Captcha As Graphical Passwords-Enhanced With Motion-Based Captcha for Secure Services

[1] Anjitha K, [2] Rijin I K
[1][2] Department of Computer Science and Engineering ,
Malabar Institute of Technology, Anjarakandy
Kannur , Kerala – India
[1] k.anjitha@gmail.com [2] rijinik@gmail.com

***Abstract*-- CAPTCHAs, also known as reverse Turing tests are real-time assessments that are commonly used by programs to tell humans and machines apart. This can be achieved by assigning and assessing or evaluating hard AI problems such that these problems could only be solved easily by human but not by machines. A new security approach based on hard AI problems and Captcha technology is known as Captcha as gRaphical Passwords (CaRP). This scheme can address many security problems such as dictionary attacks, online guessing attacks and shoulder-surfing attacks etc. In this paper, we present an enhanced security for the CaRP scheme i,e CaRP with motion-based Captcha. The movement of Captcha ensures high security over the normal CaRP scheme. Motion-based captcha can provide a great challenge for humans in exploiting the remarkable perceptual abilities or skills of humans to unravel structure-from-motion. Thus it can thwart many attacks, can enforce more security and it stipulates security along with usability to legitimate users in dealing with real time applications.**

***Index Terms*-CaRP, Shoulder-surfing attack, dictionary attack, hotspots, CAPTCHA.**

I. INTRODUCTION

Computer security is critical in almost any technology driven industry which operates on computer systems. The main aim in security is to provide cryptographic systems that are computationally infeasible for attackers to gain access to the system. When designing a computer system, there are many aspects to be taken into consideration, among that one of the main factor is security, which prove to be very important. For example the problem of integer factorization is a technique used in RSA. The discrete logarithm is used in Diffie-Hellman Key Exchange, Digital Signature Algorithm, Elliptic Curve Cryptography and so on. These primitives are based on hard AI problems.

CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) is a new paradigm for standard Internet Security. Captcha, sometimes called as reverse Turing Test is a category of challenge-response test very useful in computing to determine whether the user is human or not. Captcha helps in protecting from spam and password decryption by providing the user with a simple test that proves user is a human and not a computer trying to perform unauthorized accesses or break into a password protected account.

A. Applications of CAPTCHAs

Captcha is well-known for its efficiency in protecting websites and other online applications by validating and ensuring that the user is a human; and is neither a bot nor an automatic machine. The Captcha have many applications in the field of internet security. Some security applications include :

1. Comments Spam Prevention

Comments spam is used mostly in blogs and forums to increase search engine ranking of websites. A spammer who need some free traffic to his website will add comments with some textual links to his website. So using Captcha technology in blogs or forums in adding comments option will block the automatic machines from spamming. Bots cannot pass Captcha test.

2. Online Polls

Captchas have a major role in the results of an online poll to ensure that human votes are counted. Captcha prevents the the possibility of biased results (by bots) and also ensures that only humans are taking part in the poll.

3. Search Engine Bots

Inorder to protect confidential pages on the website that need not be revealed by bots, a powerful tool is to use Captcha. So that it prevents all kinds of bots from entering the website.

4. Free Email Services

Most of the companies like Yahoo!, Google provide free email services so they suffer from different types of attacks. Bots register for free email accounts.This situation can be prevented by using Captcha. It asks the user to read words from the distorted words to confirm that it is a human. The bots cannot pass this challenge and this type of problem is known as hard AI (Artificial Intelligence) problem.

5. Preventing Dictionary Attacks

It helps in preventing a computer from being able to search through the entire password space through the involvement of humans to type the password.

B. Characteristics of CAPTCHAs

There are different types of Captcha used in the recent years. Modern text-based Captchas uses three abilities- invariant recognition, segmentation, and parsing to correctly complete the task with better efficiency and consistency. The characteristics are the summary of [1] : The test must be such that it can be easily solved by the human.

2. Automatic generation and grade-ability

The test must be automatically generated and graded by the machine. The machine must not be able to respond to the test and it is one of the main requirement. The administration requires little human intervention.

