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. 3, Issue 9, September 2015

A Survey on Login Authentication System using Captcha as Graphical Passwords Techniques

Tejaswi S. Pawar[1], Rupali G. Sawant[2], Pramod S. Bothe [3], Sharmila A.Chopade[4]

B.E Student, Dept. of Computer Engineering, Dr.D.Y.Patil Institute of Engineering & Technology, Talegaon, Pune University, India[1, 2, 3]

Professor, Dept. of Computer Engineering, Dr.D.Y.Patil Institute of Engineering & Technology, Talegaon, Pune University, India[4]

ABSTRACT: Now a day, vulnerability is a major issue in computer security. Computer and Information security is supported by passwords. The password is used in Authentication process. The traditional authentication method uses text-based password which is also called alphanumeric password, but it has some drawbacks, so graphical password scheme is developed to overcome vulnerabilities of this traditional password scheme. The graphical is easier to remember and difficult to guess than text. But major drawback of graphical scheme is it is vulnerable to shoulder surfing attack and also sometimes to spyware attack. So another technique to graphical password a Captcha technique is developed. The main advantage of Captcha is that it can't be identified by bots. From the unwanted bots, Captcha gives protection but with this protection there are some limitations of Captcha and to overcome the limitations a new technique is developed which is CaRP (Captcha as Graphical Passwords). CaRP is combination of captcha and graphical password. It is clicking an event which is performed at various points on image in sequence to get new password. In this paper, we are going to survey existing CaRP techniques.

KEYWORDS: Graphical password, password, CaRP, Captcha, security primitive.

I. INTRODUCTION

Now a day, security is the most important factor in an information security program for authentication. The text-based and Graphical passwords are used in the authentication process, but the best alternative for text-based password is a graphical password. The graphical password can reduce the burden of human memory as human mind to remember graphics and images better. Graphical passwords are vulnerable to shoulder surfing and spyware attacks, password, registration and log-in process needs more storage space. So the best alternative to graphical scheme is CAPTCHA (Completely Automated Public Turing-test to tell Computers and Humans Apart). Captcha is a type of challenge-response is generated by a human not by a computer. It is a program that generates and grade tests that are human solvable, but current computer programs do not have the ability to solve them. A new security primitive namely, a novel family of graphical password systems builds Captcha technology that is called a Captcha as graphical Passwords (CaRP). CaRP is click based graphical passwords, in which an order of clicks on an image is used to get a password. Contrasting other click-based graphical passwords, images used in CaRP are Captcha challenges and a new CaRP image is generated for every login attempt.

The application where captcha as a graphical password include: i) Captcha as graphical password can be used in many internet applications specifically in the e-backing application, where users had to solve the different captcha at each login. ii) By using the CaRP the entry of spam emails are reduced. Here the email service provider uses the captcha as a graphical password to log into the system so the spam bots cannot log into the system because they are not able to solve the captcha.

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. 3, Issue 9, September 2015

II. RELATED WORK

A. *Graphical Password Techniques*

Graphical password techniques are developed to overcome the limitations of text-based passwords. Graphical passwords consist of recognizing the images or sometimes to recognize the image and click the particular points or area on the image rather than typing the characters like text-based password. In this way, the problems that arise from the text-based passwords are reduced. Graphical password techniques are categorized as follows: i) Recognition Based scheme ii) Recall Based scheme iii) Cued Recall Based scheme.

A *recognition-based* scheme has to select the certain number of images from a set of random images in an order as a password, and for authenticating the user has to identify (recognize) those images in a same order. There are three schemes under this system: i) Method 1: Dhamija and Perrig proposed a graphical authentication technique depends on to the hash visualization method. In their system, the user is asked to select a certain number of images from a set of random images generated by a program. The user will be required to identify the preselected images in order to be authenticated. ii) Method 2: Sobrado and Birget developed a graphical password scheme work with the surfing shoulder problem. In the first technique, the system will show a number of passes-objects. A user needs to recognize pass-objects and click inside the outside hull formed by all the pass-objects for authentication. iii) Method 3: "Pass face" Real User Corporation developed these techniques. The idea is as follows: The user will be asked to choose four images of human facing as their future password security. In authentication stage, the user sees a grid of nine faces, consisting of one face previous chosen by the user & eight decoy faces. The user recognizes and clicks anywhere on the known face. This procedure is repeated for several rounds.

