A Shoulder Surfing Resistant Graphical Authentication System

Sarath S. Nair[1], Farhan Ahmed[2], Mohd. Inamalhasan Faras[3], Abraham George[4]
[1,2,3,4]Student, Dept. of Computer Science and Engg., M. S. Ramaiah Institute of Technology, Bengaluru, India

***Abstract*: Authentication based on passwords is used largely in applications for computer security and privacy. However, human actions such as choosing bad passwords and inputting passwords in an insecure way are regarded as "the weakest link" in the authentication chain. Rather than arbitrary alphanumeric strings, users tend to choose passwords either short or meaningful for easy memorization. With web applications and mobile apps piling up, people can access these applications anytime and anywhere with various devices. This evolution brings great convenience but also increases the probability of exposing passwords to shoulder surfing attacks. Attackers can observe directly or use external recording devices to collect users' credentials. To overcome this problem, we proposed a novel authentication system PassMatrix, based on graphical passwords to resist shoulder surfing attacks. With a one-time valid login indicator and circulative horizontal and vertical bars covering the entire scope of pass- images, PassMatrix offers no hint for attackers to figure out or narrow down the password even they conduct multiple camera-based attacks.**

***Keywords*: Graphical Passwords, Authentication, Shoulder Surfing Attack.**

1. Introduction

Graphical password authentication schemes were developed to address the problems and weaknesses associated with textual passwords. Based on some studies such as those in$ humans have a better ability to memorize images with long-term memory (LTM) than verbal representations. Image-based passwords were proved to be easier to recollect in several user studies. As a result, users can set up a complex authentication password and are capable of recollecting it after a long time even if the memory is not activated periodically. However, most of these image-based passwords are vulnerable to shoulder surfing attacks (SSAs). This type of attack either uses direct observation, such as watching over someone's shoulder or applies video capturing techniques to get passwords, PINs, or other sensitive personal information. Authentication based on passwords is used largely in applications for computer security and privacy. However, human actions such as choosing bad passwords and inputting passwords in an insecure way are regarded as "the weakest link" in the authentication chain. Rather than arbitrary alphanumeric strings, users tend to choose passwords either short or meaningful for easy memorization. With web applications and mobile apps piling up, people can access these applications anytime and anywhere with various devices. This evolution brings great convenience but also increases the probability of exposing passwords to shoulder surfing attacks. Attackers can observe directly or use external recording devices to collect users' credentials. To overcome this problem, we proposed a novel authentication system PassMatrix, based on graphical passwords to resist shoulder surfing attacks. With a one-time valid login indicator and circulative horizontal and vertical bars covering the entire scope of pass-images, Pass Matrix offers no hint for attackers to figure out or narrow down the password even they conduct multiple camera-based attacks.

2. Problem statement

Authentication based on passwords is used largely in applications for computer security and privacy. However, human actions such as choosing bad passwords "and inputting passwords in an insecure way are regarded as the weakest link" in the authentication chain. Rather than arbitrary alphanumeric strings, users tend to choose passwords either short or meaningful for easy memorization. With web applications and mobile apps piling up, people can access these applications anytime and anywhere with various devices. This evolution brings great convenience but also increases the probability of exposing passwords to shoulder surfing attacks. Attackers can observe directly or use external recording devices to collect users' credentials. Objective of the project is to develop the application which resist Shoulder Surfing attacks in Graphical Authentication System.

3. Shoulder surfing attack

Due to the fact that shoulder surfing has been a real threat to authentication systems with either textual or graphical passwords, many novel authentication schemes were proposed to protect systems from this attack. Unfortunately, most of them were unsuccessful to alleviate the threat if the shoulder-surfing attack is camera-based. For instance, some schemes such as PIN-entry method and spyresistant keyboard were designed based on the difficulties of short-term memory. Camera-based shoulder surfing attacks can easily crack the passwords of these schemes. The password spaces of other schemes such as those in CAPTCHA-based method and Pass-icons can be narrowed down by camera-based shoulder surfing attacks. The proposed authentication system PassMatrix takes full advantage of adding extra information to obfuscate the login process, using an approach to point out the locations of pass-squares implicitly instead of typing or clicking on password objects directly. Since the horizontal and vertical bars are circulative and thus cover the entire area of the image, the password space will not be narrowed down even if the whole authentication process is recorded by attackers. Furthermore, the login indicator for each pass-image varies so that each pass-image is an independent case. Thus, no pattern can be extracted from a set of pass-images in an authentication trial, neither from multiple login processes. With the above security features, PassMatrix should be strong enough to resist shoulder surfing attacks, even if the attacks are camera-equipped.

