

**Shoulder Surfing Attack Resistant System**¹Rahul Kulkarni, ²Tushar Tagadpallewar, ³Kunal Mahajan, ⁴Ajinkya Khalate^{1,2,3,4}Computer Department, Sinhgad Institute of Technology

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 permits user to attest by coming into pass-word in graphical approach at insecure places as a result of user ne'er ought to click directly on secret icons. Usability testing of this mechanism showed that novice users were able to enter their graphical secret accurately and to recollect it over time.

Keywords- Shoulder surfing, attack, 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**1. Multi-touch passwords for mobile device access**

Authors: I. 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.

2. The doodb graphical password database: Data analysis and benchmark results

AUTHORS: M. Martinez-Diaz, J. Fierrez, and J. Galbally

Description: We gift DooDB, a doodle information containing knowledge from one hundred users captured with slightly screen-enabled mobile device beneath realistic conditions following a scientific protocol. The database contains 2 corpora: 1) doodles and 2) pseudo-signatures, that are simplified finger-drawn versions of the written signature. The dataset includes real samples and forgeries, made beneath worst-case conditions, wherever attackers have visual access to the drawing method. applied math and qualitative analyses of the info are bestowed, examination doodles and pseudo-signatures to written signatures. Time variability, learning curves, and discriminative power of various options also are studied. Verification performance against forgeries is analyzed exploitation progressive algorithms and benchmark results are provided.

3. Graphical Password-Based User Authentication With Free-Form Doodles

Authors: M. Martinez-Diaz, J. Fierrez, and J. Galbally

Description: User authentication mistreatment straightforward gestures is currently common in transportable devices. during this work, authentication with free-form sketches is studied. Verification systems mistreatment dynamic time distortion and mathematician mixture models square measure planned supported dynamic signature verification approaches. the foremost discriminant options square measure studied mistreatment the consecutive forward floating choice algorithmic program. the consequences of the time lapse between capture sessions and also the impact of the coaching set size also are studied. Development and validation experiments square measure performed mistreatment the DooDB information, that contains passwords from one hundred users captured on a wise phone touchscreen. Equal error @IJAERD-2016, All rights Reserved

rates between third and eight square measure obtained against random forgeries and between twenty first and twenty second against adept forgeries. High variability between capture sessions will increase the error rates.

III. EXISTING SYSTEM

Using ancient text passwords or PIN methodology, users have to be compelled to kind their passwords to certify themselves and therefore these passwords is disclosed 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 obstacle, we tend to planned a shoulder surfing resistant authentication system primarily 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 or touching 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 Pass Matrix, 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 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 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 Pass Matrix.

ADVANTAGES

1. Highly secured
2. Device compatible
3. Easy 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:

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 discretize the selected images by using pass matrix approach into x into y grids by calculating h_t and w_t 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. CONCLUSION

Proposed a shoulder surfing resistant authentication system supported graphical passwords, named PassMatrix. Employing a one-time login indicator per image, users will show the placement of their pass-square while not directly clicking or touching it, that is Associate in Nursing action prone to shoulder surfing 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 tend to enforce a PassMatrix image on mechanical man and meted out user experiments to judge the memorability 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 PassMatrix 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.

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 2015, 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, 2014, 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, 2013.
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.
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.