Impact Factor (SJIF): 4.542

International Journal of Advance Research in Engineering, Science & Technology

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

Volume 4, Issue 6, June-2017

SHOULDER SURFING ATTACK

Priti Panmand
M.E. Computer Engineering
RMDSSOE
Pune, India

Prof. Pradnya Kasture
Dept. Of Computer Engg
RMDSSOE
Pune, India

Abstract — Authentication supported passwords is employed mostly in applications for laptop security and privacy. However, human actions like selecting unhealthy passwords associate degreed inputting passwords in an insecure approach area unit considered the weakest link within the authentication chain. Instead of discretionary alphabetical strings, users tend to decide on passwords either short or substantive for straightforward acquisition. With net applications and mobile apps stilt up, folks will access these applications anytime and anyplace with numerous devices. This evolution brings nice convenience however additionally will increase the chance of exposing passwords to shoulder aquatics attacks. Attackers will observe directly or use external recording devices to gather user's credentials. to beat this downside, we have a tendency to planned a completely unique authentication system PassMatrix, supported graphical passwords to resist shoulder aquatics attacks. With a one-time valid login indicator and circulatory horizontal and vertical bars covering the whole scope of pass-images, PassMatrix offers no hint for attackers to work out or slender down the secret even they conduct multiple camera-based attacks. We have a tendency to additionally enforce a PassMatrix example on golem and administered real user experiments to judge its memorability and usefulness. From the experimental result, the planned system achieves higher resistance to shoulder aquatics attacks whereas maintaining usability.

Keywords- PassMatrix, Authentication, Shoulder Surfing Attack, Birget, Sobrado.

I. INTRODUCTION

The shoulder surfing attack in Associate in Nursing attack that may be performed by the soul to get the users parole by looking at over the users shoulder as he enters his parole. As standard parole schemes are prone to shoulder surfboarding, Sobrado and Birget planned 3 shoulder surfboarding resistant graphical parole schemes. However, most of the present graphical parole schemes are prone to shoulder-surfing [7-10], an acknowledged risk wherever Associate in nursing assaulter will capture a parole by direct observation or by recording the authentication session. Attributable to the visual interface, shoulder-surfing becomes Associate in nursing exacerbated downside in graphical passwords. The shoulder surfing attack in Associate in nursing attack that may be performed by the soul to steal the users parole credentials by looking at over the users shoulder as he enters his parole. As standard parole schemes are prone to shoulder surfboarding, Sobrado and Birget planned 3 shoulder surfboarding resistant graphical parole schemes. However, most of the present graphical parole schemes are prone to shoulder-surfing [7-10], a acknowledged risk wherever associate in nursing assaulter will capture a parole by direct looking at or by recording the authentication session of the user device.

Due to the visual interface, shoulder-surfing becomes an exacerbated drawback in graphical passwords. 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 publicly, they will expose their passwords to unknown parties unconsciously. Folks with malicious intent might watch the total authentication procedure through ubiquitous video cameras and police investigation instrumentation, or maybe a mirrored image on a window. Once the aggressor obtains the secret, they might access personal accounts which would positively create an excellent threat to ones assets. Shoulder surfing attacks have gained additional and additional attention within the past decade. exploitation antecedently ancient ways like matter passwords or PIN methodology, users ought to kind their passwords to certify themselves and therefore these passwords may be discovered simply if somebody peeks over shoulder or uses recording devices like cell phones shoulder surfriding attacks have exhibit an excellent threat to users privacy and confidentiality as mobile devices are getting indispensable in trendy life.

In 2006, Wiedenbeck et al. planned PassPoints during which the user picks up many points (3 to 5) in a picture throughout the creation section and re-enters every of those pre-selected click-points during a correct order among its tolerant sq. throughout the login section. Examination to ancient PIN and matter passwords, the Pass- Points theme considerably will increase the password space and enhances password memorability. We present, this graphical authentication theme is prone to shoulder surfboarding attacks. Hence, supported the PassPoints, we tend to add the thought of victimization one-time session passwords and distractors to develop our PassMatrix authentication system

that's proof against shoulder surfboarding attacks. We tend to gift a secure graphical authentication system named PassMatrix that protects users from changing into victims of shoulder surfboarding attacks once inputting passwords publicly through the usage of one-time login indicators. A login indicator is haphazardly generated for every pass-image and can be useless when the session terminates. The login indicator provides higher security against shoulder surfboarding attacks, since users use a dynamic pointer to means the position of their passwords instead of clicking on the password object directly.

