International Journal of Engineering Research and General Science Volume 4, Issue 1, January-February, 2016
ISSN 2091-2730

Graphical Password Scheme: CAPTCHA

Sonali S. Pawar , Prof. Pravin P. Kalyankar

Computer Science and Engineering, Dr. B.A.M.University, Aurangabad
e-mail: sonali.pawar052@gmail.com
Contact No. :9665144137

Abstract- Today's, Many security primitives are used for secure user authentication which are mostly based on hard mathematical problems. Using hard AI problems for security is emerging as a new paradigm, but has been underexplored. Captcha as graphical passwords (CaRP) is one of the new security primitive based on hard AI problems which is a novel family of graphical password systems built on Captcha technology. As its name implies that CaRP is the combination of both CAPTCHA and Graphical password scheme. CaRP addresses a number of security problems altogether, it offers reasonable security and usability with some practical applications for improving online security.

Keywords— *CaRP, gimpy, CAPTCHA, Pix ,bongo, graphical password, automated boats.*

I. Introduction

CAPTCHA(pronounced as cap-ch-uh) which stands for ―Completely Automated Public Turing test to tell Computers and Humans Apart". CaRP addresses a number of security problems altogether, such as online guessing attacks, relay attacks, shoulder-surfing attacks etc. CaRP password can be found by guessing it in search set from dictionary. A Fundamental task in security is to create cryptographic primitives based on hard mathematical problems that are computationally intractable. This can be achieved by using graphical passwords along with CAPTCHA. The term Captcha was coined in 2000 by Luis Von Ahn, ManuelBlum, Nicholas J. Hopper It is the word verification test to ensure that the response is only generated by humans and not by a computer .It is mainly used to prevent automated software's (bots) from performing actions on behalf of actual humans. Generally text passwords have been widely used for user authentication, however it is seen that text passwords are insecure for variety of reasons.

As compared to textual passwords ,graphical password schemes are believed to be more secure and more resilient to dictionary attacks. Text Passwords can be found within a fixed number of trials.Captcha is now a standard Internet security technique to protect online email and other services from being abused by bots. The main goal of Captcha is to put forth a test which is simple and straight forward for any human to answer but for a computer it is almost impossible to solve. Usually this test is conducted at the end of a sign up form while signing up for Gmail or Yahoo account. For example free web based e-mail services allow people to create an account free of charge.

II. Materials and methods

A. A Way to Avoid Guessing Attacks

In a guessing attack, number of trials are attempted to enter an password ,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. Mathematically, let G be the set of password guesses before any trial, p be the password to find, T denote the probability that p is tested in trial T. Let I_n be the set of password guesses tested in trials up to (including) T_n. The password guess to be tested in n-th trial T_n is from set $G \backslash I_{n-1}$, i.e., the relative complement of I_{n-1} in G. If $p \in G$, then we have

$$p\,(T = p \mid T_1 \neq p, \ldots, T_{n-1} \neq p) > p(T = p), \qquad (1)$$

and

$$\left.\begin{array}{l} I_n \rightarrow G \\ p(T = pT_1 \neq p, \ldots, T_{n-1} \neq p) \rightarrow 1 \end{array}\right\} \text{with } n \rightarrow |G|, \qquad (2)$$

where $|G|$ denotes the cardinality of G. From Eq. (2), the password is always found within $|G|$ trials if it is in G; otherwise G is exhausted after $|G|$ trials. Each trial determines if the tested password guess is the actual password or not, and the trial's result is deterministic.

B. Main Modules

- ***Graphical Password*** :

In this module, Users are having authentication and security to access the detail which is presented in the Image system. User must have to register first to access or search the details, user should have the account in that.

- ***Captica in Authentication****:*

It is efficient to use both Captcha and password in a user authentication protocol, which we call *Captcha-based Password Authentication (CbPA) protocol*, to counter online dictionary attacks after inputting a valid pair of user ID and password, The CbPA-protocol in requires solving a Captcha challenge unless a valid browser cookie is received. For an invalid pair of user ID and password the user being denied access. For this reason user has to cross the challenge of Captcha on or before accessing or searching of some data.

- ***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.

- ***Security Of Underlying Captcha*****:**

CaRP is Computational intractable in recognizing objects in CaRP images. It is Fundamental to CaRP. It is also necessary to provide security for Captcha, existing analyses on Captcha security were mostly case by case or used an approximate process. No theoretic security model has been established yet. Generally Object segmentation is used for this purpose but it is also considered as a computationally expensive, combinatorially-hard problem, which modern text Captcha schemes rely on.

