AUTHORIZATION USING CAPTCHA AS GRAPHICAL PASSWORD

[1]S.A. GULAVE, [2]S.G. MUNGAL, [3]N.B. DHAWALE, [4]S.S. CHAVAN

[1,2,3,4]Final year Students of Computer Science Engineering, Sanjivani College of Engineering, Kopargaon, SavitribaiPhule Pune University
E-mail: [1]sonaligulave9@gmail.com, [2]mungal.shraddha12@gmail.com,
[3]nayanabd1994@gmail.com, [4]swap9021@gmail.com

Abstract- Many security problems are based mainly on hard mathematical problems. Using hard AI problems for security is appearing as new sample but has been in under-development. In this paper we present a new security scheme known as Captcha as gRaphical Password (CaRP). This scheme is concept of Graphical Password built on top of Captcha. CaRP addresses number of security problems such as guessing attacks, relay attacks, and many more such security problems. CaRP also addresses a well-known problem of graphical password such as image hotspot. CaRP fits well with some practical applications to improve online security.

Keywords- Captcha,Carp, Dictionary Attack, Graphical Password, Password, Password Guessing Attack.

I. INTRODUCTION

CAPTCHA(Completely Automated Public Turing test to tell Computers and Humans Apart) is scheme which is used to differentiate humans from bots by presenting a challenge e.g. a puzzle which is hard to solve for computer programs but are easy for humans. Many security schemes are relying on hard mathematical problems.

Hard AI (Artificial Intelligence) technique to solve security problems is initially introduced in [1]. Under this Captcha is first invented. In this paper we present the new security scheme known as Captcha as gRaphical Passwords (CaRP). CaRP is a combination of two schemes or technologies which are Captcha and Graphical Passwords.

CaRP is new security scheme which is typically built on Captcha technology. It overcomes number of security problems such as online guessing attacks, relay attacks etc. CaRP also address the image hotspot problem. CaRP uses sequence of clicks on generated image to obtain the user's password. For every login attempt a new CaRP image is get generated. In this we are going to use three sub-techniques from which one is text based where text character based image is get generated and instead of entering password through keyboard user has to enter his or her password through sequence of clicks on generated text based image.

II. RELATED WORK

[A] Graphical Passwords:

A graphical password is an authentication system that works by having the user select from images, in a specific order, presented in graphical user interface (GUI). For this reason a graphical-password approach is sometimes called as graphical user authentication (GUA). A graphical password is easier than text-based password for most people to remember. Graphical passwords may offer better security than text-based passwords because many people, in an attempt to memorize text-based passwords, use plain words (rather than the recommended jumble of characters). A dictionary search can often hit on a password and allow a hacker to gain entry into a system in seconds. But if a series of selectable images is used on successive screen pages, and if there are many images on each page, a hacker must try every possible combination at random. If there are 100 images on each of the 8 pages in an 8-image password, there are 100^8, or 10 quadrillion (10,000,000,000,000,000), possible combinations that could form the graphical password! If the system has a built-in delay of only 0.1 second following the selection of each image until the presentation of the next page, it would take (on average) millions of years to break into the system by hitting it with random image sequences. There are three categories of graphical password based upon their task involved in memorizing and entering the password. They are recognition, recall and cued recall.

A *recognition-based* scheme usually asks users to memorize a portfolio of images during password creation, and then recognize their images from among inducement. It uses different types of images such as faces, unsystematic art, everyday objects etc. In this Passfaces [7] is commonly used technique. In this scheme user selects portfolio of faces from database to create password. During authentication, a sequence of candidate faces is presented for the user to select the face belonging to her portfolio of password. This process is repeated several times, each time with a different panel. A successful login requires correct selection in each time. The set of images in each round or panel remains same but they are shuffled.

A *recall-based* scheme requires a user to regenerate the same interaction result without cueing. Recall – based scheme includes Draw-A-Secrete (DAS) scheme in which user has to draw his/her password on a 2D grid. Then system encodes the grid cells as a password. Pass-Go is another scheme under recall-based scheme. Pass-Go scheme improves the usability of DAS. In Pass-Go scheme, system

encodes the grid intersections instead of encoding grid cells. BDAS scheme also comes under recall-based scheme. In BDAS, background images get added to DAS scheme in order to create more complex passwords.

