Impact Factor (SJIF): 5.301

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 5, Issue 5, May-2018

SHOULDER SURFING ATTACK RESISTENT GRAPHICAL AUTHENTICATION SYSTEM

Kiran thorat, Nishant Mehare, Amarnath Sutar, Vaishnavi Lavhale, Prof. Gaurav Gupta
Department of Computer Engineering
kiranthorat80@gmail.com , nishantmehare@gmail.com ,amarnath.sutar.007@gmail.com ,
vaishnavilavhale@gmail.com, guptagaurav.be@gmail.com

Abstract - When users input their passwords in a very public place, they'll be in danger of attackers stealing their secret. Associate degree assaulter will capture a secret by direct observation or by recording the people authentication session. This is often cited as shoulder-surfing and may be an illustrious risk, of special concern once authenticating publically places. Till recently, the sole defense against shoulder-surfing was the alertness on the part of the user. Shoulder surfing resistant secret authentication mechanism assure shoulder-surfing resistant authentication to user. It permit user to attest by coming into password in graphical approach at unconfident places as a result of user ne'er ought to click directly on secret icons. Usability testing of this mechanism showed that beginner users were able to enter their graphical secret accurately and to recollect it over time.

Keywords- Shoulder surfing, attack, and authentication

I. INTRODUCTION

The shoulder surfing attack inside an attack which resolve be performed by the important person to get the user's report by look more than the user's shoulder as he enter his word. However, most of this graphical word schemes are responsible to shoulder-surfing a famous risk wherever an recommended will capture a word by direct observation or by recording the authentication session. Owing to the visual interface, shoulder-surfing becomes AN exacerbated drawback in graphical passwords. A graphical word is simpler than a text-based word for many individuals to recollect. Suppose an 8- character word is important to achieve entry into a selected electronic network. Secured passwords may be created that are proof against approximation, lexicon attack. Key-loggers, shoulder-surfing and social engineering. Graphical passwords are employed in authentication for mobile phones, ATM machines, E-transactions.

II. LITERATURE SURVEY

Multi-touch passwords for mobile device access

Authors: Oakley and A. Bianchi

Description: Draw-a-Secret codeword schemes, just like the Google robot Pattern Lock, entail stroke out a form on barely screen. This paper explores techniques for increasing the richness of this input modality (multitouch input, off-target interaction) so as to extend codeword entropy and resistance to observation. A formative user study highlights user perceptions and usefulness problems with reference to this style house and suggests directions for future development of this idea.

III. EXISTING SYSTEM

Using antique text passwords or PIN methodology, users have to be obligated to kind their passwords to confirm themselves and therefore these passwords is disclose simply if somebody peeks over shoulder or uses video devices like cell phones shoulder water sport attacks have posed a good threat to users' privacy and confidentiality as mobile devices are getting indispensable in fashionable life. Within the period, the graphical capability of hand-held devices was weak; the color and element it might show was restricted. With the increasing quantity of mobile devices and net services, users will 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 anyplace. Whereas work into these services publically, they'll expose their passwords to unknown parties unconsciously.