3. Challenging For Machines

The test is based on hard AI problem and thus it must be hard for the machines to solve.

4. Robustness enhanced when database publicized

The test of attacking will be difficult if the database, from which the test is generated, is publicized.

5. Resistance to no-effort attacks

The test must be resistant to no-effort attacks. These attacks are those that can solve Captcha without solving hard AI problem.

A new graphical password system having Captcha technology is known as Captcha as gRaphical Passwords (caRP). This scheme is a new security primitive related to hard AI problems. It is actually a click-based password scheme where the user can have sequence of clicks on the image to provide the password. CaRP image is different for every login attempts. CaRP offers protection against online dictionary attacks which have been a threat to online services. Carp also ensure safety against relay attacks. The Carp mechanism needs to solve a Captcha in every login attempt. This is done by increasing the difficulty of Carp images. If combined with dual-view technologies, Carp is found to be robust against shoulder-surfing attacks. So our new proposed scheme is a combination of CaRP technology with motion-based images. The static plane Captcha images are mostly used in the recent years. But these static images are posing a great threat to the security. There are many segmentation and merging technologies due to which these types of Captchas can be easily traced and identified by a bot. So many network service programs are attacked by bot programs. Thus enhanced Captcha need to be proposed for ensuring safety and also increasing practicability.

The remaining paper is organized as follows: Background and related work is presented in Section II. Section III presents CaRP schemes. Proposed work is provided in Section IV. The Section V consists of security analysis . We conclude the paper with Section VI.

II. BACKGROUND AND RELATED WORK

A. Graphical Passwords

Graphical passwords consists of pictures to authenticate the legitimate users. There are large number of graphical password schemes being proposed. They can be grouped into three categories : RECOGNITION, RECALL, CUED RECALL [2].

1) Recognition Based Scheme: This scheme requires identifying images belonging to a user's password portfolio. When creating passwords, it ask users to memorize a series of images and then identify their images to log in. The main application of this system is Passfaces [3] where user selects images from a database for the creation of a password. During the authentication proceess, a set of faces belonging to the user's portfolio is displayed for the selection. This procedure is repeated for several rounds. A successful login requires user to select images in the correct order for each round.

2) Recall Based Scheme: This scheme requires users recall and reproduce a secret drawing. It is also known as draw metric systems. The real time application includes Draw-A-Secret (DAS) [4] which allows users to draw their password on a 2D grid. The system then encodes the sequence of grid cells that the user used for drawing password. Pass-Go [5] improves the DAS's scheme by encoding only the grid intersection points and not the grid cells. BDAS scheme [6] provides a base for strong passwords by adding background images to DAS.

3) Cued Recall Scheme: This scheme provides an external cue to help in memorizing and entering the password. This system is also known to be as locimetric system, they are also referred as click-based graphical password scheme. One important application is PassPoints [7]. The user can select some points on an image and the same points need to be clicked during authentication. Cued Click Points (CCP) [8] uses one image per click and the next image is selected by a deterministic function. To improve CCP, another scheme called Persuasive Cued Click Points (PCCP) [3] was introduced. Here user selects a point inside a viewport for creating a password. This helps in more complex click points in a password.

B. Captcha As Graphical Passwords

CaRP technique uses a new image for ever login process for the same user. This scheme can thwart guessing attacks. A CaRP image consists of alphabets, images, numbers etc, which forms the set of visual objects. Normally CaRP schemes are click-based graphical passwords. CaRP can be used in secure internet applications such as e-banking, online shopping etc which needs a Captcha for the login attempt.

CaRP can also be used in e-mail services so that it increases the spammer's cost and reduces the spam emails. A human involvement is must to login into the account, so even if the bot knows the password, he is denied from accessing the email services. This leads to reduced outbound spam traffic.

