Enhancement in Graphical Authentication System for Resisting Shoulder Surfing

Sonali Bhandurge[1] Prof. Varsha Dange[2]
[1]Student [2]Guide
[1,2]Savitribai Phule Pune University, DPCOE, Wagholi, Pune India

Abstract— In this computing world, computer security and confidentiality can only be gained by providing authentication based on passwords. It becomes hectic to memorize textual passwords that are too long just for the sake of security. Thus allowing some users to choose small memorizing passwords which tend to be insecure and are considered as the weakest link in authentication chain. Graphical passwords are always considered as a flipside to the alphanumeric or textual passwords. The advances made in web applications and mobile apps empower user to access these applications anywhere without any time constraint. This improvement brings great comfort but at the same time thus increasing chances of exposing passwords to the Shoulder Surfing attack. In shoulder surfing attack, attacker observes directly or with the help of external devices for gathering user credentials. To blow away this problem a novel authentication system, PassMatrix with color authentication system to resist shoulder surfing is been represented in this paper. With a onetime valid login indicator and circulative horizontal and vertical bars covering the entire scope of pass-images and choosing color sequence, PassMatrix with color authentication system offers no evidence for attackers to discover the password even if multiple attempts of camera-based attacks were performed.

Key words: Authentication, Graphical Passwords, Shoulder Surfing Attack

I. INTRODUCTION

Textual passwords are been utilized from decades as a medium of authentication. As textual password may contain several lower case and upper case letters, it is evaluated strong enough for resisting against the brute force attack. However, it is a tedious task of memorizing and recalling strong textual passwords. Thus, it allows users to select passwords that are easy to remember and recall. There may be users who may choose a common password for numerous accounts. As stated in an article in Computer world, a security team ran a network password cracker and it outstandingly cracked approximately 80% of user employee's password nearby within 30 seconds. Textual passwords are considered as an insecure medium of authentication as it is difficult recalling and maintaining strong passwords. Numerous graphical password authentication schemes [3], [4], [5], [6], [8] were developed to overcome the problems related to textual passwords. Based on research performed in [10], it was analysed that humans have a strong and better ability to recollect and memorize images with Long-Term Memory (LTM) than verbal representations. Image based passwords are considered as a good option to recollect passwords in an easier way. Users tend to establish complex authentication password and have capability for recognize it after a long time even if memory is not activated periodically. Image-based passwords have various advantages but at its flipside it is vulnerable to shoulder surfing attacks (SSAs). In shoulder surfing attack, the attacker either makes use of direct observation, such as watching over someone's shoulder or applying video capturing techniques to acquire some sensitive personal information regarding a victim. Some human actions such as electing bad passwords for new accounts and providing inputs passwords in an insecure way for later logins is considered as weakest link in authentication process. Hence, a need arises to overcome these vulnerabilities by proposing an authentication scheme. In this paper, an assured authentication system is represented named as PassMatrix with Hybrid Textual Authentication Scheme, that shelter user from being victim of shoulder surfing attack while inputting password in public though the usage of one-time login indicators. A login indicator is generated randomly for each and every pass-image and it will be of no use as soon as the session terminates. Obtaining security against the shoulder surfing attack is gained by login indicators as a dynamic pointer is used by users to point out position of their passwords rather than clicking on password object directly. In Hybrid Textual Authentication Scheme, user rates colours from 1 to 8 and memorizes the rating. During login process, after user has filled up his username an interface is generated based upon the colours picked by user. Interface is considered as a grid of size 8*8 which contains random number digits from 1-8 and it also contains strips of colours. The colour grid has 4 pairs of colours each pair represents row and column of grid. A session password is generated based upon the rating. In this way a secure and efficient graphical authentication is being represented.

