Volume 5, Issue 6, June 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Enhanced User Graphical Password Authentication with an Usability and Memorability

Saraswati B. Sahu*
Information Technology &
RGPV, India

Associate Prof. Angad Singh
Information Technology &
RGPV, India

Abstract— Authentication is the process to provide guaranteed information security and the graphical password authentication method is a convenient and easy process to provide authentication. The major problem of user registration, mostly text base password, is well known. If the login user be inclined to select a simple password which is frequently in his mind it becomes straightforward for attackers to guess. If the password is machine generated it is mostly complicated for user to keep in mind. User authenticated password using cued click points graphical password scheme includes memorability, usability and security evaluations. This paper is on enhanced user graphical password authentication with an usability and memorability, so that users select more random or more difficult to guess passwords. In click-based graphical passwords, image or video frames provide database to load the image, and then give authenticated access to all information in database.

Keywords— User authentication, graphical password scheme, cued recall, video frame as a password, usability, memorability, security.

I. INTRODUCTION

Security has been an issue from the inception of computer systems. Secured systems must be usable to maintain intended security. Password Authentication Systems have either been usable and not secure, or secure and not usable. Increasing either tends to complicate the other. Today, authentication is the principle method to guarantee information security and the most common and convenient method is password authentication .Authentication word comes from Greek authentiko means "real, genuine", authentes, "author". In other word it can define as is the act of confirming the truth of an attribute of a single piece of entity. Traditional alphanumeric passwords are strings of letters and digits, which are easy and familiar to essentially all users. Text based passwords are nothing but string of characters. For text passwords, peoples always creates password which is easy to remember but these passwords are easy for attackers to break. Due to the limitation of human memory, most users tend to choose short or simple passwords which are easy to remember .Surveys show that frequent passwords are personal names of family members, birth date, or dictionary words. In most cases, these passwords are easy to guess and vulnerable to dictionary attack. Users have many passwords for personal computers, social networks, E-mail, and more. They may decide to use one password for all systems to decrease the memory burden, which reduces security .Moreover, Text based passwords are vulnerable to shoulder surfing attack, spyware attack and social engineering attack etc. Biometric and tokens are used as an alternative to text based passwords but has its own drawbacks such as it requires extra hardware so these methods are costly. Like alphanumeric passwords, graphical passwords are knowledge-based authentication mechanisms. Graphical password authentication techniques are (1)Recognition Based (2)Pure Recall Based (3)Cued Recall Based.The main goal of graphical passwords is to use images or shapes to replace text, since numerous cognitive and psychological studies demonstrated that people perform far better when remembering pictures than words. This paper to find the best method to provide the enhanced user graphical password with memorability, usability and security of graphical passwords using culturally familiar pictures.

II. BACKGROUND

Token based passwords are the most popular user authentication method, but have security and usability problems. An alternative to this is biometric systems. Graphical passwords offer another alternative, and are the focus of this paper. Click-based graphical passwords: Graphical password systems are a type of knowledge-based authentication that attempt to influence the human memory for visual information [11].

A. Recognition Based

Recognition based Systems which are also known as Cognometric Systems or Searchmetric Systems. Recognition based techniques involve identifying whether one has seen an image before. The user must only be able to recognize previously seen images, not generate them unaided from memory. In recognition-based systems, a group of images are displayed to the user and an accepted authentication requires a correct image being clicked or touched in a particular order. Some examples of recognition-based system are Awase-E [7] system Authentication Graph and Pass faces[8] system.
A recognition-based scheme and concluded that users can still remember their graphical password even after one or two

months. Their study supports the theory that human remember images better than text. In addition for example, the commercial system uses images of human faces. Although a recognition-based graphical password seems to be easy to remember, this increases the usability.

