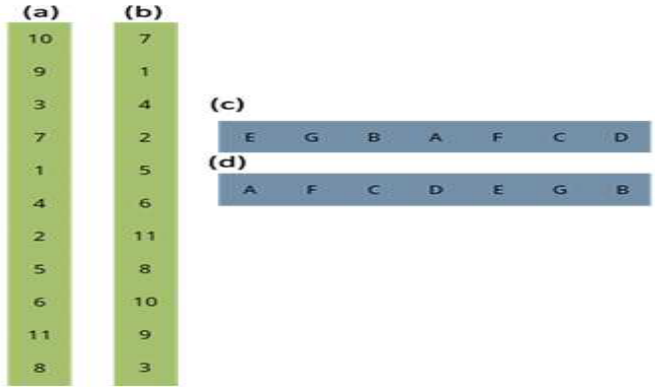


Fig. 8. Horizontal scroll bar (on the right/blue) and vertical bar (on the left/green). A pass-square acts similar to a password digit in the text-based password system. The user is authenticated only if each pass-square in each pass-image is correctly aligned with the login indicator.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 6, June 2017

The details of how to align a login indicator to a pass-square will be described in the next section.

Database. The database server contains several tables that store user accounts, passwords (ID numbers of passimages and the positions of pass-squares), and the time duration each user spent on both registration phase and login phase. PassMatrix has all the required privileges to perform operations like insert, modify, delete and search

3.2 PassMatrix

PassMatrix's authentication consists of a registration phase and an authentication phase as described below:

3.2.1 Registration phase

Figure 9 is the flowchart of the registration phase. At this stage, the user creates an account which contains a username and a password. 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 trade-off between security and usability of the system [42]. The only purpose of the username is to give the user an imagination of having a personal account.The username can be omitted if PassMatrix is applied to authentication systems like screen lock. The user can either choose images from a provided list or upload images from their device as pass-images. Then the user will pick a passsquare for each selected pass-image from the grid, which was divided by the image discretization module. The user repeats this step until the password is set.

3.2.2 Authentication phase

Figure 10 is the flowchart of the authentication phase. At this stage, 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.

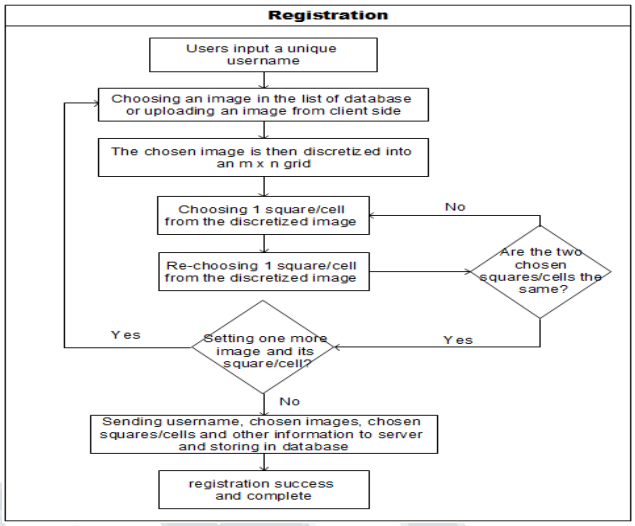


Fig. 9. The flowchart of registration phase in PassMatrix.

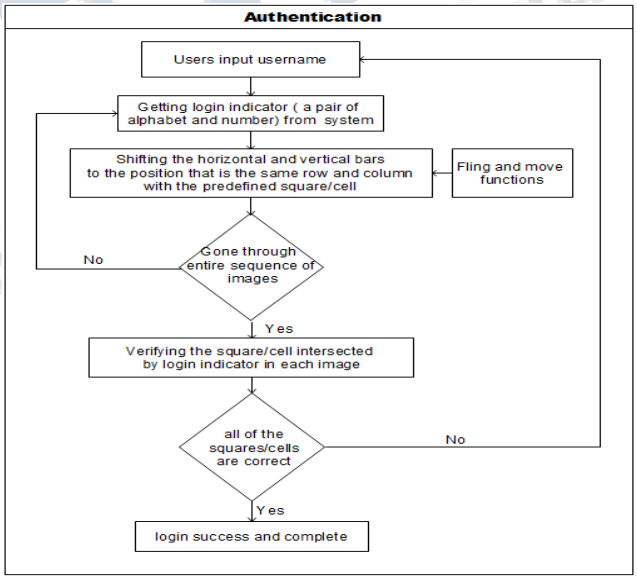


Fig. 10. The flowchart of authentication phase in PassMatrix.

