International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 04 | Apr-2018 www.irjet.net p-ISSN: 2395-0072

Authentication Using Graphical Password

Amrut Pallewar[1], Sparsh Raina[2], Sanjeev Sonawane[3], Kisalay[4]

[1,2,3,4] *Department of Computer Technology, D Y Patil College of Engineering Ambi, Pune, Maharashtra, India.*

Abstract - *The users input their passwords in a public place, they may be at risk of attackers stealing their password. An attacker can capture a password by direct observation or by recording the individual's authentication session. This is referred to as shoulder surfing and is a known risk, of special concern when authenticating in public places. Until recently, the only defense against shoulder-surfing was the alertness on the part of the user. Shoulder surfing resistant password authentication mechanism assure shoulder surfing resistant authentication to user. It allows user to authenticate by entering pass-word in graphical way at insecure places because user never have to click directly on password icons. Usability testing of this mechanism showed that novice users were able to enter their graphical password accurately and to remember it over time. However, the protection against shoulder-surfing comes at the price of longer time to carry out the authentication.*

Key Words: *Tactile UI, Security, PIN entry, H5.2, Haptic I/O, Security, Human Factors.*

1. INTRODUCTION

The shoulder surfing attack is an attack that can be performed by the adversary to obtain the users password by watching over the users shoulder as he enters his password. However, most of the current graphical password schemes are vulnerable to shoulder-surfing a known risk where an attacker can capture a password by direct observation or by recording the authentication session. Due to the visual interface, shoulder-surfing becomes an exacerbated problem in graphical passwords. A graphical password is easier than a text-based password for most people to remember. Suppose an 8- character password is necessary to gain entry into a particular computer network. Strong passwords can be produced that are resistant to guessing, dictionary attack. Key-loggers, shoulder-surfing and social engineering. Graphical passwords have been used in authentication for mobile phones, ATM machines, E-transactions.

1.1 Motivation of the project

We refer to the Pass Points in which the user picks up several points (3 to 5) in an image during the password creation phase and re-enters each of the pre-selected click-points in a correct order within its tolerant square during the login phase. Comparing to traditional PIN and textual password space and enhances password memorability. Unfortunately, this graphical authentication scheme is vulnerable to shoulder surfing attacks. Hence, based on the Pass Points, we add the idea of using one-time session passwords and distracters to develop our Pass Matrix authentication system that is resistant to shoulder surfing attacks.

1.2 A New Graphical Password scheme

System presents a secure graphical authentication framework named Pass Matrix that protects users from becoming victims of shoulder surfing attacks while inputting passwords out in the open through the use of one-time login indicators. A login indicator is randomly produced for each pass-picture and will be futile 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. The following are the goals and objectives of the new system:-

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. PROCEDURE:

2.1. Registration phase:

In 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 n is decided by the user after considering the trade-off between security and usability of the system. The only purpose of the username is to give the user an imagination of having a personal account. Then the systems will Discretization the selected images by using pass matrix approach into x into y grinds by calculating ht and wt of images. Then system will create the graphical based password after clicking on the images selected from I.

2.2. Authentication phase:

A login indicator LI is comprised of a letter and a number is created by the login indicator generator module. The LI will be shown when the user login with his email. In this case, the indicator is conveyed to the user by visual feedback. The indicator can also be delivered through a predefined image. Generating horizontal and vertical access control for login indicator based user selected images at the time of registration this access control will change at every login time i.e. LI is defined for one time use only. The generated access control will be send to user registered email address. User will enter the graphical password based on generated pass-values i.e. access controls.

2.3. Steps in Pass-Matrix:

1) At the time of registration user fill the details as well as selected images.

2) That images apply to pass matrix.

3) The pass matrix defined to rows and column i.e number and character.

4) At the time login user choose that images when user select the images at the time of registration.

5) All pass values are shuffled and randomly generate the sequence by using login indicator.

6) Creating user access control then notify user about access control.

7) Selected pass value for login and adding secrete bit.

3. APPLICATIONS:

1) During online transaction.

2) Authenticating online social media.

3) ATM Operating.

4) System Password Security.

5) Banking Application.

