ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

CCP Based Graphical Authentication System

Chimanpure Neha[1], Pachhade Rasika[2], Godalkar Nivedita [3]

B. E. Student, Dept. of Computer Engineering, SCSMCoE, Ahmednagar, Maharashtra, India[1]

B. E. Student, Dept. of Computer Engineering, SCSMCoE, Ahmednagar, Maharashtra, India[2]

B. E. Student, Dept. of Computer Engineering, SCSMCoE, Ahmednagar, Maharashtra, India[3]

ABSTRACT: Authentication based on passwords is used largely in applications for computer security and privacy. However, human actions such as choosing bad passwords andinputting passwords in an insecure way are regarded as the weakest link in the authentication chain. As people can access their application anytime and anywhere,it increase the probability of exposing password to shoulder surfing attack. To overcome this problem, we proposed a novel authentication system based on graphical passwords to resist shoulder surfing attacks. In our system Authentication process is carried out by threetechniques: CCP based Authentication, Doodle Based Intersection, and PassBYOP. Theuser can set their password using any technique as per his/her convenience.

KEYWORDS: Shoulder Surfing, CCP, Doodle Based Intersection, PassBYOP, Authentication

I. INTRODUCTION

Text based passwords are the most widely used authentication method fordecades. As Text based passwords consist of numbers and upper- and lower-case letters, these areconsidered strong enough to resist against brute force attacks. However, a strong text based password is hard to memorize and recollect. Therefore, users tend to choose passwordsthat are either short or from the dictionary, rather than random alphanumeric strings. Even worse, it is common casethat users may use only one username and password for multiple accounts.

Various graphical password authentication schemes were developed to solve the problems and weaknesses associated with text based passwords. Based on some studies it is proved that humans have a better ability to memorize images with long-term memory than verbal representations. Image-based passwords were proved to be easier torecollect in several user studies. The human actions such as choosing bad passwords fornew accounts and inputting passwords in an insecure way for later logins are regarded asthe weakest link in the authentication chain. Therefore, an strong authentication scheme shouldbe designed to overcome these problems and weakness in text based password.

To overcome this problem, we proposed a novel authentication system based on graphical passwords to resist shoulder surfing attacks. In our system Authentication process is carried out by three techniques: CCP based Authentication, Doodle Based Intersection, PassBYOP.

In CCP based Authentication technique, user have to select 5 images for password. Each image is divided into grid, from this grid user have to select one cell. The same process is applied to all five images. The password is formed by combining all selected cell from all 5 images. In Doodle based Intersection technique the user has to select one password containing doodles from doodle-grid. While entering password, for first symbol/letter (first doodle from password) user have to click on one doodle from row and one doodle from column whose intersection point is your password's first symbol/letter. Similarly user have to do for remaining doodles from password. In PassBYOP technique, user can set any real-time image as password. During registration process, user have to take any real-time image.This real-time image is get divided into row-column grid, and from these grid user have to select one block as his/her password. Next time while login, user have to take photo of same real-time image and have to select the same block he/she selected whileregistration processthen feature extraction is performed on that block, and if the feature are matched with the registered image then only the user is get authenticated. The usercan set their password using any technique as per his/her convenience.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

II. RELATED WORK

There are various research work is done in field of security and also in making authentication process more secure. In last few years there are lots of study on password authentication has been done in the literature. Among all of these proposed schemes, our focus is mainly on the graphical-based authentication systems. To design this system we have studied the various papers who have worked on graphical password schemes. Reviews on some of them are given in this section.

In order to defend the shoulder surfing attacks with video capturing, FakePointer [1] was introduced in 2008 by T. Takada. In addition to the PIN number, the user will get a new ”answer indicator” each time for the authentication process. The answer indicator is a sequence of n shapes if the PIN has n digits. At each login session, the FakePointer interface will present the user an image of a numeric keypad with 10numbers, with each key (number) on top of a randomly picked shape. The numeric keys, but not the shapes, can be moved circularly using the left or right arrow keys. During authentication, the user must repeatedly move numeric keys circularly as until the first digit of the PIN overlaps the first shape of the answer indicator on the keypad and then confirm a selection by pressing the space key. This operation is repeated until all the PIN digits are entered and confirmed.

