Multilevel Security through Image Recognition CAPTCHA and 9-Dots CaRP

Sushama Kulkarni
School of Computational Sciences, S. R. T. M. University
Nanded, Maharashtra, India
sushama.s.kulkarni@gmail.com

Dr. H. S. Fadewar
School of Computational Sciences, S. R. T. M. University
Nanded, Maharashtra, India
fadewar_hsf@yahoo.com

Abstract— CAPTCHA based security is an indispensable part of any website in current era. As CAPTCHAs are evolving against various attacks, rigid techniques for CAPTCHA designing are consequent. Web Security through CaRP is a promising area. In this paper, we propose a novel multilevel security system through combination of image recognition based CAPTCHA and a 9-dots panel based CAPTCHA as gRaphical password (CaRP). We have also analysed the user acceptance for the same.

***Keywords*— Completely Automatic Public Turing test to tell Computers and Humans Apart (CAPTCHA), CAPTCHA as gRaphical Password (CaRP), Web security, Authentication, Mouse dynamics**

I. INTRODUCTION

CAPTCHA is a reverse turing test to identify human and bots apart. It effectively repels several types of attacks on web.
As this war is getting fierce day by day, bots and CAPTCHAs are continuously improving technologically. Current CAPTCHA techniques aspire to use hard AI problems to implement security measures. One of the emerging techniques is the use of CAPTCHA as gRaphical Password (CaRP). It combines graphical password and CAPTCHA scheme. CaRP requires user to perform some mouse dynamics based tasks.

CaRP provides robust security against online dictionary attacks and relay attacks. CaRP implements Captcha-based Password Authentication (CbPA) protocol to counter online dictionary attacks. CbPA-protocol mandates the user to solve a CAPTCHA challenge right after the user provides a valid user ID and password pair. Thus CaRP satisfies the basic requirement of user friendly interface for human being and higher complexity for bots.

II. GRAPHICAL PASSWORD TECHNIQUES

A. Recognition based Technique

Recognition based technique requires user to memorize some set of previously selected images and recognize those images from a set of random images at the time of login.

ClickText requires user to click a sequence of characters which are randomly arranged in set of 33 characters on a 2D space. It authorizes user if password characters are clicked in specified sequence [1].

ClickAnimal uses sequence of animal names as password. CAPTCHA is generated by arranging 2D animal images on a cluttered background [1]. Here an alphabet consists of similar animals e.g. dog, horse, pig etc. It has smaller password space as compared to Click Text CaRP.

Passfaces needs user to choose a set of human faces during registration phase and identify those preselected human faces from a random set of human faces at the time of authentication [2].

Déjà vu scheme uses similar approach like Passfaces but it uses random art pictures instead of human faces [3]. These art images are difficult to remember for a user, thus login phase takes longer time.

B. Recall based Technique

Recognition based technique requires user to reproduce or select something which he had produced or selected in registration phase.

Draw-A-Secret technique (DAS) asks the user to draw something in a 2D grid canvas and reproduce the same drawing during authentication phase [4]. Similarly Passdoodle allows user to use freehand drawing without a visible grid as a password [5].

C. Cued Recall based Technique

Cued Recall based techniques provide user an image or set of images from which user have to select click point as the password. It also provides some hints which help users to reproduce their passwords with high accuracy.

Greg blonder proposed a method in which presents the user with pre-stored images and asks to tap region by pointing location on image. It is more vulnerable as clicking region is small and simple [6].

Passpoints requires the user to set sequence of clicks on an image as his password and reproduce the same sequence of clicks during authentication phase [7]. Cued Click-Points (CCP) method reduced hotspots and improvised usability of Passpoints. This method asks user to click on one point per image for a sequence of images [8]. It displays the next image on the basis of location of the previous clickpoint.

III. PROPOSED SYSTEM

All of the graphical passwords discussed in section II offer a single level of security, thus they are prone to bot attacks. In this section we propose a novel technique to repel imposters and bots by combining multiple security methods.

A. Modules

Security methods which are combined in our approach are:

- Token based authentication.
- Click based image recognition CAPTCHA.
- 9-Dots panel CaRP.
- One Time Password (OTP).