4. Use case Diagram:

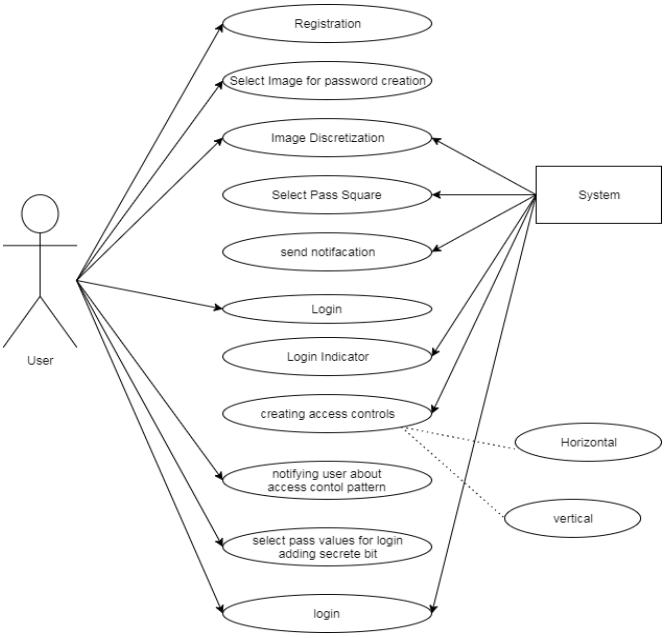

Diagram 1: Use case diagram of Authentication Phase

5. System Architecture Diagram

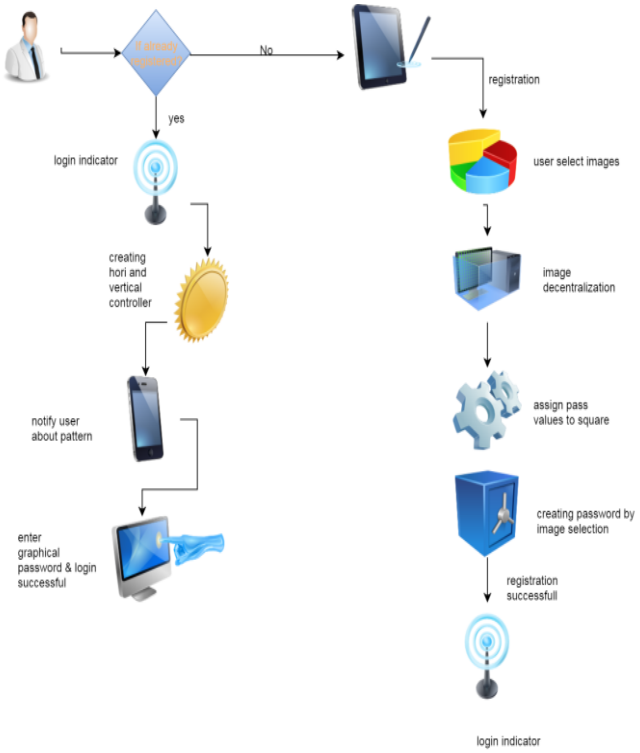

Diagram 2: Diagram showing the system architecture of authentication using graphical passwords.

6. CONCLUSION:

System conclude that in the proposed shoulder surfing resistant authentication system based on graphical passwords, named Pass Matrix. 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..In Pass Matrix, a password consists of only one pass-square per pass-image for a sequence of n images. Pass Matrixes' authentication consists of a registration phase and an authentication phase as described below: At this stage, the user creates an account which contains a user name and a password. So finally System resolve shoulder surfing attack very easily.

7. ACKNOWLEDGMENT:

We would like to show our gratitude to Dr.MininathNighot (HOD, Computer Engg.) for sharing their pearls of wisdom with us during the course of this research, and we thank the reviewers for their insights.

We are also immensely grateful to Prof. Santosh Biradar for their comments on an earlier version of the manuscript, although any errors are our own and should not tarnish the reputations of these esteemed persons.

8. REFERENCES:

[1] 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.

[2] 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.

[3] 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.Tavel, P. 2007 Modeling and Simulation Design. AK Peters Ltd.

[4] Z. Zhen, 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.

[5] X. Bai, W. Gu, S. Chellappan, X. Wang, D. Xian, and B. Ma, "Pas: predicate-based authentication services against powerful passive adversaries," in 2008 Annual Computer Security Applications Conference. IEEE, 2008, pp. 433–442.

[6] L. Wang, X. Chang, Z. Ren, H. Go, 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.

[7] D. Kim, P. Dumpy, 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.Spector, A. Z. 1989. Achieving application requirements. In Distributed Systems, S. Millender

[8] A. Bianchi, I. Oakley, V. Kotukus, 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.

[9] 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.

[10] 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.

[11] T. Kwon, S. Shin, and S. Na, "Covert attention 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.

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