1) Basic CaRP Authentication: Like all other Captcha schemes, CaRP also have user authentication phase for providing login access permissions. The authentication function is done by the authentication server. The process is : The authentication server (AS) stores the salt value 's' and hash value 'H' computed by H(p,s) for each user account. This system does not store the password p. When a user request reach the server, the AS generates a CaRP image and record the positions of objects and send to the user for clicking the password. A CaRP password consists of some clickable points on the image or visual objects. The coordinates of the user clicked points are recorded at the user side and send to AS along with the corresponding user ID. The As then maps the received coordinates onto the corresponding CaRP image and it recovers clickable points of the objects, p'. The AS retrieves the salt value of that account and calculates the new hash value H(p',s). The stored hash value of the account and the new hash value are compared. If both the hash values are matching, then authentication succeeds. This is the Basic CaRP Authentication procedure and is shown in Fig.1.

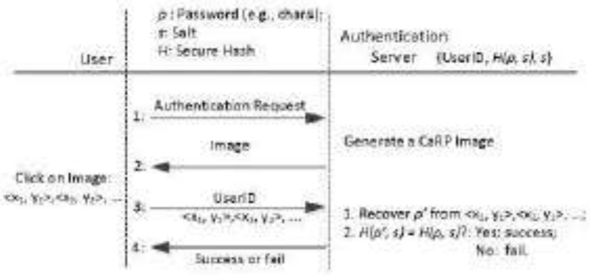

Fig. 1. CaRP authentication process

III. CARP SCHEMES

CaRP schemes are click-based graphical password schemes. CaRP schemes can be broadly classified into two categories: RECOGNITION and RECOGNITION-RECALL schemes. In recognition scheme, the images are analysed and these recognized objects are used as cues for entering the password. Recognition-recall is a combination of both recognition and cued-recall. Thus it has the advantages of both the schemes i,e it is easy for human memory and also have large password space.

A. Recognition-Based CaRP

In this scheme, passwords are a collection of visual objects in the alphabet. Mainly there are three types of recognitionbased CaRP- ClickText, ClickAnimal, AnimalGrid [9]. Click- Text is based on text Captcha where characters are arranged randomly on a 2D space. Confusing Characters are avoided. They are different from text Captcha as these text Captchas are arranged in order from left to right. During authentication, the user click on the characters in the image in the same oreder. Fig.2 shows a ClickText image with 33 characters. ClickAnimal is a technology on the top of Captcha Zoo [10]. It consist of 3D models of animals to create 2D animals with different lightning effects, colors, textures etc. The password is a long sequence of animal names such a "Dog, Cat, Turkey,....". AnimalGrid is developed to increase the password space. So it is a combination of ClickAnimal and Click-ASecret (CAS). For entering the password, first ClickAnimal image is displayed, when a user selects an animal, an nxn grid appears with the grid size depending on the bounding rectangle of the selected animal.

B. Recognition-Recall CaRP

In this system, password consists of some invariants points of objects. For an object, a point is said to be an invariant point if it has a fixed relative value in different fonts. Users must recognise the images of the objects and use these identified objects as cues to identify the password within a tolerance range. TextPoints and TextPoints4CR techniques are commonly used in recognition recall CaRP [9]. The characters in TextPoints contains some invariant points and they form a set of clickable points. Here password is a sequence of clickable points and a character can have multiple clickable points. So TextPoints have larger password space compared to ClickText. The TextPoints4CR is a challengeresponse technique. It is formed by modifying TextPoints. The authentication server stores the password for each account. And each character appears only once in the TextPoints4CR image.

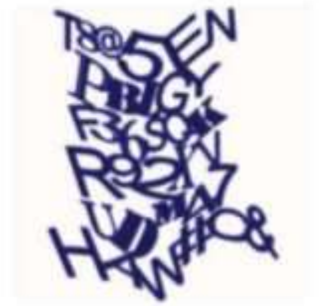

Fig. 2. A ClickText image

IV. PROPOSED WORK

The proposed scheme consists of enhancing the Captcha schemes with motion. The Captchas are provided with random movement so that the objects will be in motion. Also changing complex background texture, leads to dynamic change in target and background characteristics distribution. This new scheme can be applied to clickText and ClickAnimal in the CaRP schemes. The idea is to provide users with a random set of characters (codeword) moving in a dynamic fashion, and solving the captcha by entering the correct codeword. For enhanced security, these movement will be in different trajectories. This will overcome the attack based on vision techniques.

