IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

CARP: CAPTCHA as A Graphical Password Based Authentication Scheme

Shraddha S. Banne[1], Prof. Kishor N. Shedge[2]

Student, Dept. of Computer Engg, S.V.I.T, Chincholi, Sinnar, Nashik, India[1]

Assistant Professor, Dept of Computer Engg, S.V.I.T, Chincholi, Sinnar, Nashik, India[2]

Abstract: This research aims to study the existing password schemes and to design and develop a new improved graphical password scheme. CaRP is Captcha as a graphical password. With the hybrid use of CAPTCHA and graphical password it can addresses a number of security problems altogether. In information security, user authentication is a major problem in every system. And for authentication purpose every system depends on password whether it is textual password or graphical password. CAPTCHA is a test build by computer programs which human can pass but computer programs cannot pass. In this paper, we discuss the strengths and limitations of each method and present a combination of CaRP and graphical password scheme which is protected to the common attacks suffered by other authentication schemes.

Keywords: Graphical Password, CaRP, CAPTCHA, Authentication, Security.

I. INTRODUCTION

User authentication now-a-days is a major problem in authentication system. And for authentication purpose computer security depends on password. There are some important characteristics of password.

1. Password should be changeable.
2. It should quickly and easily executable.
3. It should easy to remember.

Authentication is unavoidable task in security where we use text password as a security technique but text passwords are threaten by many attacks. Such as phishing, brute force attack, dictionary attack etc. among this phishing is a serious threat to text based password. Phishing is an action of getting information such as username, password, contact no. or any other details by masquerading. Another problem with text based password is the difficulty of remembering passwords.

To address the problems with traditional username password authentication scheme, an alternative authentication method such as Graphical password is a solution to text based password. Because human ability to recall pictures is more whether they are line drawing object or real object than textual password. In Graphical password user set image instead of text as his password. Because of these above advantages, there is a growing interest in graphical password. In addition to web login application and work-stations, graphical passwords have also been used to ATM machines and mobile devices.

CAPTCHA (Completely Automated Public Turing tests to tell Computers and Humans Apart) is programs that generate tests that are human solvable, but current computer programs do not have the ability to solve them. a captcha is a program that protect sites against bots, resisting automatic adversarial attacks, and it has many applications for practical security, contain online polls, free email services, search engine bots, preventing from dictionary attacks, spam and worms etc.

CaRP is Captcha as a graphical password. Which is a combination of captcha and graphical password and used as a single entity for authentication. CaRP is a click-based graphical password scheme. Unlike other click-based graphical passwords, images used in CaRP scheme are Captcha challenge for the user, and for every login attempt a new CaRP image is generated. CaRP addresses a number of security problems altogether, that is online guessing attacks, relay attacks, and, if combination with dual-view technologies like graphical password or text password can minimize shoulder-surfing attacks.

In this paper we conduct a comprehensive survey of existing graphical password techniques and CaRP techniques. We will discuss the strengths and limitations of each technique and future research direction will be point out in this area. This paper will be particularly useful for Information security researchers who are interested in developing new graphical password algorithms also industry practitioners who are interested in deploying graphical password techniques.

II. BACKGROUND(LITERATURE REVIEW)

The term graphical password was originally introduced by Greg Blonder in 1996. Graphical password is the password where user set his/her password as picture or image. Graphical password has been proposed as an alternative to text based, because human ability to recall pictures is more than text. Psychological studies had shown that people can remember pictures better than text Picture. Text Images are generally easier to be remembered or recognized than text, especially images which are even easier to be remembered than random images.

