Captcha as Graphical Passwords- A Novel Approach

Bhupendra Shivhare
Department of Computer science and Engineering
Oriental Institute of Science and Technology, Bhopal, Madhya Pradesh, India

Jijo S Nair
Department of Computer science and Engineering
Oriental Institute of Science and Technology, Bhopal, Madhya Pradesh, India

Abstract- Many security related problem is based on hard mathematical problem. By the using hard artificial problem for security is new paradigm. But this paradigm has achieved limited success. In this work we present a new security primitives based on a hard artificial intelligence problem, namely, a new family of graphical passwords integrating with Captcha technology which we call Captcha as gRaphical passwords (CaRP) system. CaRP resolve online guessing attack. A CaRP passwords can found only probabilistically by automatic guessing attack if passwords is in search set. CaRP also offers a new approach to eliminate image hotspot problem in PassPoints system. ClickText is recognition based CaRP scheme. This scheme is based to text Captcha. In ClickText scheme user is click on Captcha image to generate passwords. This Captcha image contain 33 characters. In our proposed work we use 34 alphanumeric characters. We set rotation, scaling, overlapping and warping of characters light level. This process is increased usability of system and retains the security at the same level.

Keywords – Captcha, Graphical Passwords, CaRP, CbPA, Security and Usability Primitives.

I. INTRODUCTION

Captcha as gRaphical passwords (CaRP) [1] is a new security primitive that is combines the features of Captcha and graphical password that enhanced security as well as usability. CaRP concept is based on hard Artificial Intelligence. Captcha is also based on hard Artificial Intelligence [2]. Captcha distinguishes human from machine by presenting a puzzle or a challenge. In our work we used the concept of click based graphical password, but graphical image is based on Captcha concept. CaRP provides the protection against online dictionary attack. Online dictionary attack is a major security threat in various online services [3]. CaRP increase usability of system by clicking on image. In text password if we make easy password than it can be easily crake or if we can make difficult password than it can be difficult to remember. Solution of this problem in some context is that we can make our password in a graphical form [4]. In current scenario an image is generate by Captcha engine that is also known as ClickText image, a user click on that image to generate password [5].

Captcha based Password Authentication (CbPA) that is required to solve a Captcha challenge after entering a valid username and password. Like Captcha, CaRP is also used in reduced spam email in addition to provide security.

CaRP approach can be applied on touch-screen device, and many e-banking systems. For example ICBC bank is required solving a Captcha challenge in every login attempt.

CaRP can also address security problem such as relay attack, shoulder-surfing attack (if we combined with dual-view technology). Image hotspot is major security problem in click-based graphical password such as PassPoints. CaRP provides well approach to reduce hotspot problem that occur in click based graphical password.

So we can say CaRP is not solve all the security related problem but it can provides better security and usability as compared to existing system.

II. PROPOSED ALGORITHM

A. ClickText CaRP scheme

ClickText is a recognition-based CaRP system built on top of text Captcha. Its alphabet includes characters without any visually-confusing characters. For example, Letter "O" and digit "0" might cause confusion in CaRP images, so thus one character will be excluded from the alphabet. In proposed ClickText images is generated by less distortion and light warping effect. Various parameters includes while generating a ClickText image like rotation of

characters, scaling of characters and overlapping of characters. This CaRP scheme is accept only Capital letters. We use 34 alphanumeric characters for usability purpose. ClickText is passwords of sequence like “146HGW”.