DISADVANTAGES

(1) Security weakness

(2) The easiness of obtaining passwords by observers in public

(3) The compatibility issues to devices

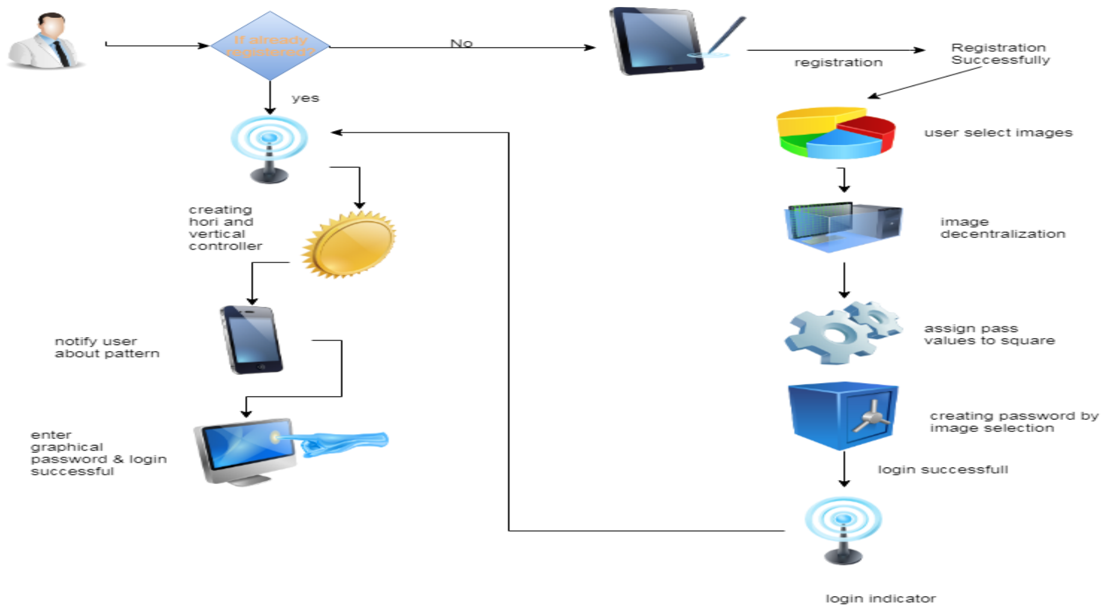
IV. PROPOSED SYSTEM

To overcome this obstruction, we tend to intended a shoulder surfing resistant authentication system first and foremost based on graphical passwords, named Pass Matrix. Employing a one-time login indicator per image, users will suggests the situation of their pass-square while not directly clicking it , that is associate action liable to shoulder aquatics attacks. As a result of the look of the horizontal and vertical bars that cowl the complete pass-image, it offers no clue for attackers to slim down the watchword area though they need over one login records of that account. In PassMatrix, a watchword consists of just one pass-square per pass-image for a sequence of n pictures. The quantity of pictures (i.e., n) is user-defined. In PassMatrix, users select one sq. per image for a sequence of n pictures instead of n squares in one image as that within the PassPoints theme. PassMatrix's authentication consists of a registration part associated an authentication part as represented below: At this stage, the user creates associate account that contains a username and a watchword. The watchword consists of just one pass-square per image for a sequence of n pictures. The quantity of pictures (i.e., n) is set by the user when considering the trade-off between security and value of the system. At this stage, the user uses his/her username, watchword and login indicators to log into PassMatrix.

ADVANTAGES

1. Highly secured
2. Device compatible
3. Easy to handle

V. SYSTEM ARCHITECTURE


If already registered?
No
registration
Registration Successfully
yes
user select images
image decentralization
creating hori and vertical controller
assign pass values to square
notify user about pattern
creating password by image selection
enter graphical password & login successful
login successfull
login indicator

.

VI. 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.Rgistration phase:

In this stage we have only registered user name password and some other information fill it.

2. Login phase:

i. In this stage, the user creates an account which contains a username . 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.

3. 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.

RESULTS

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 PassMatrix 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 PassMatrix. 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 have to choose passquares 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.

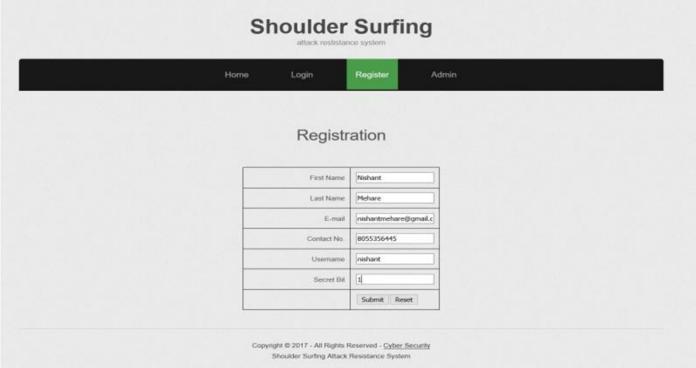
d) They knew that they should set three or more pass-images.

3) **Practice phase**: Participants were told to log into their account. They repeated this step until they thought they knew how to control the horizontal and vertical bars. The PassMatrixsystem 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.