Fig.1 PassFaces Scheme

B. Pure Recall-based

Recall-based authentication schemes, also called draw metric systems [6], require users to remember a previously created drawing without the help of cues. As one of the first recall-based schemes, Draw-A-Secret (DAS) [10] lets users draw a shape on a two-dimensional grid. Other relevant systems in this category include BDAS [1], which adds background images to the DAS grid, the grid-free PassDoodle [9] and Pass-Go [9], a snap-to-grid system that also incorporates colors. One advantage of recall-based systems is the fact that they often have theoretical password spaces comparable to text passwords. On the other hand, the effective password spaces can differ largely due to repeating patterns in user choice, e.g. users tend to choose passwords in the center with only few strokes. Another problem with such schemes is shoulder surfing attacks, since the drawings are always fully visible on screen.

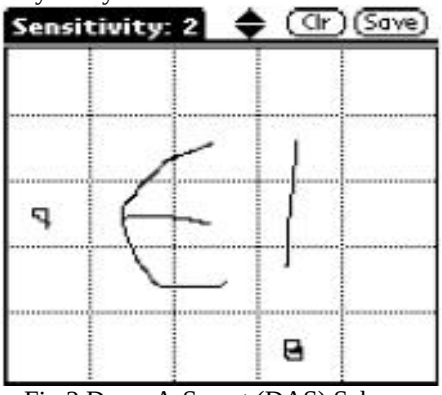

Fig.2 Draw-A-Secret (DAS) Scheme

C. Cued Recall

Pure recall can still be a difficult task for humans to carry out, a number of cued recall systems have been proposed. As the name suggests, users are given cues to remember their passwords. Most commonly, people are supposed to locate specific points within an image in order to login. A prime example in this category is PassPoints [4], where users are supposed to identify 5 spots on a picture in the right order. The click points are acceptable if they are within the predefined level of tolerance.

Fig.3 Pass Point Scheme

To reduce hotspots and improve usability of click-based graphical password schemes, Chiasson et al. [2] proposed Cued Click-Points (CCP), a variation of PassPoints in which users click on one point per image for a sequence of images. The next image is displayed based on the location of the previous click-point, that is, each image after the first is a deterministic function of the current image and the coordinates of the user-entered click-point. If users click an incorrect point, a wrong image will be displayed. It is meaningless to attackers without knowledge of the correct password.

However, analysis of user choice revealed that users tended to select click-points falling within known hotspots. The main motivation behind for click based graphical passwords is the hypothesis that people are better at remembering images than artificial words. Visual objects seem to offer a much larger set of usable passwords. For example we can recognize the people we know from thousands of faces; this fact is used to implement proposed an authentication system.

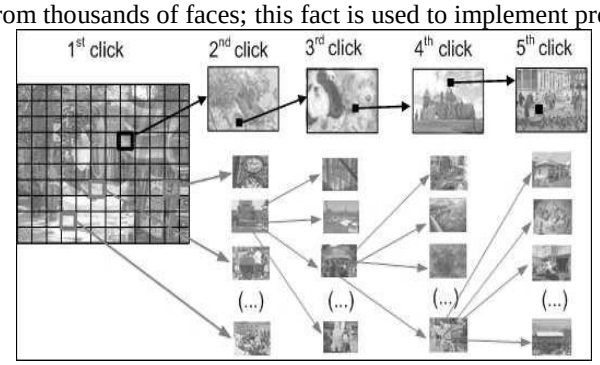

Fig.4 A user navigates through images to form a CCP

III. SYSTEM DESIGN

The system model involves three basic modules (1) Registration (2)Login (3)Forgot password.

A. Registration

In the registration first of all user has to register themselves by filling the basic information then in next phase create the cued click points on images provided by the system and move to the last phase in that user has to select a frame from video as well as write frame text(password). After the successful completion of all the above phase user finally registered with the system.

B. Login

While login user has to enter the user name and password. Then after has to create a click points in a particular sequence and finally has to enter the frame text.

C. Forgot Password

In case if the user forgot password then user can fetch the text password by providing user name.

