Contemporary Approach for Graphical Password using CAPTCHA

Bhagyashri Sarda, Bhagyashri Kapre

Abstract— Cyber security is an important issue to implement. Different types of user authentication methods are used to achieve this goal. It helps to avoid misuse or illegal use of highly sensitive and confidential data. Text and graphical passwords are mainly used for authentication functioning. But due to various pitfalls, they are erroneous for data security. Text passwords are un assured for reasons and graphical are tight secured in comparison but are sensitive to shoulder surfing attacks. Hence by using graphical password system and CAPTCHA technology a new security primitive is proposed. We call it as CAPTCHA as gRaphical Password (CaRP). CaRP is a combination of both a CAPTCHA and a graphical password scheme. In this paper we conduct a encyclopedic analysis of existing CaRP techniques namely ClickText, ClickAnimal and AnimalGrid. We discuss the advantages and disadvantages of each method and point out research direction in this area. We also try to answer "Are CaRP as secured as graphical passwords and text based passwords?" and "Is CaRP protective to relay attack?

Index Terms— Captcha, CaRP, dictionary attack, password, graphical password.

I. INTRODUCTION

In security to provide secure access to object the primary task is cryptographic primitives based on hard mathematical problem which are very unmanageable in computation.

An exciting new paradigm which is based on hard AI (Artificial Intelligence) proposed in [7]. In this a new primitive invented which is known as a Captcha. This is standard Internet security technique which protects online services from being misused by bots.

As compare to first techniques that is cryptography the second technique that is Captcha has achieved limited success. The demanding and impressive open problem is to create a new security based on hard AI problem. In this paper, we introduce a contemporary family of graphical password systems which combine Captcha technology, this technology known as CaRP (Captcha as gRaphical Passwords. In this method we use click-based graphical password with Captcha challenges unlike other click based graphical images. To derive our password we need to click on Captcha images sequentially. CaRP hit security against online dictionary attack on password. This hazard is universal and considered as one of the top cyber security opportunity [3]. CaRP also provide security across relay attack where Captcha test are deliver to humans to figure out. To create a new account on Facebook Koobface was a relay attack to ignore Facebook Captcha.

Revised Version Manuscript Received on July 04, 2016.

Ms. Bhagyashri Sarda, Department of Computer Science and Engineering, MGM's College of Engineering, Nanded, India.

Prof. Bhagyashri Kapre, Department of Computer Science and Engineering, MGM's College of Engineering, Nanded, India.

CaRP feel necessity for crack the Captcha in every login. CaRP carry different type of application for example,

1. Touch screen devices have inconveniency on typing passwords for secure Internet application such as online shopping, e-banking etc. in this situation the CaRP offer easy and secure access to bank account or online shopping.
2. By using CaRP in email application the spam bot was unable to log into email account even if bot knows the userid and password correctly of any account. The CaRP hike the spammer's performance charge.

II. BACKGROUND AND RELATED WORK

A. Graphical Password

A huge number of graphical password patterns are available. Graphical passwords are mainly divided into three categories: recognition, recall, and cued recall. They can be categorized on basis of remembering and entering passwords. Each type can be briefly discuss here more information can be found in [2].

Recognition based scheme have a password to remind the portfolio of images and at the login time decoys the same images. The broadly used recognition based scheme is Passfaces in this scheme first user have to select a set of human faces. During authorization a group of human's faces is presented. Number of round should be taken by using different set of images. For correct authorization each round is completed without an error.

Recall based scheme also known as drawmetric scheme in this particular scheme user draw their password either on grid or blank canvas and during authorizations they recall and reproduce the password. In this scheme at the time of authorization the password can be recall without any clue so the password is hard to memorize. The first technique which is under recall based scheme is DAS (Draw-A-Secrete). In DAS user draw their password on 2-D grid using mouse. Passwords compulsory draw by continuous without pen-up.

Cued recall based scheme having technique to give a clue to the user as compare to pure recall based system so that's why this technique reduce the load of memory from the users. The official method under this graphical password is known as PassPoints. In PassPoints the user select the password by clicking on image which is appear at the time of signup in sequence. During authorization process the user select the same point accurately in sequence by using mouse.

B. Captcha

A **CAPTCHA** "Completely Automated Public Turing test to tell Computers and Humans Apart" is a type of challenge-response test used in computing to determine

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

whether or not the user is human.

The Captcha is categorized into two types: text Captcha and Image-Recognition Captcha. The first depends upon character recognition even though the next depends on recognition of non-character materials. Security of text Captchas continues to be broadly studied. Captcha is now almost a standard security mechanism for addressing undesirable or malicious Internet bot programs and major web sites such as Google, Yahoo and Microsoft all have their own Captchas.