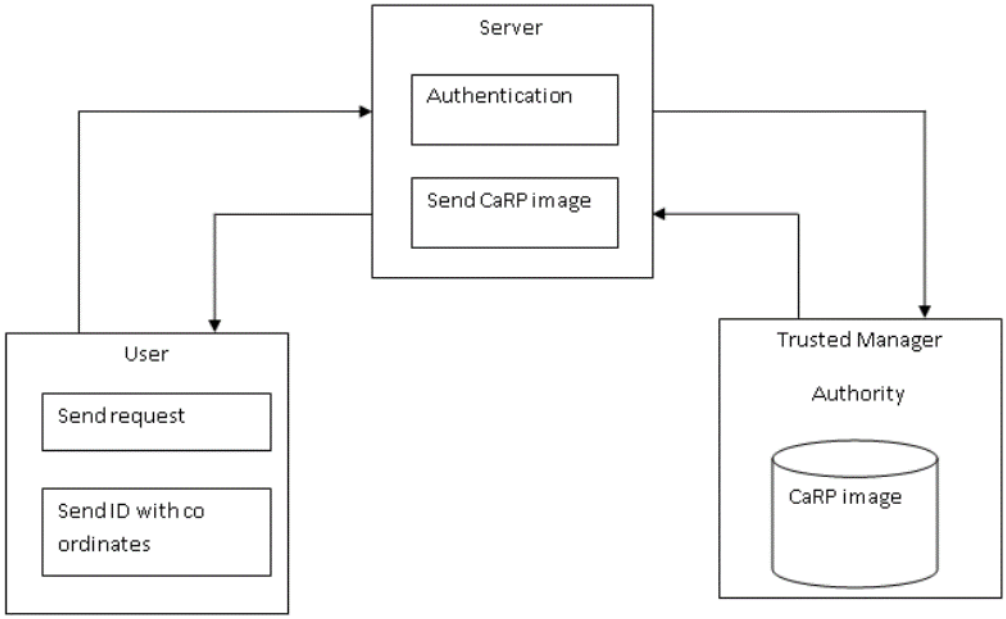

Figure 1. Proposed system architecture

If user wants to enter his/her passwords then he/she click visual characters in sequence like ‘1’, ‘4’, ‘6’, ‘H’, ‘G’, ‘W’. A ClickText alphabet is arranged in 2D space. The authentication server relies of ground truth of alphabet so it uses a tolerance range of each character.

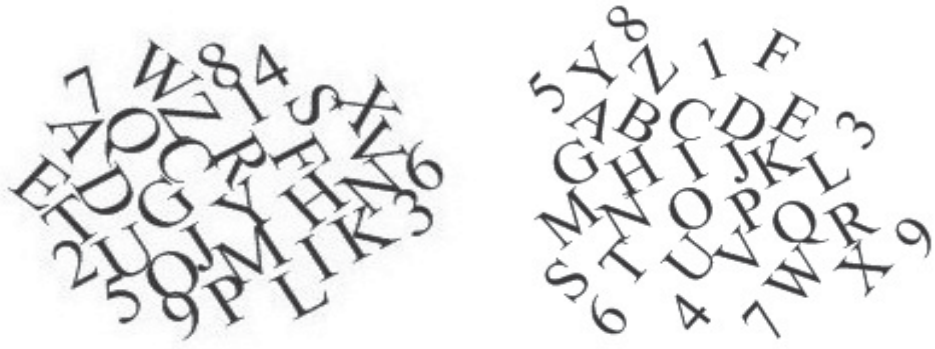

Figure 2. Different ClickText CaRP images

B. User authentication in ClickText CaRP scheme –

Like other graphical passwords scheme, we assume that ClickText scheme is used with extra defense such as secure channels between clients and the authentication server over Transport Layer Security (TLS). User sends authentication request to the server with visual object IDs or clickable points of pictorial objects that user selects. Server request for the ClickText image over Trusted Authority Manager and archives the location of the object from

the image and sends that image to the user. Server analyzes the coordinates sent by the user and authentication successes if the value matches.