Registration :

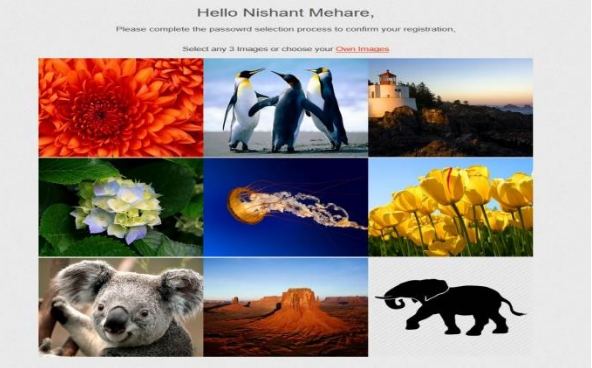


Shoulder Surfing
attack restistance system

Registration

First Name	Nishant
Last Name	Mehare
E-mail	nishantmehare@gmail.c
Contact No.	8055356445
Username	nishant
Secret Bit	1
	Submit Reset

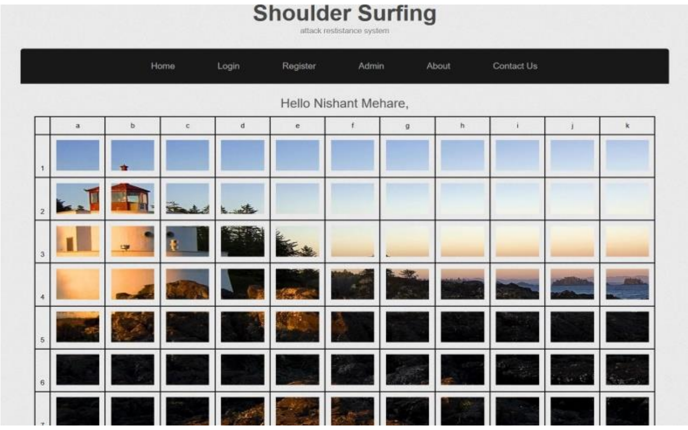
Copyright © 2017 - All Rights Reserved - Cyber Security
Shoulder Surfing Attack Resistance System



Hello Nishant Mehare,

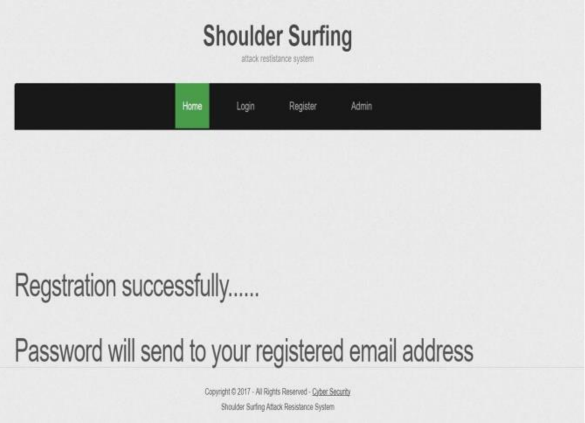
Please complete the passowrd selection process to confirm your registration,

Select any 3 Images or choose your Own Images



Shoulder Surfing
attack restistance system

Hello Nishant Mehare,



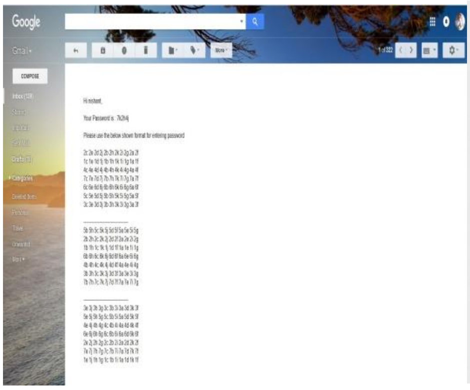
Shoulder Surfing
attack restistance system

Regstration successfully......