C. *Captcha in Authentication*

To use Captchas in authentication a new protocol which is known as Captcha based Password Authentication Protocol (CbPA) is proposed in [4]. The CbPA used to overcome online dictionary attack which is major security attack now days. In CbPA protocol user solves the Captcha challenge by inputting valid pair of userid and password unless a valid browser cookie is received. This protocol has facility to give Captcha challenge to invalid pair of id and passwords before being accesses is rejected.

The improved version of CbPA protocol is proposed in [5] storing cookies completely on user-trusted machines and applying a Captcha challenge only the quantity of unsuccessful login attempts for the account has pass a edge.

A new improvement is added in [6] by applying slight threshold for unsuccessful login makes an attempt from unknown machines however an enlarge threshold for unsuccessful makes an attempt from known machines with a previous successful login inside a given timeframe.

III. Overview of Captcha as Graphical Password

The CaRP (Captcha as gRaphical Password) schema is proposed in [1]. The fusion of Captcha and graphical passwords are used to authenticate users for trusted accesses in any system. In CaRP to generate an image during signup or login use an alphabet of visible entity like alphanumerical character, animals which are same. The advantage of CaRP is user can use any visible entity as a password by clicking on that but in Captcha these facilities is not provided. The CaRP can have two types: *recognition* and *recognition-recall*. The division of CaRP is done on the basis of memory task that is memorizing and entering a password. Second technique is fusion of recognition and cue recall technique. This works by recognizing an image and using the recognized objects as cues to enter a password. It holds the advantage of both technique recognition advantage of being easy for human memory and the cued-recall advantage of a big password space [1].

Fig. 1 shows the flowchart of basic authentication in CaRP technique. The basic CaRP in authentication work by using following steps:

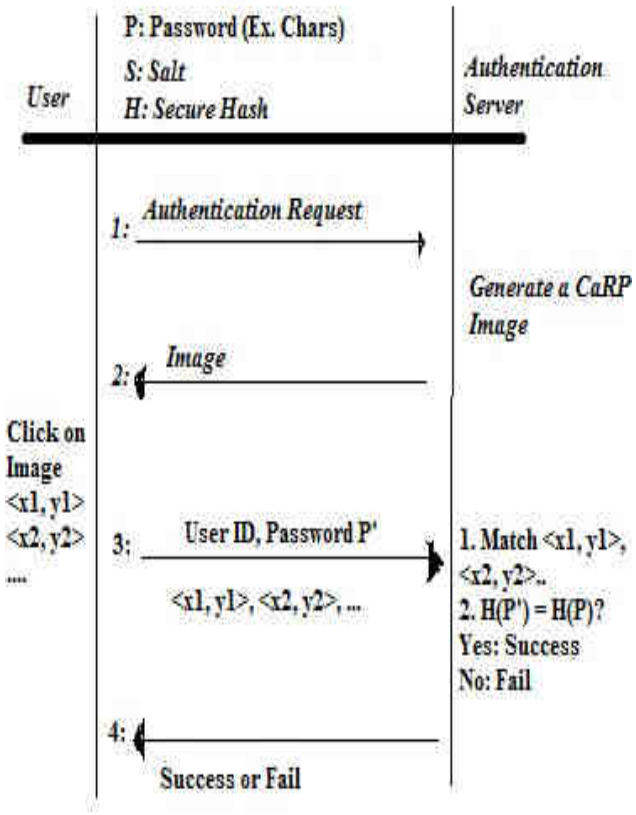

Fig. 1 Flowchart of basic CaRP proposed architecture

Step1: for authentication purpose user give the ID i.e. User ID and send it to Authentication Server (AS).
Step2: AS stores the hash value of password for each and every userid.
Step3: Upon receiving login request the CaRP image is generated
Step4: User click the password
Step5: Co-ordinates of CaRP images which is click by user as a password are sent to the AS
Step6: AS maps the co-ordinate and compare it co-ordinate of that user id which is stored in database
Step7: AS calculate the hash value of password
Step8: Compare it with for that particular userid which is stored in database
Step9: The login is successful if only if the hash values of password and user click Co-ordinates are match otherwise fail.