1) *Token based authentication:* A token is a piece of data that has no meaning or use on its own, but when it is combined with the correct tokenization system, it becomes a vital player in securing the application. Token based authentication ensures that each request to a server is accompanied by a signed token which the server verifies for authenticity and only then responds to the request.

The proposed system requires user to enter the unique user name registered at the sign up phase for each future sign in attempt.

2) *Click based Image Recognition CAPTCHA:* We have reused Google reCAPTCHA which provides a checkbox for user verification as human.

Google reCAPTCHA takes advantage of classic Computer Vision problem of image labelling and the fact that most of the bots do not execute JavaScript and consequently they are unable to identify the correlation between the displayed text and the DOM or required actions.

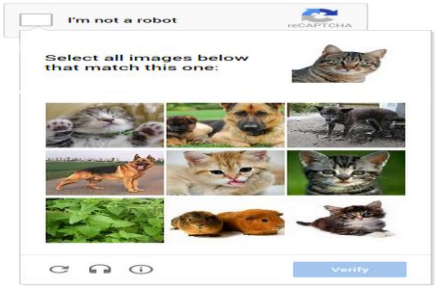

Fig. 1 Google reCAPTCHA challenge

3) *9-Dots panel CaRP:* We have incorporated a 9-Dots panel which acts as mouse dynamics based CaRP. It is similar to DAS CaRP scheme but instead of a visible grid, it provides a 9-Dots panel. User has to draw the same pattern which was registered during sign up phase. Pattern is drawn using a mouse or touchpad by connecting the desired dots on the 9-dots panel. As most of the mobile devices offer the same system of 9-Dots panel based password security, this 9-Dots panel provides user friendly interface and simplicity.

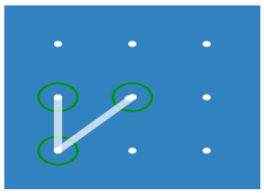

Fig. 2 A screenshot of 9-Dots panel CaRP

4) *One Time Password (OTP):* A one-time password (OTP) is a password that is valid for only one login session. One-time passwords are a form of strong authentication, providing much better protection to replay attacks.

Although the proposed system allows multiple attempts to solve the Click based image recognition CaRP for a user, it does not allow more than 3 attempts to solve 9-Dots panel CaRP. If a user fails to solve the 9-Dots panel CaRP within 3 attempts, system sends an automatic mail containing a One Time Password (OTP) to pre-stored email account for that specific user. It asks user to enter that OTP in order to proceed for sign in process.

Fig. 3 Screenshot of proposed systems' sign in page

B. Algorithm

1) Algorithm for Sign Up:

Step1: Once user clicks 'Sign Up' button on the homepage, redirect him/her on the Sign Up page.

Step2: User has to enter a unique username and a valid email address. User clicks on the 'I'm not a robot' checkbox.

Step3: When user clicks the 'I'm not a robot' checkbox, system will display an image based captcha challenge.

Step4: **If** user correctly verifies the image based captcha then he/she will be allowed to proceed.
Otherwise system will present a new challenge of the image based captcha to be solved.

Step5: User is asked to draw a 9-dots pattern twice, which will be used as password for future Sign Ins.

Step6: If 2 patterns drawn by the user on 9-dots panel of graphical captcha are not matching then user gets a message that two patterns should be the same. Go to Step5.

Step7: If the username provided by the user already exists then user is asked to provide some other unique username. Go to Step2.

Step8: If the user correctly draws the same pattern twice and the username provided by user is unique then system will allow him/her to land in the private account page and consider the Sign Up process has been successfully completed and redirects user to the private page.

Step9: Internally system stores the username, email address and graphical password for future authentication purpose.

Step10: Stop.

2) Algorithm for Sign In:

Step1: When registered user visits the homepage, he/she has to enter the preregistered username in the designated textbox and click on the 'I'm not a robot' checkbox.

Step2: When user clicks the 'I'm not a robot' checkbox, system will display an image based captcha challenge.

Step3: If user correctly verifies the image based captcha then he/she will be allowed to proceed. Otherwise system will present a new challenge of the image based captcha to be solved.

Step4: User is asked to draw a 9-dots pattern registered during 'Sign Up' process.

Step5: **If** user draws a wrong pattern or the username provided by user is non-existent for the pattern drawn and drawAttempt <= 3 then system displays a message that no user with the provided username and password was found. Go to Step1.

