Secure Login Authentication (Captcha as a Graphical Password)

Mohitesh Armorikar[1] Siddhesh Adlikar[2] Sanket Bodake[3] Sanket Sud[4] Mr. Prathamesh Tugaonkar[5]

[1,2,3,4,5]Department of Computer Engineering

[1,2,3,4,5]Terna Engineering College, Nerul, Navi Mumbai

Abstract— Now a days, vulnerability is a major issue in computer security. The password is used in Authentication process which provides security up to a specific level. Also, Captcha is used for online purposes. But it is just to verify if the user is a bot or a human. In our project, we will be using Captcha as a Graphical Password (CaRP). CaRP is a series or sequence of clicks which lead towards the formation of password. Hence, making it more secured and more protected from the attacks of the attacker.

Key words: password, CaRP, Captcha, security primitive, animal grid, Login history

I. INTRODUCTION

Authentication allows the users to confirm their identity on any web application. The three major areas where human computer interaction is important are Authentication, Security operations, and Developing secure systems. We focus on the authentication and transaction problem. Password is used for authentication, which are used to control access to a resource. The password is kept secret from unauthorized access, and those who want to gain access to the resource are tested if they know the password and they are granted or denied access accordingly. Many researchers have found an alternative approach which is the graphical password. The password input is convenient and it is more user friendly in terms of recall ability. The main motivation of graphical passwords is that people are better at remembering images than text words. In addition, graphical password utilizes an easier and more human friendly memorization strategy recognition based memory, instead of a recall based memory for textual password. To overcome the shortcomings of text based passwords, animal grid to login history image as a graphical password system has been proposed. Human brains can process graphical images easily. Graphical passwords are superior to the text based passwords due to this human characteristic. These methods assume if the number of possible pictures is sufficiently large, the possible password space of a graphical password scheme may exceed that of text-based password and therefore it is virtually more resistant to attacks such as dictionary attacks. Many graphical password schemes have already been introduced. Graphical password techniques can be classified into two categories; recognition-based and recall based. In recognition-based systems, a series of images are presented to the user and a successful authentication requires correct images being clicked in a right order. In recall-based systems, the user is asked to reproduce something that he or she created or selected earlier during the registration. Paper is organized as follows. Section II describes types of graphical password techniques and captcha. Section III represents a comparison table of the different survey papers that we have referred. Section IV presents the Future works. Finally, Section V presents conclusion. Section VI provides the references.

II. RELATED WORKS

A. Graphical Password Techniques:

Graphical password techniques are developed to overcome the drawbacks of text based passwords. Graphical passwords consist of recognizing the images and click the particular points on the image rather than typing the characters like the text-based password. In this way, the problems arising from the text-based passwords are reduced. Graphical password techniques are categorized as follows:

1) Recognition Based scheme
2) Recall Based scheme
3) Cued Recall Based scheme.

A recognition based scheme has to select certain number of images from a set of random images in an order as a password. For authenticating, the user has to identify (recognize) those images in the same order.

A recall-based scheme requires a user to reproduce something that he selected or created earlier during registration.

B. Captcha:

Completely Automated Public Turing Test to tell Computers and Human Apart [1] (Captcha) finds the difference in humans and bots. Captcha has two types: Text Captcha and Image Recognition Captcha

1) Text Captcha:

Microsoft Captcha is relied on background noise and random character strings to resist or minimize the automated attacks. The Captcha used by Google, Yahoo! share similar properties, such as a lack of background noise or distortion for a character or word images. EZ-Gimpy uses word images that employ character distortion and clutter. Personal print uses a low quality picture by degrading parameters to fragment and add noise to the character images.

2) Image Recognition Captcha

Captcha consist of a combination of images .The user must recognize the images given to him to solve the given puzzle problem. As shown in Figure.2 user has to select the cat images as the password characters.[1]

C. Captcha as Graphical Password (CaRP):

An Overview CaRP has a new image which is generated for every login attempt even for the same user. A Recognition-based CaRP technique is used as password in a series of visual objects alphabet. Preview 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. Password is a sequence of some invariant points of objects. A non-variant point of an object is the point that has a fixed relative position in various incarnations of the object and it

can be uniquely identified by users no matter how the object appears in CaRPimages.

1) ClickText:

ClickText has a recognition-based CaRP scheme. CaRP techniques use CAPTCHA as its principle. Alphabet set of ClickText comprises of alphanumeric characters. A ClickText password is a series of characters in the alphabet.

e.g. =DEF@b2SK78, which is a similar to the text password. A ClickText image is different from usual CAPTCHA as all the characters of alphabet set must be included in the CaRP image. The CAPTCHA engine generates such CaRP image. When image is generated, then each characters location in the image is recorded which is 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 in order for users to type them sequentially. Fig. 3 shows a ClickText image with an alphabet of 33 characters [1].

2) ClickAnimal

ClickAnimal is a recognition-based CaRP technique. It has a series of similar animals such as dog, pig, like that. The password in this technique is a sequence of animal names like = Cat, Dog, Turkey, Most of the models are created or each and every animal. The CAPTCHA generation activity are used to get 2D models by applying different types of views, colours, and optional distortions and it is used to generate the Click Animal image. The final resulting 2D animals are then arranged on clustered backgrounds like grassland. The number of similar animals is less than the number of available characters.

