International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Merging CAPTCHA and Graphical Password on NP Hard Problems in AI: New Security Enhancing Technique

Nayan Gawande

Computer Engineering, J. S. P. M, Tathawade, Pune, India - 411033

Abstract: ***CAPTCHA (Completely Automated Public Turing Test to tell computers and human apart) is a test build by computer programs which human can pass but computer programs cannot pass. A new technology is built over the captcha called graphical captcha which is resilient to dictionary attacks and hence more secure. With the hybrid use of CAPTCHA and graphical password one can addresses a number of security problems such as relay attacks, online guessing attacks and also shoulder surfing attacks. CaRP (Captcha as a graphical password) is not act as a cure all technique but it stipulates security and usability to legitimate users in real time applications.***

Keywords: CAPTCHA, graphical password, CaRP, dictionary attacks, security, legitimate user.

1. Introduction

Authentication is inevitable task in security where we use text password as a security technique but text passwords are threaten by many attacks [2]. Another traditional authentication approach for security is alphanumeric password which uses letters, upper and lower case characters and some special characters. Biometric is another way for security where human body part is used as a password with resilient to shoulder surf attack. [1,2] Nowadays, advanced technologies make use of Graphical Password, CAPTCHA, CaRP (captcha as a graphical password) for authentication purpose.[3]

1.1 Graphical password:

Graphical password makes use of a picture, part of a picture or number of pictures together to authenticate legitimate user. These schemes are resilient to dictionary attacks but are prune to shoulder surfing attacks. Graphical password can be grouped into three types based on memorability of the user: RECOGNITION, RECALL, CUED RECALL. [2]

1.1.1 Recognition based system: It is also known as search metric systems which generally ask users to memorize a portfolio of images during password creation and then identify their images from among decoys to log in. Recognition-based systems use various types of images like faces, random art, everyday objects, and icons. Spoofing attacks are more difficult with recognition based systems. In recognition schemes, the system must know which images belong to a user's portfolio in order to display them. This current information must be stored such that its original form is available with the system.

Real Time Application for Recognition based system: Passfaces
This system makes use of the human ability to recognize faces. To register with the system the user selects four faces from a large database of available choices. When a user wishes to authenticate themselves they are presented with an array of nine faces, arranged in three rows of three. One of the faces is part of the user's password while the other eight are incorrect. The user then touches the face to select it and the system then displays the next set of faces. The challenges continue until the user has selected four faces, it is at this point that the user passes or fails authentication. There are a number of issues with this system; some relate to security and others relate to usability. The main usability concern, which is becoming more and more redundant as network speeds increase, is the time it could take to load the faces. This issue is particularly relevant when the authenticating server is based in a remote location, as is likely to be the case with public space interactions [4, 5].

1.1.2 Recall based system: It is also known as drawmetric systems because users recall and reproduce a secret drawing. In these systems, users typically draw their password either on a blank canvas or on a grid. Retrieval is done without memory prompts or cues. The system is prune to Phishing attacks. A phishing website can copy the login page from a authorized site, including the area for drawing the graphical password. Once user enters their username and password, this information can be used by attackers at the authorized site.

Real Time Applications for Recall Based system: Draw-A-Secret

In this system, users draw their password on a 2D grid using a stylus or mouse (Figure 1). A drawing can consist of one continuous pen stroke or preferably several strokes separated by "pen-ups" that restart the next stroke in another cell. To log in, users repeat the same path through the grid cells. The system encodes the user-drawn password as the sequence of coordinates of the grid cells passed through in the drawing, yielding an encoded DAS password. The length is the number of coordinate pairs summing across all strokes [3].

Other Recall based schemes:

BDAS: BDAS (background image for Draw A Secret) is a panacea for weak DAS password. The background images in

this scheme reduced the amount of symmetry within password images and make users to choose longer passwords [8].

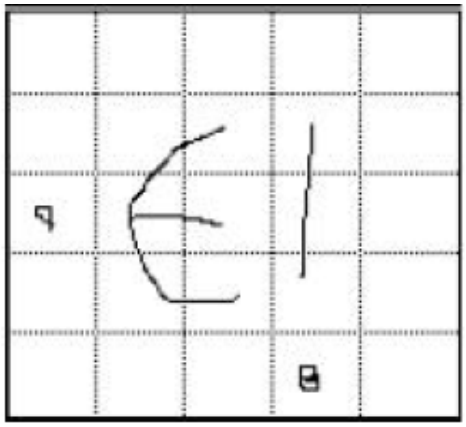

Figure 1: Draw A Secret

1.1.3 CUED Recall System: In cued recall scheme, users remember and then focus on specific location within the image. This system is also known as locimetric system which sometime also called as clicked based graphical password.