A *recall-based* scheme requires a user to reproduce something that he created or selected earlier during the registration stage. Three techniques are: i) Method 1: "Draw-A-Secret (DAS) Scheme" Here the user will draw a simple picture on 2D grid. The coordinates of a grid are occupied by the picture are stored in the order of the drawing. During authentication, the user will be told to re-draw the picture. If the drawing touches the same sequence, then the user is authenticated. ii) Method 2: "Signature Scheme" Here authentication is conducted by having the user drawing their signature using the mouse. iii) Method 3: "Pass-point Scheme" Here the user will click on any place on an image to create a password. A tolerance around each chosen pixel is calculated. In order to be authenticated, the user must click within the tolerances in the correct sequence [3].

In a *Cued-recall* based scheme Pass Points [3] is a click based cued recall scheme where a user requires clicking a sequence of points anywhere on an image to create a password. At the time of authentication user require to re-clicking the same sequence. Cued Click Points (CCP) [5] is similar to PassPoints but uses one image per click, with the next image selected by a deterministic function. Persuasive Cued Click Points (PCCP) extend CCP where user has to select a point inside a randomly positioned viewport.

Graphical password has some limitations: i) Password registration and log-in process take too long. ii) Require more storage space than text-based passwords.

B. *Captcha*

Completely Automated Public Turing Test to tell Computers and Human Apart [1] (Captcha) finds the difference in humans and bots in solving the hard AI problems. It is a test to check user is Human and not a computer device. Captcha has two types: Text Captcha which is recognition of non-character objects and Image Recognition Captcha relies on recognition of images.

i) *Text Captcha:* PayPal and Microsoft Captcha are both relied on background noise & random character strings to resist to automated attacks. The Captcha used by Google, Yahoo! all share similar properties, such as a lack of background noise of distortion for a character or word images and extreme crowding for an adjacent character. Random Captcha images are captured humanly reliably by site in the form of pixel, marginal probabilities and site by site covariance. EZ-Gimpy uses word images which employ character distortion and clutter. Personal print uses a low quality picture by degrading parameters to thicken, crowd, fragment and add noise to character images. These Captcha are shown in Figure.1

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. 3, Issue 9, September 2015

Figure 1.Captcha Images

ii*) Image Recognition Captcha*: Captcha consist of combination of images [6]. The user has to recognize the images given to him to solving the given puzzle problem. As shown in Figure.2 user has to select the cat images as the password characters.

Figure 2.Image based captcha.

Image recognition has some limitations: i) Image recognition sometimes very difficult to read. ii) Image recognition captcha not compatible with users with disabilities iii) Image recognition is time-consuming to decipher. iv) It is greatly enhance Artificial Intelligence.

C. *Converting Captcha to CaRP*

Any visual Captcha scheme which is relying on recognizing two or more predefined types of objects can be converted to a CaRP. All the text Captcha schemes and IRCs meet this requirement. Those IRCs that depends on recognizing a single predefined type of objects can also be converted to CaRPs by adding more types of objects. Captcha scheme that is converted to a CaRP scheme typically requires a case by case study, in order to ensure both Security plus Usability. We will present several CaRPs built on top of image-recognition and text Captcha schemes. Some IRCs depends on identifying objects whose types are not predefined. A typical example is Cortcha which depends on context-based object recognition where the object to be recognized can be of any type. These IRCs cannot be converted into CaRP as a set of pre-defined object types is required for constructing a password.

D. *Captcha as Graphical Password (CaRP):* An Overview

CaRP has a new image is generated for every login attempt even for the same user. Alphabet which is used in CaRP of visual objects (E.g. Alphanumerical characters, similar animals, etc.) to generate a CaRP image, which is also a Captcha challenge.

The main difference between Captcha images and CaRP images is all the visual objects in the alphabet should appear in a CaRP image to allow a user to input any password security but not necessarily in a Captcha image. Some of the Captcha techniques can be converted to CaRP schemes. CaRP schemes are click based graphical passwords. As per the memory tasks in memorizing and entering a password, CaRP schemes can be classified into two categories:

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. 3, Issue 9, September 2015

recognition-based and a new category, recognition-recall, which requires recognizing an image and using the recognized objects as cues to enter a password. Recognition-recall combines the tasks of both cued-recall and recognition, and also retains both the cued-recall advantage of a large password space [1] and the recognition-based advantage of being easy for human memory.

