e-ISSN: 2319-8753 | p-ISSN: 2347-6710

IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 5, May 2024

Impact Factor: 8.423

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305084 |

A Shoulder Surfing Resistant Graphical Authentication System

Mohammed Faizan K, Mohammed Zeeshan Mukram, Shreya S Karikatti, Pavithra P B, Yashaswini N G

U.G. Student, Department of Computer Engineering, Sri Taralabalu Jagadguru Institute of Technology, Ranebennur, Karnataka, India

U.G. Student, Department of Computer Engineering, Sri Taralabalu Jagadguru Institute of Technology, Ranebennur, Karnataka, India

U.G. Student, Department of Computer Engineering, Sri Taralabalu Jagadguru Institute of Technology, Ranebennur, Karnataka, India

U.G. Student, Department of Computer Engineering, Sri Taralabalu Jagadguru Institute of Technology, Ranebennur, Karnataka, India

Assistant Professor, Department of Computer Engineering, Sri Taralabalu Jagadguru Institute of Technology, Ranebennur, Karnataka, India

ABSTRACT: Conventional password-based authentication suffers from human vulnerabilities like weak password choices and susceptibility to shoulder surfing attacks. This paper proposes PassMatrix, a novel graphical password system designed to address these limitations. PassMatrix offers increased resistance to shoulder surfing by employing a one-time valid login indicator and dynamic, circulative bars that obscure user selections across the entire screen. This approach prevents attackers from inferring the password even through repeated observations. To evaluate usability and memorability, a PassMatrix prototype for Android was developed and tested with real users. The results demonstrate that PassMatrix achieves its security goals while maintaining user-friendliness. This makes it a promising alternative to traditional password-based authentication in scenarios where shoulder surfing is a significant threat.

KEYWORDS: Graphical Authentication, Shoulder Surfing Attacks, Password Security, PassMatrix, Usability, Memorability

I. INTRODUCTION

For many years, passwords made up of letters and numbers have been the go-to method for verifying a user's identity. While these passwords can be strong enough to resist brute force attacks where hackers try every possible combination, they come with a major drawback - memorability. Complex passwords are difficult to remember, leading users to choose weaker options like short phrases or dictionary words. This weakness is compounded by the unfortunate habit of reusing the same login information across multiple accounts. Studies have shown that a significant portion of user passwords can be cracked within a short timeframe, highlighting the insecurity of this method.

Recognizing these limitations, researchers have developed various graphical password schemes as an alternative. These schemes leverage human memory's superior ability to store images compared to text. Users find image-based passwords easier to remember, even after long periods without use. However, a major vulnerability of these graphical password systems is their susceptibility to shoulder surfing attacks. These attacks involve directly observing or recording a user entering their password, compromising the security of the system.

This paper proposes PassMatrix, a novel graphical authentication system designed to address the shortcomings of traditional password methods. PassMatrix aims to eliminate the vulnerability to shoulder surfing attacks by employing a dynamic login indicator system. This system generates a unique indicator for each login attempt, rendering any stolen information useless after a single session. By utilizing a dynamic pointer instead of directly clicking on the password image, PassMatrix offers a more secure and user-friendly authentication experience.

II. RELATED WORK

A. Existing System

Keeping in mind the end goal to be more secure than the current Android design secret key with entropy 18:57 bits against savage power assaults, clients need to set two pass-pictures and utilize the graphical strategy to get the one-time login pointers. Like the greater part of other graphical secret key verification frameworks, PassMatrix is defenseless against irregular figure assaults in light of problem area the most generally utilized confirmation technique for a considerable length of time. Involved numbers and upper-and lower-case letters, literary passwords are viewed as sufficiently solid to oppose against animal power assaults. As indicated by an article in Computer world, a security group at an expansive organization ran a system secret word wafer and shockingly broke around 80% of the representatives' passwords inside 30 seconds. Printed passwords are regularly shaky because of the trouble of keeping up solid ones.

B. Proposed System

This development brings incredible accommodation yet additionally builds the likelihood of presenting passwords to bear surfing assaults. Assailants can watch straightforwardly or utilize outside chronicle gadgets to gather clients' accreditations. To conquer this issue, we proposed a novel validation framework PassMatrix, in light of graphical passwords to oppose bear surfing assaults. With a one-time substantial login pointer and circulative level and vertical bars covering the whole extent of passpictures, PassMatrix offers no indication for assailants to make sense of or limit the secret word even they lead various camerabased assaults. a considerable measure of research on secret word validation has been done in the writing. Among these proposed plans, this paper centers mostly around the graphical-based confirmation frameworks. To keep this paper compact, we will give a concise survey of the most related plans that were said in the past segment. The precision point of view centers around the fruitful login rates in the two sessions, including the training logins. The ease of use viewpoint is estimated by the measure of time clients spent in each PassMatrix stage.