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 also be delivered through a

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 6, June 2017

predefined image or by audio feedback that we have mentioned in the previous section.
3) Next, the first pass-image will be shown on the display, with a horizontal bar and a vertical bar on 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.(see fig.12)
4) Repeat step 2 and step 3 for each pre-selected passimage.
5) The communication module gets user account information from the server through HttpRequest POST method.
6) 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 allowedto log into PassMatrix.

IV IMPLEMENTATION AND USER STUDY

Although the PassMatrix prototype was implemented on an Android system which has a small screen, it is not limited to the applications on small screen devices, for example screen locking. In fact, it could be applied to a wide range of authentication scenarios. For instance, user account login in Windows 8, email account login on web browser, and Fig. 10. The flowchart of authentication phase in PassMatrix. application login/unlock on Android OS. It can also be applied to any client device such as personal computers,laptops, tablets, mobile phones, or bank ATM due to the fact that the method of authentication is simple and the entire authentication process can be completed by only touching or clicking on the screen. In our implementation, we assumed that users download an application from Google Play [43] and register an account for later login to use the service. Since Android [44] is an open source operating system based on Linux kernel and is widely used in mobile devices such as tablet PCs and smart phones, we implemented a PassMatrix prototype on Android and carried out user experiments to evaluate its memorability and usability. In this section we will describe our PassMatrix implementation and the user study experimental design, environment, participants and procedures.The result of the user study will be shown in Section 6.

4.1 Implementation

The PassMatrix prototype was built with Android SDK 2.3.3 since it was the mainstream version of the distribution in 2012 [45]. After connecting to the Internet, users can register an account, log in a few times in practice mode, and then log in for the experiment with a client's device (see Figure 11(a)). In the client side of our prototype, we used XML to build the user interface and used JAVA and Android API to implement functions, including username checking, passimages listing, image discretization, pass-squares selection, login indicator delivery, and the horizontal and vertical bars circulation. In the server side of our implementation, we used PHP and MySQL to store and fetch registered accounts to/from the database to handle the password verification.Although in our proposed system we mentioned that users can import their own images, we used a list of 24 fixed test images in our experiment (see Figure 11(b)). Each image

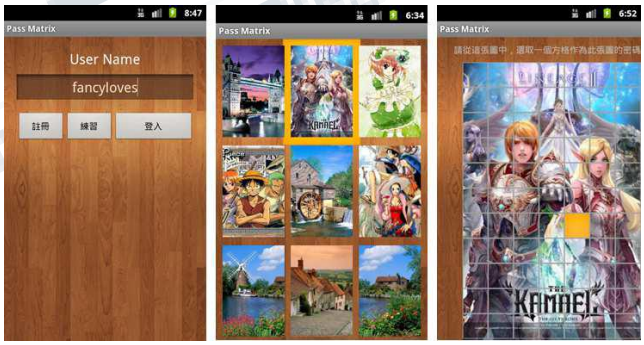


Fig. 11. (a) The Main page of PassMatrix, users can register an account,practice or start to log in for experiment. (b) Users can choose from a list of 24 images as their pass-images. (c) There are 7 X 11 squares in each image, from which users choose one as the pass-square.

is displayed in a size of 420 X 660 pixels and is discretized into 60 X 60 pixel squares. Thus, users have 7 X 11 squares to select in each image (see Figure 11(c)). After a user selects three to five images with one pass-square per image, the password will be stored as a list of

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 6, June 2017

coordinates in a database table (i.e., the locations of those selected pass-squares in the 7X11 grid). The password space depends on the number of images set by users. For instance, if a user creates an account with four images, the password space is $(7 \times 11)^4$

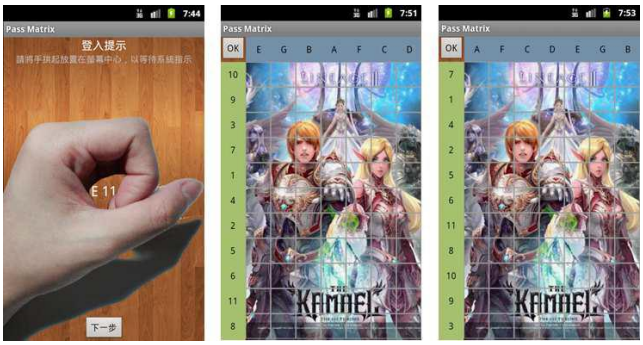


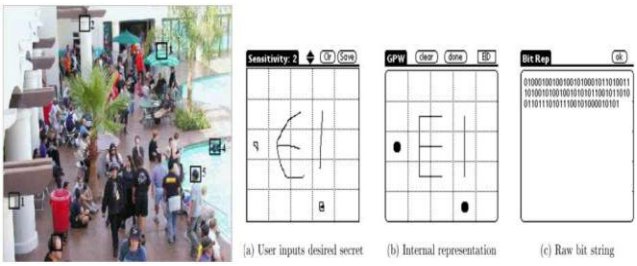
Fig. 12. (a) A visual way for users to obtain a one-time valid login indicator.

