6th International Conference on Research Developments in Applied Science, Engineering & Management
Mahratta Chamber of Commerce, Industries and Agriculture, Pune (India)
23rd March 2019 www.conferenceworld.in
Conference World
ISBN : 978-93-87793-78-1

Shoulder Surfing Resistant Graphical Password Authentication System

VedantGunjkar, Shantanu Belure, Shreya Prasad,Saurav Jaiswal
BE ,Computer Engineering[SCET]
MIT Academy of Engineering
Alandi,Pune, Maharashtra,India-412105
Prof. Rajeshwari Goudar
Computer Engineering[SCET]
MIT Academy of Engineering
Alandi,Pune, Maharashtra,India-412105

ABSTRACT
When users input their passwords or login credentials in public, they are at a risk of attackers capturing their password. Attackers can capture passwords by direct observation or by recording the individual authentication session. Traditional password techniques are textual password based which is also called alphanumeric password. The textual passwords are easy to crack through various types of attack. Psychological study says that human can easily remember pics orimages than text. So according to this fact, graphical or images passwords are easy to remember and difficult to guess. To overcome the vulnerabilities in the existing system, a graphical password technique is introduced which uses images or graphical passwords. Because of this graphic nature, nearly all the graphical password techniques are vulnerable to shoulder surfing attack. Shoulder surfing resistant password authentication system is the proposed system which assures shoulder surfing resistant authentication to user.
Keywords—Login Indicator,Pass Matrix,

I Introduction

Authentication is the procedure to give access to customers to particular system and resource. In present, there are many authentication schemes in practice like Token based authentication, Biometric based authentication, Knowledge primarily based authentication. User authentication is very essential in information protection to shield consumer privacy. The normal strategy used for authentication is entering the consumer identify and passwords. The textual passwords are brief,easy to remember and are predictable or if textual passwords are lengthy then it is challenging to remember. Users who fail to pick out and manage passwords opens up gap for attacks like hidden camera, spyware attack or key-loggers. These methods are based totally on passwords and pins which are hard to remember on limitations of human capability to recollect. On the other side many biometric authentication techniques have also been proposed. In this paper, the focus is on a knowledge based strategy which uses pictures as passwords. Graphical passwords have been proved as a suitable alternative to textual content based schemes, as it is a possibility for humans to consider pictures rather than text. The password space is large as compared to that of text based schemes which offers better resistance to attacks. Using graphical password, users can click on images to authenticate themselves rather than typing or inputting an alphanumeric string. The graphical passwords are anticipated to be more robust and secured than text-based passwords. Several studies have shown that humans remember pictures more easily compared to text. Graphical passwords hope to leverage visual information and in turn make it less difficult for users to select more secure passwords. The graphical-based techniques can be in addition divided into two categories: recognition-based and recall-based graphical techniques. Using recognition-based techniques, a user is with a set of images and the user passes the authentication via recognizing and identifying the images which the user chosen during the registration stage. Using recall-based techniques, a person is asked to reproduce something that he or she created or chosen earlier during the registration stage. The graphical password authentication approach will briefly describes the difficulties users have with traditional passwords.

ISBN : 978-93-87793-78-1

II Existing System

Using normal textual passwords or PIN method, users need to input their passwords to authenticate themselves and accordingly these passwords can be revealed without difficulty if anybody peek over shoulder or makes use of video recording devices such as cell phones, shoulder surfing attacks have posed a super threat to users privateness and confidentiality as mobile devices are becoming indispensable in modern life. In the early days, the graphical functionality of handheld devices was weak; the color and pixel it may want to exhibit used to be limited. With the increasing quantity of cellular devices and web services, customers can access their non-public accounts to send confidential business emails, add photos to albums in the cloud or remit money from their e-bank account any time and anywhere. While authenticating into these services in public, they might also expose their passwords to unknown parties unconsciously.

III. Proposed System

This system is a Shoulder Surfing Resistant Authentication System based on graphical passwords.The system uses Pass matrix as its key logic to create this type of system. Using Pass-Matrix we generate one-time login indicators per image. The horizontal and vertical control over the pass matrix covers the whole pass-image and offers no clue for attackers to narrow down the password space as they have more than one login records for a particular customer account. The proposed system offers a more secure environment for the users to authenticate in public. The administrator has the right to upload the images on the system and also holds the record of customer transactions.There are two phases of the system: Registration phase and Login phase.