Fig. 1: Captcha Images

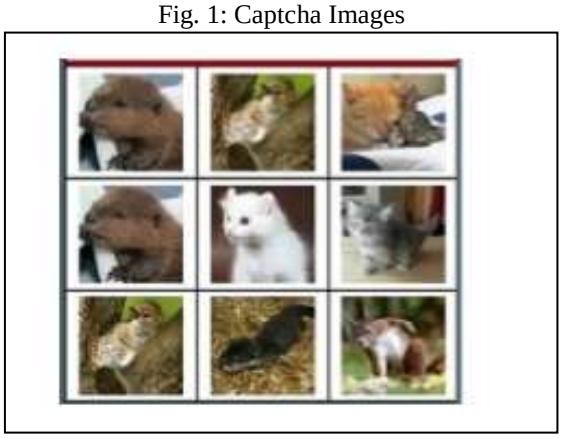

Fig. 2: Image based Captchas

Fig. 3: Clicktext CaRP Scheme

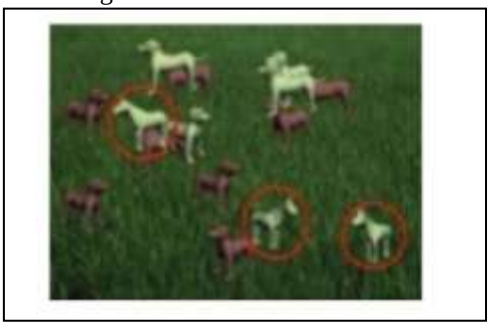

Fig. 4: Click Animal CaRP Scheme

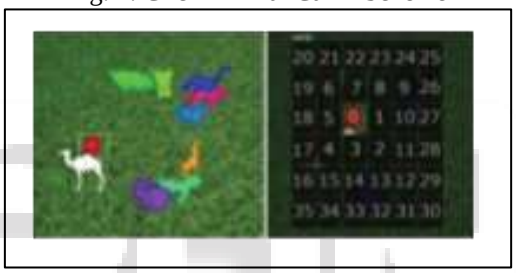

Fig. 5: A Click Animal Image(Left) 6 x 6 grid(Right)

3) Text Points 4 CR

Text Points sometimes, it can be modified to fit challenge response authentication. This variation is called as Text Points for Challenge Response or also TextPoints4CR. CaRP have some benefits given below:

1) CaRP offers protection against Automatic Online Guessing Attacks on passwords.
2) It offers protection against Shoulder Surfing Attack.
3) It offers security against spam emails sent from a Web email service.
4) It offers security against spam emails sent from a Web email service.

4) CaRP has some limitation:

1) CaRP scheme is vulnerable to phishing attack.
2) CaRP is vulnerable if both the image and user-clicked points can be captured.

III. COMPARISON TABLE

Author	Paper Title	Technique Used	Drawback
Hwan-Gue Cho, Tae-Cheon Yang	Designing Captcha Algorithm: Splitting and Rotating The Images Against	In this system using RDH technique for plain image and achieve excellence	Shoulder suffering attack not overcome

Ibrahim Furkan Ince	OCRs[2008]	performance	
Anjitha K, Rijin I K	Captcha as a Graphical Password-Enhanced with Video-based captcha for Secured sequence[2015]	Use of Captcha in Video Format using OCR.	Just used to check for any bot entry
Bin B. Zhu, Jeff Yan, Guanbo Bao, Maowei Yang	Captcha as Graphical Passwords—A New Security Primitive [2015]	Graphical password with CAS and Animal Grid combination are used.	Shoulder suffering attack can be happen.

Table 1:

IV. SURVEYING INPUTS

Our proposed system overcomes various demerits of earlier existing systems by using a dynamic Animal Grid, along with the introduction of Login History Image.

Login History image to be used during Transactions in order to increase security.

A. Algorithm

1) Step 1: Start
2) Step 2: User registers with his username and the specific Animal Grid as his password
3) Step 3: Login Process
4) Step 4: If Login successful perform Steps 5 to 7.else step 8
5) Step 5: During Transaction, User has to enter the login image.
6) Step 6: If the login image is correct then step 7 else step 8
7) Step 7: Transaction is successful and login history image sent to the user via email.
8) Step 8:Stop

V. SECURITY ANALYSIS

CaRP uses unsolved AI problems. The Login History Image and Animal Grid schemes provide an easier use than PassPoints and other Captcha. They also have large password space with more combinations in Animal Grid compared to normal text Captcha. The usability can be increased by applying different difficutly levels of images. CaRP techique if combined with dual-view technlogies can resist shoulder-surfing attack.

The new CaRP video-based Captcha can provide more security. The attacker with the idea of pixels cannott retrieve any information regarding the object. Since all the objects are moving, it is difficult to separate the background and moving objects. The movement can be applied to ClickAnimal and AnimalGrid CaRP schemes. All these schemes offer computationally higher security compared to other Captcha techniques. The scheme provides high robustness to identify higher level challenge used. So the proposed scheme can offer resistance to so many attacks and ensure high level security for a security based system

VI. CONCLUSION

CaRP authentication system is developed by graphical password based on animal grid method which uses both the combination of recall based and recognition based system. This system provides animal grid from which user will select his graphical password. To overcome this type of attack, the advance system generate the login history image where the generated image automatically generate and send to the user's email id. only user can select correct image at the time of transaction. If password is stolen by intercepter, the advance system will not allow the intercepter to do transaction into the system.

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 2015.
[2] Anjitha K, Rijin I K "Captcha as a Graphical Password-Enhanced with Video-based captcha for Secured sequence"2015 International Conference On Applied And Theoretical Computing And communication Technology (iCATccT)
[3] Hwan-Gue Cho, Tae-CheonYang "Designing Captcha Algorithm: Splitting and Rotating The Images Against OCRs" 2008 International Conference on Convergence and Hybrid Information Technology
[4] Macharla Bhanu Kumar, K. Kranthi Kumar "Enhancing CAPTCHA based Image Authentication for E-mail ID and Password" International Journal of Computer Engineering in Research Trend

