Journal of Multidisciplinary Engineering Science and Technology (JMEST)
ISSN: 3159-0040
Vol. 2 Issue 4, April - 2015

Novel Security Method Using CAPTCHA as Graphical Password

Surendra Karanam
Department of Computer Science
University of Bridgeport
Connecticut, USA
skaranam@my.bridgeport.edu

***Abstract*—Many security primitives are in light of hard numerical issues. Utilizing hard AI issues for security is rising as an emerging new ideal model, yet has been underexplored. In this paper, we introduce another security primitive in light of hard AI issues, which has built on top of the Captcha. This is nothing but Captcha as graphical passwords (CaRP). CaRP is a combination of Captcha and a graphical password. CaRP is useful in resolving many security problems namely online-guessing attacks, relay attacks. CaRP also resolves the shoulder-surfing attacks when combined with the dual-view technology. In this paper, we are going to study about the existing CaRP technologies like ClickText, AnimalGrid and ClickAnimal. We are also going to discuss about the security of CaRP against graphical passwords and text based passwords and CaRP against the relay attacks. CaRP may not be a solution for all the problems but it suits best for some applications to improve the online security.**

***Keywords*—Captcha, CaRP, Graphical, Password**

I. INTRODUCTION

Mostly, the security is provided by using the cryptographic primitives that are based on hard mathematical problems which are intractable. For example, the RSA public key cryptography depends on the integer factorization. The security primitive that is developed using the hard AI problems is CAPTCHA. Captcha is used to distinguish the human and the computer bots. The need to develop the Captcha as a security primitive has risen when an organization conducted the online poll. The online poll ended as a fraud because some computer programs are used to vote in the poll. These Captchas are hard to break by computers and easy to humans. So, Captcha is a widely known internet security primitive which is used in many applications like email and other services to resist from bots.

However, Captcha has achieved less when compared with the cryptographic primitives. In this paper, we are suggesting a new security approach which works based on hard math problems which is Captcha as gRaphical password (CaRP). It is a click-based approach and user has to click on the sequence of the images which were selected while creating the password to get the access. The images in the Captcha are randomly ordered and a new CaRP image will be generated for every login attempt. There are two kinds of CaRP: one is text CaRP and the other is Image-recognition CaRP. The text CaRP is nothing but a sequence of characters as password which is entered by clicking the characters on the CaRP image in a right sequence. CaRP protects against online dictionary attacks and is a severe security risk for many online services. It also provides the security against the relay attacks which is bypassing the Captcha. It also provides security against the shoulder-surfer attacks if the dual-view technology is combined with the CaRP. The CaRP can also work with touch screen devices which mitigate typing the passwords and also increase the operating cost of the spammer's.

II. BACKGROUND AND RELATED WORK

A. *Graphical Passwords*

Earlier multiple graphical password schemes were proposed and they were classified in to three groups according to the complexity involved in memorizing and entering passwords: recognition, recall and cued call. These categories will be illustrated here. Most of the psychological studies support that it is easy to remember the images than text for humans [6].

A recognition-based scheme need to be identified among decoys the visual objects pertaining to a Password portfolio. A complex scheme is passfaces where a user selects a portfolio of faces from a database in creating password. During authentication process, a panel of candidate faces were given to the user to select the face belonging to her portfolio. This procedure is repetitive for several rounds, every round with a different panel. A successful login need correct selection in each round. The set of images in a panel will be same between logins, but their locations were altered. It resembles passfaces but images in the portfolio are arranged in order, and a user should identify her portfolio images in the correct order. Cognitive Authentication need a user to generate a path through a panel of images as mentioned: Starting from the top-left image, scrolling down if the image is in her portfolio, or right otherwise. The user recognizes among decoys the row or column label that the path ends. This procedure is duplicated, each time with a different panel. A successful login requires that the total probability that correct answers were not

listed by chance exceeds a threshold within a given number of rounds.