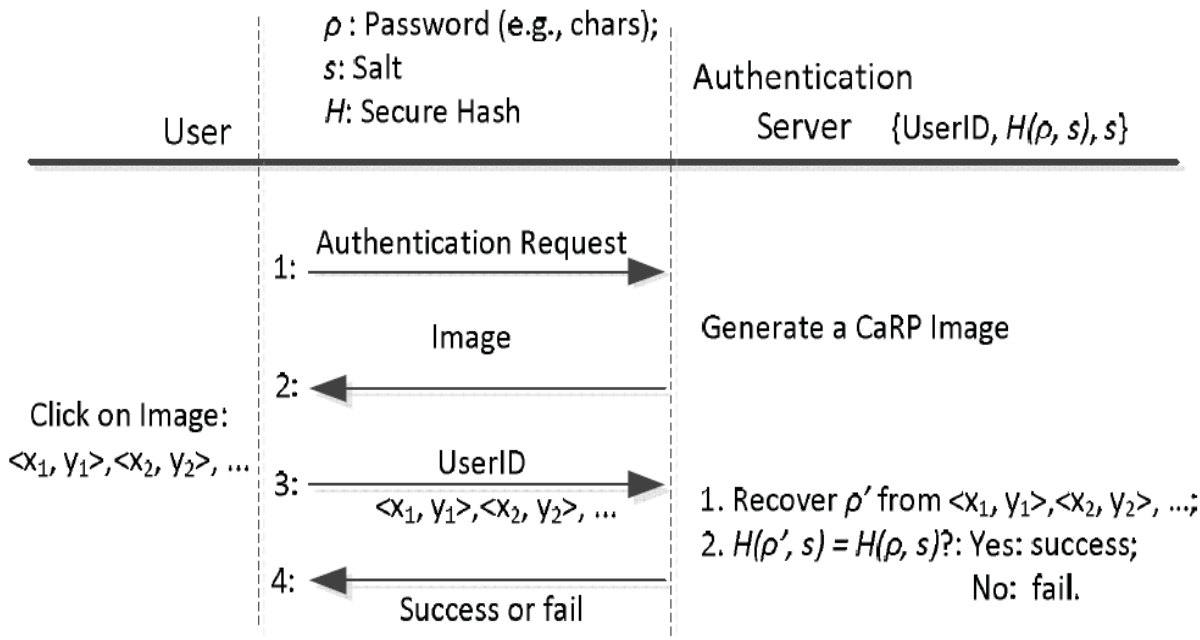

Figure 3. ClickText Authentication

B. ClickText CaRP scheme Algorithm –

- The authentication server (AS) store a salt s and hash value H (ρ, s) for each user id where ρ is the password of the account.
- By receiving a login request AS server generate a ClickText image.
- AS store the location of the objects that user selects.
- The coordinates of the click points on image are recorded.
- This coordinates are sent to the AS server along with user id.
- AS maps the received coordinates onto the ClickText image.
- AS recovers a sequence of visual object IDs or clickable points of visual objects, ρ'.
- After that AS server retrieves salt s for account.
- Calculate the hash value of ρ' with salt.
- AS compare the result with hash value store for an account.
- Authentication success if the two hash value match.

III. Experiment and Result

This research work has implemented by using MATLAB 2013a. MATLAB, which stands for MATrix LABoratory, is a state-of-the-art mathematical software bundle, which is used extensively in both academia and industry. MS access 2013 is as back end.

Figure 4. Proposed work layout.

We conducted a usability study to compare ClickText methods and proposed ClickText methods. Both scheme was tested as: a member used a web browser to interact with an authentication server, making passwords or logging into the server. Once a participant submitted his/her data to the server, the browser would show the login result.
Each member was asked to make a password that is never used before. Each passwords contains 8 click points. We also ensure that no one note down their passwords.
A member's login time in each trial was noted by the server. We define the login time as the period from the time when the server received a login request to the time when the server gave its answer to the login request, which contains the time to enter user ID and password, to produce a CaRP image, and to communicate between the server and a member's browser.
Table 1 shows the average login time of the 40 member's successful login attempts and the sample standard deviation as well as the maximum and minimum login times for both scheme.

Table -1 Login time for both schemes

SCHEME	ClickText	PROPOSED ClickText
T(s)	27.22	25.55
σ(s)	17.38	15.28
Max.(s)	65.62	60.62
Min.(s)	10.41	8.80

Where, T(s) = average login time in seconds.
$\sigma(s)$ = sample standard deviation.

IV.CONCLUSION

The past decade has seen a rising interest in using graphical passwords as an substitute to the traditional text-based passwords .Although the main argument for graphical passwords is that persons are better at memorizing graphical passwords than text-based passwords, the present user studies are very limited and there is not yet convincing evidence to support this argument. We have proposed CaRP, a new security primitive depend on unsolved hard AI problems. CaRP is both a Captcha and a graphical password system. The notion of CaRP introduces a new family of graphical passwords, which adopts a new method to counter online guessing attacks. A password of CaRP can be search only probabilistically by automatic online guessing attacks counting brute-force attacks, a preferred security property that other graphical password schemes shortage. Hotspots in CaRP images can no longer be exploited to mount automatic online guessing attacks, an intrinsic vulnerability in many graphical password schemes. CaRP forces adversaries to resort to significantly less efficient and much more costly human-based attacks. In addition to offering defense from online guessing attacks, CaRP is also resistant to Captcha relay attacks, and, if pooled with dual-view technologies, shoulder-surfing attacks. CaRP can also help decrease spam emails sent from a Web email service.

REFERENCES

[1] B. 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. Eurocrypt, 2003, pp. 294–311.

[3] M. Alsaleh, M. Mannan, and P. C. van Oorschot, "Revisiting defenses against large-scale online password guessing attacks," IEEETrans. Dependable Secure Comput., vol. 9, no. 1, pp. 128–141,Jan./Feb. 2012.

[4] R. Biddle, S. Chiasson, and P. C. van Oorschot, "Graphical passwords: Learning from the first twelve years," ACM Comput. Surveys, vol. 44, no. 4, 2012.

[5] Bhupendra shivhare and Jijo S Nair, "Survey on Captcha as Graphical Passwords" in Internation Journal of Latest Trends in Engineering and Technology (IJLTET)". In Vol. 6 Issue 3 January 2016 ISSN: 2278-621X.