Now, the remaining category of graphical passwords is *cued-recall*in which a cue is getting provided to remember and enter a correct password. Pass Points [6] is scheme under cued-recall scheme in which a sequence of points are clicked anywhere on an image. User has to remember these clicks and he/she has to re-click the same sequence at time of authentication. Cued Click Points (CCP) is another cued-recall scheme with use of one image per click.
If we compare three schemes then as per human memory, recognition is easiest but if we consider as security point of view, then recognition is weakest in guessing attacks. Typical recognition schemes stated above are having password range of 2^{13} to 2^{16} passwords. These many passwords had successfully hacked by using dictionary of 2^{31} to 2^{41} entries as per study[2].

[B] Captcha
A CAPTCHA ("**C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part") is a type of challenge-response test used in computing to determine whether or not the user is human.There are two types of captcha: text captcha and Image-Recognition Captcha(IRC). Text captcha based upon character recognition and IRC depends upon recognition of non character objects. Asirra[3] is technique belongs to IRC in which user is asked to identify all cats from panel of 12 images of cats and dogs.

[C] Captcha in Authentication
Captcha-based Password Authentication (CbPA) is a protocol in which password as well as captcha is used in user password authentication. It is required to solve captcha challenge after entering valid pair of user ID and password.

III. CAPTCHA AS GRAPHICAL PASSWORD

[A] A New Technique to Prevent Guessing Attacks
Here a legitimate users access rights to computer and network resources are compromised by identifying the user's ID/password combination of the legitimate user. Password guessing attacks can be classified into two types: Brute Force Attack and Dictionary Attacks. A Brute Force attack is a type of password guessing attack and it consists of trying every possible code, combination, or password until you find the correct one. This type of attack may take long time to identify password. A Dictionary Attack is another type of password guessing attack which uses a dictionary of common words to identify the user's password.

To prevent guessing attacks, one common approach is to design a graphical password of large password space. It makes hard to guess password and thus requires more number of trials. If we are designing a large password scheme then also they can be guess by Brute Force attack. CaRP adopts a totally different approach to prevent guessing attacks. It can be represented by following equation (1)[8]:

$$P(T=\rho \mid T1, \ldots, Tn-1) = p(T=\rho), \forall n \quad (1)$$

In this equation Tdenotes a trial, ρdenotes password to search, Tn denotes n-th trial, $p$denotes probability $p(T = \rho)$ be the probability that ρ is tested in trial T. Eq. (1) clearly says that there is no matter how many times you have trialed previously but the probability of finding password in current trial remains same. This feature makes it more efficient. Now question arise that how to implements this in our CaRP approach. We are going to produce a new image at each trialand images of different trial will be independent of each other. In this we are also going to observe ecosystem of user and we know that user enters password only during authentication and in guessing attacks, trials are executed automatically.

[B] CaRP: A Brief Introduction
The basic principle of CaRP is to produce a new image for every login attempt for same user. It uses **alphabet** of visual objects e.g. alphanumeric characters, similar animals to produce a new image which is again a captcha challenge. The major difference between CaRP image and Captcha image is that in CaRP, all visual objects of an alphabet should appear in image where there is not such compulsion in captcha.
According to memorization capacity of human, there are two major categories of CaRP scheme: Recognition and Recognition-recall which is totally new. Recognition-recall requires recognizing an image and using that object to enter a password. Recognition-recall is a scheme which combines advantages of both Recognition and of Cued recall scheme that is Recognition is easy for memorization and Cued recall having advantage of large password space.

[C]Authentication using CaRP
In Fig:1 the basic terminologies are as follows. The authentication server ***AS*** stores the salt value ***s*** that means any random value used with hash function and hash value $H(\rho, s)$where ρ is password of user. After receiving authentication request, ***AS*** generates CaRP image and presents it to user to click password. Then the coordinates of clicked points are get recorded and sent it to ***AS*** along with user ID. Then ***AS*** maps it onto CaRP image and recovers sequence of clickable points of visual objects ρ'. Then ***AS*** separates salt value from password and then calculates the hash value of ρ' and compares it with hash value stored for

that account. If both results get match then give access to account to user otherwise not.