III. OVERVIEW OF THE TECHNIQUE

There are different types of Captcha depending on the form in which they are presented to the user. The main point to be considered is the pattern in Captcha, it can be Textual Captcha and Graphical Captcha.

- ***Text Based Captcha***

These types of Captcha are simple to implement. This Captcha presents some queries to the user whose answers are only given by users and not by computers or any machines. Examples of such questions are:

1. What are twenty minus three?
2. What is the third letter in UNIVERSITY?
3. Which of Yellow, Thursday and Richard is a color?
4. If yesterday was a Sunday, what is today?

Such type of questions can be answered only by humans, which ensures that no computer program or any boat access them. Other text CAPTCHAs involves text distortions and the user is asked to identify the text hidden. The various implementations are:

a. *Gimpy and Ez-Gimpy*

Gimpy presents a set of words which belongs to dictionary, and displaying them in a distorted and overlapped manner. Gimpy then asks the users to enter a subset of the words in the image. Only human user is capable of identifying the words correctly, whereas a computer program cannot.

Ez-Gimpy is same as Gimpy Captcha,Whereas Ez – Gimpy randomly picks a single word from a dictionary and applies distortion to the text. The user is then asked to identify the text correctly. These two types are adopted by Yahoo in their signup page.

b. *Baffle Text*

This technique overcomes the drawback of Gimpy CAPTCHA because, Gimpy uses dictionary words and hence, clever bots could be designed to check the dictionary for the matching word by brute-force. This is a variation of the Gimpy. This doesn‘t contain

dictionary words, but it picks up random alphabets to create a nonsense but pronounceable text. Distortions are then added to this text and the user is challenged to guess the right word.

- ***Graphical Captcha***

These Captchas includes some sort of pictures or objects with some properties or characteristics that the user have to guess.

a. PIX

PIX is a program that has a large database of labelled images. All of these images are pictures of concrete objects (a horse, a table, a house, a flower). The program picks an object at random, finds six images of that object from its database, presents them to the user and then asks the question "what are these pictures of?" Current computer programs should not be able to answer this question, so PIX should be a CAPTCHA.

b. BONGO

BONGO asks the user to solve a visual pattern recognition problem. It displays two series of blocks, the left and the right. The blocks in the left series differ from those in the right, and the user must find the characteristic that sets them apart.

- **Audio CAPTCHAs**

The Audio Captcha is based on sound. The program picks a word or a sequence of numbers at random, renders the word or the numbers into a sound clip and distorts the sound clip; it then presents the distorted sound clip to the user and asks users to enter its contents. This CAPTCHA is based on the difference in ability between humans and computers in recognizing spoken language. The idea is that a human is able to efficiently disregard the distortion and interpret the characters being read out while software would struggle with the distortion being applied, and need to be effective at speech to text translation in order to be successful.

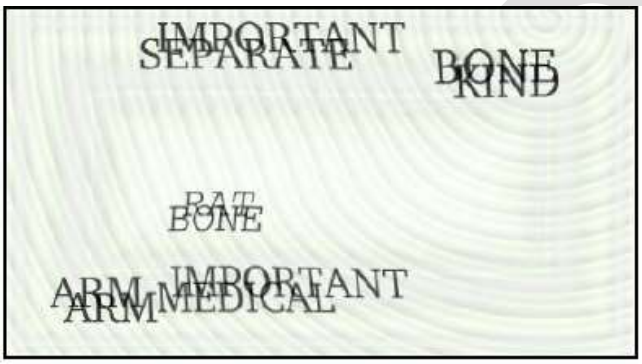

Fig.1 Gimpy Captcha

Fig.2 ez-gimpy captcha

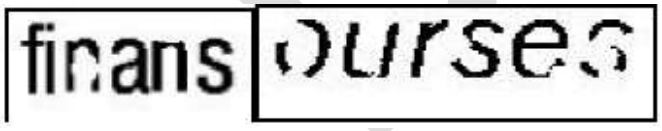

Fig. 3 baffle text captcha.

