International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org
Volume 6, Issue 5, May 2017 **ISSN 2319 - 4847**

Pictorial Authentication System to Protect against Visual Monitor Attack

Sathya Jyothi[1] , Kameswari K[2]

[1] M.Tech, CNE, Dept. of ISE, SJBIT, Bengaluru,

[2] Assistant Professor, Dept. of ISE, SJBIT, Bengaluru,

Abstract

Validation in view of passwords is utilized to a great extent in applications for PC security and protection. In any case, human activities, for example, picking awful passwords and contributing passwords in a shaky way are viewed as "the weakest connection" in the confirmation chain. Instead of discretionary alphanumeric strings, clients have a tendency to pick passwords either short or significant for simple remembrance. With web applications and portable applications heaping up, individuals can get to these applications at whatever time and anyplace with different gadgets. This development brings awesome comfort additionally expands the likelihood of presenting passwords to shoulder surfing assaults. Aggressors can watch specifically or utilize outside recording gadgets to gather clients' accreditations. To defeat this issue, we proposed a novel validation framework PassMatrix, in view of graphical passwords to oppose bear surfing assaults. With a one-time legitimate login pointer and circulative level and vertical bars covering the whole extent of pass-pictures, PassMatrix offers no indication for assailants to make sense of or limit the secret word even they direct numerous camera-based assaults. We likewise actualized a PassMatrix model on Android and completed genuine client examinations to assess its memorability and ease of use. From the exploratory outcome, the proposed framework accomplishes better imperviousness to shoulder surfing assaults while looking after ease of use.

Keywords: Graphical Passwords, Authentication, Shoulder Surfing Attack

1. INTRODUCTION

Literary passwords have been the most generally utilized verification strategy for quite a long time. Contained numbers and upper-and lower-case letters, literary passwords are viewed as sufficiently solid to oppose against beast constrain assaults. Be that as it may, a solid printed secret key is difficult to retain and recall [1]. Subsequently, clients have a tendency to pick passwords that are either short or from the lexicon, as opposed to irregular alphanumeric strings. Far more terrible, it is not an uncommon case that clients may utilize just a single username and watchword for various records [2]. Picture based passwords were turned out to be less demanding to remember in a few client considers [10], [11], [12]. Subsequently, clients can set up an unpredictable confirmation watchword and are equipped for remembering it after quite a while regardless of the possibility that the memory is not initiated intermittently. Notwithstanding, the vast majority of these picture based passwords are defenseless against shoulder surfing assaults (SSAs). This sort of assault either utilizes coordinate perception, for example, viewing behind someone or applies video catching procedures to get passwords, PINs, or other delicate individual data [13], [14],[15].

The human activities, for example, picking terrible passwords for new records and contributing passwords in an unreliable route for later logins are viewed as the weakest connection in the verification chain [16]. In this paper, we exhibit a safe graphical verification framework named PassMatrix that shields clients from getting to be casualties of shoulder surfing assaults while contributing passwords in broad daylight through the utilization of one-time login markers.

2. RELATED WORKS

In the previous a very long while, a considerable measure of research on secret key validation has been done in the writing. Among these proposed plans, this paper concentrates essentially on the graphical-based verification frameworks. In the good 'ol days, the graphical ability of handheld gadgets was powerless; the shading and pixel it could show was restricted. Under this impediment, the Draw-a-Secret (DAS) [6] system was proposed by Jermyn et al. in 1999, where the client is required to re-draw a pre-characterized picture on a 2D network. We straightforwardly extricate the figure from [6] and show it in Figure 1. On the off chance that the drawing touches similar networks in a similar grouping, then the client is verified. From that point forward, the graphical ability of handheld gadgets has consistently and endlessly enhanced with the advances in science and innovation. In 2005, Susan Wiedenbeck et al. presented a graphical validation plot PassPoints [7], and around then, handheld gadgets could as of now show high

determination shading pictures. Utilizing the PassPoint conspire, the client needs to tap on an arrangement of pre-characterized pixels on the foreordained photograph, as appeared in Figure 1

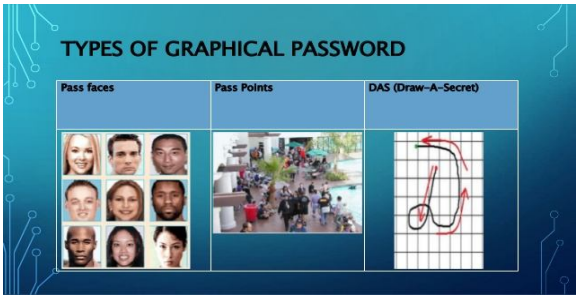

Figure 1: Types of Graphical Passwords

3. PROBLEM STATEMENT

With the expanding measure of cell phones and web administrations, clients can get to their own records to send private business messages, transfer photographs to collections in the cloud or transmit cash from their e-financial balance at whatever time and anyplace. While signing into these administrations in broad daylight, they may open their passwords to obscure gatherings unwittingly. Individuals with malignant aim could watch the entire validation strategy through ubiquitous camcorders and reconnaissance gear, or even a pondered picture a window [37]. Once the assailant acquires the secret word, they could get to individual records and that would represent an extraordinary danger to one's benefits. Bear surfing assaults have increased increasingly consideration in the previous decade. The accompanying records the exploration issues we might want to address in this review:

1) The issue of how to perform confirmation out in the open with the goal that shoulder surfing assaults can be reduced.
2) The issue of how to expand secret word space than that of the conventional PIN.
3) The issue of how to productively seek correct watchword objects amid the validation stage.