The changes can be made to the size, color and background of the animation. This will enhance the security. In the case of ClickText, the visual objects consists of characters, these characters can be provided with random motion. And in the case of ClickAnimal, the objects are the set of animals, so here movement can be given to these animals, which in turn creates difficulty in identifying those animals. The technique to create animation is by creating frames and make movement to the objects to be recognised within the frames. When the objects move from one frame to another, the temporal property of the object will be changed by changing the pixel coordinate. This change helps in changing the color, size or background effects. This is a major task for a bot to identify the characters or objects present in the animated screen. This scheme can mitigate the static OCR attacks. The objective is to achieve a safe and efficient animation CAPTCHA based on the CaRP scheme to improve the protection capability of the system against malicious visit programs. While creating motion on these CaRP scheme, the user must feel that the objects in the screen are moving smoothly with slight changes in position, angle, shape, size and color in the window. The user won't get any information regarding the motion of ClickText or ClickAnimal animation on the screen. The dynamic motion creates difficulty in predicting the movement. Normally static Captchas are in x-y plane and their motion will be pre-defined. So any malicious program can track or predict the motion by analysing the coordinates. This reveals the position of the characters on the screen, which pose a great threat to Captcha security.

The new proposed work can have the following characteristics: a changing background that can be made complex to enhance the security of CaRP schemes, multi-target discovery, changes in attributes like color, size, shape etc. The Fig.3 shows an animated Captcha with a moving background.