II. RELATED WORK

A. Paper Title: Security in Graphical Authentication [2]

1) Summary

Authentication acts as a gatekeeper for security and protection of computer system. Having a strong authentication scheme helps in detecting intruders. Textual password scheme tends to get hacked as users may use small passwords for memorization while long length passwords are tedious to memorize. It is considered as an insecure way of authentication. Graphical Authentication Systems are considered as a potential replacement for conventional authentication systems. The Graphical authentication has a better resistance power for guessing and capturing attacks and even provides powerful security.

B. Paper Title: Reducing Shoulder-surfing by Using Gaze based Password Entry [3]

1) Summary

The Eye Password is a system that eradicates the issues of shoulder surfing attack via a novel approach to user input. Through this approach user inputs by choosing from on-screen keyboards utilizing orientations of pupils. It is an expensive process.

C. Paper Title: Shoulder Surfing Resistant Password Authentication Mechanism (Using Convex hull Click Scheme) [4]

1) Summary

The Convex Hull Click Scheme is considered as shoulder surfing resisting scheme, it is a graphical password scheme that helps in guarding against the human observation, electronic captures which are part of the shoulder surfing attack. In Convex hull click scheme, icons or images are taken as graphical elements in authentication process, these icons are been randomly distributed onto the screen. The users task is recognize minimum amount of their password icons from the randomly distributed icons onto the screen. The user solves the problem by clicking within the convex hull of the pass-icons. User then mentally creates convex hull by using pass-icons. Convex hull is the considered as the area of edges that joins together set of points.

D. Paper Title: Analysis and Improvement of a PIN-Entry Method Resilient to Shoulder-Surfing and Recording Attacks [6]

1) Summary

PIN is the Personal Identification Number, which consists of four decimals digits, it is susceptible to observational attack because of its short length. Even though a PIN is strong enough then there may be recollecting problem.

E. Paper Title: Captcha as Graphical Passwords: A New Security Primitive Based on Hard AI Problems [7]

1) Summary

Captcha as graphical passwords (CaRP) is considered as a novel family of graphical password system that is built upon the Captcha technology. CaRP is a click-based graphical passwords. In this graphical password sequence of clicks on images is utilized to obtain a password. Unlike other click-based graphical passwords, images used in CaRP are Captcha challenges, and a new CaRP image is generated for every login attempt.

F. Paper Title: Now you see me, now you don't: Protecting smartphone authentication from shoulder surfers [9]

1) Summary

XSide grasps recent technologies and the recent advances for providing easy utilization along with protection against the observation attack. In authentication through XSide, user draws shapes or gestures on back or on front of the device. It can be utilized eye-free and it resists shoulder surfing.

G. Paper Title: The secure haptic keypad: A tactile password system [10]

1) Summary

Secure Haptic Keypad (SHK) is considered as alternative to the current alphabetic numeric keywords. This system was economical, robust and was intended to support human input of authentication password. It encoded password as a sequence of vibration pattern. It used patterns rather than characters and numbers. Hence, user gets confused and detecting user selection becomes tedious task.

III. PROPOSED ALGORITHM

A. Design Considerations

The system constitutes of the following modules:

- Authentication module
- Virtual keyboard generation module
- Pair-based authentication module
- Pass-matrix verification module
- File uploading module
- File downloading module

B. Description of the Proposed Algorithm

The initial task performed by PassMatrix is Login generator. It generates login indicator which includes various distinguishable characters for users during the authentication phase. Then the Image Discretization Module, it partitions each and every image or picture into squares and from this bulk of squares, user will select one square as a pass-square. After the work of Image Discretization is done the Horizontal and Vertical Axis Control module comes into picture, which consists of two scroll bars along with sequence of numbers. These bars are controlled by using the drag and fling functions by the users. The communication module helps in information transmission between the client device and the server which is authenticated. Then password is verified using the password verification module during the authentication phase. The pass square acts like a password digit in text based password system. The user is considered as authenticated user if and only if pass square in each pass-image is correctly aligned with the login indicators. All the data is stored on database server which contains tables that stores user accounts, passwords, user information.