Graphical passwords are divided into two important categories:-

1. Recognition based techniques
2. Recall based techniques

DOI 10.17148/IJARCCE.2016.5104

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

A. Recognition based technique:- In this technique user is presented with a number of images and user have to select an images among them as password. At the time of authentication user have to recognize their registration choice image. In this section we describe merit and demerit of some recognition techniques

1. Passfaces Scheme:-

Fig.1. Passface technique

Fig1. Shows the passface scheme. This method is developed in 2000. In this human faces used as a password. Where user is presented with set of human faces and user have to select on face images pre-selected in registration for several such rounds. Drawbacks of this scheme are the probability of a guessing attack is high with few authentication rounds. Also it is easily predictable or guessable. And passface scheme is vulnerable to shoulder surfing attacks.

2. Déjà vu scheme:-

Fig2. Déjà vu technique

Fig2. Shows Déjà vu scheme the Dhamjia et al. proposed Déjà vu, where users will select a certain number of random art pictures from a set of pictures generated by a system in the registration phase. During authentication, the system displays a challenging set mixes with password image & some decoy images. The user must identify the password pictures. Moreover, the art images make it difficult to record Déjà vu has several drawbacks, for example, an obscure picture is hard to remember. Login phase take longer time than textual.

3. Story Scheme:-
Fig. 3.Shows the story scheme technique. Story only needs one round authentication. User have to select password using or creating story in mind and have to remember that story at the time of authentication phase.

Fig.3. Story scheme technique

The story requires users to remember the order of images. Users who did not take the advice of using a story to guide their image selection to remember the password it is difficult for them.

B. Recall Based Technique
At the time of authentication a user is asked to reproduce or choose something which he produce or selected during the registration step.

Draw–A-Secret (DAS) Scheme:-

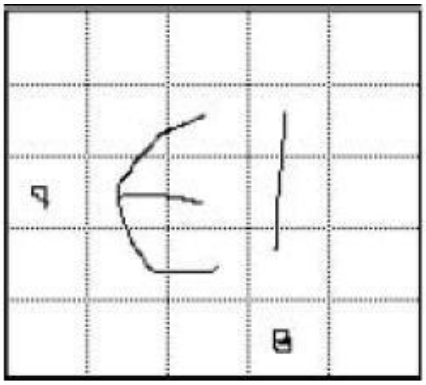

Fig.4. Draw-A-Secret technique

Fig. 4 shows the DAS scheme. It is an example of recall based technique this was proposed in 1999. In this scheme user have to draw something on 2D grid. And Redrawing at the time of authentication has to touch the same grid in the same sequence. The drawback of this method is hard to remember to draw a password in compare to other. Varenhorst presented the Passdoodle; allow users to create a freehand drawing as a password without a visible grid. A doodle should required of at least two pen-strokes anywhere on the screen and can be drawn in a number of colors. The matching process in Passdoodle is more complex than in DAS.

C. Cued Recall Based Technique
This is also called click based technique. In this technique user is presented with image or set of images & user have to select click point on that images as the password. User will successfully authenticate by entering correct click point and order of that point.

1. Blonder:-
This method proposed by Greg blonder. In this user is presented with prestored images and have to tap region by pointing location on image. Drawback of this method is simple or easily crackable and clicking region is small.

DOI 10.17148/IJARCCE.2016.5104

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

Blonder is the first technique used by the user as a graphical password.

2. Passpoint:-

Fig.5. Passpoint technique

Fig. 5 shows the clickable technique passpoint technique. It designed to overcome the limitation of Blonder technique. Where user have to set sequence of clicks as his password. And at the time of authentication user have to select correct order of clicks.

To reduce hotspots and improve usability of click-based graphical password schemes, Chiasson et al. proposed Cued Click-Points (CCP), a variation of Passpoint in which users click on one point per image for a sequence of images. On the basis of location of the previous click-point the next image will be displayed.

Below is the comparison table of all the graphical password techniques usability and drawbacks which is existing. Contain text based password, Recognition based technique, pass faces scheme, Story scheme, Recall based techniques, Draw-A-Secret, Cued Recall based Techniques etc.