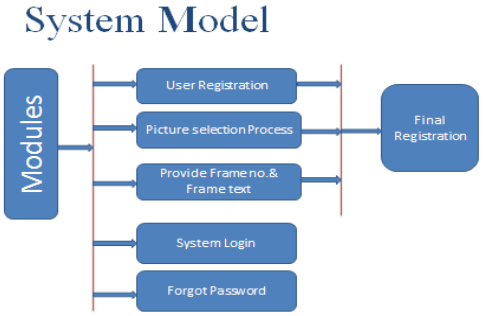

Fig.5 system model

1. Algorithms for the Registration module:

i. Register user with basic information .
ii. Create user Id and text password.
iii. User can select any image from system for graphical password.
iv. Ask the user for click points on image to generate password
v. Store information to database also ask user to select another image for another click points then goto
vi. step(iii)otherwise continue with step(iv).
vii. Ask user to load the video.
viii. Select a particular frame no. and frame text.
ix. Store the frame no. and frame text into the database.

2. Algorithms for the Login module:

i. Enter User id and text password.
ii. Compare user id and text password with database ,if match found then goto step(iii) ,otherwise step(i).
iii. Ask User for click points on image.
iv. Compare click points ,if match found then goto step(v) ,otherwise step(i).
v. Ask user to enter the frame text.
vi. Compare frame text with database if match found then goto step(vii),otherwise step(i).
vii. Login Successfully.

