ACHIEVING SHOULDER SURFING RESISTANT GRAPHICAL AUTHENTICATION

KALAIVANI.SJ,
B.TECH(INFORMATION TECHNOLOGY),
PAAVAI ENGINEERING COLLEGE,
NAMAKKAL, INDIA.
Sjkv24051996@gmail.com

SINDHUBALA.S,
ASSISTANT PROFESSOR/IT.,
PAAVAI ENGINEERING COLLEGE,
NAMAKKAL, INDIA.
sindhubalapec@paavai.edu.in

THIRUMAGAL.G,
B.TECH(INFORMATION TECHNOLOGY),
PAAVAI ENGINEERING COLLEGE,
NAMAKKAL, INDIA.
thirumagalhoney@gmail.com

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 surfing attacks. 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.

Index Terms—Graphical Passwords, Authentication, Shoulder Surfing Attack.

1 INTRODUCTION

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 shorter 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.

1.1 Motivation

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 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 smartphones, tablet sor 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, Wieden beck 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 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, we add the idea of using one-time session passwords and distractors to develop our PassMatrix authentication system that is resistant to shoulder surfing attacks.

2 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., 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.

2.1 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.

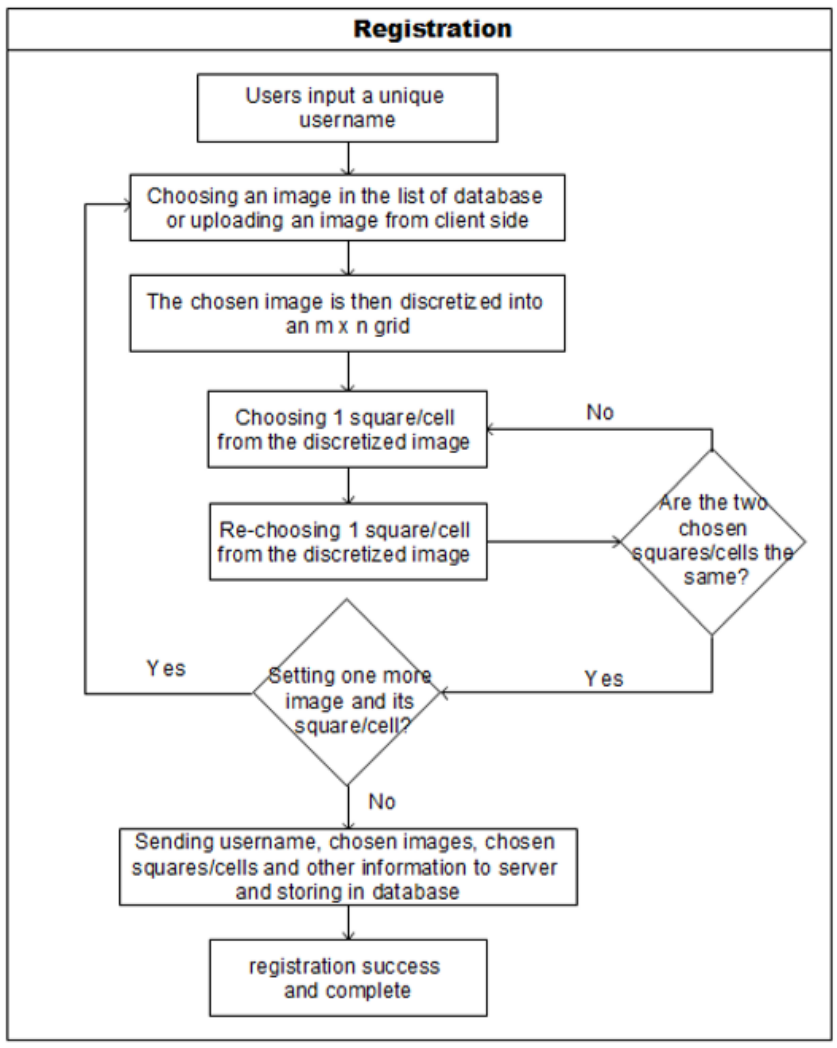

Fig. The flowchart of registration phase in PassMatrix.

2.2 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. 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 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 Figure 12).

4) Repeat step 2 and step 3 for each pre-selected pass image.

5) The communication module gets user account information from the server through Http Request 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 allowed to log into PassMatrix.

