PASSMATRIX AUTHENTICATION TO OVERCOME SHOULDERSURFING ATTACKS

Athira Dinachandran T.[1], Ambarish A.[2]

[1]M. Tech Scholar, Department of Computer Science, MCET, Desamangalam, 679532
[2]Asst. Professor, Department of Computer Science, MCET, Desamangalam, 679532

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. We also implemented a PassMatrix prototype on Android and carried out real user experiments to evaluate its memorability and usability. From the experimental result, the proposed system achieves better resistance to shoulder surfing attacks while maintaining usability.*

***Key Words*: PassMatrix, Image Password, Graphical Password**

1. INTRODUCTION

A 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.

As per the article [1] in computer world, 80% user set such easy password and those can be cracked by hackers within 30 seconds. Based on the Psychological study [2] user is able to memorize images with long terms memory rather than textual words.

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.

2. EXISTING SYSTEM

A system is an orderly group of interdependent components linked together according to a plan to achieve a specific objective. Its main characteristics are organization, interaction, interdependence, integration and a central objective. In the Existing System Users' actions such as typing from their keyboard, or clicking on the pass-images or pass-points in public may reveal their passwords to people with bad intention. Existing System is vulnerable to shoulder surfing attacks.

Type-I: Naked eyes.

Type-II: Video captures the entire authentication

process only once.

Type-III: Video captures the entire authentication process more than once.

To set up high secured authentication scheme an extra hardware can be used such as: multi-touch monitor, voice recorder, some sensors etc.[3][4] These systems provide better security than other password authentication system but such system are not affordable to every user.

To overcome the security weakness of the traditional PIN method - the easiness of obtaining passwords by observers in public - the compatibility issues to devices. A new system introduced for 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 Pass Points scheme.

PassPoints [5] technique was proposed by Susan Wiedenbeck et al. The quality of handheld devices was improved in 2005. The high resolution graphical display was available in handheld devices.

Based on the gesture drawing process a new authentication system is proposed by I. Jermyn [6], this system contains finger-drawn doodles and pseudosignatures. User needs to draw a doodle/ signature/ pattern on a touch screen handheld devices.

CAPTCHA-based method [7] is proposed by Uwe Aickelin. This method uses captcha text and image combinations for login phase. User add some captcha characters.

A PassMatrix scheme [8] is proposed for authentication. This scheme uses combination of one time login indicator and multiple password images click points. The password is selected without touching the exact password click point. But this scheme uses same images for every login session.

3. SYSTEN DESIGN

From the below design, it clearly understood the process of graphical password authentication. The password authenticated using the Login indicator to hide the original password. Hence login indicator is useful for authentication.