A Recognition-based CaRP technique used password is in a series of visual objects alphabet. Per view for the traditional recognition based on graphical password security, recognition based CaRP seems to have access to an infinite number of different visual objects. We present two recognitions based CaRP techniques and a variation next.

i) *ClickText:*

ClickText having a recognition-based CaRP scheme. CaRP techniques use captcha as its underlying the principle. Alphabet set of ClickText comprises alphanumeric characters. A ClickText password is a series of characters in the alphabet .e.g. ρ= "DE@F2SK78", which is a similar to the text password. A ClickText image is totally different from usual captcha as all the characters of alphabet set are to be included in the CaRP image. The underlying captcha engine generates such CaRP image. When image is generated, then each character's location in the image is recorded which would be used in the authentication. Characters can be put randomly in 2D space in these images which changes from text CAPTCHA where characters are typically ordered from left to right and in order for users type them sequentially Figure.3 shows a ClickText image with an alphabet of 33 characters [1].

Figure 3.ClickText CaRP Scheme [1]

ii) ClickAnimal:

ClickAnimal is a recognition-based CaRP technique built on top of Captcha Zoo. It has an alphabet of similar animals such as dog, pig, like that. The password in this technique is a sequence of animal names like ρ = "Cat, Dog, Turkey," Most of the models are created or built for each and every animal. The captcha generation activity where in 3D models are used to get 2D models by applying different types of views, colors, and optionally distortions are used for generating the Click Animal image. The final resulting 2D animals are then arranged on cluttered backgrounds like grassland. The number of similar animals is less than the number of available characters. Sometime some animals may be overlapped by some other animals in the image but its core parts are not overlapped in order for humans to identify each of them. Click Animal has been smaller alphabet, and a smaller password space, than ClickText. Figure.4 shows a ClickAnimal image with an alphabet of 10 animals. [1]

Figure 4.Click Animal CaRP Scheme [1]

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. 3, Issue 9, September 2015

iii) *Animal Grid:*

Human guessing attacks are sufficiently large effective password space should be present for CaRP techniques. If the Click animal scheme can be mixed with grid based graphical passwords, then its password space can be increased. In such authentication process, a Click Animal image is displayed first the grid can be made depending on the size of the selected animal. After an animal is selected, image of n×n grid display, with the grid-cell size equalling the bounding some rectangle of the selected animal. Each grid-cell is labelled to help identify users. Fig. 5 shows a grid 6×6 when the red turkey in the left image of Figure.5 was selected. It has been advantageous that a correct animal should be clicked in order for the clicked grid-cell on the follow-up grid to be correct. If we clicked on wrong animal is, then follow-up grid is wrong. A click on the correctly labelled grid cell of the wrong grid would be displaying a wrong grid-cell on the authentication server side when the correct grid is used [1].

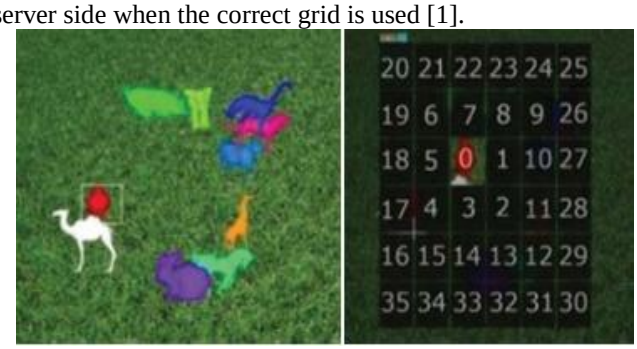

Figure 5.AClick Animal Image (Left) and 6*6 Grid (Right)
Determine by Red Turkey's Bounding Rectangle [1]

A recognition-recall CaRP, Password is a sequence of some invariant points of objects. An invariant point of an object is the point that has a fixed relative position in different incarnations of the object and it can be uniquely identified by users or humans no matter how the object appears in CaRP images.

i) *TextPoints:*

Characters are contained invariant points. Figure.6 shows some invariant points of letter “A”, which offers a strong cue to memorize and locate its invariant points.A point is to be an internal point of an object if its distance to the nearest boundary of the object exceeds a threshold. A number of sets of internal invariant points of some characters are selected to form a set of clickable points for Text Points. The internal ensure that a clickable point is unlikely occluded by a nearest character and that its tolerance area unlikely overlap with any other tolerance region of a neighboring character’s clickable points on which the image generated by the underlying Captcha engines. In a determining clickable point, the distance between any one pair of clickable points in a character must exceed a threshold so that they are perceptually separable and their tolerance regions do not overlap on CaRP images.