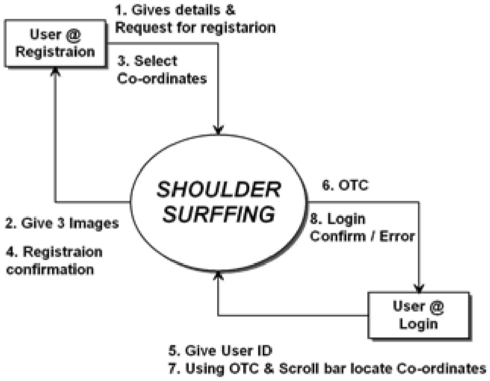

Fig. 1. Shoulder surfing

4. Pass matrix

To overcome the security weakness of the traditional PIN method, the easiness of obtaining passwords by observers in public, and the compatibility issues to devices, we introduced the graphical authentication system called PassMatrix. In PassMatrix, a password consists of only one pass-square per pass-image for a sequence of n images. The number of images (i.e., n) is user-defined. In PassMatrix, users choose one square per image for a sequence of n images rather than n squares in one image as that in the PassPoints scheme.

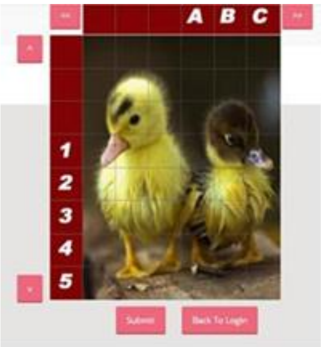

Fig. 2. PassMatrix

5. Methodology

Pass Matrix's authentication consists of a registration phase and an authentication phase as described below:

A. Registration phase

In this phase the user has to register by giving his information such as userid, user name, valid e-mail id etc., and after giving this information, randomly three images will be assigned to the user, in those images he has to select the coordinate squares of the images as the graphical password. The details of coordinates of all images will be stored in the database with respect to the specific user.

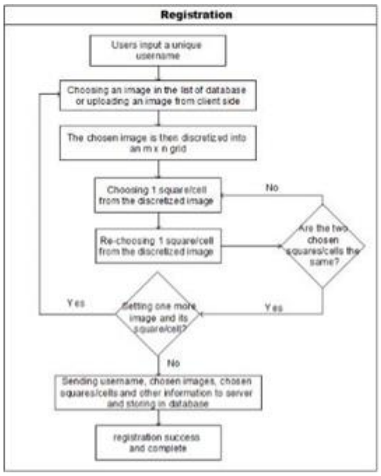
Registration
Users input a unique username
Choosing an image in the list of database or uploading an image from client side
The chosen image is then discretized into an m x n grid
Choosing 1 square/cell from the discretized image
Re-choosing 1 square/cell from the discretized image
Are the two chosen squares/cells the same?
No
Yes
Setting one more image and its square/cell?
Yes
No
Sending username, chosen images, chosen squares/cells and other information to server and storing in database
registration success and complete

Fig. 3. The flowchart of registration phase in PassMatrix.

After successful setting of the coordinates of the images, those details will be stored in the database, concatenating all the three images coordinates and generate hash code for that and store in the database with respect to the user.

B. Authentication phase

Registered user will be login to the application by using his userid and password, if the userid and password is valid One Time Password(OTP) will be sent to the user's e-mail, whereas OTP contains the random pair of vertical and horizontal slider coordinate points of all the three images.

After successful login, three assigned images will be displayed to the user with horizontal and vertical sliders, user has to set the horizontal and vertical sliders for all the three images, where the OTP coordinate value should be equal to the coordinates chosen by the user at the time of password setting. The hash code will be generated for all OTP coordinates by concatenating. if the hash code is matched with the existing hash code user can successful enter in to the home page, else, process ends and login page will display.

6. Results

The proposed authentication system PassMatrix takes full advantage of adding extra information to obfuscate the login process, using an approach to point out the locations of pass-squares implicitly instead of typing or clicking on password objects directly. Since the horizontal and vertical bars are circulative and thus cover the entire area of the image, the password space will not be narrowed down even if the whole authentication process is recorded by attackers. Furthermore, the login indicator for each pass-image varies so that each pass-image is an independent case. Thus, no pattern can be extracted from a set of pass-images in an authentication trial, neither from multiple login processes. With the above security features, PassMatrix should be strong enough to resist shoulder surfing attacks, even if the attacks are camera-equipped.