Technique	Usability	Drawbacks
Text Based Password	Typing Alpha numeric password	Dictionary attack, Brute-force search , Spyware , Shoulder surfing
Recognition Based technique	Pick several pass-pictures out of many choices	Take longer to create than text. Heavy load on db to store images.
Passface technique	Recognize & pick the pre-registered face images	Very much predictable , Create load of decoy faces on db
Story	Create story using selecting picture	Story scheme was harder to remember in compare to passface.
Recall Based Technique	Grid in which user draw a password	Limitation in grid complexity due to human error
Draw a Secret	User draw something on a 2D grid	User studies showed the drawing sequence is hard to remember
Cued Recall based technique	Click on five different area.	Hard to remember the sequence of area points .

CAPTCHA

Captcha basically differentiate between human and computer program. There are two types of captcha text and Image-recognition captcha (IRC). Text captcha is recognition of character.it contain difficulty to understand character. And image captcha relies on recognition of non character object.

CaRP:-

Bin B. Zhu, Jeff Yan, Maowei Yang, Guanbo Bao and Ning Xu [1] proposed CaRP scheme. While CaRP is a Captcha as a graphical Password. Which is a combination of captcha and graphical password and used as a single entity for authentication. CaRP is a click-based graphical password scheme. Unlike other click-based graphical passwords, images used in CaRP scheme are Captcha challenge for the user, and for every login attempt a new CaRP image is generated. CaRP image generation which turns out to be a CAPTCHA challenge for the user. CaRP can be categorized into Recognition based and Recognition-Recall.

A. Recogniton based CaRP:-

In this system, infinite number of visual objects can be accessed as a password. Sequences of alphanumeric visual objects are also used in this system.

1. ClickText**:-**

In Clicktext captcha system will generate image of number of alphanumeric characters & user have to click on image and enter password in same order. It uses 2D grid.

2. ClickAnimal:-

To generate 2D animals with different colors, textures, poses technology use 3D models of animal. It is a recognition based CaRP scheme. It develops on the top of Captcha Zoo.

3. Animal Grid**:-**

It is a combination of Click A Secret (CAS) and ClickAnimal. In this system, firstly ClickAnimal image is displayed, after the animal is selected, an image of n*n grid appears.

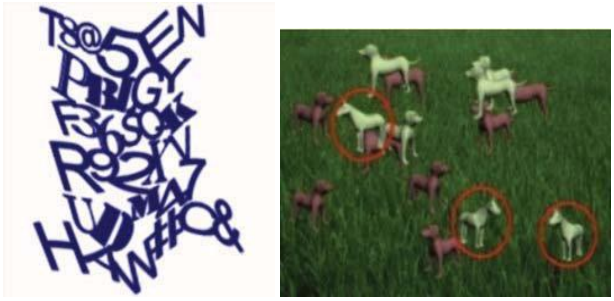

Fig.5. Clicktext & ClickAnimal CaRP Scheme

B. Recognition Recall CaRP:-

In this system, sequence of some invariants points of objects is the password. Points are the invariant points of object that has a fixed relative value in different fonts. User must identify the object image and then use identified objects as a cue to locate a password within a tolerance area. TextPoints and TextPoint4CR techniques are examples of recognition recall CaRP [1].

III. PROPOSED SYSTEM

It contain six modules that is User Registration- It will complete user registration process. Second module. User Login- After complete process of registration user will try to login into his account Through CaRP Authentication. Third is User Account means he can edit his info or other activity. Then user will enter into fourth module File Store. User can store his files for ex- doc., pdf, ppt etc in his account. If user wants security for the file then user will set graphical password as click point graphical password. And the last module he can access his account after successfully login his clickable password.