Figure 6.Some invariant points (red crosses) of "A"[1].

ii) TextPoints4CR:

CaRP scheme presented up to now, the coordinates of user-clicked some points are sent directly to the authentication server during its authentication. For more complex rules, say a challenges and response authentication

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. 3, Issue 9, September 2015

protocol, the response is sent to the authentication server instead. Text Points sometime its can be modified to fit challenge response authentication. This variation is called as TextPoints for Challenge-response or also TextPoints4CR.

CaRP have some benefits given below: i) CaRP to offer protection against Automatic Online Guessing Attacks on passwords. ii) It offers security against Human Guessing Attacks. iii) It offers protection against Shoulder Surfing Attack. iv) It offers security against spam emails sent from a Web email service. v) It offers security against spam emails sent from a Web email service.

CaRP has some limitation: i) CaRP scheme can be vulnerable to phishing attack because user-clicked points are sent to the authentication server. ii) CaRP is vulnerable if both the image and user-clicked points can be captured. (If client is compromised)

III. CONCLUSION AND FUTURE WORK

This paper presents a survey on various techniques such as textual password, graphical password, Captcha password and CaRP technique. CaRP is a combination of both a CAPTCHA and a graphical password scheme. CaRP schemes are classified as Recognition-Based CaRP and Recognition-Recall CaRP. We have discussed Recognition- Based CaRP which include ClickText, ClickAnimal and AnimalGrid techniques in this paper. Current graphical password techniques are an alternative to text password, but are still not fully secure. As a framework, CaRP does not rely on any specific CAPTCHA scheme, but CAPTCHA scheme is broken, then a new and more secure scheme appears is a CaRP scheme. Due to reasonable security and practical applications, CaRP has best potential for refinements. The usability of CaRP can be further improved by using images of different layers of difficulty based on the login history of machining.

ACKNOWLEDGEMENT

The authors would like to thank the publishers, researchers for making their resources available and teachers for their guidance. We also thank the college authority for providing the required infrastructure support. Finally, we would like to extend heartfelt gratitude to friends, family members.

REFERENCES

1. 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, June 2014.
2. R. Biddle, S. Chiasson, and P. C. van Oorschot, "*Graphical passwords: Learning from the first twelve years*," ACM Comput. Surveys, vol. 44, no.4, 2012
3. S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "*PassPoints: Design and longitudinal evaluation of a graphical password system*," Int. J. HCI, vol. 63, pp. 102–127, Jul. 2005.
4. L. von Ahn, M. Blum, N. J. Hopper, and J. Langford, "*CAPTCHA: Using hard AI problems for security*," in Proc. Eurocrypt, 2003,
5. S. Chiasson, P. C. van Oorschot, and R. Biddle, *"Graphical password authentication using cued click points*," in Proc. ESORICS, 2007,
6. P. C. van Oorschot and J. Thorpe, "*On predictive models and user drawn graphical passwords*," ACM Trans. Inf. Syst. Security, vol. 10, no. 4, pp. 1–33, 2008..
7. 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.
8. 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.
9. L. Wang, X. Chang, Z. Ren, H. Gao, X. Liu, and U. Aickelin, "*Against spyware using CAPTCHA in graphical password scheme*," in Proc. IEEE Int. Conf. Adv. Inf. Netw. Appl., Jun. 2010, pp. 1–9.
10. S. Li, S. A. H. Shah, M. A. U. Khan, S. A. Khayam, A.-R. Sadeghi, and R. Schmitz, "*Breaking e-banking CAPTCHAs*," in Proc. ACSAC, 2010, pp. 1–10.

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. 3, Issue 9, September 2015

BIOGRAPHY

Tejaswi S. Pawar is a B.E student in the Computer Engineering Department, Dr. D. Y. Patil Institute of Engineering and Technology, Ambi, Talegoan, Pune, Savitribai Phule Pune University.

Rupali G. Sawant is a B.E student in the Computer Engineering Department, Dr. D. Y. Patil Institute of Engineering and Technology, Ambi, Talegoan, Pune, Savitribai Phule Pune University.

Pramod S. Bothe is a B.E student in the Computer Engineering Department, Dr. D. Y. Patil Institute of Engineering and Technology, Ambi, Talegoan, Pune, Savitribai Phule Pune University.

Sharmila A. Chopade received Master Engineering Degree from Pune University and having 7 years of teaching experience. She has published 11 international papers and one book on data structure.