In 2011,Yang Xiang and Wazir Zada Khan[2] proposed a hybrid system for authentication. This hybrid system is a mixture of both recognition and recall based schemes. In this system during registration user have to select username and password in a conventional manner and then chooses the objects as password. After choosing the objects, the user draws those objects on a screen with a stylus or a mouse. Objects drawn by the user are stored in the database with his/her username. During authentication, the user has to first give his username and textual password and then draw pre-selected objects. These objects are then matched with the templates of all the objects stored in the database. In this system, the user will be authenticated only if the drawn sketch is fully matched with the selected object’s template stored in the database.

In 2015, Hung-Min Sun, Shiuan-Tung Chenproposed a novel authentication system PassMatrix[3], based on graphicalpasswords to resist shoulder surfing attacks.In PassMatrix, a password consists ofonly one pass-square per pass-image for a sequence ofn images. The number of images (i.e., n) is user-defined. The user has to select one pass-square for all n images. During the authentication phase the user have to enter username then the system will provide one login indicator to the user.Next, the first pass-image will be shown on thedisplay, with a horizontal bar and a vertical baron its top and left respectively. To respond to thechallenge, the user flings or drags the bars to alignthe pre-selected pass-square of the image with thelogin indicator. The same process is followed for all preselected images.Finally, for each image, the password verificationmodule verifies the alignment between the pass-squareand the login indicator. Only if all the alignmentsare correct in all images, the user is allowedto log into PassMatrix.

In 2015,Marcos Martinez-Diaz, Julian Fierrez [4] published a paper in which authentication with free-form sketches is studied. Verification systems using dynamic time warping and Gaussian mixture models are proposed, basedon dynamic signature verification approaches. The most discriminant features arestudied using the sequential forward floating selection algorithm.

Andrea Bianchi, Ian Oakley proposed a PassBYOP [5] in 2015, a graphical password scheme for public terminals that replaces thestatic digital images typically used in graphical password systems with personalizedphysical tokens, herein in the form of digital pictures displayed on a physical user-owned device such as a mobile phone. Users present these images to a systemcamera and then enter their password as a sequence of selections on live video ofthe token. Highly distinctive optical features are extracted from these selectionsand used as the password.

III. PROPOSED SYSTEM

Graphical password schemes have been proposed as a possible alternative to text-based schemes, motivated partially by the fact that humans can remember pictures better than text; psychological studies supports such assumption. Picture res are generally easier to be remembered or recognized than text. Inaddition, if the number of possible pictures is sufficiently large, the possible password space of a graphical password scheme may exceed that of text based schemes and thus presumably offer better resistance to dictionary attacks. Because of these (presumed) advantages, there is a growing interest in graphical password. In addition to workstation and web log-in applications, graphical passwords have also been applied to and mobile devices. In this CCP based graphical authentication system we have proposed 3authentication techniques:

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

1 .CCP based Authentication
2. PassBYOP
3 .Doodle-based Intersection

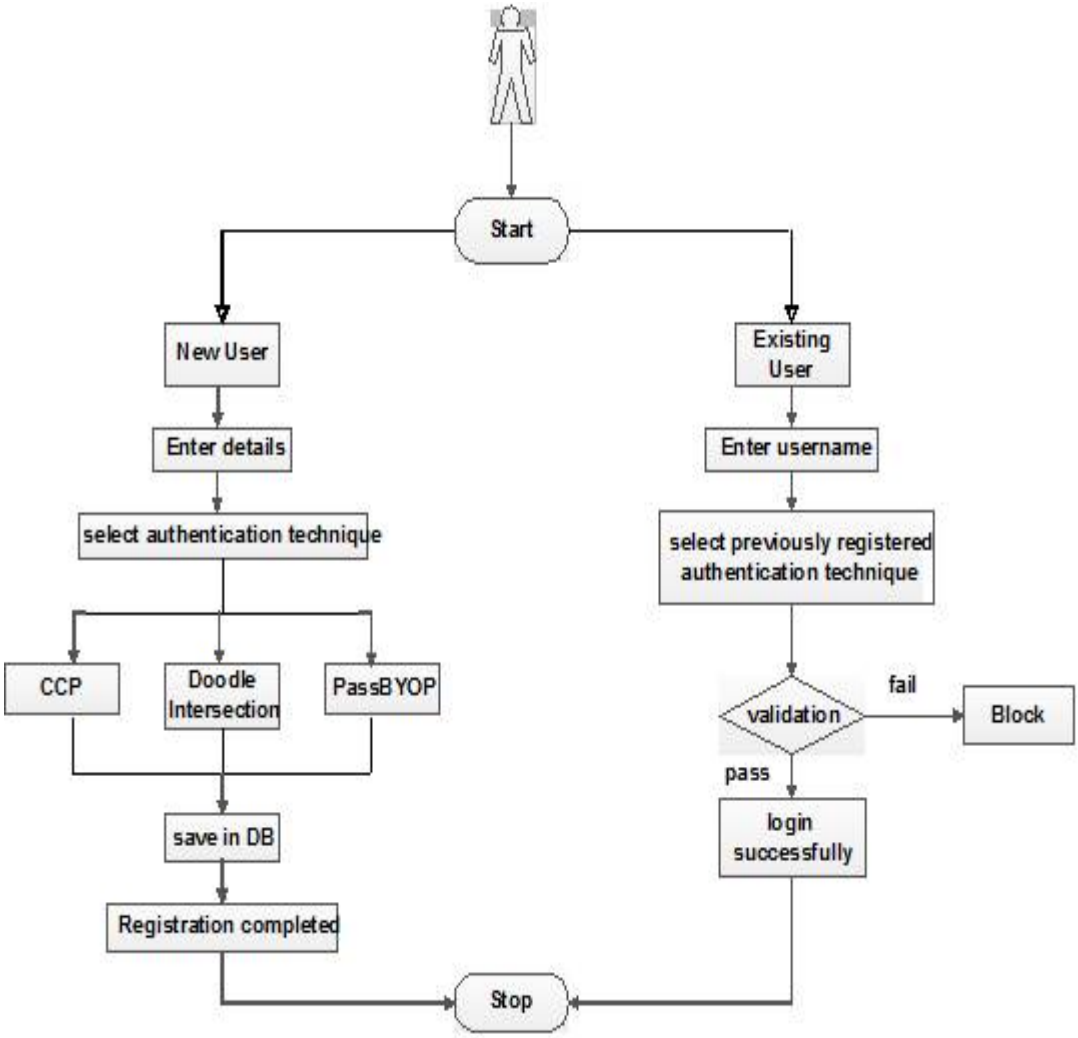

Fig 1 : system flow diagram

A. *CCP BASED AUTHENTICATION :*
In CCP based Authentication technique, user have to select 5 images for password. Each image is divided into grid, from this grid user have to select one cell. The same process is applied to all five images. The password is formed by combining the selected cell from all 5 images.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

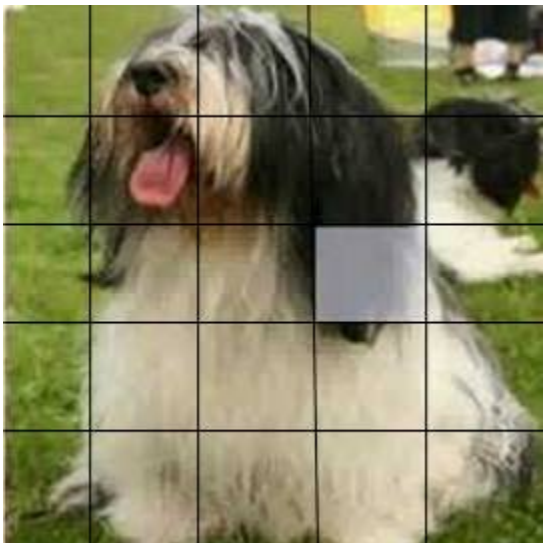

Fig 2:CCP based Authentication

B. ***PassBYOP***

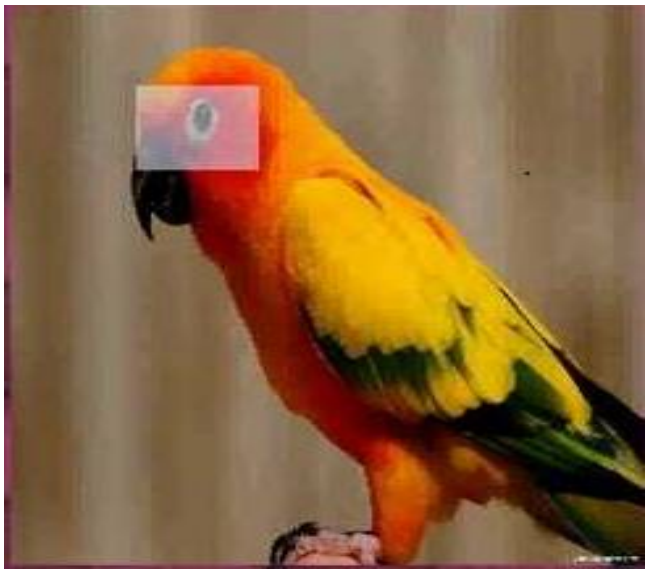

Fig 3: PassBYOP

In PassBYOP technique, user can set any real-timeimage as password. During registration process, user have to take any real-time image.This real-time image is get divided into row-column grid, and from these grid user haveto select one block as his/her password. Next time while login, user have to take thephoto of same real-time image and have to select the same block he/she selected whileregistration process then feature extraction is performed on that block, and if the featuresare matched with the registered image then only the user is get authenticated. The usercan set their password using any technique as per his/her convenience.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