(b) The permutations of alphanumerics in horizontal and vertical bars are randomly generated for each image. (c) Users can shift the
bars to the correct position so that the login indicator aligns with the pass-square.

The first step in the login phase is getting the onetime valid login indicator from the system. There are many ways to obtain the indicator and we've illustrated several examples in Section 4.1. In our implementation, we adopted the simplest way: grasping the hand with a little space left in the center and then touching the screen of smart phones (see Figure 12(a)). To protect against shoulder surfing, the indicator is not shown until the hand touches the screen and will vanish immediately when the hand leaves the screen.The number of elements on both the horizontal and vertical bars depends on the discretization degree of the images. In our implementation, there are 7 letters (from A to G) and 11 numbers (from 1 to 11) on the horizontal bar and on the vertical bar, respectively. They are used to align the one-time indicator with the pass-square in each pass-image during the authentication phase. In order to obfuscate and thus hide the alignment patterns from observers, we randomly shuffled the elements on both bars in each pass-image and let users shift them to the right position (see Figure 12(b) and (c)).We implemented two barshifting functions: dragging and flinging. Since the entire bar is shiftable and can be circulated on either side (i.e., bidirectional and circulative), users do not need to place their finger on a specific element in order to move it.

V. BACKGROUND AND RELATED WORK

In the past several decades, a lot of research on password authentication has been done in the literature. Among all of these proposed schemes, this paper focuses mainly on the graphical-based authentication systems. To keep this paper concise, we will give a brief review of the most related schemes that were mentioned in the previous section. Many other schemes such as those in [27], [28], [29], [30], [31] may have good usability, they are not graphical-based and need additional support from extra hardware such as audio, multi-touch monitor, vibration sensor, or gyroscope, etc. In the early days, the graphical capability of handheld devices was weak; the color and pixel it could show was limited. Under this limitation, the Draw-a-Secret (DAS) [6] technique was proposed by Jermyn et al. in 1999, where the user is required to re-draw a pre-defined picture on a 2D grid. We directly extract the figure from [6] and show it in Figure 1(b). If the drawing touches the same grids in the same sequence, then the user is authenticated. Since then, the graphical capability of handheld devices has steadily and ceaselessly improved with the advances in science and technology. In 2005, Susan Wiedenbeck et al. introduced a graphical authentication scheme PassPoints [7], and at that time, handheld devices could already show high resolution color pictures. Using the PassPoint scheme, the user has to click on a set of pre-defined pixels on the predestined photo, as shown in Figure 1(a) (this figure is extracted from [7]), with a correct sequence and within their tolerant squares during the login stage.



ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 6, June 2017

Fig. 1. (a) Pixel squares selected by users as authentication passwords in PassPoints [7]. (b) Authentication password drew by users and the raw bits recorded by the system database [6].

VI. CONCLUSION

6.1 Discussion

Although we discretized each image into a grid of 7 X 11, which holds 77 squares per image, we still think it is not secure enough to resist against brute force attacks or random guessing attacks. According to the result of questionnaires in the user study, users expressed that they prefer to use only 1 to 2 pass-images for screen lock after considering the trade-off between security and usability. This means that the entropies of PassMatrix in screen lock will be 6:27 bits and 12:53 bits for one pass-image and two pass-images respectively, and can be strengthened to 12:53 and 25:07 bits when obtaining login indicators through the graphical method. In order to be more secure than the existing Android pattern password with entropy 18:57 bits against brute force attacks, users have to set two pass-images and use the graphical method to obtain the one-time login indicators. Like most of other graphical password authentication systems, PassMatrix is vulnerable to random guess attacks based on hot-spot analyzing. This weakness can be improved by letting users upload their own images and therefore make it more difficult for attackers to collect statistics of hot-spots. Moreover, because images with less independent objects usually suffer more on the hot-spot problem, carefully selecting images with rich objects can alleviate the hot-spot based random guess attacks. Here we summary the features of PassMatrix. Compared with DAS [6], PassPoints [7] and Marcos's finger-drawn doodles [33], PassMatrix is strong enough to resist shoulder surfing attacks, even if the attacks are camera-equipped. And the PIN-entry method [34], FakePointer [35], Wiedenback's scheme [36] and Color Rings [25] do not have enough computational complexity while facing to random guess attack, which PassMatrix can withstand.