II. LITERATURE REVIEW

1. Paper Name: Cryptanalysis of Password Authentication Schemes: Current Status and Key Issues
Authors:Sandeep K. Sood, Anil K.Sarje and Kuldip Singh
Description: Password is that the most ordinarily used technique for user authentication owing to its simplicity and convenience. The most advantage of passwords is that users will memories them simply without having any hardware to store them. Economical secret authentication schemes area unit needed to demonstrate the legitimacy of remote users over associate degree insecure communicating. During this paper, we have a tendency to present the survey of all presently obtainable secret primarily based authentication schemes and classified them in terms of many crucial criteria. This study can facilitate in developing completely different secret primarily based authentication techniques, that aren't at risk of completely different attack situations. Two and three party key exchange protocols need secure authentication mechanism for achieving the specified goals and satisfying the protection needs of a perfect secret primarily based authentication theme. Good cards, that area unit utilized in monetary transactions need extremely secure authentication protocols.

2. Graphical Password Authentication
Authors:ShraddhaM. Gurav,Leena S. Gawade,Prathamey K. Rane,Nilesh R. Khochare
Description: Graphical secret is one in all the choice resolution to character set secret because it is incredibly tedious method to recollect character set secret. Once any application is given user friendly authentication it becomes straightforward to access and use that application. One in all the key reasons behind this technique is in line with psychological studies human mind will simply bear in mind pictures than alphabets or digits. During this paper we have a tendency to area unit representing the authentication given to cloud by mistreatment graphical secret. We've projected cloud with graphical security by means that of image secret. We have a tendency to area unit providing one in all the algorithms that area unit supported choice of username and pictures as a secret. By this paper we have a tendency to try to grant set of pictures on the idea of alphabet series position of characters in username. Finally cloud is given this graphical secret authentication.

3. Paper Name: The design and analysis of graphicalpasswords
Authors: Ian Jermyn, Alain Mayer, Fabian Monrose, Michael K. Reiter, and Aviel D. Rubin
Description: In this paper we have a tendency to propose and assess new graphical watchword schemes that exploit options of graphical input displays to attain higher security than text- based mostly passwords. Graphical input devices alter the user to decouple the position of inputs from the temporal arrangement during which those inputs occur, and that we show that this decoupling are often won't to generate watchword schemes with considerably larger (memorable) watchword areas. So as to judge the safety of 1 of our schemes, we have a tendency to devise a completely unique thanks to capture a set of the" passwords that, we believe, is itself a contribution. During this work we have a tendency to area unit primarily intended by devices like personal digital assistants (PDAs) that over graphical input capabilities via a stylus, and that we describe our example implementation of one of our watchword schemes on such a personal organizer, particularly the Palm Pilot.

4. Paper Name: PassPoints: Design and longitudinal evaluation of a graphical password system
Authors: Susan Wiedenbecka, Jim Watersa, Jean-Camille Birgetb, Alex Brodskiyc, Nasir Memonc
Description: Computer security depends mostly on passwords to demonstrate human users. However, users have issue basic cognitive process secrets over time if they select a secure password, i.e. secret that's long and random. Therefore, they have an inclination to settle on short and insecure passwords. Graphical passwords, that encompass clicking on pictures instead of typewriting alphanumerical strings, could facilitate to beat the matter of making secure and unforgettable passwords. During this paper we tend to describe PassPoints, a replacement and safer graphical secret system. We tend to report Associate in nursing empirical study comparison the employment of PassPoints to alphanumerical passwords. Participants created Associate in nursing practiced either an alphanumerical or graphical secret. The participants later allotted 3 longitudinal trials to input their secret over the course of six weeks. The results show that the graphical secret users created a legitimate secret with fewer difficulties than the alphanumerical users. However, the graphical users took longer and created additional invalid secret inputs than the alphanumerical users whereas active their passwords. Within the longitudinal trials the 2 teams performed equally on memory of their secret; however the graphical cluster took longer to input a secret.