A recall-based scheme needs a user to regenerate the similar interaction result without cueing. Draw-A-Secret (DAS) was the first recall-based scheme proposed. A user pulls her password on a 2D grid. The system converts the sequence of grid cells adjacent to the drawing path as a user drawn password. Pass-Go improves DAS's usability by encoding the grid intersection points rather than the grid cells. BDAS adds background images to DAS to encourage users to create more complex passwords.

In a cued-recall scheme, an external cue is given to help memorize and enter a password. Pass Points is a extensively studied click-based cued-recall scheme where a user clicks a series of points anywhere on an image in creating a password, and re-clicks the same series during authentication. Among the three types, recognition is considered the easiest for human memory whereas recall is the hardest. Recognition is weakest in resisting guessing attacks

B. Captcha

Captcha depends on the efficiency between humans and robots. There are two categories of visual Captcha (text Captcha) and Image-Recognition Captcha (IRC). The first category depends on recognition of character and the other depends on recognition of non-character objects. The security of text Captcha depends on the character segmentation difficulty which is more expensive and hard to implement [5]. It is easy to read the characters than the non-characters.

C. Captcha in Authentication

Using both the Captcha and password in user authentication is called as Captcha based password authentication. It is helpful in preventing online dictionary attacks. So, user needs to enter Captcha along with the user name and password. It is also used with recognition based graphical passwords to prevent spyware. There will be a text Captcha for every image. User has to select his pass images from other images which were selected while creating the password.

III. CAPTCHA AS GRAPHICAL PASSWORDS

A. A New Way to Thwart Guessing Attacks

In a guessing attack, a wrong password is that which is tested in an unsuccessful trial of a password guess and that should be excluded from subsequent trials. By doing more trials the number of undetermined password guesses decreases, thus leads to a better chance of typing the password

B. Carp: An Overview

In CaRP, even for the same user a new image is created for every login attempt. CaRP uses an alphabet of visual objects (e.g., alphanumerical characters, similar animals) to generate an image of CaRP, which is also a Captcha challenge. A major difference between CaRP images and Captcha images is that all the visual objects in the alphabet should appear in a CaRP image to allow a user to input any password but not necessarily in a Captcha image. Most of the Captcha schemes can be converted to CaRP schemes, as explained in the next subsection. The schemes of Carp are clicked-based graphical passwords. CaRP schemes can be classified into two categories as per memory tasks in memorizing and entering of a password,: recognition and a new category, recognition-recall, which needs to recognizing an image and using the recognized objects as cues to enter a password. Recognition-recall combines the tasks of both recognition and cued-recall, and retains both the recognition-based advantage of being easy for human memory and the cued-recall advantage of a large password space.

C. Converting Captcha to Carp

In principle, the visual Captcha schemes which are relying on recognizing two or more predefined types of objects can be converted to a CaRP Scheme. This requirement is satisfied by all the schemes of text Captcha and most IRCs. By adding more types of objects the IRCs that depend on recognizing a single predefined type of objects can also be converted to CaRP in general. To ensure both security and usability the conversion of a specific Captcha scheme to a CaRP scheme typically needs a case by case study. If the types are not predefined those are the IRCs which rely on identifying the objects.

D. User Authentication with Carp Schemes

Assume that CaRP schemes are used with additional protection such as secure channels between clients and the authentication server through Transport Layer Security (TLS) as other graphical passwords. The possible way to apply CaRP schemes in user authentication is as follows. A CaRP password is a sequence of visual object IDs or clickable-points of visual objects that the user selects. By receiving a login request, AS will give a CaRP image and it records the locations of the objects in the image, also it sends the image to the user to click his password. The coordinates of the clicked points are recorded and they will be sent to AS along with the user ID. AS maps the received coordinates onto the CaRP image, and recovers a sequence of visual object IDs or clickable points of visual objects. To recover a password successfully, each user-clicked point must belong to a single object or a clickable-point of an object. Objects in a CaRP image may overlap slightly with neighboring objects to resist segmentation. Users should not click inside an overlapping region to avoid ambiguity in identifying the clicked object [1].