IV. Types of Captcha as Graphical Password

A. *ClickText*

The broadly used CaRP is recognition based is Click Text CaRP. It uses the basic principle of text based Captcha. In Click Text CaRP techniques it uses 33 alphabets. The confusing character like 0 or O is excluded. The Click Text CaRP has all A-Z alphabets excluding O and have some special case character like #, @ etc. The Fig. 2 shows the technique of Click Text.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

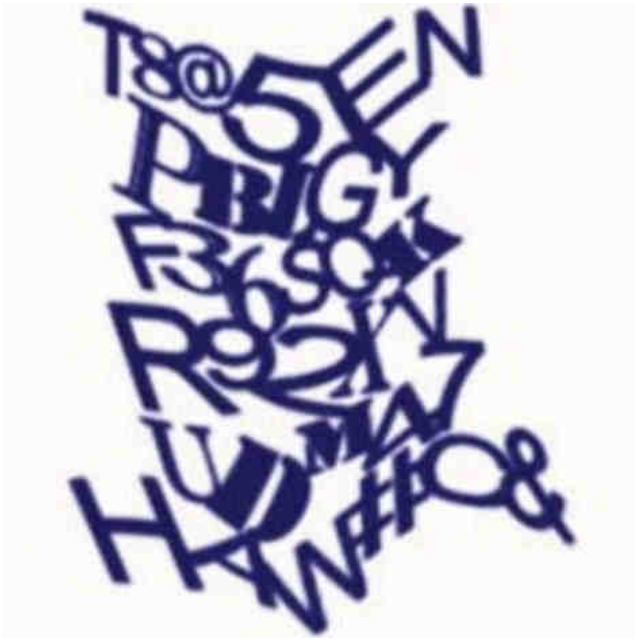

Fig. 2 Click Text CaRP Technique [1]

To set a password in Click Text technique user have to choose a password same as our text password but here by clicking on the alphabet. Click Text CaRP having some difference as compare to text based Captcha in Click Text all alphabet is presented at same time on image but in text based Captcha some of the alphabet is included at same time. One more difference in Click Text and text based Captcha is unlike text based Captcha the Click Text image arrange all 33 character on 2-D space randomly but in text based Captcha all character are placed compulsory left to right position to type them sequentially. In Click Text each character location can be recorded so that at the time of authentication when user click password the recorded value is matched by their location.

B. ClickAnimal

Click Animal is second CaRP technique build on top of the Captcha zoo model [9]. This uses password as sequence of click on animals. In this technique a Captcha zoo model is used [9]. In Captcha zoo model a background image is taken as grass and on this background a 3-D animal is placed randomly on any angel, shape, or any rotation.

Click Animal has a smaller password space as compare to Click Text.

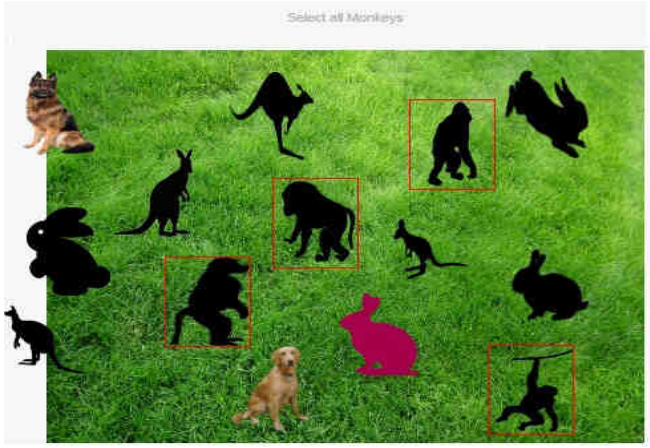

Fig. 3 Click Animal CaRP Technique [9]

C. AnimalGrid

Fig. 4 6 × 6 grid

The Animal Grid is also a recognition based CaRP. The Fig. 4 shows the 6*6 grid image. A user can select zero to multiple grid-cells matching her/his password. The coordinates of the clicked point are recorded.

V. SECURITY ANALYSIS

A. The security of primary Captcha

According to [8], the complexity of object segmentation, *C*, is exponentially dependent of the number *M* of objects contained in a challenge, and polynomially dependent of the size *N* of the Captcha alphabet:

$$C = \alpha^{M} P(N)$$

Where $\alpha > 1$ is a parameter, and *P()* is a polynomial function. A Captcha challenge typically contains 6 to 10 characters, whereas a CaRP image typically contains 30 or more characters. The complexity to break a Click-Text image is about $\alpha^{30} P(N)/(\alpha^{10} P(N)) = \alpha^{20}$ times the complexity to break a Captcha challenge generated by its primary Captcha scheme. Therefore ClickText is much harder to break than its primary Captcha scheme.

CaRP doesn't depend on any particular Captcha system. If one Captcha system gets broken, a new and more robust Captcha system may appear and be used to construct a new CaRP scheme.

B. Automatic Online Guessing Attacks

In this type of attacks a test and mistake process is performed automatically whereas dictionary can be model by hand. Captcha has the following abstract quality:
clickable points on one image are computationally-independent of clickable points on another image.