Elseif drawAttempt > 3 then system generates an OTP mail and send it to the registered email address. It redirects user to OTP verification page. Go to step6.

ElseIf username and 9-dots pattern drawn by user are valid then system will allow the user to land in the private account page and consider the Sign In process has been successfully completed and redirects user to the private page. Go to step7.

Step6: User enters the OTP in designated textbox and system verifies the OTP, if OTP is valid then system considers the Sign In process has been successfully completed and redirects user to the private page.

Step7: Stop.

IV. USABILITY STUDY

User experience encompasses all aspects of the end-user's interaction with the application. Thus this usability study focused on gaining insights in the users' point of view and his/her expectations.

For usability study we requested 18 volunteers to use our application for at least 10 days. Volunteers were a set of individuals ranging from 18 to 63 years of age with mixed level of computer and web literacy. At the end of this stipulated period, we collected their feedback through a questionnaire. Questionnaire was designed to address various aspects like users' ability to handle such applications, knowledge, skillset, and his/her views about the overall interface, security, simplicity and possibility of recommendation. We also requested suggestions optionally.

Only 55.56% of volunteers were aware of CAPTCHA concepts. 83.33% of the volunteers found the system user interface was easy to understand. All of the volunteers felt that the system offers useful feedback when they encounter a problem. On the other hand, 27.78% of the volunteers felt that the system is slow. Most importantly 83.33% of volunteers found the system to be secure and 77.78% of them found it to be simple as well.

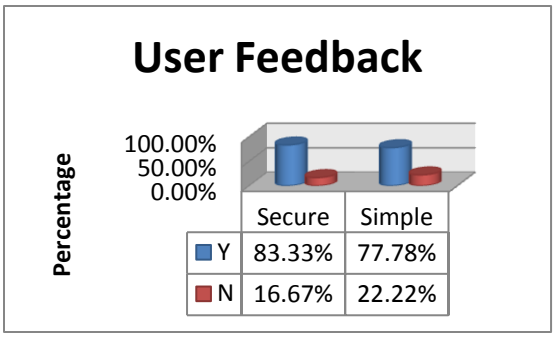

Fig. 4 User feedback on security and simplicity of proposed system

Although the number of volunteers was limited but 10 days of daily use of the proposed system shows promising feedback from the users.

V. CONCLUSION

Bots and security systems follow the Kaizen philosophy of continuous improvement. CaRP is a pivotal trend in security systems. Thus amalgamation of multiple security techniques like token based authentication, click based image recognition CAPTCHA, 9-Dots panel CaRP and One Time Password (OTP) will definitely induce a new wave of security enhancement. User feedback on the proposed system shows favourable results, encouraging such efforts in this area.

ACKNOWLEDGMENT

We wish to acknowledge volunteer participants of usability study who took time to handle the proposed system and provided their valuable feedback on the same. We are grateful to Dr. V. A. Jadhav, Head of the Department of CS & Statistics, teaching and non-teaching staff of Department of Computer Science, N. E. S. Science College, Nanded, Maharashtra, India for their extended efforts in accomplishment of the usability study.

REFERENCES

1. Bin B. Zhu, Jeff Yan, Guanbo Bao, Maowei Yang, 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, pp. 891-904, June 2014.
2. Real User Corporation, "How the Passface System Works", 2005.
3. Rachna Dhamija, Adrian Perrig, "Déjà Vu: a user study using images for authentication", in Proceedings of the 9th conference on USENIX Security Symposium, p.4-4, August 14-17, 2000, Denver, Colorado.
4. I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The Design and Analysis of Graphical Passwords," in Proceedings of the 8th USENIX Security Symposium, 1999.
5. Varenhorst, "Passdoodles: A lightweight authentication method". MIT Research Science Institute, July 2004.
6. G. Blonder, "Graphical Passwords", U.S. Patent 5559961, 1996.
7. S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy, N. Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system", International J. of Human-Computer Studies (Special Issue on HCI Research in Privacy and Security), 63 (2005) 102-127.
8. S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot, "Influencing users towards better passwords: Persuasive cued clickpoints", in Proceedings of HCI, British Computer Society, Liverpool, U.K., pp 121-130, 2008.