5. Paper Name: VIP: a visual approach to user authentication
Authors: Antonella De Angeli, Mike Coutts, Lynne Coventry Graham I. Johnson
Description: In paper the authors addresses knowledge-based authentication systems in self-service technology, presenting the design and analysis of the Visual Identification Protocol (VIP). The elemental set up behind it's to use footage instead of numbers as a way for user authentication. three utterly completely different authentication systems supported footage and visual memory were designed and compared with the quality Personal variety (PIN) approach in an passing longitudinal study involving sixty one users. The experiment self-addressed performance criteria and subjective analysis. The study and associated vogue exploration disclosed necessary info relating to users, their attitudes towards and behavior with novel authentication approaches practice footage. VIP was found to supply a promising and straightforward to use varied to the PIN. The visual code is a smaller amount difficult to remember, preferred by users and possibly safer than the numeric code. Results put together provided tips to help designers produce the foremost effective use of the natural power of visual memory in security solutions.

III. EXISTING METHODOLOGY

Most software package applications nowadays square measure written as web-based applications to be run in a web browser. Take a look at automation is nothing however employing a software package tool to run repeatable tests for such net applications. There square measure several blessings of take a look at automation. Most square measure associated with the repeatability of the tests and therefore the speed at that the tests are dead. Model-based take a look may be a software package take a look at technique during which the test cases square measure derived from a model that describes the practical aspects of the system below test. It makes use of a model to get tests that has each offline and on-line testing. To confirm that the system is behaving within the same sequence of actions. Model-based testing technique has been adopted as associate degree integrated a part of the testing method. There square measure variety of economic and open supply tools out there for helping with the event of take a look at automation. However antioxidant is probably the foremost widely-used open supply resolution for this. A take a look at automation framework may be a set of ideas, and practices that offer support for automatic software package testing. It's a strategy designed to with success perform take a look at automation. If we tend to don't have any frameworks, then it's troublesome to urge correct reports, handle checkpoints, or exception handling. We tend to could choose between any of the frameworks out there like JUnit TestNG otherwise you will style our own framework or we will choose out there IDE (Integrated development environment). Antioxidant IDE may be a Record and Playback tool. Antioxidant RC and 'Selenium WebDriver' permit you to jot down automation scripts in programming languages with nice ease.