IV. IMPLEMENTATION

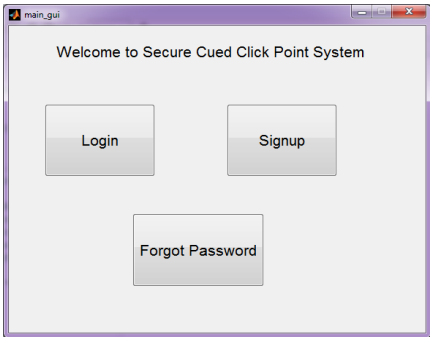

Fig.6 Home Page

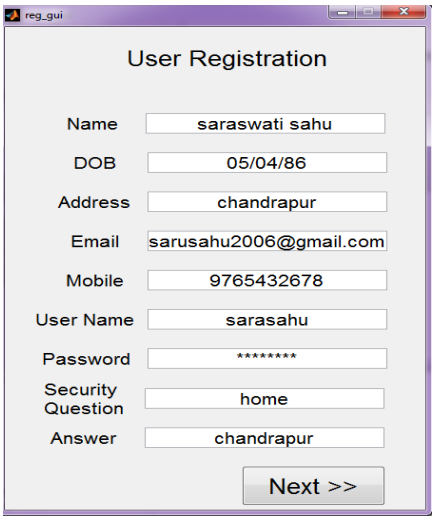

Fig.7 Registration phase-I

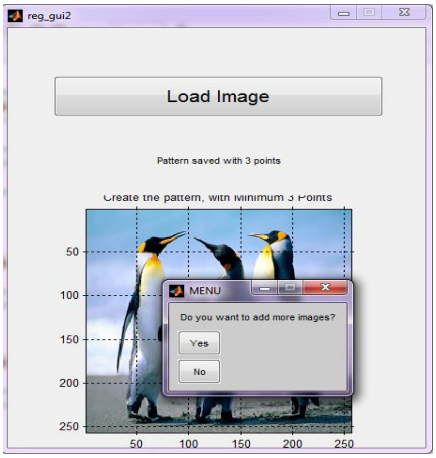

Fig.8 Registration phase-II

Fig.9 Registration phase-III

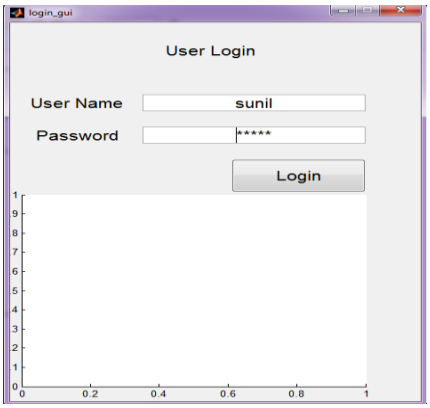

Fig.10 Login phase-I

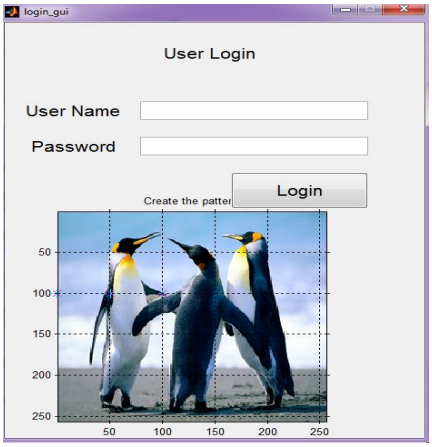

Fig.11 Login phase-II

Fig.12 Login phase-III

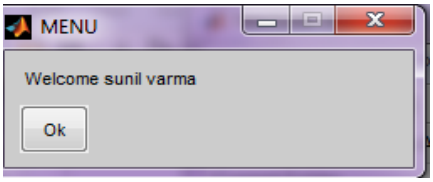

Fig.13 Login Successful

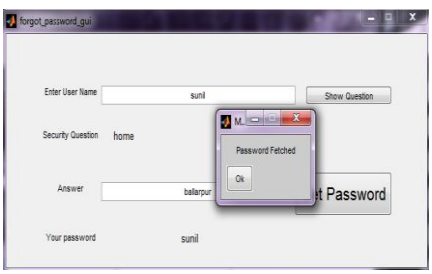

Fig.14 Forgot Password

V. RESULT ANALYSIS

Table.1 Comparative study

Schemes/ Parameters	Pass Point	Cued Click Point	PCCP	S-CCP
Images selection	System Defined	System Defined	System Defined	User Defined
Hotspot Problem	More vulnerable	vulnerable	less vulnerable	Less vulnerable
Password creation time	less time consuming	time consuming	time consuming	Time consuming
Login time	More login time than CCP	Login time less than pp	Login time more than PP	Login time less than PCCP
Usability	Good	Randomness but less usability than PP	Limited area due to viewport	Very Good, Randomness with more usability

A user study was conducted in order to investigate the objectives. Participants were asked to use the Graphical authentication. This activity took approximately minimum time to complete, depending on the participants experience of using computers. The following sections explain the model, and outline the steps and procedures the participants had to follow.

There were two main modules in the user- registration and login. In the registration module, participant‟s needs to create their text password and images password by clicking on the image for the click-based method, choosing one or more images and choosing one or more frame from video also provides the frame text. In the login module, participants were asked to log into the login by using their username and text password first, then after conformation login with image password and finally frame text password.

Participants were asked to use the methods in order as given. The following list details the tasks each participant needed to complete.

1. Register and create their user name and text password. With filling basic information. Once succeed.
2. Re-authenticating by using their username and text password, their image password and frame text password.

Upon using the prototype, all of the participant‟s actions and behaviour were observed for monitoring purposes. As this was an uncontrolled type of survey, participants were allowed to use the model as many times as they wanted.

A total of 52 participants took part in this study (males and females). The minimum age of the participants was 21 years old. The majority of the participants were drawn from the university (e.g. students, researchers, lecturers, Software developers) and all of them had more than 5 years‟ experience using computers. From observation, it was found that participants were initially little confused with the flow of graphical authentication. For example in the click-based type, the majority of them had problems reproducing their passwords (secrets). This is possibly due to their misunderstanding of this approach because when they clicked on particular points (for example clicking on the person‟s hand); they were assuming the whole image (in this case, the whole body of the person) was chosen. Only the point or the area in which they clicked would be taken into account as their password and not the whole object.