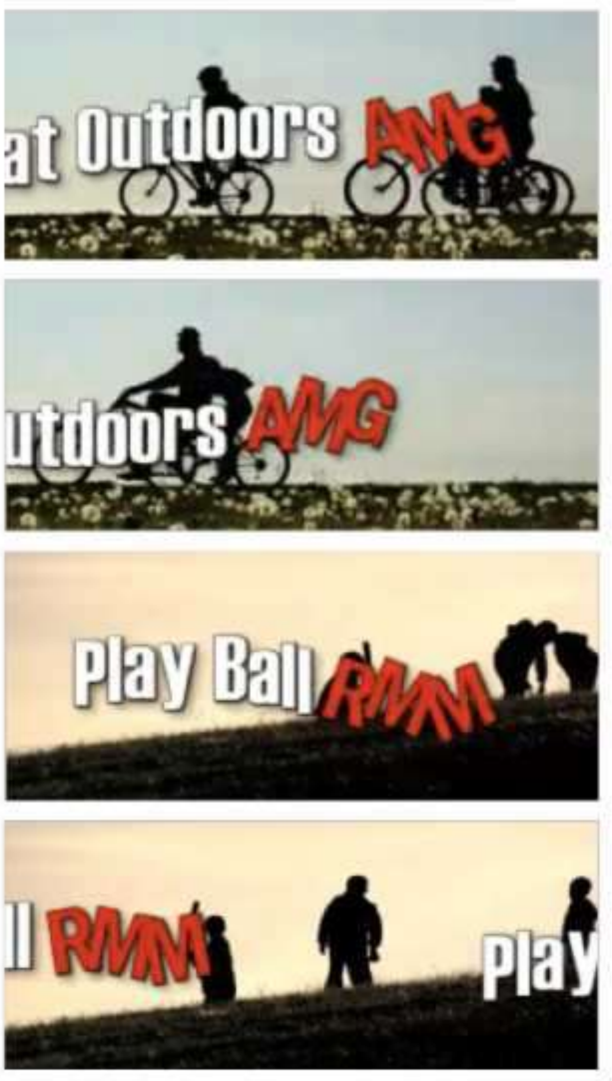

Fig. 3. Image with motion-based Captcha

V. SECURITY ANALYSIS

CaRP uses unsloved AI problems. The CickAnimal and AnimalGrid schemes provide an easier use than PassPoints and other Captcha. They also have large password space compared to normal text Captcha. The TextPoints4CR and TextPoints also have clickable points. The clickable points in one image are computationally independent of clickable points in another image. Thus the usability and practicability is increased by implementing CaRP scheme. The usability can be increased by applying different difficulty levels of images. The challengeresponse protcol ensures a high level security in the case of authentication of the systems. CaRP techique if combined with dual-view technlogies can resist shoulder-surfing attack. The new CaRP motion-based Captcha can provide more security. The attacker with the idea of pixels can't retrieve any information regarding the object. Since all the objects are moving, it is difficult to separate background and moving objects. The movement can be applied to ClickText and to ClickAnimal CaRP schemes. Both schemes can offer computationally higher security compared to other Captcha techniques. The visual objects in the techniques are moving in a random fashion. So a bot finds it difficult to solve it and detect the motion. CaRP embedded with motion will be resistant against online guessing attack, dictionary attack etc. The scheme provides high robustness to identify higher level challenge used. So the proposed scheme can offer resistance to many attacks and ensure higher level security for a security-based system.

VI. CONCLUSION

CaRP is a new security primitive depending on hard AIproblems. CaRP is a combination of both Captcha and a graphical password scheme. It consists of different schemes to enhance security. Each scheme is developed to overcome the limitations of the existing Captcha schemes. The identification of hotspots is very difficult in CaRP because this technique does not rely on one specific scheme of implementation. CaRP have high usability and practicability applications in the field of network security. The new scheme relying on CaRP with motion-based Captcha enforces more security compared to normal CaRP. The animated CaRP can ensure difficulty in solving the Captcha. The dynamic motion of characters provides a higher level of security to the system. The proposed scheme will be able to resist any attack based on static OCR recognition. The scheme have high importance in the internet systems. It is ahead of all other Captcha schemes. It provides a longer time to enter a password which is a major concern of security and usability. Thus the new scheme is an efficient technology to provide more security for security-based services.

REFERENCES

[1] Y. Rui and Z. Liu, "Artifacial: Automated reverse turing test using facial features," Multimedia Systems, vol. 9, no. 6, pp. 493–502, 2004.

[2] R. Biddle, S. Chiasson, and P. C. Van Oorschot, "Graphical passwords: Learning from the first twelve years," ACM Computing Surveys (CSUR), vol. 44, no. 4, p. 19, 2012.

[3] P. Jayanthi and R. Divya, "Captcha as graphical password-pixel based pattern recognition system,"

[4] B. Malek, M. Orozco, and A. El Saddik, "Novel shoulder-surfing resistant haptic-based graphical password," in Proc. EuroHaptics, vol. 6, 2006.

[5] H. Tao and C. Adams, "Pass-go: A proposal to improve the usability of graphical passwords.," IJ Network Security, vol. 7, no. 2, pp. 273–292, 2008.

[6] P. Dunphy and J. Yan, "Do background images improve draw a secret graphical passwords?," in Proceedings of the 14th ACM conference on Computer and communications security, pp. 36–47, ACM, 2007.

[7]S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon, "Passpoints: Design and longitudinal evaluation of a graphical password system," International Journal of Human-Computer Studies, vol. 63, no. 1, pp. 102–127, 2005.

[8] P. C. van Oorschot and T. Wan, "Twostep: An authentication method combining text and graphical passwords," in E-Technologies: Innovation in an Open World, pp. 233–239, Springer, 2009.

[9] B. Zhu, J. Yan, G. Bao, M. Mao, and N. Xu, "Captcha as graphical passwords–a new security primitive based on hard ai problems," 2014.

[10] R. Lin, S.-Y. Huang, G. B. Bell, and Y.-K. Lee, "A new captcha interface design for mobile devices," in Proceedings of the Twelfth Australasian User Interface Conference Volume 117, pp. 3–8, Australian Computer Society, Inc., 2011.