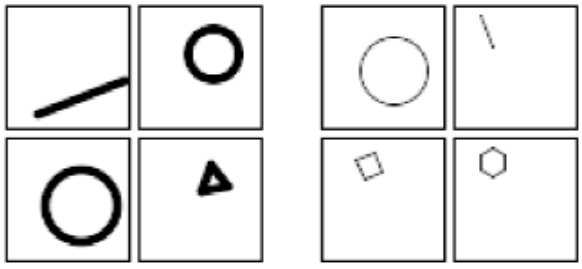

Fig.4 Bongo Captcha

IV. APPLICATIONS

- ***SECURE WEBSITE REGISTRATION.***

Many companies like Yahoo!, Microsoft, etc. offer free email services. Most of these services are not secured as they are suffered from attacks called as bots which leads to sign up for thousands of email accounts every minute. It is not sure that account is created by human; Captchas provides the solution to this problem to ensure that only humans can create their accounts and obtain free accounts.

- ***Protecting Email Addresses From Scrapers.***

Captchas provides the facility in which you can hide your email address from web scrapers. The idea is to require users to solve a CAPTCHA before showing your email address. It is an effective mechanism to protect your email address and its abuse.

- ***Online Polls.***

Now a day, many reality programs are taking their decisions depending on the audience choice. For this reason their votes are collected online. As is the case with most online polls, IP addresses of voters were recorded in order to prevent single users from voting more than once. However, some of people found a way to stuff the ballots using programs that voted for one thousands of times. One of them score started growing rapidly. The next day, another person wrote their own program and the poll became a contest between voting one person and another one. Can the result of any online poll be trusted? Not unless the poll ensures that only humans can vote.

- ***Dictionary Attacks.***

In general password system like text based passwords Dictionary attacks are made to guess the password. CAPTCHAs are used to prevent dictionary attacks in password systems. The idea is simple: prevent a computer from being able to iterate through the entire space of passwords by requiring it to solve a CAPTCHA after a certain number of unsuccessful logins. This is better than the classic approach of locking an account after a sequence of unsuccessful logins, since doing so allows an attacker to lock accounts at will.

- ***Preventing Search Engine from Bots***

Indexed webpages can found easily, however It is sometimes desirable to keep webpages unindexed to prevent others from finding them easily. Search engines bots can be prevented from reading web pages by an html tag. It may work sometimes but not sure that bots won't read a web page. Search engine bots, usually belong to large companies, respect web pages that don't want to allow them in. In this case CAPTCHAs are needed to guarantee that bots won't enter a web site.

- ***Worms and Spam.***

CAPTCHAs also offer a plausible solution against email worms and spam. It means that they will accept the emails only if the email is sent bu human and not by any automated software. This idea is now used by many companies.

V. Conclusion

- It offers reasonable security and usability and appears to fit well with some practical applications for improving online security.
- This threat is widespread and considered as a top cyber security risk. Defense against online dictionary attacks is a more subtle problem thanit might appear.
- This paradigm has achieved just a limited success as compared with the cryptographic primitives based on hard math problems and their wide applications.
- Using hard AI (Artificial Intelligence) problems for security, initially proposed in [17], is an exciting new paradigm. Under this paradigm, the most notable primitive invented is Captcha, which distinguishes human users from computers by presenting a challenge.
- CaRP also offers protection against relay attacks, an increasing threat to bypass Captchas protection. Captcha can be circumvented through relay attacks whereby Captcha challenges are relayed to human solvers, whose answers are fed back to the targeted application. Our future work concentrates on improving the login time and memorability.

REFERENCES:

[1]Bin B. Zhu, Jeff Yan, GuanboBao, Maowei Yang, and NingXu_, ―Captcha as graphical Passwords—A New Security Primitive Based on Hard AI Problems‖IEEE RANSACTION SON INFORMATION ORENSICS AND SECURITY, VOL. 9, NO. 6, JUNE 2014.

[2] Luis von Ahn, Manuel Blum and John Langford.Telling Humans and Computers Apart (Automatically) or How Lazy Cryptographers do AI. To appear in Communications of the ACM.

[3] R. Dhamija and A. Perrig, Deja Vu: A User Study Using Images for Authentication. In the 9th USENIX Security Symposium, 2000.

[4] J. Yan and A. S. El Ahmad. Usability of CAPTCHAs or usability issues in CAPTCHA design. In SOUPS _08, pages 44–52, New York, NY, USA, 2008..ACM.

[5] Greg Mori and Jitendra Malik.Breaking a Visual CAPTCHA. Unpublished Manuscript, 2002.

[6] K. Barnard, P. Duygulu, D. Forsyth, N. de Freitas, D. Blei, and M. Jordan. Match-ing words and pictures. Special Issue on Text and Images, Journal of Machine Learning Research, 3:1107{1135, 2002.

[7] Pdictionary. The internet picture dictionary. http://www.pdictionary.com, 2004.