Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 5, Issue 05, May -2018

SHOULDER SURFING

Sneha Rampure[1], Sonali Salunke[2], Snehal Khodade[3], Padmaja Kawade[4]

[1]Department of Computer Engineering, MITCOE. Pune
[2]Department of Computer Engineering, MITCOE Pune
[3]Department of Computer Engineering, MITCOE. Pune
[4]Department of Computer Engineering, MITCOE. Pune

Abstract — *when users input their passwords in an exceedingly public place, they will be at risk of attackers stealing their watchword. Associate degree wrongdoer will capture a watchword by direct observation or by recording the individuals' authentication session. This is said as shoulder-surfing and could be a far-famed risk, of special concern once authenticating in public places. Till recently, the sole defense against shoulder-surfing was the alertness on the part of the user. Shoulder surfing resistant watchword authentication mechanism assure shoulder-surfing resistant authentication to user. It allows user to demonstrate by getting into pass-word in graphical way at insecure places as a result of user never ought to click directly on watchword icons. Usability testing of this mechanism showed that novice users were ready to enter their graphical watchword accurately and to recollect it over time. However, the protection against shoulder-surfing comes at the worth of longer time to hold out the authentication.*

Keywords*: Tactile UI, security, PIN entry, user study, H5.2. User Interfaces: Haptic I/O, Security, Experimentation, Human Factors.*

I. INTRODUCTION

The shoulder aquatics attack in associate degree attack which will be performed by the soul to obtain the user's countersign by looking over the user's shoulder as he enters his countersign. As standard countersign schemes area unit susceptible to shoulder aquatics, Sobrado and Birget projected 3 shoulder aquatics resistant graphical countersign schemes. However, most of the current graphical countersign schemes area unit susceptible to shoulder-surfing a famed risk wherever associate degree aggressor will capture a countersign by direct observation or by recording the authentication session. Attributable to the visual interface, shoulder-surfing becomes associate degree exacerbated downside in graphical passwords. A graphical countersign is easier than a text-based countersign for most people to remember. Suppose associate degree 8- character countersign is important to realize entry into a specific electronic network. Sturdy passwords will be created that area unit resistant to guess, wordbook attack. Key-loggers, shoulder-surfing and social engineering. Graphical passwords are employed in authentication for mobile phones, ATM machines, E-transactions.

II. PROBLEM STATEMENT

Secure graphical authentication framework named Pass Matrix that is planned system presents that protects users from becoming victims of shoulder surfboarding attacks while inputting passwords get into the open through the employment of one-time login indicators.

Haphazardly produced for every pass-picture by a login indicator and will be futile after the session terminates. Better security against shoulder surfing attacks provided by the login indicator , since users use a dynamic pointer to point out the position of their positive identifications rather than clicking on the password object directly.

2. Goals and Objectives

- The drawback of the way to perform authentication publicly so shoulder surfboarding attacks can be relieved.
- The drawback of the way to increase positive identification house than that of the standard PIN.
- The drawback of the way to with efficiency search precise positive identification objects throughout the authentication section.
- The drawback of requiring users to con further data or to perform further computation throughout authentication.
- The drawback of restricted usability of authentication schemes that may be applied to some devices solely.

3. Scope

With the increasing quantity of mobile devices and internet services, users can access their personal accounts to send confidential business emails, transfer photos to albums within the cloud or remit cash from their e-bank account anytime and anywhere. While work into these services publicly, they may expose their passwords to unknown parties unconsciously. Individuals with malicious intent could watch the full authentication procedure through ubiquitous video

cameras and police work instrumentality, or perhaps a mirrored image on a window. Once the assailant obtains the positive identification, they may access personal accounts which would positively cause a great threat to one's assets. Shoulder surfing attacks have gained a lot of and more attention within the past decade.

III. EXISTING SYSTEM

Using ancient textual passwords or PIN methodology, users need to type their passwords to authenticate themselves and therefore these passwords are often discovered simply if somebody peeks over shoulder or uses video devices like cell phones shoulder water sport attacks have posed an excellent threat to users' privacy and confidentiality as mobile devices are getting indispensable in fashionable life. Within the period of time, the graphical capability of hand-held devices was weak; the color and pel it might show was restricted. With the increasing quantity of mobile devices and internet services, users can access their personal accounts to send confidential business emails, transfer photos to albums within the cloud or remit cash from their e-bank account anytime and anywhere. Whereas work into these services publicly, they may expose their passwords to unknown parties unconsciously.

Disadvantages of Existing System
(1) Security weakness.
(2) The easiness of getting passwords by observers publically.
(3) The compatibility problems to devices.