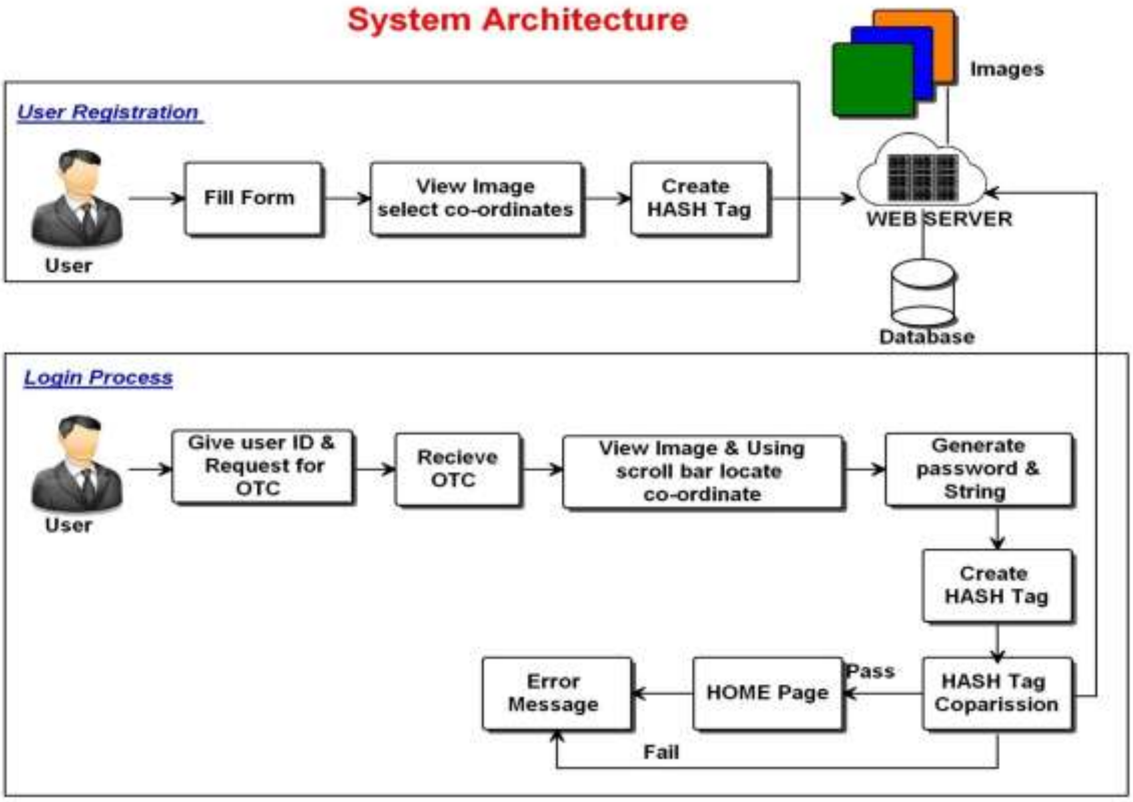

Chart -1: System Architecture

The user creates an account which contains a username and a password, one pass-square per image for a sequence of n images. For login to the passMatrix the user uses his/her username, password and login indicators.

Algorithm Steps:

Input: Registration details

Username

Output: Authentication

Step 1: Display image accordance with username

Step 2: Generate passkey

Step 3: Provide 6 by 6 grid image with scroll bars

Step 4: Check whether user input matches to registration Details

Step 5: Continue for all n Images

Step 6: If all clicks matches login successful

4. IMPLEMENTATION

4.1. User Registration

In this module user has to register by giving his information such as user id, user name, password, 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.

4.2. Hash code generation:

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.

4.3. User Login Process:

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.

4.4. Forget password and recovering phase:

The forget password and recovery module, to achieve this using an innovative idea of security questions about the user handset such as charging percentage in last 2 days.

_ Have you used camera in last two days?

_ Have you installed any of the application?

_ Have you registered any event for past 7 days?

The system can concentrate on the log files (camera, battery usage, calendar information, call log, installed applications) of the user mobile and frame the questions based on that.

5. THE ACTIVITIES OF THE DESIGN PROCESS

Interface design-describes the structure and organization of the user interface. Includes a representation of screen layout, a definition of the modes of interaction, and a description of navigation mechanisms. Interface Control mechanisms- to implement navigation options, the designer selects form one of a number of interaction mechanism; Interface Design work flow- the work flow begins with the identification of user, task, and environmental requirements. Once user tasks have been identified, user scenarios are created and analyzed to define a set of interface objects and actions.

a) Aesthetic design-also called graphic design, describes the "look and feel" of the WebApp. Includes color schemes, geometric layout. Text size, font and placement, the use of graphics, and related aesthetic decisions.

b) Content design-defines the layout, structure, and outline for all content that is presented as part of the WebApp. Establishes the relationships between content objects.

c) Navigation design-represents the navigational flow between contents objects and for all WebApp functions.

d) Architecture design-identifies the overall hypermedia structure for the WebApp. Architecture design is tied to the goals establish for a WebApp, the content to be presented, the users who will visit, and the navigation philosophy that has been established.

I. Content architecture, focuses on the manner in which content objects and structured for presentation and navigation.

II. WebApp architecture, addresses the manner in which the application is structure to manage user interaction, handle internal processing tasks, effect navigation, and present content. WebApp architecture is defined within the context of the development environment in which the application is to be implemented.

6. 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

REFERENCES

[1] K. Gilhooly, "Biometrics: Getting back to business," Computerworld, May, vol. 9, 2005.

[2] D. Nelson, U. Reed, and J. Walling, "Picture superiority effect," Journal of Experimental Psychology: Human Learning and Memory, vol. 3, pp. 485-497, 1977.

[3] 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.

[4] 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 Systems, ser. CHI '10. New York, NY, USA: ACM, 2010, pp. 1089-1092

[5] Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "The design and analysis of graphical passwords," in Proceedings of the 8th conference on USENIX Security Symposium-Volume 8. USENIX Association, 1999, pp. 1-1.

[6] 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.

[7] S. Chiasson, P. van Oorschot, and R. Biddle, "Graphical password authentication using cued click points," Computer Security-ESORICS 2007, pp. 359- 374, 2007.

[8] 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, Vol.1 PP. 1, Issue: 99, March 2016