MJRET
Open Access
Multidisciplinary Journal of Research in Engineering and Technology
Journal homepage: www.mjret.in
ISSN:2348 - 6953

GRAPHICAL PASSWORDS FOR PROVIDING A NEW SECURITY PRIMITIVE

Abhijit Nawale, Sujeet Somwanshi, Ajay Thorat, Sandesh Bharati
Department of Computer Engineering,JSPM's ICOER
Pune, India
abhijit.nawale@gmail.com, sujeetsomwanshi@gmail.com

Abstract: *CAPTCHA (Completely Automated Public Turing Test to distinguish between computers and human) is a computer program which humans can pass but computer programs cannot pass. A new technology is built over the captcha called graphical captcha which eliminates dictionary attacks and hence more secure. With the hybrid use of CAPTCHA and graphical password, one can address a number of security problems such as relay attack and online guessing attacks. Shoulder surfing attacks can also be addressed with the help of dual view technology. CaRP (Captcha as a graphical password) is not a cure all to all attacks but it stipulates security and usability to legitimate and authenticated users in real time applications. In the proposed concept, we present exemplary CaRPs built on both text Captcha and image-recognition Captcha. A user selects random and difficult images as passwords for reducing the guessing attack.*

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

1. INTRODUCTION

First time CAPTCHA was invented in 2000 at Carnegie Mellon University by John Langford, Nicholas J. Hooper and Luis Von Ahn. CAPTCHA is an acronym for “Completely Automated Public Turning Test to tell Computers and Humans Apart”. There are too many malicious threats across the Internet which may compromise your system in the absence of any secure application which provides protection against such threats. One such threat is the Bot. A Bot is a malicious program which has the capability to run automated tasks over the network and thus creating problem in the network. CAPTCHA is one such shield which can be used as a protection from these malicious programs such as Bot.
Authentication is a very necessary task in security where we use text password as a security technique. But text passwords are easy to break 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 surfing attack[1][2]. Nowadays, advanced technologies make use of Graphical Password, CAPTCHA, CaRP (Captcha as a Graphical Password) for authentication and security purpose [3].

Some types of CAPTCHAs are given below:

i. CAPTCHAs based on text.
ii. CAPTCHAs based on image.
iii. CAPTCHAs based on audio.
iv. CAPTCHAs based on video.

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 resistant to dictionary attacks but are prune to shoulder surfing attacks. Graphical password can be classified into three types based on memo ability of the user: RECOGNITION, RECALL, CUED RECALL [2].

1.1.1 Recognition based system

It is also known as search metric systems which generally requires user to memorize a portfolio of images during password creation and then identify their images from among many random images 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 five faces from a large database of available choices. When a user wishes to authenticate themselves they are presented with an array of twelve faces, arranged in four rows of four. One of the faces is part of the user's password while the other eleven are wrong. 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 five 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 draw metric 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 attack 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

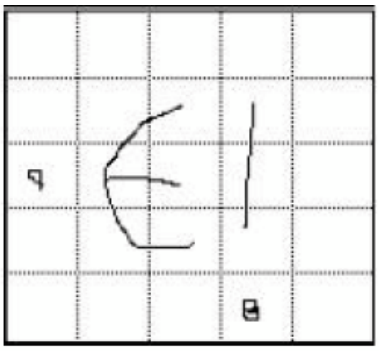

Fig.1: Draw A Secret

In this system, users draw their password on a 2D grid using a stylus or mouse (Fig.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 reduce the amount of symmetry within password images and make users to choose longer passwords [8].

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 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 Pass-Points password example where the 5 numbered boxes illustrate the tolerance area around click points [4].

Fig.2: Pass-Points

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 a distrusted client which protects the communication channel between the user and web server from key loggers. But it fails to work well in front of online dictionary attacks [6].

1.3.1 Existing system

Alpha-numeric passwords were first introduced in the 1960s as a solution to security issues that became evident as the first multi-user operating systems were being developed. As the name indicates, an alpha-numeric password is simply a string of letters and digits. Although almost any string can serve as a password, these passwords only offer good security as long as they are complicated enough so that they cannot be deduced or guessed. Commonly used guidelines for alpha-numeric passwords are:

The password should be at least 8 characters long. The password should not be easy to relate to the user (e.g., last name, birthdate). The password should not be a word that can be found in a dictionary or public directory. Ideally, the user should combine upper and lower case letters and digits. Since the best password would be a completely random one, people have devised ways to create pseudo-random passwords. One such method is to take a common word and perform certain actions on it. Using the word Dinosaur as an example, users often create passwords such as DiNoSaUr (by alternating upper and lower case), rUaSoNiD (by reversing the string), oSNaiUDr (by shuffling the string), D9n6s7u3 (combining numbers and letters). However, the better the password is, the harder it is to remember.

