International Journal of Research and Advanced Development (IJRAD)

Enhanced High-Level Security based on Feature Set and Order Sequence Graphical Authentication

Ms. R. Kavitha[1], D. Sri Pavina[2], N. Pavithra[3], K. Vaishnaovi[4]

[1]Assistant Professor, Department of CSE, Velalar College of Engineering and Technology, TN, India.
[2, 3, 4] IV Year B. E., CSE, Department of Computer Science & Engineering,
Velalar College of Engineering & Technology, Erode, TN, India.

Received Date: 14th March, 2017, Accepted Date: 2nd April, 2017.

Abstract - User authentication is one of the most important procedures required to access secure and confidential data. Authentication of users is usually achieved through text-based passwords. The text-based password of a user can be easily obtained through social engineering techniques. Apart from being vulnerable to social engineering attacks, text-based passwords are either less secure but difficult to remember. Researchers of modern days have thus gone for alternative methods wherein graphical pictures are used as passwords. The advantage over image based password is that user can create an own graphical password. Graphical passwords have been designed to make passwords more memorable and easier for people to use. In this paper, an Image-Based Authentication system is proposed with order evaluation approach that allows users choice password and simultaneously influences users to select stronger passwords. To add a layer of security, we ask the user to input own digital picture and select sequence tokens from the picture used during the registration phase. The user has to reproduce the same tokens by input the same image during his login phase. Also to enhance the security, verification is done by two phases namely, (1) Token verification and (2) Token order evaluation in the server system. This proposed system offers reasonable security and usability and appears to fit well with some practical applications for improving online security.

Keywords: PassBYOP, Token Verification, Authentication, security.

I. INTRODUCTION

Text passwords and Personal Identification Numbers (PINs) are the dominant authentication method as they are simple and can be deployed on systems including public terminals, the web, and mobile devices. Here we focus on the authentication problem. The most common computer authentication method is to use alphanumerical usernames and passwords. This method has been shown to have significant drawbacks. Graphical password systems are knowledge-based authentication techniques that leverage peoples' ability to memorize and recognize visual information more readily than alphanumeric information [3]. To overcome the shoulder surfing we came with image password for more secure authentication. In this concept, we give our picture as password which is real time images. These images can be set privately by the user for own purpose. This involves extracting the image feature and maintains these feature coordinates as a password in the server. Also, these features should be given in correct sequence order to reduce guessing attacks [4]. Three basic techniques used for authentication are (i) Knowledge-based authentication, (ii) Token based authentication and (iii) Biometric based authentication. Knowledge-based authentication technique uses something the user knows (e.g. passwords), Token based authentication technique is just as smart card which uses something the user has. Biometric based authentication technique uses unique, measurable characteristic of an individual (e.g. Iris, fingerprint) [2]. To avoid this drawback of text-based password have proposed a PassBYOP with graphical password with selection of token that combined with a point of reference of image, if image existing in a different angle that can also be able to authenticate by the user. So not only the token but also the orientation of the token presented is important [1]. The coordinates match the selection of tokens in the image. And the user can access the account.

II. IMPLEMENTATION

A. PassBYOP

Bring your own picture as your password to tackle hacking techniques and secure your account. It introduces the graphical password with a physical token to replace the static images. PassBYOP increases the resistance to attackers on password observation as attackers need to access the physical token. Hence, PassBYOP is a multifactor authentication involving the token and password.

B. Multi-Factor Authentication Scheme

Multifactor authentication system involves the combination of two or more independent processes [5]. To generate and store secrets physical tokens are used. By snapping a picture of a QR code with a mobile device, Dodson et al. proposed a challenge-response authentication system. It generates encrypted data that will be used during login. They are vulnerable to Man-in-the-Middle attacks. PassBYOP differs from the former in three ways, (i) More flexible-any complex image can be set as a PassBYOP token and (ii) Tightly Coupled - close relationship between user and system.

C. Scale Invariant Feature Transform (SIFT)

SIFT is the advanced image processing technique to extract the features in the given image. It reduces the noise level and rotation invariant and gives the accurate features. SIFT technique achieves the accuracy level of 90%.

Scale Invariant Feature Transform image processing technique is used to detect and describe the local features of the image. These features can also be used for object recognition. Using Euclidean distance matching, the feature of the image which is selected from the database is preceded using object recognition [6]. This approach to recognition can robustly identify the objects among disorder and occlusion while achieving near real-time performance.

D. Registration phase

Figure 1 shows the Registration phase of the proposed system. The user needs to register his account for the first time when he creates the account. In the registration phase, the user first wants to create the account with personal details. Each user has a unique username and text-based password for his account. Then select your image as password and pick four click points in your image. The image is set to a threshold value and click points can be clicked within that value. The threshold value can be set by the user such as 20 to 30. Finally, the user profile is created for the user.