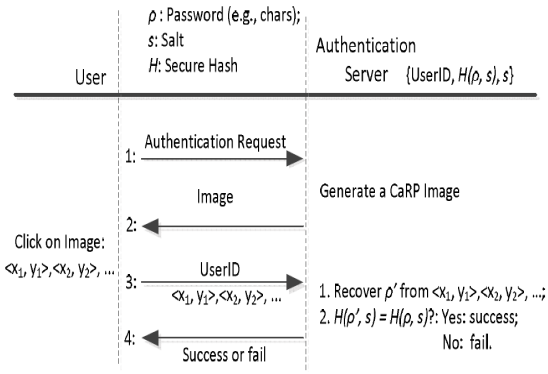

Fig. 1. Flowchart of basic CaRP authentication

IV. RECOGNITION-BASED CARP

In this section, we are going to see different schemes of *recognition-based* CaRP. There are two basic *recognition-based* schemes as explained in following sections and also some variations of these schemes.

[A] Click Text

It is very basic and simple CaRP *recognition-based* scheme and it is built on top of text captcha.In this scheme, one of the character should excluded which creates confusion e.g. letter 'O' and alphabet '0'. In this password is a sequence of alphanumeric characters like text captcha e.g. ***ρ="IN9DI8A"***.A Click Text image is generated by captcha engine same like a text captcha but **all alphanumeric characters should appear on image**. During generation of image, the location of all characters gets tracked to produce ground truth. In Click Text image, characters can be arranged randomly. Fig. (2) Shows a Click Text image of 33 characters.

Fig. 2.Click Text Image with 33 Characters

[B] Click Animal

We know that Captcha Zoo[4] is a scheme which uses a 3D model of horses and dogs to generate 2D animals with different color, size, and locations on disarranged background. User has to click on horses to pass test. Fig. 3 shows a sample image.

Fig. 3.Captcha Zoo with Circled Red

Click Animal is next recognition-based CaRP scheme built on Captcha Zoo[4] with alphabet of similar objects. Its password alphabet is of sequence of animal names. User has to select the animal names as password. 3D models are used to generate 2D animals and then these animals are gets arranged on a disarranged background. Fig. 4 indicates aClick Animal image with 10 animals.

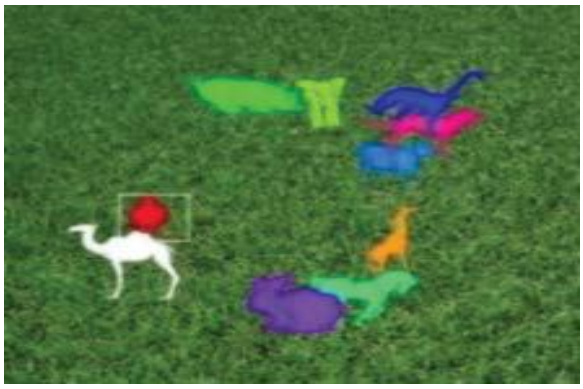

Fig. 4.A Click Animal Image

[C] Animal Grid

Since there is less number of similar animals as compared to number of available characters, the password space is less in Click Animal scheme. Therefore guessing attacks can easily break the password. And to make CaRP more secure, we need large password space also to resist attackers from guessing attacks. In order to increase the password range, it is necessary to combine it with some grid-based graphical passwords and select grid-size as per selected animal. As per DAS [5], we know that it is candidate but requires drawing on grid. To be uniform with Click Animal, we are going to change drawing with clicking. We are going to call it as Click-A-Secrete (CAS). In Animal Grid, we are going combine Click Animal with CAS to make Click Animal more efficient. Also we are going to design CaRP in such a way that the number of grid-cells will as much larger than alphabet size. At a time of designing this scheme, we are going to design it in such a way that, the user has to select correct animal in order to get correct animal grid. If user selects wrong animal then animal grid produced from it will also be wrong. If user is clicking on wrong grid

correctly then also password will be wrong and authentication gets failed.

At a time of authentication, user will get firstly a Click Animal image then he should select correct animal. After selecting correct animal, user will get an***n*n*** grid with size equaling the selected animal bounding rectangle for entering further password. After displaying Click Animal image, user has to select animal which comes first in his password. Then coordinates of clicked point are recorded and corresponding bounding rectangle is also we need to find interactively as shown in by white rectangle in Fig. 4.And then from next grid, he has to select remaining animals of his password. After selecting animal on Animal Grid and correspond remaining password, we need to record coordinates as e.g. "AP<x, y>, GP<x1,y1>, GP<x2,y2>,GP<x3,y3>,…"where, "AP<x, y>" denotes coordinates of point selected on Click Animal image and "GP<x, y>" denotes coordinates of points selected on grid imageand send it to authentication server for further process. At authentication server, using ground truth first animal is getting recovered and depending on bounding rectangle, grid image is regenerated and remaining password is recovered. Then hash value is gets calculated and compared it with stored hash value.