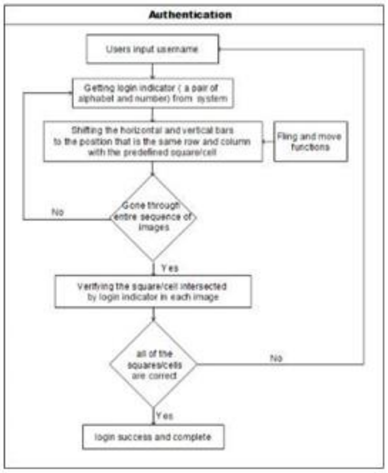
Authentication
Users input username
Getting login indicator (a pair of alphabet and number) from system
Shifting the horizontal and vertical bars to the position that is the same row and column with the predefined square/cell
Fling and move functions
Gone through entire sequence of images
No
Yes
Verifying the square/cell intersected by login indicator in each image
all of the squares/cells are correct
No
Yes
login success and complete

Fig. 4. The flowchart of authentication phase in PassMatrix

The past work done on this system requires to enter OTC manually rather than vertical bars which are implemented in our system. The implementation of vertical and horizontal bars prevents the need to enter the OTC manually with keyboard which again is prone to shoulder surfing attacks. Our system due to the addition of vertical and horizontal bars overrides the need to enter the OTC manually through the keyboard which is an improvement to such graphical authentication system to rule out all the possible kinds of shoulder surfing attacks. In our system, OTC has to be combined with the co-ordinates of the selected PassMatrix to login to the system. This ensures that even if a person knows your co-ordinates, it cannot be used to successfully login to the system. Similarly, if the OTC is exposed, it cannot be used alone to login to the system. Addition of these small features ensures to prevent all possible kinds of shoulder surfing attacks.

7. Conclusion

With the increasing trend of web services and apps, users are able to access these applications anytime and anywhere with various devices. 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, we proposed a shoulder surfing resistant authentication system based on graphical passwords, named PassMatrix. Using a one-time login indicator per image, users can point out the location of their pass-square 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 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. 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. process, using an approach to point out the locations of pass-squares implicitly instead of typing or clicking on password objects directly. Since the horizontal and vertical bars are circulative and thus cover the entire area of the image, the password space will not be narrowed down even if the whole authentication process is recorded by attackers. Furthermore, the login indicator for each pass-image varies so that each pass-image is an independent case. Thus, no pattern can be extracted from a set of pass-images in an authentication trial, neither from multiple login processes. With the above security features, PassMatrix should be strong enough to resist shoulder surfing attacks, even if the attacks are camera-equipped.

The past work done on this system requires to enter OTC manually rather than vertical bars which are implemented in our system. The implementation of vertical and horizontal bars prevents the need to enter the OTC manually with keyboard which again is prone to shoulder surfing attacks. Our system due to the addition of vertical and horizontal bars overrides the need to enter the OTC manually through the keyboard which is an improvement to such graphical authentication system to rule out all the possible kinds of shoulder surfing attacks. In our system, OTC has to be combined with the co-ordinates of the selected PassMatrix to login to the system. This ensures that even if a person knows your co-ordinates, it cannot be used to successfully login to the system. Similarly, if the OTC is exposed, it cannot be used alone to login to the system. Addition of these small features ensures to prevent all possible kinds of shoulder surfing attacks.

References

[1] D. Weinshall, "Cognitive authentication schemes safe against spyware," *2006 IEEE Symposium on Security and Privacy (S&P'06)*, Berkeley/Oakland, CA, 2006, pp. 6 pp. 300.

[2] P. Shinde and P. K. N. Shedge, “PASSMATRIX-An Authentication System to Resist Shoulder Surfing Attacks On predictive models and user drawn graphical passwords,” International Research Journal of Engineering and Technology, vol. 5, no. 3, pp. 296-299, March 2018.

[3] A. E. Dirik, N. Memon, and J. C. Birget, “Modeling user choice in the PassPoints graphical password scheme,” Symposium On Usable Privacy and Security (SOUPS) 2007, July 18-20, 2007, Pittsburgh, PA, USA.

[4] B. Pinkas and T. Sander, “Securing passwords against dictionary attacks,” CCS '02 Proceedings of the 9th ACM conference on Computer and communications security, pp. 161-170, November 2002.

[5] M. Alsaleh, M. Mannan and P. C. van Oorschot, "Revisiting Defenses against Large-Scale Online Password Guessing Attacks," in *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 1, pp. 128-141, Jan.-Feb. 2012.

[6] https://www.javatpoint.com