IV. RECOGNITION BASED CARP

A. ClickText

It is one of the recognition-based Captcha as graphical password schemes. Its underlying principle

is using the text Captcha. ClickText password contains a series of characters that include alphabets, numbers and non-alphanumeric characters like ''SKS@1991" and it doesn't include the characters that are difficult to distinguish like O and 0(zero). ClickText engine generates the ClickText image with the characters that are generated randomly and these character locations are captured to identify the characters based on the users clicked points. ClickText image is different from the normal Captcha. In Captcha, the characters are arranged from left to right and user has to manually enter the characters in the same order that are positioned using the keyboard. But, in ClickText image, all the characters are arranged randomly in multiple rows and user has to click the characters in the same order that the characters are in the password like "S","K", "S", "@", "1", "9", "1" for password "SKS@1991" [1].

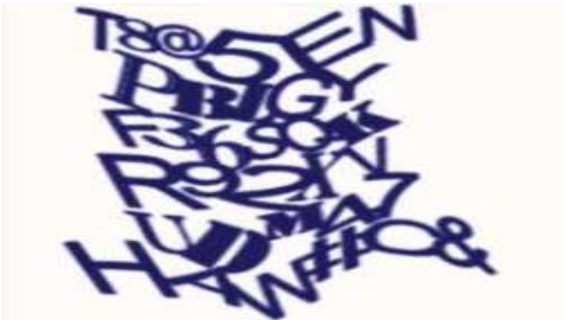

Fig. 1. ClickText

B. *ClickAnimal*

Captcha Zoo is a Captcha scheme that generates the 2D models by using the 3D models of the horse and dog with different colors, poses, textures, and uses grass background to display the image. The user has to click all the horses in the image in the process of authentication.

ClickAnimal is also recognition-based Captcha as graphical password scheme. It has built on the top of the Captcha Zoo and has an alphabet of similar objects as pig, cat, dog, horse. The sequence of animal names is the password as "cat, dog, pig, horse". The Captcha is generated as the 2D images by using the 3D models with different color, view, texture and distortions. These 2D animals are displayed on cluttered background like grassland. Sometimes, images may be overlapped by other images but the core parts are not overlapped to make it easy to identify by the users.

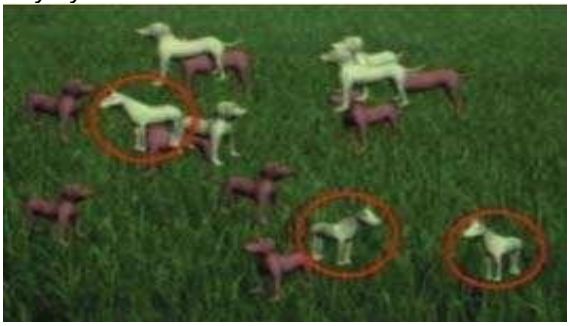

Fig. 2. ClickAnimal

C. *AnimalGrid*

ClickAnimal password space is smaller because it uses smaller alphabet. But, CaRP should have a larger password space to handle the human guessing attacks. To increase the password space, the grid based graphical password has to be used in combination with ClickAnimal. So, The AnimalGrid is a combination of ClickAnimal and Click-A-Secret. In the process of authentication, the user has to select the animal from the ClickAnimal image. Once the Animal is selected, an image of n*n grid appears with the size of the selected image bounding rectangle size. For the user identity, each cell is labeled. The advantage is the user has to click the correct animal to become the clicked grid-cell correct. If user click on the wrong animal, the corresponding grid cell is wrong.