IV. SYSTEM ARCHITECTURE

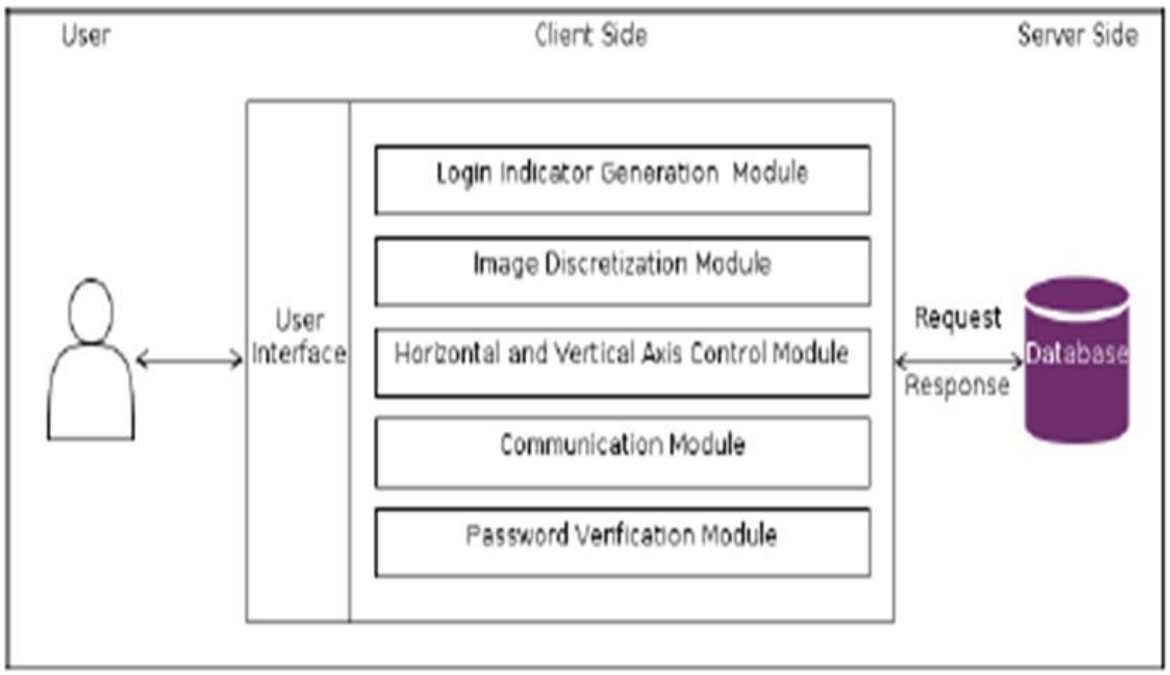

Figure 4.1. System Architecture and Design

1. Image Discretization Module:
This module divides each image into squares, from which users would choose one as the pass-square. As shown in Figure 5, an image is divided into a 7 * 11grid. The smaller the image is discretized, the larger the password space is. However,

the overly concentrated division may result in recognition problem of specific objects and increase the difficulty of user interface operations on palm-sized mobile devices.

2. Login Indicator Generator Module:
This module generates a login indicator consisting of several distinguishable characters (such as alphabets and numbers) or visual materials (such as colors and icons) for users during the authentication phase. In our implementation, we used characters A to G and 1 to 11 for a 7 * 11 grid. Both letters and numbers are generated randomly and therefore a different login indicator will be provided each time the module is called. The generated login indicator can be given to users visually or acoustically in our system we are sending these patterns on users email.

3. Horizontal and Vertical Axis Control Module:
There are two scroll bars: a horizontal bar with a sequence of letters and a vertical bar with a sequence of numbers.

4. Communication Module:
This module is in charge of all the information transmitted between the client devices and the authentication server. Any communication is protected by SSL (Secure Socket Layer) protocol and thus, is safe from being eavesdropped and intercepted.
5. Password Verification Module:
This module verifies the user password during the authentication phase. A pass Horizontal scroll bar (on the right/blue) and vertical bar (on the left/green). Square acts similar to a password digit in the text-based password system. The user is authenticated only if each pass-square in each pass-image is correctly aligned with the login indicator.

A. ALGORITHMS:

1. Registration phase:
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 (i.e., 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. The username can be omitted if PassMatrix is applied to authentication systems like screen lock. The user can either choose images from a provided list or upload images from their device as pass-images. Then the user will pick a pass square for each selected pass-image from the grid, which was divided by the image discretization module. The user repeats this step until the password is set.

2. Authentication phase:
The user uses his/her username, password and login indicators to log into PassMatrix. The following describes all the steps in detail:
1) The user inputs his/her username which was created in the registration phase.
2) A new indicator comprised of a letter and a number is created by the login indicator generator module. The indicator will be shown when the user uses his/her hand to form a circle and then touch the screen. In this case, the indicator is conveyed to the user by visual feedback. The indicator can be delivered to user by email.
3) Next, the first pass-image will be shown on the display, with a horizontal bar and a vertical bar on its top and left respectively. To respond to the challenge, the user flings or drags the bars to align the pre-selected pass-square of the image with the login indicator. For example, if the indicator is (E, 11) and the pass-square is at (5, 7) in the grid of the image, the user shifts the character E to the 5th column on the horizontal bar and 11 to the 7th row on the vertical bar
4) Repeat step 2 and step 3 for each pre-selected pass image.
5) The communication module gets user account information from the server through HttpRequest POST method.
6) Finally, for each image, the password verification module verifies the alignment between the pass square and the login indicator. Only if all the alignments are correct in all images, the user is allowed to log into PassMatrix.

V. MATHEMATICAL MODULE

Let S be the Whole system which consists:
S= {IP, Pro, OP}.
Where,
IP is the input of the system.
Pro is the procedure applied to the system to process the given input.
OP is the output of the system.
A. Input:
IP = {u, I, LI, ht, wt, pv, n}.
Where,
u be the user.