In Registration phase, the user creates an account on the system with unique login credentials. After entering the prerequisites for registration like name,age,address,etc the user proceeds to create its preliminary password. Withprerequisites user has to set the secret bit which is main feature of this system.To create the preliminary password, user first selects 3 images out of the given images uploaded by the administrator. After selecting the images, using pass-matrix the selected images are discritized into 77 pass-squares per image. Out of the 77 pass-squares, user selects one pass-square from all the three selected images.The selected pass-squares are denoted by co-ordinates like 1B,3C etc. The preliminary password is set and sent to user on its registered e-mail or phone number. Also, it gets stored in the administrator's database.

In Login phase, the user authenticates in the system with its unique credentials and multiple login indicators. After setting the preliminary password the system generates multiple login indicators using the pass matrix. At every login session the user obtains new login indicators on their preferred platform like e-mail or phone number. User authenticates in the system by adding the secret bit to the login indicator and then inputting it on the system. At every login session their is a human effort required to obtain the multiple login indicators and adding the secret bit to the password.

3.1 Relevant mathematics

Let S be the Whole system which consists:

S = [I,P,O] Where,

- I is the input to the system.
- P is the procedure applied to the system to process the given input.
- O is the output of the system. A. Input:

  IP = [u,I,LI,pv,n].
  Where
- u be the user.
- I be set of images or pics for creating graphical password.

- pv be the pass values of the chossen image for generating graphical password.
- LI be the login indicator which is used at the time of login.
- n be the number of images or pics which is chosen for creating graphical based password from set of images I..

- Procedure:

1. Registration phase:

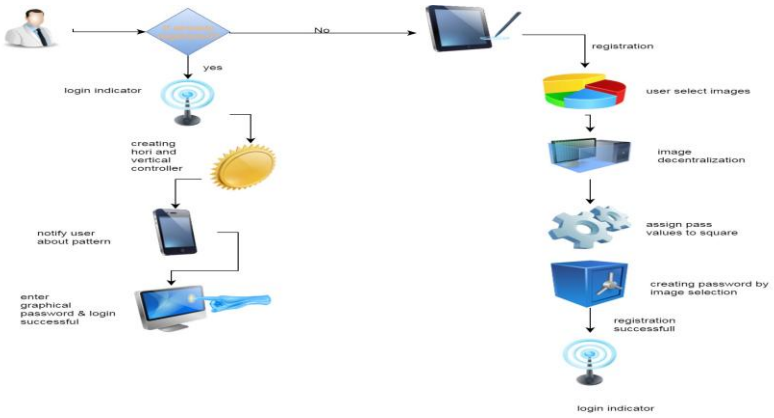
- In this phase, user creates his profile in the proposed system by entering personal details,username,secret bit and graphical password which are stored in database.

The graphical password is set by the user by selecting a sequence of 'n' images from 'I'.The number of images n selected is decided by the user after considering the trade-off between security as well as usability of the system

- Then the system will discritize the selected 'n' images by using pass matrix approach into 7*11 matrix which generates 77 pass-squares of each image.
- Then the user has to select any one pass-square from each of those 'n' images. The generated password is a sequence of co-ordinates of each pass-square selected which is recorded in the database and sent to the user on its registered email id as Login Indicator.
- The Registration phase is completed with a confirmation mail received at the user end with login indicator.

2. Login Phase:

- For step-1 login which is based on recognition based approach,user is asked for username. Afteruser enters his correct username he has to enter the graphical password. For this, user is presented with a grid of n images, randomly placed on the grid.
- A login indicator LI is comprised of a representation of the 7*11 discritized image and the pass-squares to be selected is created by the login indicator generator module using pass-matrix.
- The LI will be shown when the user approaches a login session with his registered email id. In this case, the indicator is conveyed to the user.
- A Generating horizontal and vertical access control is created for login indicator based user selected images (7*11 discritized image matrix) which changes or transforms at every login session i.e. LI is defined for one time use only.
- The generated access control or login indicator will be send to user registered email address.
- In step-2 Login, user will enter the graphical password with the secret bit on the proposed system which authenticates the entered password



3.2 Analysis of the system

For testing 30 different users (15 Male, 15 Female) are considered. The users test the system for 15 times. First 5 attempts are considered as practice sessions and next 10 sessions are considered as login attempts. The accuracy is calculated using practice sessions and login attempts.