Table.1 Lab Study Result

Parameter	Pass Point	Cued click Point	PCCP	S-CCP
Login time	9-25s	7s	11-89s	24s
Success rate	38-94%	96%	83-94%	97.11%

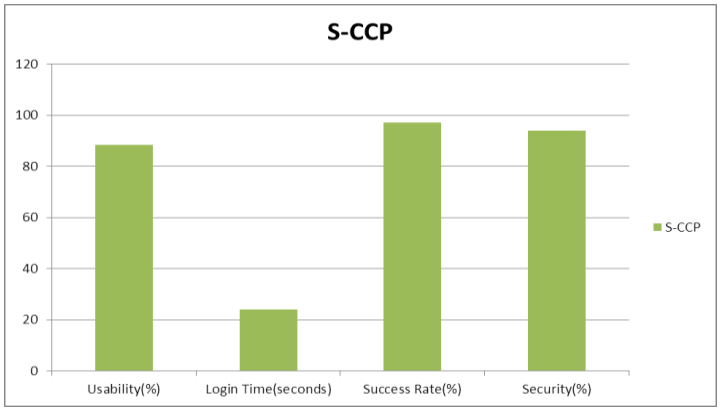

Fig.15 Result Analysis Chart

VI. CONCLUSION

The proposed 3-factor proposed method scheme shows secure as a usable and memorable certification method. By delightful benefit of clients capability to recognize images and the memory trigger associated with text password. The proposed method has advantages over PassPoints, Cued Click Point, and Persuasive Cued Click Point in terms of usability and also security. Being click point as on images shown and having to remember click-point on given image appears easier than having to remember an ordered series of clicks.

Generally, there are many drawbacks associated with the textual passwords such as brute-force and dictionary attack. Alike is the folder with the graphical passwords which include shoulder-surfing and are very expensive to implement. In this proposed thesis, it is made use of both the textual and graphical password techniques to decrease vulnerability.

The proposed method offers a more secure alternative to PassPoints, Cued Click Point, and Persuasive Cued Click Point method. This proposed method increases the workload for attackers by forcing them to first acquire text password, secondly images sets for each user and video frame text, It works for hotspot reduction on each of used images and increase randomness in case of click points.

VII. FUTURE SCOPE

In future development, proposed authentication techniques based on text and images will propose for online applications. These techniques will generate session passwords and are resistant to different attacks. However this schemes completely new to the users.Proposed authentication techniques should be verified extensively for usability and effectiveness. This technique can also be developed as windows application such as a folder locker or in banking application. In future development will also add hashing in password to prevent from rainbow table attack also the increase security. We can add reset password and feedback module. Also we can limit a user from enter the wrong password.

REFERENCES

[1] Lopez, Nicolas , Matias, Long, Darrell -" Even or Odd: A Simple Graphical Authentication System", Latin America Transactions, IEEE (Revista IEEE America Latina), Vol:13, Issue: 3), pp. 804 – 809, March 2015.

[2] Wei-Chi Ku , Dum-Min Liao, Chia-Ju Chang, Pei-Jia Qiu- " An enhanced capture attacks resistant text-based graphical password scheme", Communications in China (ICCC), 2014 IEEE/CIC International Conference ,pp.204-208, 13-15 Oct. 2014.

[3] Burgbacher, U., Pratorius, M., Hinrichs, K.- "A behavioral biometric challenge and response approach to user authentication on smartphones", Systems, Man and Cybernetics (SMC), 2014 IEEE International Conference,pp.3328-3335, 5-8 Oct. 2014.

[4] Aljahdali, H.M., Poet, R. -"Challenge Set Designs and User Guidelines for Usable and Secured Recognition-Based Graphical Passwords", Trust, Security and Privacy in Computing and Communications (TrustCom), 2014 IEEE 13th International Conference,pp.973-982, 24-26 Sept. 2014.

[5] Bin B. Zhu, Jeff Yan, Guanbo Bao, Maowei Yang, and Ning Xu- "Captcha as Graphical Passwords- A New Security Primitive Based on Hard AI Problems", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 6, pp.891-904, JUNE 2014.