I be set of images used for creating graphical password.
ht be the height of image.
wt be the width of the image.
pv be the pass values of the selected image for generating graphical password.
LI be the login indicator used at the time of login.
n be the number of images chosen for creating graphical based password from set of images I.

B. Procedure:

1. Registration phase:

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 (i.e., 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. The username can be omitted if PassMatrix is applied to authentication systems like screen lock. The user can either choose images from a provided list or upload images from their device as pass-images. Then the user will pick a pass square for each selected pass-image from the grid, which was divided by the image discretization module. The user repeats this step until the password is set.

2. Authentication phase:

The user uses his/her username, password and login indicators to log into PassMatrix. The following describes all the steps in detail:

1) The user inputs his/her username which was created in the registration phase.
2) A new indicator comprised of a letter and a number is created by the login indicator generator module. The indicator will be shown when the user uses his/her hand to form a circle and then touch the screen. In this case, the indicator is conveyed to the user by visual feedback. The indicator can be delivered to user by email.
3) Next, the first pass-image will be shown on the display, with a horizontal bar and a vertical bar on its top and left respectively. To respond to the challenge, the user flings or drags the bars to align the pre-selected pass-square of the image with the login indicator. For example, if the indicator is (E, 11) and the pass-square is at (5, 7) in the grid of the image, the user shifts the character E to the 5th column on the horizontal bar and 11 to the 7th row on the vertical bar
4) Repeat step 2 and step 3 for each pre-selected pass image.
5) The communication module gets user account information from the server through
HttpRequest POST method.
6) Finally, for each image, the password verification module verifies the alignment between the pass square and the login indicator. Only if all the alignments are correct in all images, the user is allowed to log into PassMatrix.

C. Output:

The Passwords remain the dominant means of authentication in day todays systems due to of their simplicity, legacy deployment and ease of revocation. Unfortunately, common approaches to entering passwords by the way of keyboard, mouse, touch screen or any traditional input device, are mostly vulnerable to attacks such as shoulder surfing attack and password snooping attack. Present approaches to reducing shoulder surfing typically also decrease the usability of the system; mostly requiring users to use security tokens, interact with systems that do not provide direct feedback or they need additional phases to prevent a malicious observer from easily disambiguating the input to determine the password/PIN. Previous gaze-based authentication methods do not support traditional password schemes. We present a secure graphical authentication system named PassMatrix that protects users from becoming victims of shoulder surfing attacks when inputting passwords in public through the usage of one-time login indicators. A login indicator is randomly generated for each pass-image and will be useless 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**.**

VI. ADVANTAGES

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

VII. APPLICATIONS

1. Banking Sector
2. Any online transactions

VIII. CONCLUSION AND FUTURE SCOPE

Introduced a shoulder surfing attack resistant authentication system on graphical based passwords, named PassMatrix. Using a one-time login indicator per image, users can point out the location of their pass-square values

without directly clicking 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 web based application and carried out user experiments to evaluate the memorability and usability the system. Based on the analytical 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.In future we can use video frames as input.

ACKNOWLEDGMENT

Authors want to acknowledge Principal, Head of department and guide of their project for all the support and help rendered. To express profound feeling of appreciation to their regarded guardians for giving the motivation required to the finishing of paper.

REFERENCES

[1] Hung-Min Sun, Shiuan-Tung Chen, Jyh-Haw Yeh and Chia-Yun Cheng, A Shoulder Surfing Resistant Graphical Authentication System, IEEE Transactions on Dependable and Secure Computing, 2016.

[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. 1319.

[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, AINAW07. 21st International Conference on, vol. 2. IEEE, 2007,pp. 467472.

[4] 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. 17.

[5] 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. 479483.

[6] 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. 44.

[7] 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. 102127, 2005.

[8] A. Paivio, T. Rogers, and P. Smythe, Why are pictures easier to recall than words? Psychonomic Science, 1968.

[9] D. Nelson, U. Reed, and J. Walling, Picture superiority effect, Journal of Experimental Psychology: Human Learning and Memory, vol. 3, pp. 485497, 1977.

[10] 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 AdvancedVisual Interfaces. ACM, 2002, pp. 316323.