3.1 ATTACK MODEL

Shoulder Surfing Attacks Based on past research [20], [21], [25], [34], [35], clients' activities, for example, writing from their console, or tapping on the pass-pictures or pass-focuses out in the open may uncover their passwords to individuals with awful aim. In this paper, in view of the methods the assailants utilize, we sort bear surfing assaults into three sorts as beneath:

1) Type-I: Naked eyes.
2) Type-II: Video catches the whole confirmation prepare just once.
3) Type-III: Video catches the whole confirmation prepare more than once. The last sorts of assaults require more exertion and strategies from aggressors. Subsequently, if a validation plan can oppose against these assaults, it is additionally secure against past sorts of assaults. A portion of the proposed validation plans [4], [5], [6], [7], [25], [38], including conventional content secret key and PIN, are defenseless against shoulder surfing Type-I assaults and hence are likewise subject to Type-II and Type-III assaults. These plans uncover passwords to assailants when clients enter their passwords by straightforwardly squeezing or tapping on particular things on the screen. Different plans, for example, those in [19], [34] can oppose against Type-I however are defenseless against Type-II and Type-III assaults since the assailants can break passwords by converging their video catches from numerous means of the whole verification prepare.

4. PASSMATRIX

PassMatrix is composed of the following components (see Figure 2):

_ Image Discretization Module
_ Horizontal and Vertical Axis Control Module
_ Login Indicator generator Module
_ Communication Module
_ Password Verification Module

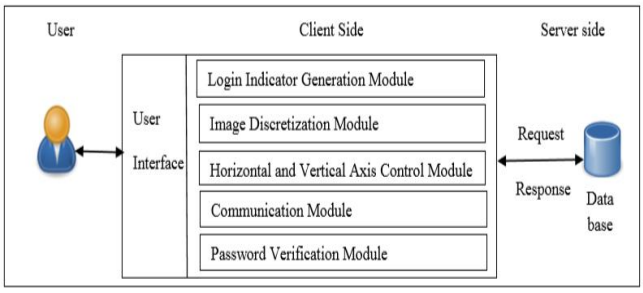

Figure 2: Overview of PassMatrix

Image Discretization Module. This module divides each image into squares, from which users would choose one as the pass-square. As shown in Figure 2, 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 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.

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.
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.

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.

Password Verification Module. This module verifies the user password during the authentication phase. 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. PassMatrix's validation comprises of an enrollment stage and a confirmation stage as depicted beneath:

Registration stage: At this stage, the client makes a record which contains a username and a secret word. The watchword comprises of just a single pass-square per picture for a grouping of n pictures. The quantity of pictures (i.e., n) is chosen by the client in the wake of considering the exchange off amongst security and ease of use of the framework [42]. The main motivation behind the username is to give the client a creative energy of having an individual record.

Authentication stage: At this stage, the client utilizes his/her username, secret word and login pointers to sign into PassMatrix. The accompanying depicts every one of the means in detail:

1) The client inputs his/her username which was made in the enrollment stage.
2) Another marker included a letter and a number is made by the login pointer generator module. The marker will be demonstrated when the client employments. his/her hand to frame a circle and after that touch the screen. For this situation, the marker is passed on to the client by visual criticism. The marker can likewise be conveyed through a predefined picture or by sound input that we have specified in the past area.
3) Next, the primary pass-picture will be appeared on the show, with a level bar and a vertical bar on its top and left separately.
4) Repeat step 2 and step 3 for each pre-chosen pass picture.
5) The correspondence module gets client account data from the server through Http Request POST technique.
6) Finally, for each picture, the secret key check module confirms the arrangement between the pass square and the login pointer. Just if every one of the arrangements are right in all pictures, the client is permitted to sign into PassMatrix.

5. IMPLEMENTATION

The PassMatrix model was worked with Android SDK 2.3.3 since it was the standard variant of the dispersion in 2012 [45]. In the wake of associating with the Internet, clients can enroll a record, sign in a couple times practically speaking mode, and afterward sign in for the explore different avenues regarding a customer's gadget. In the customer side of our model, we utilized XML to construct the UI and utilized JAVA and Android API to actualize capacities, including username checking, pass pictures posting, picture discretization, pass-squares determination, login marker conveyance, and the flat and vertical bars course. In the server side of our execution, we utilized PHP and MySQL to store and get enlisted records to/from the database to deal with the secret word confirmation.