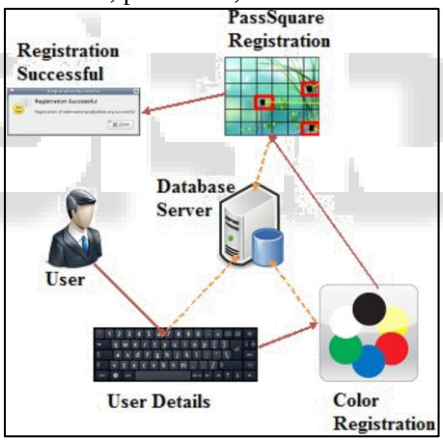

Fig. 1: Registration System

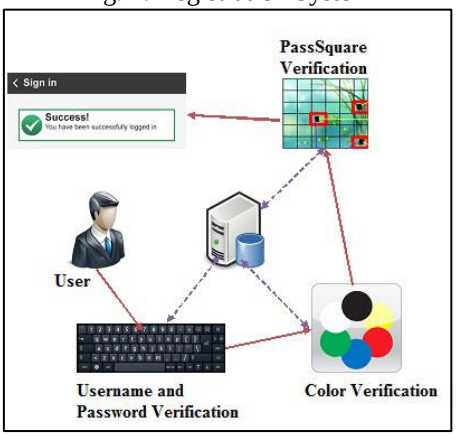

Fig. 2: Authentication System

After the PassMatrix process has been successfully done the Hybrid Textual Authentication starts working. In this scheme user rates colours from 1 to 8 and memorizes the rating the way user feels comfortable. Similar ratings can be

utilize for different colours. During login process, after user has fills up his username an interface is generated based upon the colours picked by user. Interface is considered as a grid o size 8*8 which contains random number digits from 1-8 and it also contains strips of colours. The colour grid has 4 pairs of colours each pair represents row and column of grid.

A session password is generated based upon the rating given by user. In this the first colour of every pair in colour grid represents an row and the second represents column of the number grid The number retrieved from the intersection of row and column of the grid is regarded as session password. Thus, this entire process provides security and resist from shoulder surfing attack.

1) Algorithms

a) AES Algorithm

1) Step 1: Key Expansions:

For each round AES needs a different 128-bit block of round key also one more.

2) Step 2: Initial Round

Add Round Key–with a block of the round key, each byte of the state is combined using bit wise XOR.

3) Step 3: Rounds

– Sub Bytes–in this step each byte is replaced with another byte.
– Shift Rows–for a certain number of steps, the state's last three rows are moved cyclically.
– Mix Columns–on the columns of the state a mixing operation operates, in each column combining the four bytes.

4) Step 4: Final Round (no Mix Columns)

– Sub Bytes
– Shift Rows
– Add Round Key.

IV. PSEUDO CODE

1) Step 1: Fill the registration form.
2) Step 2: Give rating to the colors
3) Step 3: Select PassMatrix.
4) Step 4: Verify username and password.
5) Step 5: If user entered username and password are correct then verify pair based authentication.
6) Step 6: If pair based authentication successful then, verify PassMatrix.
7) Step 7. If PassMatrix are verified then upload and download the files.

V. SIMULATION RESULTS

User cannot proceed if selection of wrong pass squares performed.