III. IMPLEMENTATION

A. MODULE: IMAGE DESCRITIZATION

This module separates each picture into squares, from which clients would as the pass-square. A picture is isolated into a 7x11 network. The littler the picture is descritized, the bigger the secret word pick one space is. Consequently, in our execution, a division was set at 60 pixel interims in both level and vertical headings, since 60 pixel-square is the best size to precisely choose particular questions on touch screens.

B. FLAT AND VERTICAL AXIS CONTROL MODULE:

There are two parchment bars: a flat bar with a grouping of letters and a vertical bar with a succession of numbers. This control module gives drag and excursion capacities to clients to control the two bars. Clients can throw either bar utilizing their finger to move one alphanumeric at once. They can likewise move a few checks at any given moment by dragging the bar for a separation. The bars are utilized to verifiably point the area of the clients pass-square.

C. LOGIN INDICATOR GENERATOR MODULE:

This module produces a login marker comprising of a few recognizable characters, for example, letter sets and numbers or visual materials, for example, hues and symbols for clients amid verification stage. In our usage, we utilized characters A to G and 1 to 11 for a 7 x 11 framework. The two letters and numbers are produced arbitrarily and in this manner an alternate login pointer is given each time the module is called.

D. PASSWORD VERIFICATION MODULE:

This module confirms the client secret key amid the validation stage. A pass-square acts like a secret key digit in the content based watchword framework. The client is confirmed just if the each pass-square in each pass-picture is effectively lined up with the login pointer.

E. COMMUNICATION MODULE:

This module is responsible for all the data transmitted between the customer gadgets and the verification server. Any correspondence is secured by SSL(Secure Socket Layer) convention and subsequently, is protected from being listened stealthily and caught.

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305084 |

IV. EXPERIMENTAL RESULTS

FIG 1. CHOOSE FILE TO UPLOAD

FIG 2. VIEW FILES PAGE

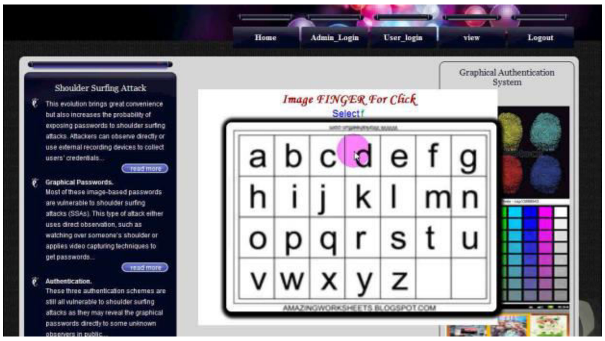

FIG 3. GRID PASSWORD

FIG 4. EDIT PROFILE

Fig 5. View attacker details

V. CONCLUSION

With the expanding pattern of web administrations and applications, clients can get to these applications whenever and anyplace with different gadgets. Keeping in mind the end goal to ensure clients' computerized property, validation is required each time they attempt to get to their own record and information. Utilizing conventional printed passwords or PIN strategy, clients need to type their passwords to validate themselves and hence these passwords can be uncovered effortlessly on the off chance that somebody looks over shoulder or uses video record To defeat this issue, we proposed a shoulder surfing safe verification framework in view of graphical passwords, named Pass Matrix. Utilizing a one-time login marker per picture, clients can bring up the area of their pass-square without specifically clicking or touching it, which is an activity defenceless against bear surfing assaults. In view of the outline of the flat and vertical bars that cover the whole pass-picture, it offers no hint for aggressors to limit the secret word space regardless of whether they have more than one login records of that record. Moreover, we actualized a Pass Matrix model on Android and completed client tests to assess the memorability and ease of use. The test result demonstrated that clients can sign into

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |
|| Volume 13, Issue 5, May 2024 ||
| DOI:10.15680/IJIRSET.2024.1305084 |

the framework with a normal of 1:64 tries (Median=1), and the Total Accuracy of all login trials is 93:33% even two weeks after enrolment. The aggregate time devoured to sign into Pass Matrix with a normal of 3:2 pass-pictures is in the vicinity of 31:31 and 37:11 seconds and is viewed as worthy by 83:33% of members in our client think about. The review information in the client think about likewise demonstrated that Pass Matrix is down to earth in reality. Misapplications is one of the valuable application in the present circumstance. This is the easy method to speak with the administrator. Worker cost assert work process turned into an early possibility for enablement as it could take out treatment of supporting cost bills and rather utilize the camera of Smartphone to catch the bill..

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," 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/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 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-hatgoogle-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 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. 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 passwordbased 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: Teleduplication 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.
[46] J. Thorpe and P. van Oorschot, "Human-seeded attacks and exploiting hot-spots in graphical passwords," in Proceedings of 16th USENIX Security Symposium on USENIX Security Symposium. USENIX Association, 2007, p. 8.
[47] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: effects of tolerance and image choice," in Proceedings of the 2005 symposium on Usable privacy and security. ACM, 2005, pp. 1–12.
"Android 2.2 platform highlights," http://developer.android.com/sdk/android-2.2-highlights.html