V. IMPLEMENTATION DETAILS

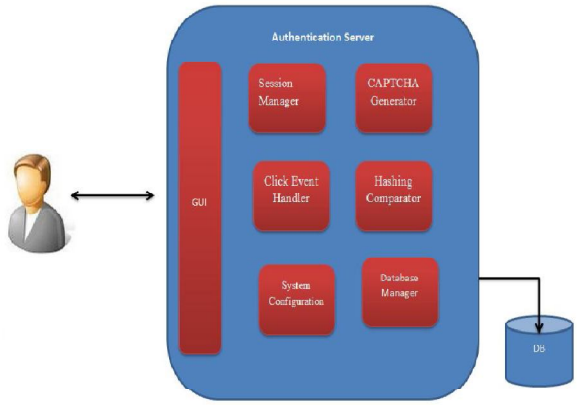

Fig.5. Architecture Diagram

In this section we are going to see that basic architecture of this whole CaRP scheme which we are going to implement. In further sub-sections we are going to see components of this architecture.

GUI:
This module contains RICH user interface. These are web-pages through which user can interact with system.

Click Event Handler:
As a part of password input, user will provide clicks on a captcha images. This module will care of all such events and covert them into <x,y> coordinates of shown images. This module will be always sync with captcha generator module.

Session Manager:
The term user session refers to a series of user application interactions that are tracked by the server. Here Sessions are used for maintaining user specific state, including persistent objects and authenticated user identities, among many interactions. This module will track the session of the user and responsible for generating and maintaining of per user session.

CAPTCHA Generator:
In this module the required CAPTCHA's will get generate. This module takes Strings as input and its goal is to generate images that are easy to understand for humans but impossible or at least very hard for a computer. This will be multi-threaded module which will support multiple requests at a time.

Hashing Comparator:
This module is used to generate the hash of the password stored in database. It also help to compare the hash encoded password coming from user and the one kept in database. Here SHA-256 hashing function will be used to generate the hash of passwords.

System Configuration:
This is system level configuration module which takes the responsibility to read, update the values. Like the username and passwords of database, number of sessions to handle at a time, number of database connections etc. will be stored here.

Database Manager:
This module Integrate with a backend such as databases. This provides reusable logic to interact with another system. All the database related activities like connect, disconnect, insert, select, update, delete are performed at here. All other modules take help of Database manager to connect to Database.

CONCLUSION

To overcome disadvantages of only text-based captcha, we introduced a new scheme known as CaRP which combines advantages of both captcha as well as graphical passwords. CaRP relies on unsolved hard AI problems. CaRP introduces CaRP image which is again a captcha challenge. It encounters various guessing attacks. This captcha challenge is used for every login attempt and also makes trials of guessing attacks computationallyindependent of each other. CaRP can also help to reduce the spam emails.

REFERENCES

[1] 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.

[2] P. C. van Oorschot and J. Thorpe, "On predictive models and user drawn graphical passwords," *ACM Trans. Inf. Syst. Security*, vol. 10,no. 4, pp. 1–33, 2008.

[3] J. Elson, J. R. Douceur, J. Howell, and J. Saul, "Asirra: A CAPTCHA that exploits interest aligned manual image categorization," in *Proc.ACM CCS*, 2007, pp. 366–374.

[4] R. Lin, S.-Y. Huang, G. B. Bell, and Y.-K.Lee, "A new CAPTCHAinterface design for mobile devices," in *Proc. 12th Austral. User Inter.Conf.*, 2011, pp. 3–8.

[5] 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.

[6] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon,"PassPoints: Design and longitudinal evaluation of a graphical passwordsystem," *Int. J. HCI*, vol. 63, pp. 102–127, Jul. 2005.

[7] (2012, Feb.). *The Science Behind Passfaces* [Online]. Available:http://www.realuser.com/published/ScienceBehindPassfaces.pdf

[8] Bin B. Zhu, Jeff Yan, GuanboBao, Maowei Yang, and NingXu"Captcha as Graphical Passwords-A New SecurityPrimitive Based on Hard AI Problems," in IEEE Transactions On Information Forensics And Security,vol. 9, No. 6, June 2014.

★★★