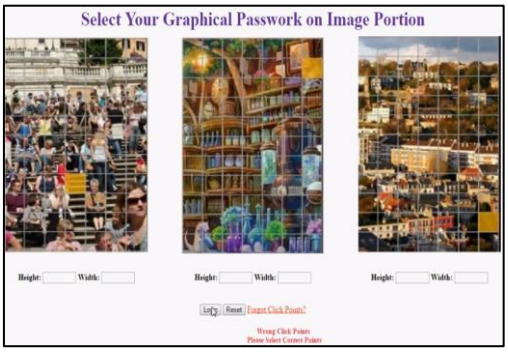

Fig. 4: Wrong PassMatrix selection

Block user if he try with three times

Fig. 5: User Block

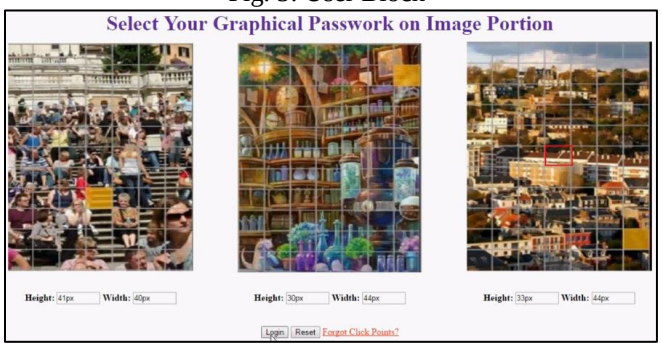

Fig. 6: Login through PassSquare

VI. CONCLUSION AND FUTURE WORK

With the increasing trend of web services and apps, users are able to access these applications anytime and anywhere with various devices. In order to protect user's digital property, authentication is required every time they try to access their personal account and data. However, conducting the authentication process in public might result in potential shoulder surfing attacks. Even a complicated password can be cracked easily through shoulder surfing. Using traditional textual passwords or PIN method, users need to type their passwords to authenticate themselves and thus these passwords can be revealed easily if someone peeks over shoulder or uses video recording devices such as cell phones. To overcome this problem, a shoulder surfing resistant authentication system based on graphical passwords, named PassMatrix was proposed. Using a one-time login indicator per image, users can point out the location of their PassSquare without directly clicking or touching it, which is an action vulnerable to shoulder surfing attacks. Because of the design of the horizontal and vertical bars that cover the entire PassImage, it offers no clue for attackers to narrow down the password space even if they have more than one login records of that account. Additional to it more security is provided by using color authentication scheme where rating of colors is performed and upon it from the matrix password is generated.

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] Robert G. Rittenhouse, Junaid Ahsenali Chaudry and Malrey Lee, "Security in Graphical Authentication," International Journal of Security and Its Applications Vol. 7, No. 3, May, 2013, pp. 347-356.
[3] 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.

[4] Professor Sandeep Samleti, Chandan Kumar ,Vijay Prakash, Nitin Kumar, Sunil Kumar, "Shoulder Surfing Resistant Password Authentication Mechanism (Using Convex hull Click Scheme)," International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 3, March 2014, pp. 5689-5691.
[5] I. Oakley and A. Bianchi, "Multi-touch passwords for mobile device access," in Proceedings of the 2012 ACM Conference on Ubiquitous Computing, ser. UbiComp 12. New York, NY, USA: ACM, 2012, pp. 611-612.
[6] Taekyoung Kwon and Jin Hong, "Analysis and Improvement of a PINEntry Method Resilient to Shoulder-Surfing and Recording Attacks," IEEE transactions on information forensics and security, 2015, pp. 278-292.
[7] Bin B. Zhu, Jeff Yan, Guanbo Bao, Maowei Yang, and Ning Xu, "Captcha as Graphical PasswordsA New Security Primitive Based on Hard AI Problems," IEEE transactions on information forensics and security, VOL 9, NO. 6, JUNE 2014, pp. 891-904.
[8] A. Bianchi, I. Oakley, V. Kostakos, 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. TEI0 11. New York, NY, USA: ACM, 2011, pp. 197-200.
[9] A. De Luca, M. Harbach, E. von Zezschwitz, M.-E. Maurer, B. E. Slawik, H. Hussmann, and M. Smith, "Now you see me, now you dont: Protecting smartphone authentication from shoulder surfers," in Proceedings of the 32Nd Annual ACM Conference on Human Factors in Computing Systems, ser. CHI 14. New York, NY, USA: ACM, 2014, pp. 2937-2946.
[10] A. Bianchi, I. Oakley, and D. S. Kwon, "The secure haptic keypad: A tactile password system," in Proceedings of the SIGCHI Conference on Human Factors in Computing.

