ISSN 2395-1621

Captcha as Graphical Passwords and Authentication for High Security in Cloud

[#1]Miss.Kakade Priyanka Suresh, [#2]Miss.Jaykar Sonali Bhaskar
[#3]Miss.Lavand Dipali Shamrao,[#4]Mr.Randive Digvijay

[1]priyanka.kakade8@gmail.com
[2]sonalijaykar1990@gmail.com
[3]deepalawand34@gmail.com
[4]digvijayrandive11@gmail.com

[#1234]Dept. of Computer Engineering H.S.B.P.V.T. COE, Kashti
Tal:-Shrigonda, Dist-Ahmednagar Maharashtra, India.

ABSTRACT

In this paper we providing new security primitive based on hard AI problem. In which we are using Graphical based password for providing security. For providing security for AI problem namely, a novel family of Graphical Password built on top of captcha technology, which we call Captcha as Graphical Password (CaRP).It is both a Captcha and Graphical Password scheme. Carp used in many security problems such as online guessing attack, relay attacks, online polling. Carp offers reasonable security and usability for improving online security

***Keywords*:- Graphical Password, Password, CaRP captcha, Dictionary attack, Password guessing attack, security primitive**

ARTICLE INFO

Article History

Received:30th September 2015

Received in revised form :

2nd October 2015

Accepted:6th October, 2015

Published online :

9th October 2015

I. INTRODUCTION

The most commonly used Authentication technique for user is to submit user name and password. It is easy to break using dictionary attack so we know the vulnerability and it is difficult to remember password. For this purpose studies are shown that users tend to pick short or password that are easy to remember. Unfortunately, these passwords can be easily broken or guessed. According to Computer world's new article, the security teams in the large company's crack the password within 30 seconds; they are identified about 80% of the passwords. However we focus on another alternative i.e. Graphical Password. It is also called as Click-Based Password. Captcha is a standard Internet Security technique to protect online banking, online email and other services that being abused by bots. For that CaRP is used i.e. Captcha as Graphical Password, where the sequence of images are given in the box and user has to choose one image from the all images to derive password. Always a new CaRP image is generated for each login attempt. CaRP requires solving captcha challenge in each login.

Typical application scenario for CaRP includes:

1) CaRP can be applied on the touch screen devices whereon typing password is difficult, especially for secure internet banking such as e-bank. In many banking system captcha is applied in the login session. For example, ICBC (www.icbc.com.cn), the largest bank in the world, requires solving captcha challenge for each login attempt. CaRP usedfor security and authentication purpose. CaRP increases spammers operating task and help in reducing spam emails.

II. BACKGROUND SYSTEM

A. Graphical Password:

A large number of graphical password schemes have been generated. They can be classified into two schemes according to task memorizing and entering password: recognition, recognition-recall. More information can be found in a recent review of Graphical Password.

A recognition scheme requires recognizing an image and using recognized objects as cues to enter a password. Recognition-recall combines the tasks of both recognition and cued-recall. In a cued recall scheme requires a user to regenerate the same interaction result without cueing, an external queue is provided to help memorize and enter a password.

B. Captcha in Authentication:

Captcha is used in authentication. To use both captcha and password in a user authentication protocol, which we call

Captcha based Authentication Protocol, used to counter dictionary attack. After inputting a valid pair of user ID and password the CbPA-protocol requires solving a Captcha challenge. For solving any captcha challenge user has to enter valid user id and password.

C. Thwart Guessing Attack:

In thwart guessing attack, guessed password is tested in an unsuccessful trial is determined wrong and excluded from subsequent trials. Mathematically let S be the set of password, ρ is the password to find, T denotes the trial and T_n denote n-th trial, $p(T = \rho)$ the probability that p is tested in trial T, E_n set of password guess tested in trial up to T_n ,then we have

$p\ (T = \rho | T_1 \neq \rho. \ldots T_{n-1} \neq \rho) > p(T = \rho)$, (1)

And

$$E_n \rightarrow S$$

$p\ (T = \rho | T_1 \neq \rho. \ldots T_{n-1} \neq \rho) \rightarrow 1$ with $n \rightarrow |S|$, (2)