DOI 10.17148/IJARCCE.2016.5104

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

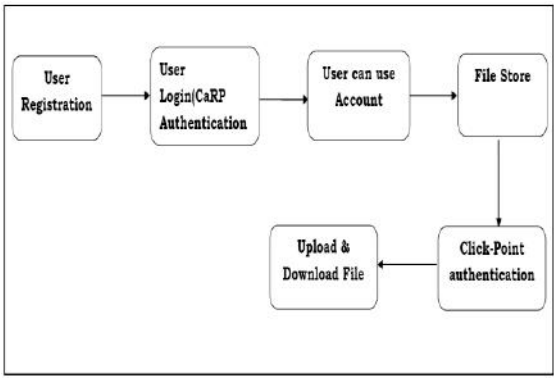

Fig6. Architecture Diagram

IV. METHODOLOGY

Proposed system mainly consists of two authentication step. 1. Is in the time of Registration and 2. At the time of uploading or downloading file (or an accessing account). In proposed system first user will create account by entering details such as Username, Textual password, E-mail Id, Contact No.etc. Then in next window system use CaRP authentication Scheme. In that system generate set of images for the user. & ask user to select a correct graphical captcha. After selecting graphical captcha if this captcha is correct user can enter into the account otherwise not. In next while accessing account if user want to set the security for his/her files. Then he can set using the next authentication process. In that system will ask user that do you want security? If answer is yes then an image is presented to user and user has to select click-point as the password. And next time if the click-point is correct then & then he can upload & download files from the account.

V. IMPLEMENTATION

ALGORITHM OF PROPOSED SYSTEM:-

Step 1. Start
Step 2. User can register by username, password, Email-id Contact no.
Step 3. Computer generate graphical captcha for registered user
Step 4. User will select Captcha
Step 5. Authentication of User: User will enter his details Which he entered at the time of registration
Step 6. Computer program ask the user to choose the correct graphical Captcha
Step 7. User selects the graphical captch
Step 8. Is selected image captcha is correct?
1. If Yes
Step 9. User can access his account.
Step I: User can Upload & Download file From File Storage
Step II: If User Want Security for Individual File.
Login step -User click on point of image & Set the Security for individual file
2. if NO
Step 10. User can login again
Step 11. Stop.

VI. RESULT

In testing session, 15 completed with no mistakes in proposed CaRP method based on File store while the others, to a greater or less extent, made some incorrect submissions. This captcha method gain best human success rate 92%. 75% of test participant say that CARP is easy to use. Or also no complicated operation on password. Or easy to remember than other text or graphical, captcha passwords

High Human success rate shows that less chances of requiring multiple attempts of captcha to access account. This comparison shows that proposed CaRP (Captcha as a graphical password) system is user friendly, easy to use, language independent.

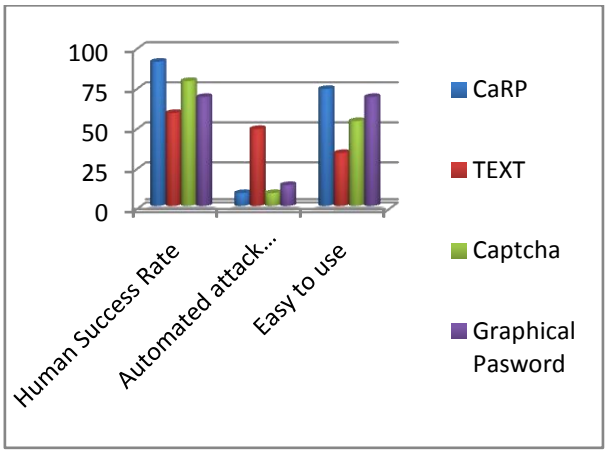

Fig 1: Captcha Password

Fig 2: File Upload

DOI 10.17148/IJARCCE.2016.5104

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

Fig 3: Security for File

VI. CONCLUSION

Alternative to textual password is graphical password. In this paper, a survey over existing graphical password protection techniques and Captcha techniques has been presented. A review over the advantages and limitation of the password protection techniques is also presented. The goal of this research is study the existing graphical password techniques and captcha techniques & develop a new improved graphical password technique combined with a CaRP. CaRP introduces new primitive of graphical password. Also password of system will easy to remember and highly secure. CaRP is built on Captcha technology. which take random images at all time.