C. ***DOODLE BASED INTERSECTION***

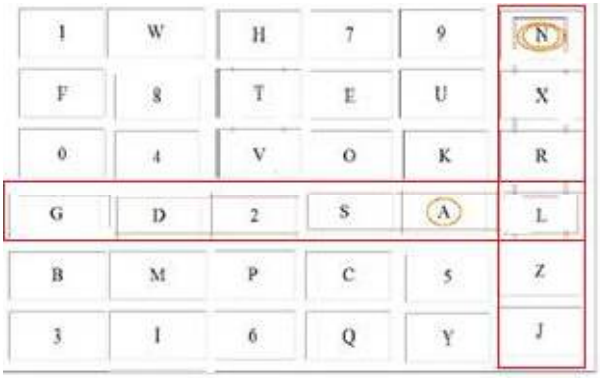

Fig 4:Doodle Based Intersection

In Doodle based Intersection technique the user have to select one password containing doodles from doodle-grid. While entering password, for first symbol/letter (first doodle from password) user have to click on one doodle from row and one doodle from column whose intersection point is your password's first symbol/letter. For example in above image if you have selected 'A' from row and 'N' from column then 'L' is selected as password's symbol. Similarly user have to do for remaining doodles from password.

IV. CONCLUSION AND FUTURE WORK

The traditional way of authentication like text based passwords; alphanumeric password seemed to be difficult enough to be remembered. As most of customers/ users requestare for forgot password there is need for different kind of password system which wouldbe well enough in easy to remember and not difficult or not at all able to be guess or broken.For such situation we propose a graphical authentication techniques based on CCP i.e.Cued Clock point those are secured than any other numeric based techniques and remembrance is notan issue.

REFERENCES

1. T. Takada, "fakepointer: An authentication scheme for improving security against peeping attacks using video cameras," in Mobile Ubiquitous Computing, Systems, Services and Technologies, 2008. UBICOMM' 08. The Second International Conference on. IEEE, 2008
2. Wazir Zada Khan, Mohammed Y Aalsalem and Yang Xiang, "A Graphical Password Based System for Small Mobile Devices", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 2, September 2011,ISSN (Online): 1694-0814
3. Hung-Min Sun,Shiuan-Tung Chen,Jyh-Haw Yeh and Chia-Yun Cheng,"A Shoulder Surfing Resistant Graphical Authentication System",DOI 10.1109/TDSC.2016.2539942, IEEE Transactions on Dependable and Secure Computing, 2015
4. Marcos Martinez-Diaz, Julian Fierrez, and Javier Galbally,"Graphical Password-Based User Authentication With Free-Form Doodles",IEEE transactions on human-machine systems,2015
5. Andrea Bianchi, Ian Oakley, and Hyoungshick Kim, "PassBYOP : Bring Your Own Picture For Securing Graphical Password", IEEE transactions on human-machine systems,2015
6. Tzong-Sun,Wu, Ming-Lun, Lee, Han-Yu, Lin and Chao-Yuan,Wang (2014), "Shoulder-surfing-proof Graphical Password Authentication Scheme," International Journalof Information Security, Vol. 13, Issue 3, pp. 245-254, Springer Berlin Heidelberg.
7. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The design and analysis of graphical passwords," in Proc. 8th USENIX Security Symp., 1999, p. 1.
8. Wiedenbeck, J. Waters, Sobrado, L. and Birget, J.C. (2006), "Design and Evaluation of a Shoulder-surng Resistant Graphical Password Scheme," Proc. of the Working Conference on Advanced Visual Int-eaces, pp. 177-184. 415
9. Dhamija, R. and Perrig, A. (2000), "Deja Vu: A User Study using Images for Authentication", Proc. 9"' USENIX Security, pp. 1-4.
10. Eluard, M., Maetz, Y. and Alessio, D. (2011), "Action-based Graphical Password: Click-a-Secret," IEEE International Conference on Consumer Electronics, pp. 265-266.