Figure 3. Main pages of PassMatrix

6. RESULTS

We investigated the gathered information from our examinations and reviews to assess the adequacy of the proposed framework. The outcomes are introduced in two points of view: exactness and ease of use. The exactness viewpoint concentrates on the fruitful login rates in both sessions, including the practice logins. The ease of use viewpoint is measured by the measure of time clients spent in each PassMatrix stage. The aftereffects of these two investigations unequivocally proposed that PassMatrix is down to earth to utilize.

7. CONCLUSION

With the expanding pattern of web administrations and applications, clients can get to these applications at whatever time and anyplace with different gadgets. Keeping in mind the end goal to secure clients' advanced property, validation is required each time they attempt to get to their own record and information. Be that as it may, leading the confirmation procedure in broad daylight may bring about potential shoulder surfing assaults. Indeed, even a muddled watchword can be broken effectively through shoulder surfing. Utilizing customary literary passwords or PIN strategy, clients need to sort their passwords to verify themselves and hence these passwords can be uncovered effectively on the off chance that somebody looks over shoulder or uses video recording gadgets, for example, phones. To conquer this issue, we proposed a shoulder surfing safe confirmation framework in view of graphical passwords, named PassMatrix. PassMatrix model on Android and done client tests to assess the memorability and ease of use.

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), 2014International 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. USENIXAssociation, 1999, pp. 1–1.

[7] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, "Passpoints: Design and longitudinal evaluation of a graphicalpassword 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 Transactions 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/mobile marketing-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 Proceedings 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 passive adversaries," in 2008 Annual Computer Security Applications 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.
[26] "Black hat: Google glass can steal your passcodes," https://www.technologyreview.com/s/529896/black-hat-google- glass-can-steal-your-passcodes/.
[27] A. De Luca, M. Harbach, E. von Zezschwitz, M.-E. Maurer, B. E.Slawik, H. Hussmann, and M. Smith, "Now you see me, now you don't: Protecting smartphone authentication from shoulder surfers," in Proceedings of the 32Nd Annual ACM Conference on Human Factors in Computing Systems, ser. CHI '14. New York,NY, USA: ACM, 2014, pp. 2937–2946.
[28] E. von Zezschwitz, A. De Luca, and H. Hussmann, "Honey,i shrunk the keys: Influences of mobile devices on passwordcomposition and authentication performance," in Proceedings ofthe 8th Nordic Conference on Human-Computer Interaction: Fun, Fast,Foundational, ser. NordiCHI '14. New York, NY, USA: ACM, 2014,pp. 461–470.
[29] 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. 197–200.

[30] 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. 1089–1092.
[31] I. Oakley and A. Bianchi, "Multi-touch passwords for mobile device access," in Proceedings of the 2012 ACM Conference on Ubiquitous Computing, ser. UbiComp '12. New York, NY, USA: ACM,2012, pp. 611–612. [32] M. Martinez-Diaz, J. Fierrez, and J. Galbally, "The doodb graphical password database: Data analysis and benchmark results," Access ,IEEE, vol. 1, pp. 596–605, 2013.
[33] M. Martinez-Diaz, J. Fierrez, and J. Galbally, "Graphical password based user authentication with free-form doodles," IEEE Transactions on Human-Machine Systems, vol. PP, no. 99, pp. 1–8, 2015.
[34] V. Roth, K. Richter, and R. Freidinger, "A pin-entry method resilient against shoulder surfing," in Proceedings of the 11th ACM conference on Computer and communications security, ser. CCS '04.New York, NY, USA: ACM, 2004, pp. 236–245.
[35] 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. 395–400.
[36] 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.
[37] B. Laxton, K. Wang, and S. Savage, "Reconsidering physical key secrecy: Tele duplication via optical decoding," in Proceedings of the 15th ACM conference on Computer and communications security.ACM, 2008, pp. 469–478.
[38] X. Suo, Y. Zhu, and G. Owen, "Analysis and design of graphical password techniques," Advances in Visual Computing, pp. 741–749,2006.
[39] A. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. Smith, "Smudge attacks on smartphone touch screens," in USENIX 4th Workshop on Offensive Technologies, 2010.
[40] S. Chiasson, P. van Oorschot, and R. Biddle, "Graphical password authentication using cued click points," Computer Security–ESORICS 2007, pp. 359–374, 2007.
[41] "Secure socket layer ssl," http://en.wikipedia.org/wiki/Transportn Layern Security.
[42] L. Cranor and S. Garfinkel, Security and Usability. O'Reilly Media,Inc., 2005.
[43] "Google play," https://play.google.com/store/.
[44]"Android developer,"http://developer.android.com/index.html.
[45] "Android version of distribution," http://developer.android.com/resources/dashboard/platform-versions.html.