IV. PROPOSED SYSTEM

To overcome this downside, we tend to plan a shoulder surfing resistant authentication system based on graphical passwords, named Pass Matrix. Using a one-time login indicator per image, users will entails the placement of their pass-square without directly clicking or touching it, that is associate degree action prone to shoulder surfing attacks. due to the look of the horizontal and vertical bars that cowl the complete pass-image, it offers no clue for attackers to slim down the word area notwithstanding they need quite one login records of that account. In Pass Matrix, a word consists of just one pass-square per pass-image for a sequence of n pictures. The amount of pictures (i.e., n) is user-defined. In Pass Matrix, users select one sq. per image for a sequence of n pictures instead of n squares in one image as that within the Pass Points theme. Pass Matrix's authentication consists of a registration part associate degreed an authentication phase as delineated below: At this stage, the user creates associate degree account that contains a username and a word. The word consists of just one pass-square per image for a sequence of n pictures. The quantity of images (i.e., n) is decided by the user when considering the trade-off between security and usability of the system. At this stage, the user uses his/her username, word and login indicators to log into Pass Matrix.

Advantages of planned System

1. Extremely secured
2. Device compatible
3. Straightforward to handle

V. Mathematical Model

Let S be the Whole system which consists:
S= {IP, Pro, OP}.
Where,

A. IP is the input of the system.
B. Pro is the procedure applied to the system to process the given input.
C. OP is the output of the system.

A. Input:
IP = {u, I, LI, ht, wt, pv, n}.
Where,

1. u be the user.
2. I be set of images used for creating graphical password.
3. ht be the height of image.
4. wt be the width of the image.
5. pv be the pass values of the selected image for generating graphical password.
6. LI be the login indicator used at the time of login.
7. n be the number of images chosen for creating graphical based password from set of images I.

B. Procedure:

1. Registration phase:

i. 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.
ii. 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.
iii. 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.
iv. Then system will create the graphical based password after clicking on the images selected from I.

2. Authentication phase:

i. A login indicator LI is comprised of a letter and a number is created by the login indicator generator module.
ii. 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.
iii. 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.
iv. The generated access control will be send to user registered email address.
v. User will enter the graphical password based on generated pass-values i.e. access controls.

C. Output:

Secure and authenticated system based on Pass Matrix based graphical password system.

VI. ALGORITHM

1. At time of registration user fill the details as well as select 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 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. Select pass value for login and adding secrete bit.

Procedure follow by project:-

1) **Introduction phase:** We explained the basic idea and purpose of Pass Matrix with a presentation and showed participants how to use the system with some simple animations.

2) **Registration phase**: Participants created an account consisting of a username and a password in Pass Matrix. In the introduction phase, participants were educated by our tutorial so that

a) They knew that they should register their account in a private place. Hence it is safe to choose pass-squares by simply clicking on them during the registration phase.
b) They knew that they should choose the pass quares that do not contain light objects but are meaningful to them.
c) They knew that they should re-choose the chosen square in each pass-image for confirmation.
d) They knew that they should set three or more pass-images.

3**) Practice phase**: Participants were told to log into their account in a practice mode. They repeated this step until they thought they knew how to control the horizontal and vertical bars. The Pass Matrix system gives the authentication feedback to users only after the whole password input process is completed, not in between each pass-image.

4) **Login phase:** After practicing, participants were requested to log into their account formally in a login mode.

5) Participants were also asked to answer a short demographic questionnaire about some simple personal data and their personal experience on mobile phones or authentication systems.

6) Each participant was then given an answer sheet, containing the information of a third person's two previous login records. Participants were asked to figure out the third person's pass-squares from these two given

login records. An incentive gift was provided if they are able to successfully crack the password in ten tries (i.e., ten guesses on the answer sheet). Two weeks were given to crack the password.

