



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

Security through CAPTCHA Using Graphical Password

Aiswarya U, Beshiba Wilson

PG Student, Dept. of CSE, Lourdes Matha College of Science and Technology, Trivandrum, Kerala, India

Associate Professor & HOD, Dept of CSE, Lourdes Matha College of Science and Technology, Trivandrum, Kerala, India

ABSTRACT: CAPTCHA (Completely Automated Public Turing tests to tell Computers and Humans Apart) is a program that generates and tests that are human solvable, but the capabilities of current computer programs. It is based on mathematical problems. Captcha as graphical passwords (CaRP) is a new security primitive based on hard AI problems. A number of security problems altogether, such as online guessing attacks, relay attacks is addressing CaRP. CaRP is a popular graphical password system. CaRP offers reasonable security and usability that appears with different practical applications for improving online security.

KEYWORDS: CaRP, Graphical password, hotspot, security primitive, Captcha

I. INTRODUCTION

A graphical primitive is based on mathematical problems that deal with crypto graphic primitive. It is a text-based password schemes that development of graphical password schemes [1]. It is a standard Internet security technique to protect online email and other services. This is a challenging problem. CAPTCHA uses algorithm based on hard AI problem.

The documentation of CaRP is very simple but universal. It is a click-based graphical password, and a sequence of clicks on an image is used to derive a password. Captcha can communicate on multiple-object classification that can be differentiated to a CaRP scheme. In this paper present CaRPs found on both text Captcha and image-acceptance Captcha. When we entered to click the right character sequence on CaRP images, one of the test CaRP password is a sequence of characters like a text password. An exciting new model using hard AI (Artificial Intelligence) problems for security [2]. An advantage in that they are resistant to recap attacks. Different applications on CaRP are:

1. It can be applied on touch-screen device; it is used to secure internet applications such as e-banks. Different banking systems have applied Captcha user login [3].
2. CaRP increases operating cost and to reduce spam emails.

A new security primitive relying on unsolved hard AI problems. Here two CaRP schemes can be implemented is encouraging. For example consider animal grid and click text have better password than current text password. These papers consist of three modules namely:

1. Graphical password
2. File security
3. USB authentication.

1. Graphical password:

Graphical password gives user strong front end security. In this Module when user registers a new account, system randomly generate multiple images and ask user to pick one. This should be his/her Authenticated Image. This graphical password act secondary security to our system. In the Pass Points graphical password scheme a password consists of a sequence of click points that the user chooses in an image. The image is displayed on the screen by the system.

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

2. File Security

In this module when users try to upload his/her file, system asks for an image security. System generates an image and ask user to pick any of the hot spot position to create a lock. Once the hotspot lock is created then for downloading we have to pick the right hotspot otherwise the system will not download the file.

3. USB authentication

A more recent development is the move by some companies towards USB keys or tokens to provide authentication security that protects access to enterprise user accounts for website, software systems and networks.

II. RELATED WORK

An authentication system is based on animal grid and click text [1].Captcha is based on hard AI problems. In graphical password [1] can classify recognition, recall, and cued recall password.A recognition-based scheme that identifying the visual objects belonging to a password container. This process repeats several stages.A recall-based scheme requires a user to reproduce the same interaction result without continue. Draw-A-Secret (DAS) [4] was the first recall-based scheme. A cued-recall scheme is provided to help memorize and enter a password. Pass point [9] is widely used click based cued-recall scheme. In [5]Captcha and password in a user authentication protocol,Captcha-based Password Authentication (CbPA) protocol, to counter online dictionary attacks.Captcha used with recognition-based graphical passwords [6][7] used text Captcha display the images.

III. CAPTCHA AS A GRAPHICAL PASSWORD

A. CaRP: Overview

CaRP[11][12] can generate a new login for the same user. A CaRP image can generate an alphabet of visual objects such as alphanumeric characters,animals, birds etc.The main difference between visual object that alphabet can present a CaRP image as input.

CaRP image are click-based graphical password.CaRP can be classified into two:recognition and a new category. Recognition-recall means it recognizing an image and that recognized objects as suggestentering a password. Recognition-recall combines both recognition and cued-recall and advantage is easy for human memory and the cued-recall advantage of a large password space.



Fig 1: Select image for Login

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

B. Converting Captcha to CaRP

Many visual Captcha scheme carry on recognizing two or more predefined types of objects to be converted to a CaRP. A typical example is Cortcha[8] is context-based object recognition. Text Captcha schemes and most IRCs meet their requirement. Recognizing a single predefined type of objects IRCs can communicate and to be converted to CaRPs.

C. Recognition-based[10]

A password is a sequence of visual objects in the alphabet. It is a traditional recognition based graphical passwords. A different visual object can access an infinite number of Recognition-based CaRP. Recognition-based system that uses different images like natural images faces etc.