This survey on existing techniques will help in developing more efficient & secure graphical password based authentication schemes to provide the better security to the user data. The proposed system consists of text password, CaRP authentication scheme and individual graphical password technique. This technique is highly secure. It provides protection from various attacks on the password scheme.

ACKNOWLEDGEMENT

I would like to express my profound gratitude and deep regard to my Project Guide **Prof. K.N. Shedge,** for his exemplary counsel, valuable feedback and constant fillip throughout the duration of the project. His suggestions were of immense help throughout my project work. Working under him was an extremely knowledgeable experience for me.

REFERENCES

[1] Shraddha S.Banne, Prof. K.N.Shedge,"A Review Graphical password Based Authentication Scheme",International Journal of Science & Research(IJSR), Volume 3 Issue 10, October 2014.

[2] Shraddha S.Banne, Prof. K.N.Shedge," A Novel Graphical Password Based Authentication Method Using CAPTCHA", International Journal of Informative & Futuristic Research (IJIFR), Volume 2 Issue 11 July 2015

[3] Bin B. Zhu, Je Yan, Guanbo Bao, Maowei Yang, and Ning Xu,``Captcha as a Graphical Passwords A New Security Primitive Based on Hard AI Problems",IEEE Trans, Vol. 9, No. 6, pp 891-904, June 2014.

[4] S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot, ``Inuencing users towards better passwords: Persuasive cued click-points", in Proc. HCI, British Computer Society, Liverpool, U.K., pp 121-130, 2008.

[5] S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot, ``User interface design affects security: Patterns in click-based graphical passwords", Int. J. Inf. Security, vol. 8, no. 6, pp. 387-398, 2009.

[6] G. Blonder, Graphical Passwords, U.S. Patent 5559961, 1996.

[7] Xiaoyuan Suo, Ying Zhu, G. Scott. Owen, "Graphical Passwords: A Survey", Department of Computer Science Georgia State University.

[8] A. Dirik, N. Memon, and J.-C. Birget, "Modeling User choice in the Pass-Points graphical password scheme", in 3rd Symp. Usable Privacy and Security(SOUPS), Pittsburgh, PA, pp. 20-28, 2007.

[9] Chippy. T and R. Nagendran, Defences Against Large Scale Online Password Guessing Attacks By Using Persuasive Click Points, International Journal of Communications and Engineering, Volume 03 No.3, Issue: 01 March2012 .

[10] D. Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical pass-word schemes", in Proc. 13th USENIX Security Symp., San Diego, CA, pp. 151-164, 2004.

[11] Robert Biddle, Sonia Chiasson and P.C.van Oorschot. Graphical Passwords: Learning from the First Twelve Year. School of Computer Science, Carleton University, Jan 4, 2012.

[12] Liming Wang, Xiuling Chang, Zhongjie Ren, Haichang Gao, Xiyang Liu, Uwe Aickelin, "Against Spyware Using CAPTCHA in Graphical Password Scheme"

[13] Luis von Ahn, Manuel Blum, Nicholas J. Hopper, and John Langford, "CAPTCHA: Using Hard AI Problems For Security"

[14] S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy, N. Memon, ``PassPoints: Design and longitudinal evaluation of a graphical password system", International J. of Human-Computer Studies (Special Issue on HCI Research in Privacy and Security), 63 (2005) 102-127.

[15] Xiaoyuan, S., Z. Ying, et al. (2005). "Graphical passwords: a survey", Computer Security Applications Conference, 21st Annual.

[16] H. Gao, X. Liu, S.Wang, and R. Dai, "A new graphical password scheme against spyware by using CAPTCHA," in Proc. Symp. Usable Privacy Security, 2009, pp. 760–767.

[17] M. Alsaleh, M. Mannan, and P. C. van Oorschot, "Revisiting defenses against large-scale online password guessing attacks," IEEE Trans. Dependable Secure Comput., vol. 9, no. 1, pp. 128–141, Jan./Feb. 2012.