From Eq. (2) $|S|$ denote the cardinality of S, the password is always found within $|S|$ trials. In which each trial determines if the tested password guess is the actual password or not, and the trial's result is deterministic. Captcha as Graphical Password (CaRP) adopts a different approach to counter automatic guessing attacks. It aims at realizing the following equation:

$p(T = \rho | T_1, \ldots, T_{n-1}) = p(T = \rho), \forall n$ (3)

Eq. (3) indicates that each trial is computationally independent of other trials. There is no matter how many trials executed previously, the chance of finding the password in the current trial always remains the same. By examining the authentication system, we noticed that human users enter passwords during authentication, whereas the trial and error process in guessing attacks is executed automatically. The invariants among images must be intractable to machines to thwart automatic guessing attacks. This requirement is the same as ideal Captcha, leading to creation of CaRP, a new family of graphical passwords robust to online banking, online guessing attacks.

III. CAPTCHA AS GRAPHICAL PASSWORDS

A. CaRP: An Overview

In Captcha based Graphical Password (CaRP).In which it uses an *alphabet* of visual objects such as alphanumerical characters, similar animals to generate a CaRP image, which is also a Captcha challenge. CaRP schemes are Captcha based Graphical Password we can say it as clicked-based graphical passwords. CaRP can be classified into two categories: recognition 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 both recognition and cued-recall, also retains recognition-based advantage of being easy for human memory and the cued-recall advantage of a large password space. CaRP schemes of each type will be presented later.

B. Converting Captcha to CaRP:

All text Captcha schemes and most IRCs meet the given requirement i.e. any visual Captcha scheme relying on recognizing two or more predefined types of objects can be converted to a CaRP. Those IRCs that rely on recognizing a single predefined type of objects can also be converted to CaRP in general by adding more types of objects. For conversion of a specific Captcha scheme to a CaRP scheme typically requires a case study, to ensure both security and usability. In some image-recognition Captcha (IRCs) rely on identifying objects whose types are not predefined. For example Captcha which relies on context-based object recognition wherein the object to be recognized can be of any type. In which these IRCs cannot be converted into CaRP since a set of pre-defined object types is essential for constructing a password.

C. User Authentication With CaRP Schemes:

In user authentication like other graphical passwords, we assume that CaRP schemes are used with additional protection such as secure channels between clients and the authentication server through Transport Layer Security (TLS). Most simple way to apply CaRP schemes in user authentication is as follows. In authentication the authentication server *AS* stores a salt *s* and a hash value $H(\rho, s)$ for each user ID, where ρ is the password of the account and not stored. A Captcha as Graphical Password (CaRP) password is a sequence of visual object IDs or clickable-points of visual objects that the user selects. After receiving a login request, *AS* generates a CaRP image, records the locations of the objects in the image, and sends the image to the user to click her password. After that the coordinates of the clicked points are recorded and sent to *AS* along

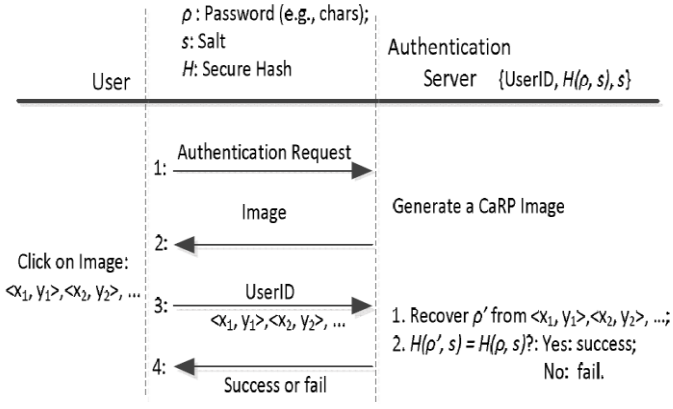

Fig. 1. Flowchart of basic CaRP authentication.

with the user ID. Then *AS* maps the received coordinates onto the CaRP image, and recovers a sequence of visual object IDs or clickable points of visual objects, ρ', that the user clicked on the image. Then authentication server (*AS*) retrieves salt *s* of the account, calculates the hash value of ρ' with the salt, and compares the result with the hash value stored for the account. Authentication is done successfully only if the two hash values match. This process is called the *basic CaRP authentication* and shown in Fig. 1. Advanced

authentication with CaRP, for example, challenge-response, will be presented in Section V-B. To recovering any kind of password successfully, each user-clicked point must belong to a single object or a clickable point of an object. The objects present in a CaRP image may overlap slightly with neighboring objects to resist segmentation. To avoid ambiguity user should not click inside an overlapping region in identifying the clicked object. The given concept is not a usability concern in practice since overlapping areas generally take a tiny portion of an object.