D. Cued based

An external based cue is used to help memorize and then continue as password. Pass point can be used. It is a click based scheme. We can select a portion from the image and that image can be used for login otherwise it cannot see any files and share files etc.



Fig 2: Pass point scheme

IV. SYSTEM DESIGN

A. Problem Statement

Existing system allow authentication security to graphical password that has control as username in text format. The knowledge based authentication that measure extraordinarily text based passwords. Users has to produce unforgettable passwords that are truthful for attackers to guess, because the system assigned passwords are difficult for users to recollect, a graphical password authentication system that to encourage users with password that are unforgettable. New concepts like recognition pass point; recall based and cued click points. Cued click points is the latest technique that provides hot spot pictures. This paper overcomes authentication concepts incorporate with graphical username and password techniques.

B. Proposed Statement

For click image, pools of image can be displayed, the user select their needed passwords by done through enter via click based mostly. The system provides better security and higher security. Captcha has the following properties:

- CaRP image are computationally-independent.
- Guessing attacks are mutually independent.

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

C. System Architecture

- Robust authentication system using CaRP and Captcha
- It is helpful to login the system for any many application.
- Robust and easy login system for any application to avoid remembering login to users.

D. Working Methodology

A new user can register an account and they can add their photo and then create picture security because other users cannot see our files. Once we create a graphical password then that user can login their account to their predefined passwords. Then user can view their files and send mails to another user. During registration stage user can add their name, email id, username and password.

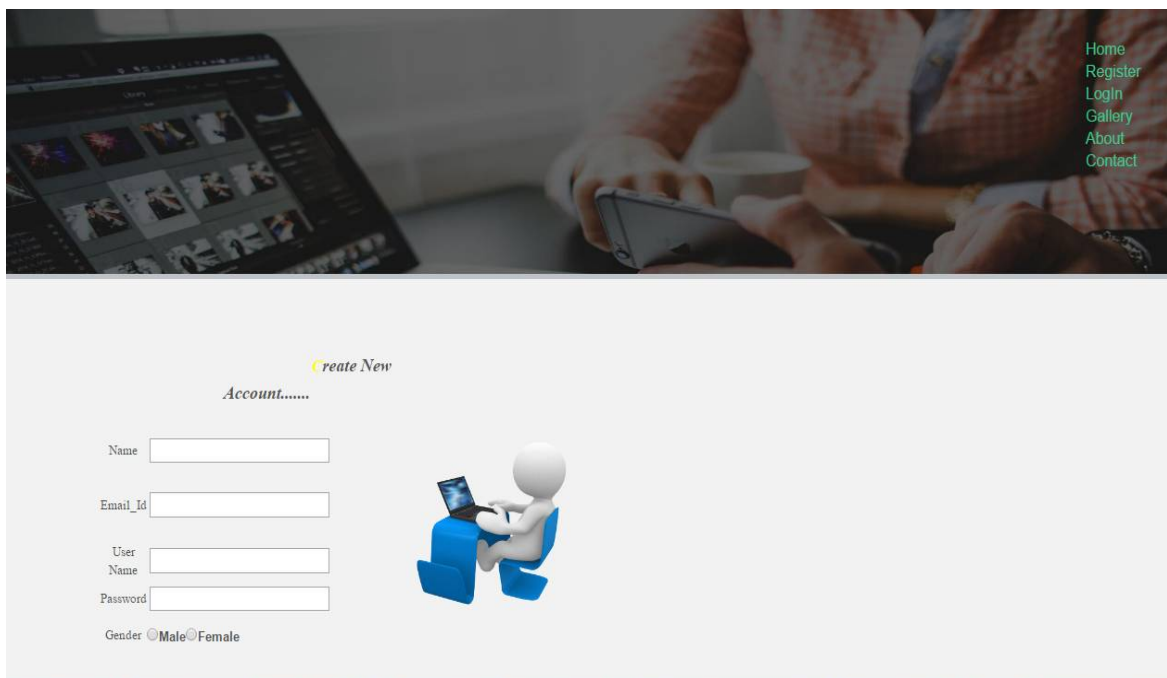


Fig3 : Registration page for a new user.

V. IMPLEMENTATION AND RESULT ANALYSIS

A. CaRP User authentication

CaRP schemes in user authentication are as follows [1]. The authentication mechanisms to user to recollect simply his/her credentials and supply a good security for the user to secure your account for further hardware for application.