- Accuracy:

Based on the practice sessions and login sessions, accuracy of the system is calculated as:

$$PracticeAccuracy = \frac{successfulpracticeattempts}{totalpracticeattempts} \quad (1)$$

$$LoginAccuracy = \frac{successfulloginattempts}{totalloginattempts} \quad (2)$$

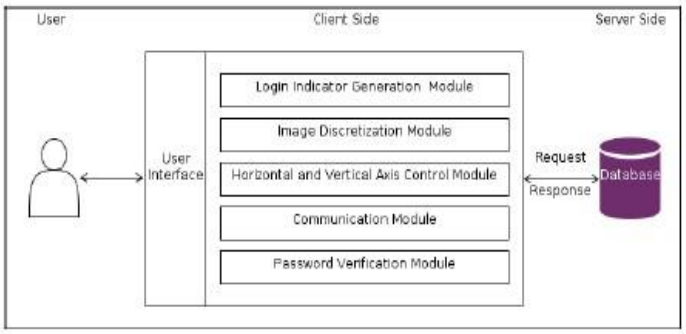
- Password Space:

To calculate the Password Space we use Permutation and Combination.

$$C[n, r] = \frac{n!}{[n-r]!r} \quad (3)$$

Let us select 3 images out of 9 in the given system S.
So, I = 9, n = 3
C(9,3) = 9! / (3!* (9-3)!) = 84
Now, selecting 1 pass-square out of 77 from each of the 3 selected images.
C(77,1) + C(77,1) + C(77,1) = 231
Total Password Space = 84 * 231 = 19,404

IV System Architecture



V. CONCLUSION

With growing shoulder surfing attacks, we have proposed this system which uses Graphical Password Authentication for a Net Banking Application through which shoulder surfing attacks can be alleviated. The Graphical Password Authentication System uses Pass Matrix to generate unique passwords or login indicators at every new login session. The dynamic generation of login indicators is done through Pass Matrix. The proposed system is an advanced modification to the existing system which provides an easy and secure environment to the

users while authenticating in public. The generated login indicators are conveyed to the users on their preferred convenience like mobile number or e-mail. Users refer the login indicators to input their password and authenticate easily. The system also provides a three-layered secured authentication which eliminates the unauthorized login attempts at multiple levels. The system is advanced with an addition of secured bit which is used to login at the final step and known only to the user which makes the existing system more advanced and secured. Thus, the advancement overcomes the drawbacks of the existing system and exhibits its features to provide a safe and secured mean to authenticate in the system.

REFERENCES

[1] Yi-Lun Chen, Wei-Chi Ku*, Yu-Chang Yeh, and Dun-Min Liao *" A Simple Text-Based Shoulder Surfing resistant Graphical Password Scheme."*, Department of Computer Science, National Taichung University of Education, Taiwan.

[2] PhadSunil ,Malkar Ganesh , DhaktodeMayur , Khalane Rakesh and Prof.P.B.Vikhe. *"Graphical Password Authentication Using Cloud"*, Computer Engineering, P.R.E.C, Maharashtra, India

[3] Manu Kumar, Tal Garfinkel, Dan Boneh and Terry Winograd , The system of EyePassword.

[4] M.Kannadasan, J.Amarnadhareddy, K.Venkata Raman proposed *Shoulder surfing resistant graphical Authentication System* , at International Journal of Scientific Engineering Research Volume 8, Issue 5, May-2017.

[5] A.A.Ghasad ,A. B. Deshmukh ,A. B. Bardekar*PASSMATRIX Based Shoulder surfing resistant graphical authentication system* , at International Journal of Advance Engineering and Research Development.

[6] Volekar Roth, Kai Richter, Rene Freidinger., *A Pin entry method resilient to Shoulder Surfing* ,

[7] Amit kalamkar, SwetaChaugule, Swati Lavate, Dinesh Dalvi*Pass sequence acting as OTP using login indicator preventing shoulder surfing attacks* ,

[8] T SudharanSimha , D Srinivasulu,*Pass Matrix checks for Login Authentication* ,

[9] Haichang Gao, Zhongjie Ren, XiulingChang,XiyangLiu,UweAickelin*,"A New Graphical Password Scheme Resistant to Shoulder-Surfing"*, at the Fifth International Conference on Image and Graphics, 2009.

[10] Martinez-Diaz, Marcos, Julian Fierrez, and Javier Galbally. *Graphical passwordbased user authentication with free-form doodles.* , IEEE Transactions on HumanMachine Systems 46.4 (2016): 607-614.