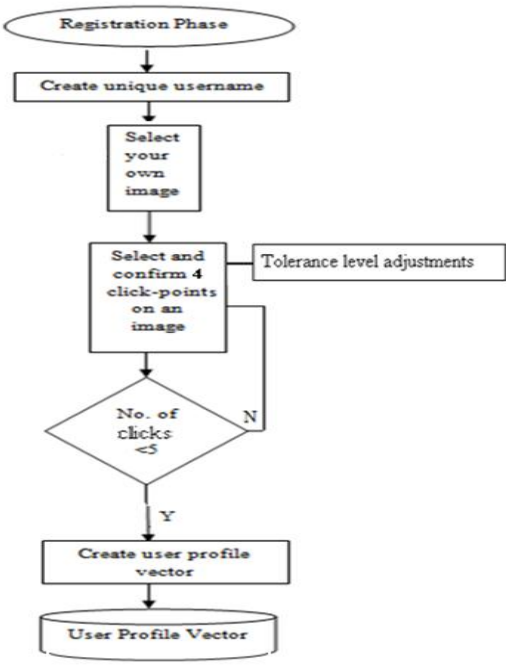

Fig. 1 Registration Phase

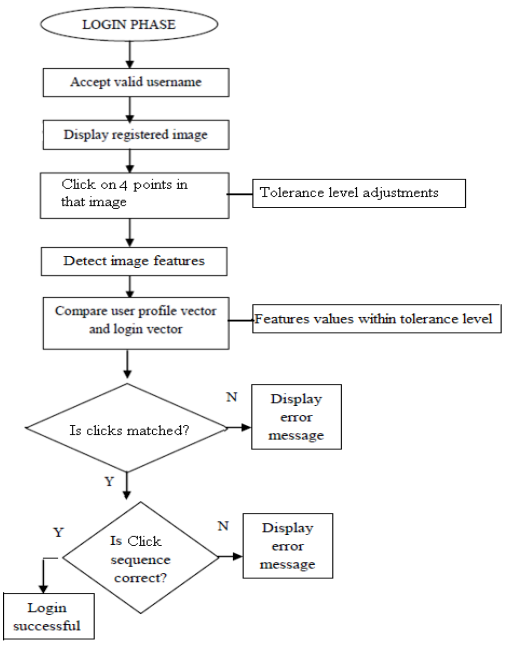

Fig. 2 Login Phase

E. Login phase

Figure 2 shows the Login phase of the proposed method. Whenever the user needs to access their account, they need to login. The login phase involves multifactor authentication. First is text-based authentication followed by image password. When the user inputs an image and selects the four click points in the image. feature extraction is done on the clicked points and stored on the server. Euclidean distance matching algorithm is used to compare the entered image with the image in the database. Euclidean distance matching is to compare the feature coordinates of registered image and the feature coordinates of current image.

III. DISCUSSION

By taking advantage of users' ability to recognize images and the memory trigger associated with seeing a new image, PassBYOP has advantages over other systems regarding usability. But in proposed system user verification process is not achieves high-level security so we focus on verification process and propose Feature points with order evaluation approach i.e. not only verify feature points but also verify the order of feature points. During registration the feature points are stored in the server with its order sequence and match the feature points and its sequence thus achieve high-level security and also provide better usability.

This module assessed the reliability of PassBYOP with order evaluation approach in order to determine suitable thresholds for the equality of two password items regarding the minimum number of image features they should possess and the percentage of image features that should match. Evaluate our proposed system seeks to make graphical passwords more secure against intelligent guessing and shoulder-surfing attacks.

In this paper, order evaluation approach is used for more enhanced security. This method checks for succession order of the click points. It is matched by the coordinates of the selected click points. Every successfully matched click point leads to the comparison of next selected point. Figure 3 illustrates the selection of click points in sequence order.

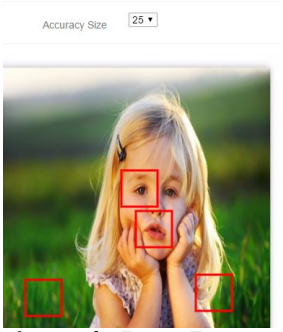

Fig. 3 Selection of click points for Feature Extraction with sequence order

IV. CONCLUSION

Authentication based on passwords is used largely in applications for computer security and privacy. Passwords should be easy to remember and user authentication should be executable quickly by users. And also it should difficult to guess by hackers. Passwords should be unique for every user. This design allows user to have any images and let users choose any places that attract them and are easier to remember Graphical passwords and alphanumeric passwords are vulnerable to shoulder surfing. We overcome this attack and password observation attack with image set of feature in sequence order. PassBYOP substantially increases resistance to shoulder-surfing attacks compared with existing graphical password schemes. PassBYOP conserves the beneficial properties of graphical passwords while increasing their security. The proposed scheme shows promise as a usable and memorable authentication mechanism.

REFERENCES

[1] Z. Zhao and G. J. Ahn, "On the security of picture gesture authentication," in Proc. 22nd USENIX Security Symp., pp. 383-398, 2013.
[2] S. Chiasson, C. Deschamps, E. Stobert, M. Hlywa, B. Freitas Machado, A. Forget, N. Wright, G. Chan, and R. Biddle, "The MVP Web-Based Authentication Framework," Proceedings Financial Cryptography and Data Security (FC), LNCS, 2012.
[3] J. Thorpe and P. Van Oorschot, "Human-seeded attacks and exploiting hotspots in graphical passwords," Proc. USENIX Security Symp., pp. 8, 2007.
[4] S. Chiasson, J. Srinivasan, R. Biddle and P.C. Van Oorschot, "Centered Discretization with Application to Graphical Passwords," Proc. USENIX Workshop Usability, Psychology, and Security (UPSEC), April 2008.
[5] R. Dhamija and A. Perrig, "Deja Vu: A User Study using Images for Authentication", Proceedings of 9th USENIX Security, pp. 1-4, 2000.
[6] M. Eluard, Y. Maetz and D. Alessio, "Action-based Graphical Password: Click-a-Secret," IEEE International Conference on Consumer Electronics, pp. 265-266, 2011.