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

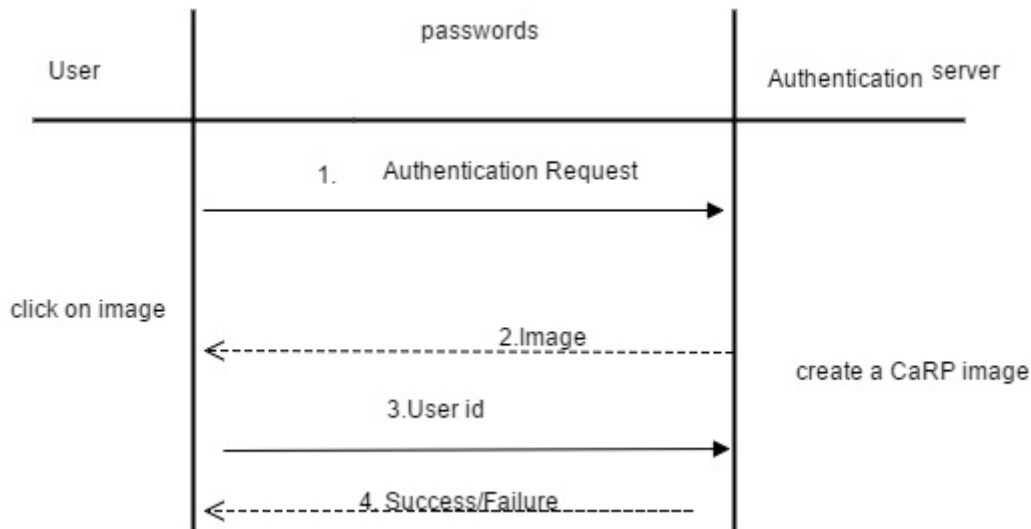


Fig 4: Flowchart of basic CaRP authentication

B. Registration

1. Select an image for username.
2. Click the point image for Password.
3. Enter the required field such as Email, Mobile Number, and Gender.
4. Once you click Register button then the user authentication will be available, to be verified successfully.

C. Advantage

- It takes too long process.
- It is easier to remember than text strings.
- It is faster compared to existing systems.

D. Application

- It can be applied on touch screen devices.
- Every login challenge to make effort to an online guessing attack computationally.

VI. CONCLUSION AND FUTURE WORK

This paper tells about CaRP, a security primitive attack that depends on AI issues. The system users can freely choose their password and the servers are required to retain only the pair user ID and password. The password authentication scheme can prevent the replay attack; the intruder cannot obtain a login password through the open network and replay the password to login to a server. It can be used to relay attack and shoulder surfing.

The system can offer new steps for the safety of authentication. The system can offer new security, therefore it would be useful for many online systems for authentication purposes for industry-level projects, banking systems for identifying the right user, social networking. CaRP has good analysis, which calls for useful future work.



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirccce.com

Vol. 5, Issue 4, April 2017

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. L. von Ahn, M. Blum, N. J. Hopper, and J. Langford, "CAPTCHA: Using hard AI problems for security," in Proc. Euro crypt, 2003, pp. 294–311..
3. 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.
4. H. Tao and C. Adams, "Pass-Go: A proposal to improve the usability of graphical passwords," Int. J. New. Security, vol. 7, no. 2, pp. 273–292, 2008.
5. B. Pinkas and T. Sander, "Securing passwords against dictionary attacks," in Proc. ACM CCS, 2002, pp. 161–170
6. H. Gao, X. Liu, S. Wang, and R. Dai, "A new graphical password scheme against spyware by using CAPTCHA," in Proc. Symp. Usable Privacy Security, 2009, pp. 760–767.
7. L. Wang, X. Chang, Z. Ren, H. Gao, X. Liu, and U. Aickelin, "Against spyware using CAPTCHA in graphical password scheme," in Proc. IEEE Int. Conf. Adv. Inf. Netw. Appl., Jun. 2010, pp. 1–9
8. B. B. Zhu et al., "Attacks and design of image recognition CAPTCHAs," in Proc. ACM CCS, 2010, pp. 187–200.
9. 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. 102–127, Jul. 2005.
10. Bin B. Zhu and Jeff Yan, "Towards New Security Primitives Based on Hard AI Problems", Newcastle University UK, 2013.
11. G. Moy, N. Jones, C. Harkless, and R. Potter, "Distortion estimation techniques in solving visual CAPTCHAs", in Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognition., pp. 23–28, Jul. 2004.
12. S. Chiasson, P. C. van Oorschot, and R. Biddle, "Graphical password authentication using cued click points", In Proc. of ESORICS, pp. 359–374 2017.

BIOGRAPHY

Aiswarya Uis is a PG student in Computer Science and Engineering in Lourdes Matha College of Science and Technology, Trivandrum, Kerala. Shedid B Tech degree in Lourdes Matha College of Science and Technology.

Ms.Beshiba Wilsonis is an Associate Professor & HOD in Computer Science and Engineering in Lourdes Matha College of Science and Technology, Trivandrum, Kerala. Her research interests are Image Processing, Pattern Recognition, Artificial Neural Network, and Computer Graphics.