Real Time Application of Cued Recall System: Pass-Points
It again is a recall based method of authentication, with the twist that the image acts as a cue to assist with the task of recollection. This system effectively falls between a pure recognition based and a pure recall based system. To register with the system the user must select an image they wish to use and then select the points they wish to authenticate with. This again brings the issue of allowing user selection as it has been shown that here many users are inclined to choose images that they associate with. The other major issue is that the image must not be too cluttered or too sparse. The figure 2 shows the PassPoints password example where the 5 numbered boxes illustrate the tolerance area around click points [4].

Figure 2: PassPoints

1.2 CAPTCHA
Completely Automated Public Turing tests to tell Computers and Humans Apart abbreviated as CAPTCHA is a program that generates and grades tests that are human solvable, but beyond the capabilities of current computer programs. CAPTCHA is now almost a standard security mechanism for addressing undesirable or malicious Internet bot programs and major web sites such as Google, Yahoo and Microsoft all have their own CAPTCHAs. CAPTCHA is categorized into two: Text CAPTCHA which relies on character recognition and Image recognition CAPTCHA which deals with the recognition of non-character objects. It is used to prevent sensitive user inputs on an untrusted client which protects the communication channel between the user and web server from keyloggers. But it fails to work good in front of online dictionary attacks [6].

1.3 Captcha as a gRaphical Password (CaRP)

CaRP ia a new way to thwart a guessing attacks. In a guessing attack, a password guess tested in failed trial is determined wrong and excluded from subsequent trials. The number of undetermined password guesses decreases with more trials, leading to a better chance of finding the password [1]. Mathematically, let P be the set of password guesses before any trial, ρ be the password to find, A denote a attempts whereas An denote the n-th trial, and p(A = ρ) be the probability that ρ is tested in attempt A. Let Sn be the set of password guesses tested in trials up to An. The password guess to be tested in n-th attempt An is from set P|Sn−1, i.e., the relative complement of Sn−1 in P. If ρ ε P, then we have

$$p\,(A = \rho | A1 \mathrel{!}= \rho, \ldots, An-1 \mathrel{!}= \rho) > p(A = \rho) \qquad (1)$$

and

$$Sn \rightarrow P$$

$$p(A = \rho | A1 \_= \rho, \ldots, An-1 \_= \rho) \rightarrow 1 \quad \text{with } n \rightarrow |P| \qquad (2)$$

CaRP fallen for following two types of guessing attacks:

i. Automatic Guessing Attacks apply an automatic attempt and error process but P can be manually constructed.

ii. Human Guessing Attacks apply a manual attempt and error process. CaRP adopts a completely different approach to counter automatic guessing attacks. It aims at realizing the following equation in an automatic guessing attack.

$$p(A = \rho | A1, \ldots, An-1) = p(A = \rho), \forall n \qquad (3)$$

Eq. (3) means that each attempt is computationally independent of other attempt. Specifically, no matter how many attempts run previously, the chance of finding the password in the current attempt always remains the same. That is, a password in P can be found only probabilistically by automatic guessing (including brute-force) attacks, in contrast to existing graphical password schemes where a password can be found within a fixed number of trials.

1.3.1 Recognition based CaRP: In this system, infinite number of visual objects can be accessed as a password. Sequences of alphanumeric visual objects are also used in this system. ClickText, ClickAnimal, AnimalGrid are the 3 techniques used in CaRP [1]. ClickText is a noval technology for text CAPTCHA where characters can be arranged randomly on 2D space. It is different from text CAPTCHA challenge which is generally ordered from left to right

sequence and user has to enter the data in that way. In ClickText, user click on the image which contains number of alphanumeric characters generated by CAPTCHA engine and user has to enter the password in same order. ClickAnimal: This technology uses 3D models of animals to generate 2D animals with different textures, colors. It is a recognition based CaRP scheme developed on the top of Captcha Zoo. AnimalGrid: It is a combination of Click A Secret (CAS) and ClickAnimal. In this system, firstly ClickAnimal image is displayed, after the animal is selected, an image of n*n grid appears.