[6] Si Chen, Muyuan Li, Zhan Qin, Bingsheng Zhang- " AcousAuth: An acoustic-based mobile application for user authentication", Si Chen ; Dept. of Comput. Sci. & Eng., State Univ. of New York at Buffalo, Buffalo, NY, USA ; Muyuan Li ; Zhan Qin ; Bingsheng Zhang ,pp.215-216, April 27 2014-May 2 2014.

[7] Ms. Shilpa Veerasekaran , Prof. Alka Khade , Prof. V.B Gaikwad- "Using Persuasive Technology in Click Based Graphical Passwords",International Journal of Emerging Trends & Technology in Computer Science - Volume 3, Issue 2, pp.32-36, March – April 2014.

[8] A.Abuthaheer, N.S.Jeya Karthikka, T.M.Thiyagu- "Cued Click Points Graphical Images and Text Password along with Pixel based OTP Authentication", International Journal of Computer Applications (0975 – 8887) Volume 87 , pp.45-48, February 2014.

[9] Gurav, S.M. Gawade, L.S., Rane, P.K., Khochare, N.R- "Graphical Password Authentication: Cloud Securing Scheme", Electronic Systems, Signal Processing and Computing Technologies (ICESC), 2014 International Conference , pp.479 – 483, 9-11 Jan 2014.

[10] V.Prasath, R.Buvanesvari, P.Nithin, S.Banu, K.Rajeswari- "Graphical Password Authentication Using Persuasive Cued Click-Points Mechanism", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-6, pp.142-145, January 2014.

[11] Vaibhav Moraskar, Sagar Jaikalyani- "Cued Click Point Technique for Graphical Password Authentication", International Journal of Computer Science And mobile Computing-Vol. 3, Issue. 1, pp.166-172, January 2014.

[12] Smita Chaturvedi, Rekha Sharma- "Securing Image Password by using Persuasive Cued Click Points with AES Algorithm", International Journal of Computer Science and Information Technologies, Vol. 5 (4) , pp.5210-5215, 2014.

[13] Md. Asraful Haque, Babbar Imam- "A New Graphical Password: Combination of Recall & Recognition Based Approach", World Academy of Science, Engineering and Technology International Journal of Computer, Control, Quantum and Information Engineering Vol:8, No:2, pp.310-315,2014.

[14] Haichang Gao, Ning Liu, Kaisheng Li, Jinhua Qiu-" Usability and Security of the Recall-Based Graphical Password Schemes", High Performance Computing and Communications & 2013 IEEE International

Conference on Embedded and Ubiquitous Computing (HPCC_EUC), 2013 IEEE 10th International Conference , pp.2237 – 2244, 13-15 Nov. 2013.

[15] Renaud, K., Mayer, P., Volkamer, M., Maguire, J.- "Are graphical authentication mechanisms as strong as passwords?", Computer Science and Information Systems (FedCSIS), 2013 Federated Conference, pp.837 – 844, 8-11 Sept. 2013.

[16] Lavanya Reddy L,K.Alluraiah- "Enhanced Cued Click Point Method for Graphical Password Authentication", International journal of advanced research in computer science and software engineering, Volume 3, Issue 8, pp.321-326, August 2013.

[17] Binitha .V.M- "Persuasive cued click based graphical password with scrambling for knowledge based authentication technique with image scrambling", IOSR journal of computer engineering,vol.13, issue 2, pp.14-24,July-Aug 2013.

[18] Haichang Gao, Wei Jia, Fei Ye and Licheng Ma- "A Survey on the Use of Graphical Passwords in Security", JOURNAL OF SOFTWARE,-VOL.8, pp.1678-1698, JULY 2013.

[19] Iranna A M1,Pankaja Patil2- "Graphical Password Authentication using Persuasive Cued Click Point", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 2, Issue 7, pp.2963-29,July 2013.

[20] Ms. Shilpa. L. Dhapade- "Implementation of Persuasive Cued Click-Points Techniques for Folder Security", International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 6, pp.2005-2012, June – 2013.