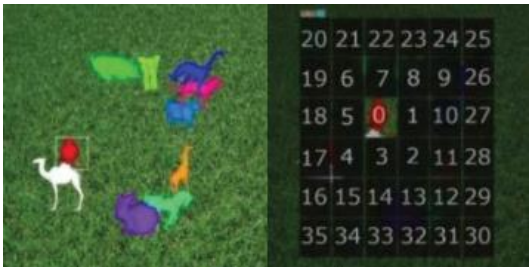

Fig. 3. AnimalGrid

V. SECURITY ANALYSIS

A. *Security of Underlying Captcha*

There is no prominent security model established on Captcha security. The modern Captchas depends on the object segmentation which is expensive and hard. The complexity(C) is defined as $C = \alpha M\ P\ (N)$, where P (N) is a polynomial function and $\alpha>1$. A Captcha challenge contains 6 to 10 characters, whereas a CaRP image contains 30 or more characters. Therefore Captcha scheme is less hard to break than ClickText. Moreover Carp characters are two dimensionally arranged. So, segmentation is difficult due to one more dimension. As a result, in ClickText, we can maintain same security in underlying Captcha by reducing the distortions in images to increase usability.

B. *Human Guessing Attacks*

In this type of attack, humans manually enter the passwords as process of trial and error. Humans are slow compared to computers; so, human's takes long time to guess the password. According to the recent study, users are interested to select a password with a length of 6-8 characters and are not interested to use non-alphanumeric characters. If ClickText has same password length then for 1000 people, it takes 1.7 days and for 1 person, it takes 4.5 years to crack the password [1].

C. *Shoulder-Surfer Attachs*

This kind of attacks happen when one enter password in public places. The best example is banking ATM's. CaRP is not efficient for shoulder

attacks, but with the below dual-view technology CaRP can prevent the shoulder attacks. The dual technology shows two images on the LCD screen at a time. One is called private image and other is called as public image. The private image is visible only for the user and the public image is visible to the others who is observing the clicked points from different angles. These observed clicked points are not useful because the new independent images are used for the next login. However, the Pass Point uses a static image which is private image. So, the attacker cannot see the image but the clicked points are helpful to find the password.

D. Relay Attacks

There are many ways to do relay attacks by hackers. One way to carry out the attack is to have human surfers to solve the Captcha challenge to continue the website surfing. The other way is hiring the humans to solve the Captcha challenges. But, the CaRP is not vulnerable to the relay attacks because the task that the person is hired to perform and the image that is used in CaRP is different from those used to solve the Captcha challenge. This makes it hard to help to test a password guess by attempting to solve a challenge. And, the hired person will not participate unless he is paid to perform the task. Even though the hired person solve the Captcha challenge, it is not useful in password guess because the Captcha challenge generates randomly for every login attempt

VI. CONCLUSION

The paper introduces a new security primitive which is based on hard AI problems that is “Captcha as gRaphical Password (CaRP)”. CaRP is a Captcha combined with a graphical password. There are two types of CaRP schemes. One is Recognition-based CaRP and the other is Recall-based CaRP. We discussed about the former one i.e. Recognition-based CaRP which have ClickText, ClickAnimal and AnimalGrid techniques. The graphical passwords are not fully secure even though they are alternatives to text passwords. CaRP doesn’t depend on any single Captcha scheme. There is a good scope for the refinements in CaRP because of the security and usability. By using different images of varied difficulty levels based on the user’s login history and the machine used to login.

REFERENCES

[1] B. B. Zhu, J. Yan, G. Bao, M. Yang, and N. Xu, “CAPTCHA as Graphical Passwords—A New Security Primitive Based on Hard AI Problems”, IEEE TRANSACTIONS, JUNE 2014.

[2] M. Dailey, C. Namprempre,“A Text-Graphics Character CAPTCHA for Password Authentication”.

[3] T. S. R. Kiran, Y. R. Krishna, “Combining Captcha and graphical passwords for user authentication” , International Journal of Research in IT & Management, April 2012.

[4] L. Wang, X. Chang, Z. Ren, H. Gao, X. Liu, “Against Spyware Using CAPTCHA in Graphical Password Scheme”.

[5] L.V. Ahn, M. Blum, N. J. Hopper, and J. Langford, “CAPTCHA: Using Hard AI Problems For Security”.

[6] X Suo, Y Zhu, G. S. Owen, “Graphical Passwords: A Survey”, Computer Science Department , Georgia State University.