6.2 Conclusion

With the increasing trend of web services and apps, users are able to access these applications anytime and anywhere with various devices. In order to protect users' digital property, authentication is required every time they try to access their personal account and data. However, conducting the authentication process in public might result in potential shoulder surfing attacks. Even a complicated password can be cracked easily through shoulder surfing. Using traditional textual passwords or PIN method, users need to type their passwords to authenticate themselves and thus these passwords can be revealed easily if someone peeks over shoulder or uses video recording devices such as cell phones. To overcome this problem, we proposed a shouldersurfing 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 implemented a PassMatrix prototype on Android and carried out user experiments to evaluate the memorability and usability. The experimental result showed that users can log into the system with an average of 1:64 tries (Median=1), and the Total Accuracy of all login trials is 93:33% even two weeks after registration. The total time consumed to log into PassMatrix with an average of 3:2 pass-images is between 31:31 and 37:11 seconds and is considered acceptable by 83:33% of participants in our user study. Based on the experimental results and survey data, PassMatrix is a novel and easy-to-use graphical password authentication system, which can effectively alleviate shoulder-surfing attacks. In addition, PassMatrix can be applied to any authentication scenario and device with simple input and output capabilities. The survey data in the user study also showed that PassMatrix is practical in the real world.

REFERENCES

[1] S. Sood, A. Sarje, and K. Singh, "Cryptanalysis of password authentication schemes: Current status and key issues," in Methods and Models in Computer Science, 2009. ICM2CS 2009.Proceeding of International Conference on, Dec 2009, pp. 1–7.

[2] 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. 479–483.

[3] K. Gilhooly, "Biometrics: Getting back to business," Computerworld,May, vol. 9, 2005.

[4] R. Dhamija and A. Perrig, "Deja vu: A user study using images for authentication," in Proceedings of the 9th conference on USENIX Security Symposium-Volume 9. USENIX Association, 2000, pp. 4–4.

[5] "Realuser," http://www.realuser.com/.

[6] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "The design and analysis of graphical passwords," in Proceedings of the 8th conference on USENIX Security Symposium-Volume 8. USENIX Association, 1999, pp. 1–1.

[7] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, "Passpoints: Design and longitudinal evaluation of a graphical password system," International Journal of Human-Computer Studies,vol. 63, no. 1-2, pp. 102–127, 2005.

[8] A. Paivio, T. Rogers, and P. Smythe, "Why are pictures easier to recall than words?" Psychonomic Science, 1968.

[9] D. Nelson, U. Reed, and J. Walling, "Picture superiority effect,"Journal of Experimental Psychology: Human Learning and Memory,vol. 3, pp. 485–497, 1977.

[10] S. Brostoff and M. Sasse, "Are passfaces more usable than passwords? a field trial investigation," PEOPLE AND COMPUTERS,pp. 405–424, 2000.

[11] A. De Angeli, M. Coutts, L. Coventry, G. Johnson, D. Cameron,and M. Fischer, "Vip: a visual approach to user authentication," in Proceedings of the Working Conference on Advanced Visual Interfaces.ACM, 2002, pp. 316–323.

[12] B. Ives, K. Walsh, and H. Schneider, "The domino effect of password reuse," Communications of the ACM, vol. 47, no. 4, pp. 75–78,2004.

[13] J. Long and K. Mitnick, No Tech Hacking: A Guide to Social Engineering,Dumpster Diving, and Shoulder Surfing. Elsevier Science,2011.

[14] T. Kwon, S. Shin, and S. Na, "Covert attentional shoulder surfing:Human adversaries are more powerful than expected," IEEETransactions on Systems, Man, and Cybernetics: Systems, vol. 44, no. 6,pp. 716–727, June 2014.

[15] "Google glass snoopers can steal your passcode with a glance,"http://www.wired.com/2014/06/google-glass-snoopers-cansteal-your-passcode-with-a-glance/.

[16] M. Sasse, S. Brostoff, and D. Weirich, "Transforming the weakest linka human/computer interaction approach to usable and effective security," BT technology journal, vol. 19, no. 3, pp. 122–131,2001.

[17] "Mobile marketing statistics compilation," http://www.smartinsights.com/mobile marketing/mobilemarketing- analytics/mobile-marketing-statistics/.

[18] D. Hong, S. Man, B. Hawes, and M. Mathews, "A password scheme strongly resistant to spyware," in Proceedings of International conference on security and management, 2004.

[19] D. Tan, P. Keyani, and M. Czerwinski, "Spy-resistant keyboard: Towards more secure password entry on publicly observable touch screens," in Proceedings of OZCHI-Computer-Human Interaction Special Interest Group (CHISIG) of Australia. Canberra, Australia:ACM Press. Citeseer, 2005.

[20] M. Kumar, T. Garfinkel, D. Boneh, and T. Winograd, "Reducing shoulder-surfing by using gaze-based password entry," in Proceedingsof the 3rd symposium on Usable privacy and security. ACM, 2007, pp. 13–19.