1.3.2 Recognition Recall CaRP: In this system, password is a sequence of some invariants points of objects. An invariant points of object is a point that has a fixed relative value in different fonts. User must identify the object image and then use identified objects as a cues to locate a password within a tolerance range. TextPoints and TextPoint4CR techniques are used in recognition recall CaRP [1].

(a) TextPoints: In TextPoints characters contain invariant points which offer a strong cue to memorize and locate its invariant points. A point is said to be an internal point of an object if its distance to the closest boundary of the object exceeds a threshold. A set of internal invariant points of characters is selected to form a set of clickable points for TextPoints. A password is a sequence of clickable points. A character can typically contribute multiple clickable points. Therefore TextPoints has a much larger password space than ClickText. For challenge-response authentication protocol, a response is sent to the authentication server.

(b) TextPoint4CR: TextPoints can be modified to fit challenge-response authentication. This modification is called TextPoints for Challenge-Response or TextPoints4CR. Unlike TextPoints wherein the authentication server stores a salt and a password hash value for each account, the server in TextPoints4CR stores the password for each account. Another difference is that each character appears only once in a TextPoints4CR image but may appear multiple times in a TextPoints image. This is because both server and client in TextPoints4CR should generate the same sequence of discretized grid-cells independently.

2. Proposed System

The proposed system consists of mainly three different models that are user, server and trusted authority manager as shown in figure 3.

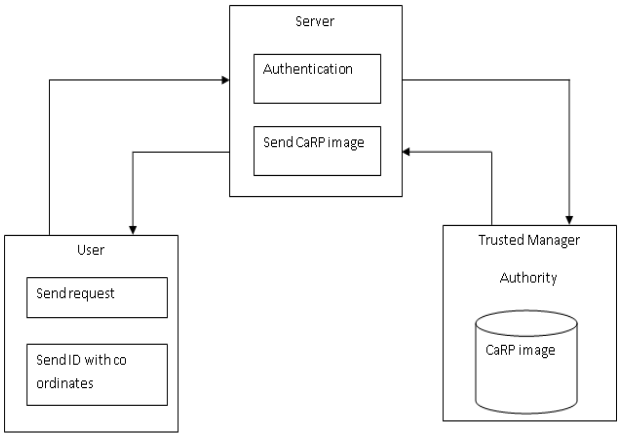

Figure 3: System Architecture

User sends authentication request to the server with visual object IDs or clickable points of visual objects that user selects. Server request for the CaRP image through Trusted Authority Manager and records the location of the object from the image and sends that image to the user. Server calculates the coordinates sent by the user and authentication successes if the value matches.

3. Conclusion and Future Work

Captcha as a graphical password introduces new family of graphical password which acts as a firewall for online guessing attacks. This new security measure works efficiently on unsolved hard AI problems. It is resistant to captcha relay attack and shoulder surfing attack. A password of CaRP can only be recognized through brute force attack. It can be improved with the use of images of different levels of difficulty based on login history of user. Further the usability of CaRP image is improved through images of different level of hardness based on log in history of the user and the machine used for the log in purpose.

Acknowledgement

I would like to thank my guide Dr. P. K. Deshmukh for his help and guidance throughout this project and the semester, without him this would not have been possible.

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 891
[2] 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.
[3] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, “The design and analysis of graphical passwords,” in Proc. 8th USENIX SecuritySymp., 1999, pp. 1–15.
[4] 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.
[5] M. Alsaleh, M. Mannan, and P. C. van Oorschot, "Revisiting defenses against large-scale online password guessing attacks," IEEE Trans. Dependable Secure Comput., vol. 9, no. 1, pp. 128–141, Jan./Feb. 2012.
[6] 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.
[7] B. Pinkas and T. Sander, "Securing passwords against dictionary attacks," in Proc. ACM CCS, 2002, pp. 161–170.
[8] P. Dunphy and J. Yan, "Do background images improve 'Draw a Secret' graphical passwords," in Proc. ACM CCS, 2007, pp. 1–12.

Author Profile

Nayan R. Gawande, have completed Bachelor of Engineering in Information Technology from K. J. Somaiya College of Engineering, Mumbai in 2012. She has passed Bachelor of Engineering with first class. Currently, she is pursuing Masters of Engineering in Computer Science and Engineering from J.S.P.M`s Rajarshi Shahu College Of Engineering, Tathawade, Pune. She is doing research on "How to use CAPTCHA with Graphical Password for enhancement in security on NP hard problems in Artificial Intelligence.