A. SYSTEM ARCHITECTURE

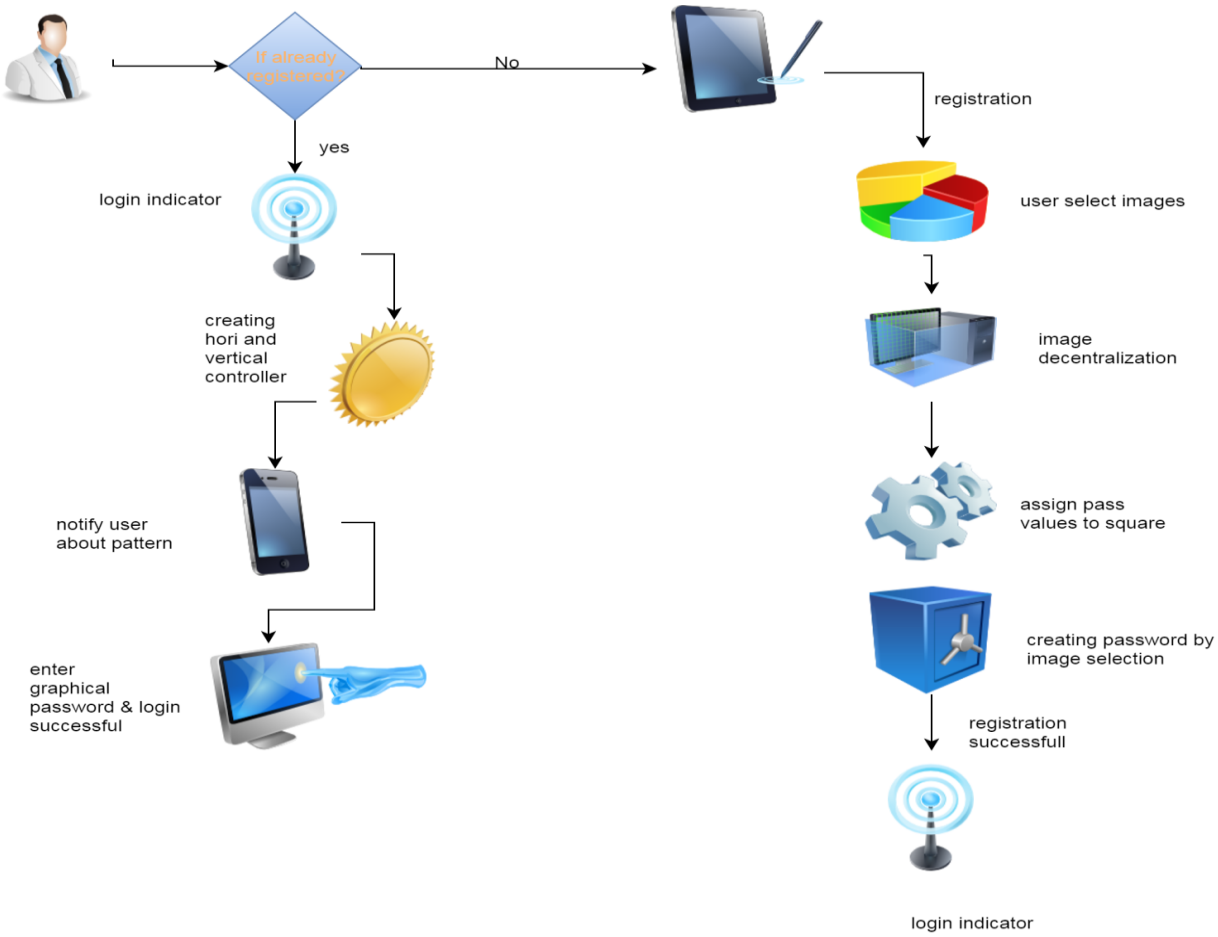

Fig.: System Architecture

B. HARDWARE REQUIREMENT

- System Processors : Core2Duo
- Speed : 2.4 GHz
- Hard Disk : 150 GB

VII. APPLICATION

- At online transaction.
- To online social media.

VIII. CONCLUSION AND FUTURE WORK

Proposed a shoulder surfing resistant authentication system based on graphical passwords, named Pass Matrix. employing a one-time login indicator per image, users can denote the situation of their pass-square while not directly clicking or touching it, which is associate action liable to shoulder surfboarding attacks. because of the planning of the horizontal and vertical bars that cover the whole pass-image, it offers no clue for attackers to slim down the positive identification area even though they have over one login records of that account. what is more, we have a tendency to enforced a Pass Matrix paradigm on automaton and meted out user experiments to judge the memorability and value. The experimental result showed that users can log into the system with a median of 1:64 tries (Median=1), and therefore the Total Accuracy of all login trials is 93:33% even time period once registration. the full time consumed to log into Pass Matrix with a median of 3:2 pass-images is between 31:31 and 37:11 seconds and is taken into account acceptable by 83:33% of participants in our user study. based on the experimental results and survey knowledge, Pass Matrix is a novel and easy-to-use graphical positive identification authentication system, which can effectively alleviate shoulder-surfing attacks. additionally, Pass Matrix can be applied to any authentication state of affairs and device with simple input and

output capabilities. The survey data in the user study conjointly showed that Pass Matrix is practical within the globe. we can enhance the system by using video frames to pick out the image to generate the pass matrix.

ACKNOWLEDGMENT

We acknowledge Principal, Head of department and guide Prof.Asmita Gorave of our project for all the support and help rendered. We express profound feeling of appreciation to our regarded guardians for giving the motivation required to the finishing of paper.

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. 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.
4. 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.
5. A. Paivio, T. Rogers, and P. Smythe, "Why are pictures easier to recall than words?" Psychonomic Science, 1968.
6. D. Nelson, U. Reed, and J. Walling, "Picture superiority effect," Journal of Experimental Psychology: Human Learning and Memory, vol. 3, pp. 485–497, 1977.
7. 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.