C. Human Guessing Attacks

Test and mistake process is used but here human are used to enter a password. As compare to computer humans are very slow to guessing the passwords using test and mistake process. For Click-Text with 8 characters password space is 33^{8} for Click-Text having 33 characters in image. For

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

click animal having 10 animal to click is having password space 10^8. If we assume that 1000 people work 8 hours per day without any break in human guessing attacks and that each employee take 30 seconds to finish one trial. It would take them on average $0.5*33^8*30$ which is approximately 2007 years to break a Click Text Captcha, $0.5*10^8*30$ for Click Animal password.

D. Relay Attacks

Relay attacks may be performed in different ways. Captcha challenges can be relayed to a high-volume Website hacked or controlled by opponents to have human surfers solve the challenges in order to continue surfing the Website. Relayed to sweatshops where humans are hired to solve Captcha challenges for small payments. The images used in CaRP are very different from those used to solve a Captcha challenge. This significant change makes it strong for a person to wrongly assistance trial a password guess by trying to solve a Captcha challenge. Therefore it would be unlikely to get a large number of unaware people to mount human guessing attacks on CaRP.

If sweatshops are payment to fund human guessing attack, we can make a approximate guess of the cost. We adopt that the value to click one password on a CaRP image is the same as solving a Captcha challenge. Using the lowest retail price, $1, reported [10] to work out 1000 Captcha challenges, the approximate value to break a 26-bit password is $0.5*2^{26}*1/1000$, or approximately 33.6 US dollar.

E. Shoulder Surfing Attacks

Shoulder-surfing attacks are a danger when graphical passwords are entered in a public place such as bank ATM machines. CaRP is not strong to shoulder-surfing attacks by itself. However, combined with the following dual-view technology, CaRP can prevent shoulder-surfing attacks. Commonly-used LCDs show different brightness and color depending on the viewing angle, the dual-view technology can use software alone to display two images on a LCD screen simultaneously, one public image viewable at most view-angles, and the other private image viewable only at a specific view-angle [11]. When a CaRP image is displayed as the "private" image by the dual-view system, a shoulder-surfing attacker can capture user clicked points on the screen, but cannot capture the "private" CaRP image that only the user can see. However, the acquire user-clicked points are useless for another login try, where a new, computationally-independent image will be used and thus the captive points will not represent the correct password on the new image anymore.

VI. CONCLUSION

We have forth put CaRP, a new safety primitive depending on not yet solved hard AI problems. CaRP is both a Captcha and a graphical password blueprint. The method of CaRP adds a new family of graphical passwords, which approves a new character to counter online guessing attacks. CaRP techniques are categorized as Recognition-Based CaRP and Recognition-Recall CaRP. CaRP is also resistant to Captcha relay attack, and if we combine with dual-view technologies shoulder-surfing attacks. CaRP can also help to reduce spam emails sent from a web mail service. More efforts and time will required in CaRP as compare to simple Captcha.

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.HP Tipping Point
3. HP TippingPoint DVLabs, Vienna, Austria. (2010). Top Cyber Security Risks Report, SANS Institute and Qualys Research Labs [Online].
4. B. Pinkas and T. Sander, "Securing passwords against dictionary attacks," in Proc. ACM CCS, 2002, pp. 161–170.
5. P. C. van Oorschot and S. Stubblebine, "On countering online dictionary attacks with login histories and humans-in-the-loop," ACM Trans. Inf. Syst. Security, vol. 9, no. 3, pp. 235–258, 2006.
6. 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.
7. L. von Ahn, M. Blum, N. J. Hopper, and J. Langford, "CAPTCHA: Using hard AI problems for security," in Proc. Eurocrypt, 2003, pp. 294–311.
8. K. Chellapilla, K. Larson, P. Simard, and M. Czerwinski, "Building segmentation based human-friendly human interaction proofs," in Proc. 2nd Int. Workshop Human Interaction Proofs, 2005, pp. 1–10.
9. R. Lin, S.-Y. Huang, G. B. Bell, and Y.-K. Lee, "A new CAPTCHA interface design for mobile devices," in Proc. 12th Austral. User Inter. Conf., 2011, pp. 3–8.
10. M. Motoyama, K. Levchenko, C. Kanich, D. McCoy, G. M. Voelker, and S. Savage, "Re: CAPTCHAs—Understanding CAPTCHA-Solving Services in an Economic Context," in Proc. USENIX Security, 2010, pp. 435–452.
11. S. Kim, X. Cao, H. Zhang, and D. Tan, "Enabling concurrent dual views on common LCD screens," in Proc. ACM Annu. Conf. Human Factors Comput. Syst., 2012, pp. 2175–2184.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.