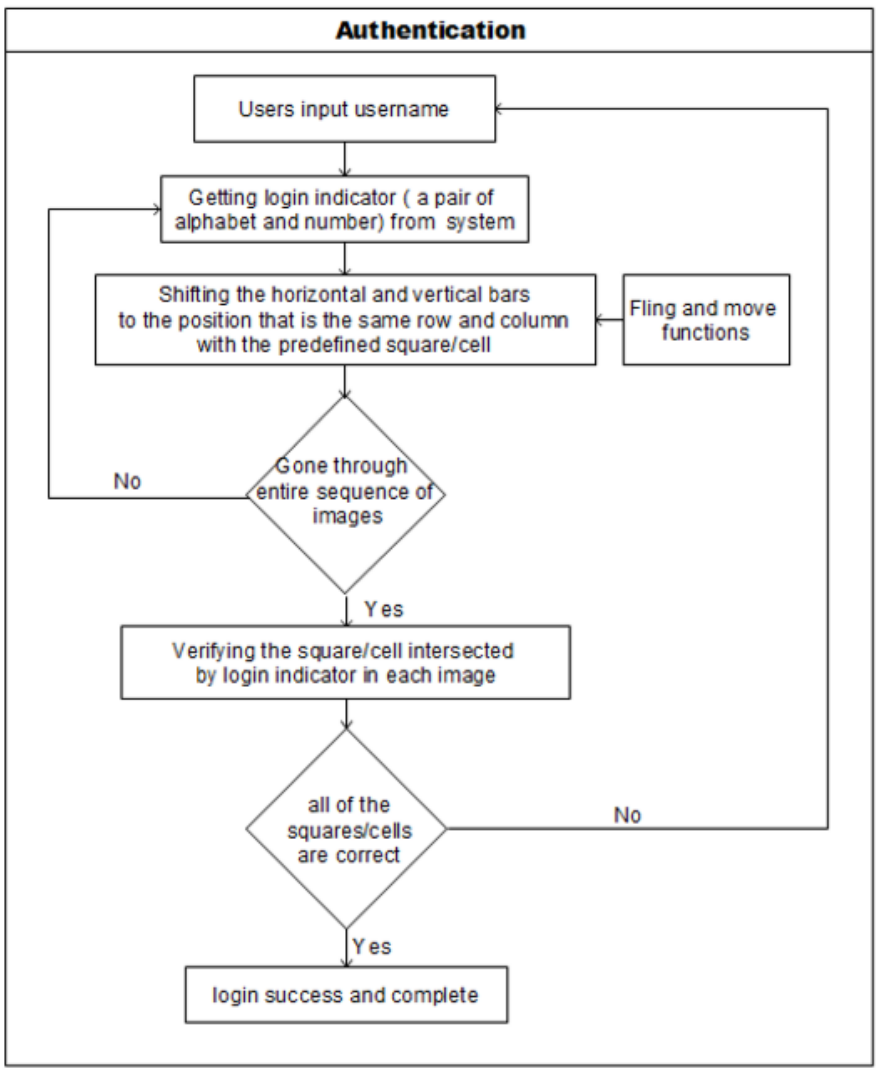

Fig. The flowchart of authentication phase in PassMatrix

3 SHOULDER SURFING ATTACK

Due to the fact that shoulder surfing has been a real threat 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. For instance, some schemes such as PIN-entry method [34] and spyresistant keyboard [19] 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 [24], Pass-icons [18] and Colorings [25] can be narrowed down by camera-based shoulder surfing attacks. The proposed authentication system PassMatrix takes full advantage of adding extra information to obfuscate the login process, using an approach to point out the locations of pass-squares implicitly instead of typing or clicking on password objects directly. Since the horizontal and vertical bars are circulative and thus cover the entire area of the image, the password space will not be narrowed down even if the whole authentication process is recorded by attackers. Furthermore, the login indicator for each pass-image varies so that each pass-image is an independent case. 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.

4. SMUDGE ATTACK

A smudge attack [39] is an implicit attack where attackers attempt to extract sensitive information from recent users' input by inspecting smudges left on touch screens. Since both the horizontal and vertical bars in PassMatrix are scrollable, shifting on any element within the bar can circulate the whole bar. Thus, users do not have to shift the bars by touching the login indicators. The smudge left by users may be quite fixed, but it only indicates the habitual stretching range of the thumb or finger. The length of the smudge left on the screen also provides no useful information since the login indicator is generated randomly for each pass-image and the permutations of elements on both bars are also randomly re-arranged in each pass-image and in each login session. Therefore, the proposed PassMatrix is immune from smudge attacks.

5. 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 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 implemented a PassMatrix prototype on Android and carried out user experiments to evaluate the memorability and usability. The experimental result showed that user scan login to 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 login to 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.

6. 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 SecuritySymposium-Volume9. 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,” IEEE TransactionsonSystems,Man,andCybernetics: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-surfingby usinggaze-based passwordentry,” inProceedings of the 3rd symposium on Usable privacy and security. ACM, 2007, pp. 13–19.

[21] H. Zhao and X. Li, “S3pas: A scalable shoulder-surfing resistant textual-graphical password authentication scheme,” in Advanced Information Networking and Applications Workshops, 2007, AINAW’07. 21st International Conference on, vol. 2. IEEE, 2007, pp. 467–472.

[22] X. Bai, W. Gu, S. Chellappan, X. Wang, D. Xuan, and B. Ma, “Pas: predicate-based authentication services against powerful passiveadversaries,”in2008AnnualComputerSecurityApplications Conference. IEEE, 2008, pp. 433–442.

[23] Z. Zheng, X. Liu, L. Yin, and Z. Liu, “A stroke-based textual password authentication scheme,” in Education Technology and Computer Science, 2009. ETCS’09. First International Workshop on, vol. 3. IEEE, 2009, pp. 90–95.

[24] 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. 760–767.

[25] D. Kim, P. Dunphy, P. Briggs, J. Hook, J. Nicholson, J. Nicholson, and P. Olivier, “Multi-touch authentication on tabletops,” in Proceedings of the 28th international conference on Human factors in computing systems. ACM, 2010, pp. 1093–1102.