Password will send to your registered email address

Copyright © 2017 - All Rights Reserved - Cyber Security
Shoulder Surfing Attack Resistance System

Login and Verification:

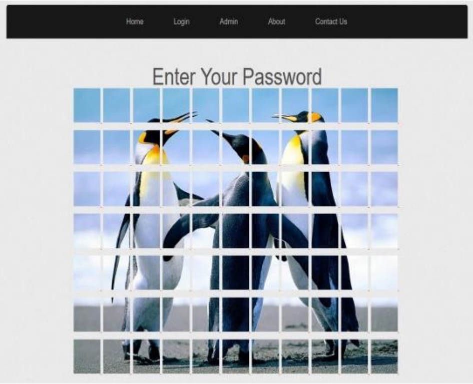


Hi nishant,

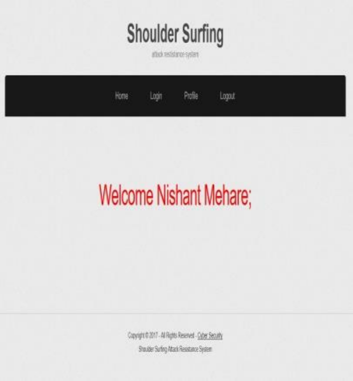
Your Password is : 7k2h4j

Please use the below shown format for entering password

```
2c 2e 2d 2j 2b 2h 2k 2i 2g 2a 2f
1c 1e 1d 1j 1b 1h 1k 1i 1g 1a 1f
4c 4e 4d 4j 4b 4h 4k 4i 4g 4a 4f
7c 7e 7d 7j 7b 7h 7k 7i 7g 7a 7f
6c 6e 6d 6j 6b 6h 6k 6i 6g 6a 6f
5c 5e 5d 5j 5b 5h 5k 5i 5g 5a 5f
3c 3e 3d 3j 3b 3h 3k 3i 3g 3a 3f
____________________
5b 5h 5c 5k 5j 5d 5f 5a 5e 5i 5g
2b 2h 2c 2k 2j 2d 2f 2a 2e 2i 2g
1b 1h 1c 1k 1j 1d 1f 1a 1e 1i 1g
6b 6h 6c 6k 6j 6d 6f 6a 6e 6i 6g
4b 4h 4c 4k 4j 4d 4f 4a 4e 4i 4g
3b 3h 3c 3k 3j 3d 3f 3a 3e 3i 3g
7b 7h 7c 7k 7j 7d 7f 7a 7e 7i 7g
____________________
3e 3j 3h 3g 3c 3b 3i 3a 3d 3k 3f
5e 5j 5h 5g 5c 5b 5i 5a 5d 5k 5f
4e 4j 4h 4g 4c 4b 4i 4a 4d 4k 4f
6e 6j 6h 6g 6c 6b 6i 6a 6d 6k 6f
2e 2j 2h 2g 2c 2b 2i 2a 2d 2k 2f
7e 7j 7h 7g 7c 7b 7i 7a 7d 7k 7f
1e 1j 1h 1g 1c 1b 1i 1a 1d 1k 1f
```



Enter Your Password



Shoulder Surfing
attack restistance system

Welcome Nishant Mehare;

Copyright © 2017 - All Rights Reserved - Cyber Security
Shoulder Surfing Attack Resistance System

CONCLUSION

Proposed a shoulder surfing resistant confirmation system supported graphical passwords, named Pass Matrix. employ a one-time login indicator per image, users will show the placement of their pass-square while not directly clicking or touching it, which is Associate in nursing action prone to shoulder surfboarding attacks. As a result of the planning of the horizontal and vertical bars that cowl the complete pass-image, it offers no clue for attackers to slim down the positive identification area albeit they need over one login records of that account. Moreover, we be inclined to implement a Pass Matrix image on automatic man and meted out user experiment to judge the memo ability and usefulness. The experimental result showed that users will log into the system with a median of 1:64 tries (Median=1), and also the Total Accuracy of all login trials is 93:33% even period of time once registration. The entire 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. Supported the experimental results and survey knowledge, PassMatrix may be a novel and easy-to-use graphical positive identification authentication system, which might effectively alleviate shoulder-surfing attacks.

REFFERENCES

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. 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. 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