Shoulder Surfing Resistant Graphical Authentication System

Nishant Pawar[1], Amir Shaikh[2], Rakesh More[3], Altaf Shaikh[4]

Sir Visvesvaraya Institute of Technology Nashik

Abstract - In modern IT world computer as well as information security is the most significant challenge. Authorized users should access the system or information. Password ensures that computer or information can be accessed by those who have been granted right to view or access them. Traditional password technique is a textual password which is also called alphanumeric password. But these textual passwords are easy to crack through various types of attack. So to overcome these vulnerabilities, a graphical password technique is introduced. 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.

Keywords - Graphical Password, Usability Authentication, Authentication, Shoulder Surfing Attacks, Graphical Passwords

I. Introduction

Textual passwords have been the most generally utilized validation strategy for quite a long time. Involved num-bers and upper-and lower-case letters, literary passwords are viewed as sufficiently solid to oppose against animal power assaults. In any case, a solid printed secret word is difficult to remember and recall. Thusly, customers tend to pick passwords that are either short or from the word reference, instead of unpredictable alphanumeric strings. Shockingly more repulsive, it isn't a remarkable case that customers may use only a solitary username and mystery word for various records. Shoulder surfing technique of gathering information such as usernames and passwords by watching over a person's shoulder while he/she logs into the system, by helping attackers to gain an access to the system person using the system keyboard is unaware that such action is monitored.

Today, authentication is achieved through the use of password technique. To prove and maintain the identity every user uses a password authentication. The traditional method of password is a textual (alphanumeric) password. It is the combination of alphabets, digits and special symbols. But it has various limitations. To remember easily, here the passwords are kept short and simple like personal names, family member names, birth dates, pet names, phone numbers etc. and so vulnerable to various types of attacks like easy to guess, brute force, dictionary attack, shoulder surfing, hidden camera, social engineering and malicious softwares like keylogger, spyware etc. To overcome these limitations users can use the strong (complex) password. But it is difficult to remember. So to memorize easily users write the password on paper and so it is easily available to anyone. Also nowadays various accounts are maintained by users for various purposes like personal computer, social network, email, online transactions etc. and to remember easily users can use the same password for all accounts and it reduces the security. So to reduce the shortcomings of textual passwords a new technique is developed which is a Graphical Password

.

II. MOTIVATION FOR THE PROJECT

When entering a PIN1 or password to access a phone, computer or ATM machine you might try to perform the authentication process discretely in case someone is watching. A graphical password system that has been implemented in a shoulder-surfing resilient way can be used without forcing the user to hide the process. In theory implementing this type of system could be a relatively simple task. However, depending on the area of usage the user will only accept some level of complexity before the system is deemed too difficult to use. Hence, creating a graphical password that is both user friendly and shoulder-surf resistant is a tougher task.

.

III. EXISTING SYSTEM

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. Therefore, users tend to choose passwords that are either short or from the dictionary, rather than random alphanumeric string.

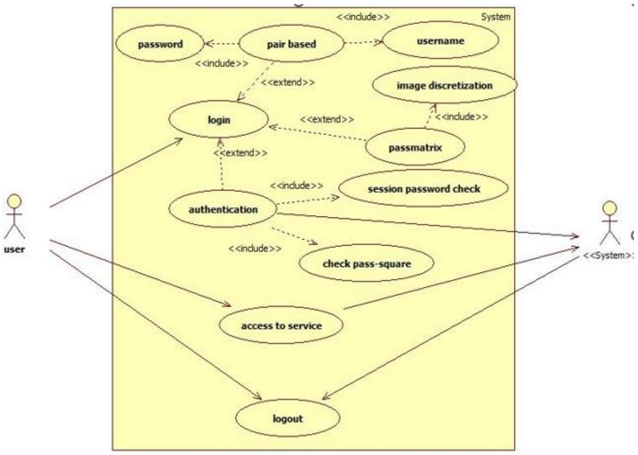

Fig: Use Case Diagram

IV. PROPOSE SYSTEM

Registration Phase:

1. A user creates his profile by getting into personal details and username. 2. Then the twenty five pictures square measure conferred to the user. These pictures square measure common to any or all the users. The user must choose some range of pictures to line as a secret. The user will repeat any image. this is often a secret for the user's step-I authentication. 3. After this user will choose any image from the stored image database or from the local memory according to his choice 4. currently he's conferred with question set and this image. The user must choose any 3 queries from this set. 5. To answer a question user has to click on any point on the image. So for three questions there will be three different points. Individual point is called as ROA (Region-Of-Answer). So there are three different ROAs for three different questions. Each ROA is described by a square (center and some tolerance in both X and Y axis).

Login Phase:
1. For step-I authentication user is asked for user name and graphical secret. The user should enter an accurate username and for graphical secret there ought to be an accurate choice of pictures in a very successive manner. The order of pictures at intervals the set can vary at
each login.
2. After this, and freelance of whether or not or not it's correct, for step-II authentication, the preselected image and therefore the preselected 3 queries are shown to the user.
3. Here the order of queries are going to be random. The user should click on the proper ROAs in line with the order of queries.
4. when the triple-crown entries (selections) in each the steps the user is a certified user to access the actual system.

V. SYSTEM SPECIFICATION

Hardware Requirements:
• System : Pentium IV 3.5 GHz or Latest Version.
• Hard Disk : 40 GB.
• Monitor : 14' Colour Monitor.
• Mouse : Optical Mouse.
• Ram : 1 GB.

Software Requirements:
• Operating system : Windows 10 or Windows 11.
• Coding Language : Java / J2EE (Jsp,Servlet)
• Data Base : My Sql Server
• Documentation : MS Office
• IDE : Eclipse Galileo
• Development Kit : JDK 1.6
• Server: Tomcat 6.0

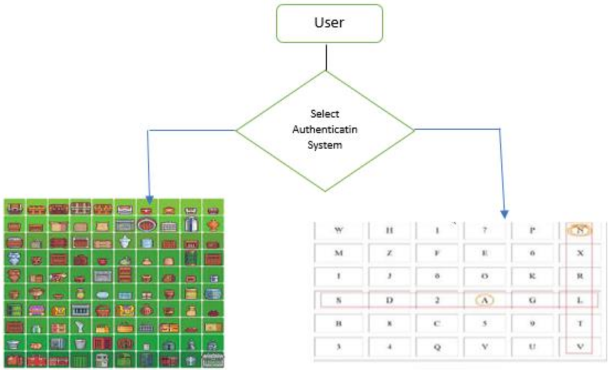

Figure: System Architecture Diagram

V1. 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 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] K. Gilhooly, "Biometrics: Getting back to business," Computer-world, 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.

[2] 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.

[3] 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

[4] M. Sasse, S. Brostoff, and D. Weirich, "Transforming the weakest linka human/computer interaction approach to usable and effec-tive security," BT technology journal, vol. 19, no. 3, pp. 122–131, 2001. [18] D. Hong, S. Man, B. Hawes, and M. Mathews, "A password scheme strongly resistant to spyware," in Proceedings of Interna-tional conference on security and management, 2004.

[5] 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 Interac-tion Special Interest.

[6] 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.

[7] 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. \

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] K. Gilhooly, “Biometrics: Getting back to business,” Computerworld, May, vol. 9, 2005.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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