IV. RECOGNITION-BASED CaRP

For recognition-based CaRP scheme, a password is a sequence of visual objects in the alphabet. For each view of traditional recognition based graphical passwords, recognition-based CaRP seems to have access to an infinite number of different visual objects. For this purpose we present two recognition-based CaRP schemes and a variation next.

A. ClickText

ClickText is a recognition-based Captcha based authentication (CaRP) scheme built on top of text Captcha. Text captcha is combination of the alphabet, numbers and special symbol, so its alphabet comprises characters without any visually-confusing characters. For example, digit "0" and alphabet "O" may cause confusion in CaRP images, and thus one character should be excluded from the alphabet. A ClickText password is a sequence of characters in the alphabet, e.g., ρ ="AB#9CD87", which is similar to a text password.

Fig. 2. A ClickText image with 33 characters.

Fig. 3. Captcha Zoo with horses circled red.

Fig.4. a Click Animal image (left) and 6 × 6 grid (right) determined by red turkey's bounding rectangle.

B. Click-Animal

In click-animal captcha Zoo is a Captcha scheme which uses 3D models Of horse and dog to generate 2D animals with different textures, colors, lightings and poses, and arranges them on multiple different background. In which user clicks all the horses in a challenge image to pass the test. It is recognition-based CaRP scheme built on top of Captcha Zoo, with an alphabet of similar animals such as dog, horse, pig; etc. Its password is a sequence of animal names such as

ρ = "Turkey, Cat, Horse, Dog…"

C. Animal Grid

In Animal Grid the number of similar animals is much less than the number of available characters. In Click Anima lit has given a smaller alphabet, and thus a smaller password space, than ClickText. CaRP should have a sufficiently-large effective password space to resist human guessing attacks.

V. CONCLUSION

CaRP is both a Captcha and a graphical password scheme. A desired security property that other graphical password schemes lack. CaRP is also resistant to Captcha relay attacks, and, if combined with dual-view technologies shoulder-surfing attacks. CaRP can also help to reduce spam emails sent from a Web email service. More efforts will be attracted by CaRP than ordinary Captcha. CaRP does not rely on any specific Captcha scheme.

CaRP uses Animal Grid and ClickText had better password memorability than the conventional text passwords, and the usability of CaRP can be further improved by using images of different levels of difficulty based on the login history of the user and the machine used to log in.

REFERENCES

[1] Biddle, S. Chiasson, and P. C. van Oorschot, "Graphical passwords Learning from the first twelve years", ACM Comput. Surveys, vol. 44, no. 4, 2012.J.

[2] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin," The design and analysis of graphical passwords", in Proc. 8th USENIX Security Symp., 1999, pp. 1 to 15.

[3] H. Tao and C. Adams," Pass-Go: A proposal to improve the usability of graphical passwords" ,Int. J. Netw. Security, vol. 7, no. 2, pp. 273 to 292, 2008.

[4] 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 to 127, Jul. 2005.

[5] P. Golle, Machine learning attacks against the Asirra CAPTCHA, in Proc. ACM CCS, 2008, pp. 535 to 542.

[6] L. von Ahn, M. Blum, N. J. Hopper, and J. Langford, CAPTCHA: Using hard AI problems for security, in Proc. Eurocrypt, 2003, pp. 294 to 311.

[7] B. B. Zhu *et al.*, "Attacks and design of image recognition CAPTCHAs," in *Proc. ACM CCS*, 2010, pp. 187–200.

[8] J. Yan and A. S. El Ahmad, "A low-cost attack on a Microsoft CAPTCHA," in *Proc. ACM CCS*, 2008, pp. 543–554.

[9] 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. Magniya Davis et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 2015, 148-151.