The most common computer authentication method is to use alphanumerical usernames and passwords, it provides the basis for access control and user accountability they are versatile and easy to implement and use. Alphanumerical passwords are required to satisfy two contradictory requirements. They have to be easily remembered by a user, while they have to be hard to guess by impostor. Users are known to choose easily guessable and/or short text passwords.

1.3.2 Drawbacks

Drawback of alpha-numeric password is the dictionary attack. Because of the difficulty in remembering random strings of characters, most users tend to choose a common word, or a name. Unfortunately, there are several tools that allow an individual to crack passwords by

automatically testing all the words that occur in dictionaries or public directories. This attack will usually not uncover the password of a predetermined user; but studies have shown that this attack is usually successful in finding valid passwords of some users of a given system.

In existing system, password is mostly of text oriented. So the password can be broken by intruders by masquerading, brute force attack, dictionary attack etc. There are some application existing with graphical passwords, their major drawback is larger memory space. Some have prone to shoulder surfing attack.

In Cued Click Point, the user has to select click point in five different images in sequence based on the previous image. The drawback of the concept is it is difficult to remember the click points in different images.

1.3 Captcha as a gRaphical Password (CaRP)

CaRP is a new way to thwart 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 guessing the password [1]. Mathematically, let P be the set of password guesses before any trial, ρ be the password to find, A denote the 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

$$p\,(A = \rho | A1 != \rho, \ldots, An-1 != \rho) > p(A = \rho) \quad \ldots\ldots\ldots\ldots\ldots\ldots (i)$$

and

$Sn \rightarrow P$

$$p(A = \rho | A1\_ = \rho, \ldots, An-1\_ = \rho) \rightarrow 1 \; with\, n \rightarrow |P| \quad \ldots\ldots\ldots\ldots\ldots (ii)$$

CaRP falls 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.

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

Eq.(iii) 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].

i. **ClickText:** 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.

ii. **ClickAnimal:** This technology uses 3D models of animals to generate 2D animals with different textures, colors. These 2D animals as a result are then arraned on a background which is clustered. Some animals may be obstructed by other animals in the image but their essential parts are not obstructed so as to identify by the humans. It is a recognition based CaRP scheme developed on the top of Captcha Zoo.

iii. **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 point 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 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 discreet 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 Fig.3.

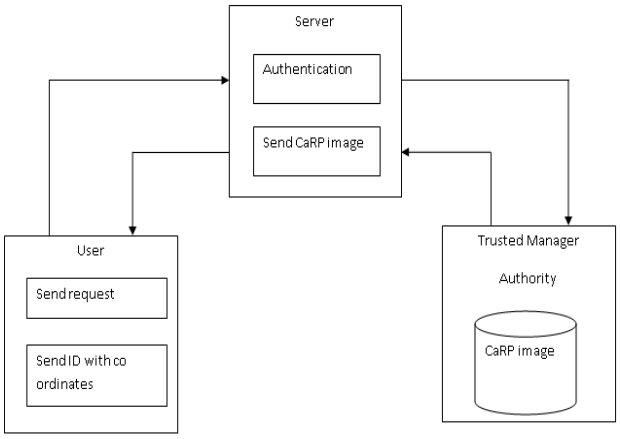

Fig.3: System Architecture

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.

2.1 Main Modules

Implementation is the stage of the project when the theoretical design is turned out into a working system. The important module in proposed system is as follows:

2.1.1 Graphical Password

In this module, Users are having authentication and security to access the detail which is presented in the Image system. Before accessing or searching the details user should have the account in that otherwise they should register first.

2.1.2. Captcha in Authentication

Captcha-based Password Authentication (CbPA) protocol uses captcha and password in user authentication protocol. The CbPA-protocol requires solving a Captcha challenge after inputting a valid pair of user ID and password unless a valid browser cookie is received. For an invalid pair of user ID and password, the user has a certain probability to solve a Captcha challenge before being denied access.

2.1.3 Thwart Guessing Attacks

In a guessing attack, a password guess tested in an unsuccessful 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. To counter

guessing attacks, traditional approaches in designing graphical passwords aim at increasing the effective password space to make passwords harder to guess and thus require more trials. No matter how secure a graphical password scheme is, the password can always be found by a brute force attack. In this paper, we distinguish two types of guessing attacks: automatic guessing attacks apply an automatic trial and error process but S can be manually constructed whereas human guessing attacks apply a manual trial and error process.

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 Prof. Nilesh Sable for his help and guidance in this project, 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.