Prevention Of Brute Force Attack Using CAPTCHA And PGRP

[1] Sathya.S,[2] Lavanya.M
[1] II nd M.E (CSE), Department of Computer Science,
[2] IInd M.E(CSE), Department of Computer Science, Oxford
Engineering College, Trichy-9.
[1]sathyasubban@gmail.com,[2]lavanya.oec@gmail.com

Abstract- **Textual passwords are the most common method used for authentication. But textual passwords are vulnerable to eves dropping, dictionary attacks, social engineering and shoulder surfing. New security primitive based on hard AI problems, namely, a novel family of graphical password systems built on top of Captcha technology, which call Captcha as graphical passwords (CaRP). CaRP is both a Captcha and a graphical password scheme. CaRP also offers a novel approach to address the well- known image hotspot problem in popular graphical password systems, such as Pass Points, that often leads to weak password choices. CaRP is not a panacea, but it offers reasonable security and usability and appears to fit well with some practical applications for improving online security and also implement for Text can be combined with images or colors to generate session passwords for authentication. Session passwords can be used only once and every time a new password is generated. The two techniques are proposed to generate session passwords using text and colours which are resistant to shoulder surfing, and also implement PGRP protocol for prevent any vulnerable attackers.**

Key Terms: **Captcha as Graphical Password (CaRp) , Artificial Intelligence (AI) , Password guessing Resistance Protocol (PGRP).**

INTRODUCTION

Authentication is one of the five pillars of information assurance (IA) Computer security depends largely on passwords to authenticate human users. However, users have difficulty remembering passwords over time if they choose a secure password, i.e. a password is long and random. Therefore, the users tend to choose short and insecure passwords. Graphical passwords, which consist of clicking on images rather than typing alphanumeric strings, may help to overcome the problem of creating secure and memorable passwords. Authentication is the act of confirming the truth of an attribute of a datum or entity. This might involve confirming the identity of a person or software program, tracing the origins of an artifact, or ensuring that a product is what it’s packaging and labeling claims to be. In art, antiques, and anthropology, a common problem is verifying that a person has the said identity, or a given artifact was produced by a certain person or was produced in a certain place or period of history.

Introduced the topic with graphical password is an authentication system that works by having the user select from images, in a specific order, presented in a graphical user interface. For this reason, the graphical-password approach is sometimes called Graphical User Authentication (GUA). A graphical password is easier than a text-based password for most people to remember. Suppose an 8-character password is necessary to gain entry into a particular computer network. Instead of w8KiJ72c, for example, a user might select images of the earth (from among a screen full of real and fictitious planets), the country of France (from a map of the world), the city of Nice (from a map of France), a white stucco house with arched doorways and red tiles on the roof, a green plastic cooler with a white lid, a package of Gouda cheese, a bottle of grape juice, and a pink paper cup with little green stars around its upper edge and three red bands around the middle.

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 8image 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. Human factors are often considered the weakest link in a computer security system. Patrick et al. Point out that there are three major areas where human computer interaction is important: authentication, security operations, and developing secure systems. The most common computer authentication method is for a user to submit a user name and a text password.

The alternative technique is used in this project, using pictures as passwords. Graphical password schemes have been proposed as a possible alternative to text- based schemes, motivated partially by the fact that humans can remember pictures better than text, psychological studies supports such assumption. Pictures are generally easier to be remembered or recognized than text. In addition, if the number of possible pictures is sufficiently large, the possible password space of a graphical password scheme may exceed that of text based schemes and thus presumably offer better resistance to dictionary attacks.

SYSTEM OVERVIEW-OUTLINE OF THE APPROACH

Password is a sequence of some invariant points of objects. An invariant point of an object is a point that has a fixed relative position in different incarnations of the object, and thus can be uniquely identified by humans no matter how the object appears in CaRP images. To enter a password, a user must identify the objects in a CaRP image, and then use the identified objects as cues to locate and click the invariant points matching her password. Each password point has a tolerance range that a click within the tolerance range is acceptable as the password point.

CaRP is click-based graphical passwords, where a sequence of clicks on an image is used to derive a password. Unlike other click-based graphical passwords, images used in CaRP are Captcha challenges, and a new CaRP image is generated for every login attempt. The notion of CaRP is simple but generic. CaRP can have multiple instantiations. In theory, any Captcha scheme relying on multiple object classification can be converted to a CaRPscheme. To present exemplary CaRPs built on both text Captcha and image-recognition Captcha. One of them is a text CaRP wherein a password is a sequence of characters like a text password, but entered by clicking the right character sequence on CaRP images.

CaRP is click-based graphical passwords, where a sequence of clicks on an image is used to derive a password. Unlike other click-based graphical passwords, images used in CaRP are Captcha challenges, and a new CaRP image is generated for every login attempt. The notion of CaRP is simple but generic. CaRP can have multiple instantiations. In theory, any Captcha scheme relying on multiple- object classification can be converted to a CaRP scheme. To present exemplary CaRPs built on both text Captcha and image-recognition Captcha. One of them is a text CaRP wherein a password is a sequence of characters like a text password, but entered by clicking the right character sequence on CaRP images.

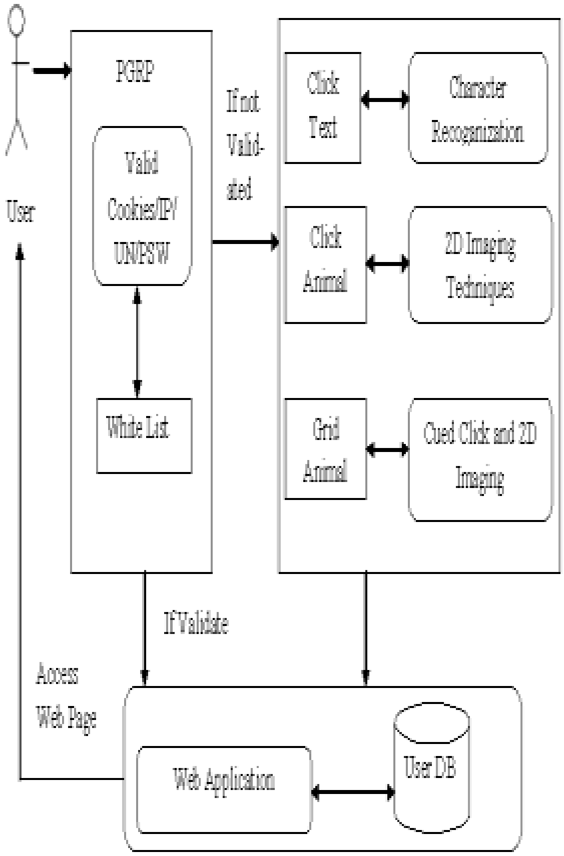

Fig 1: System Overview

CaRP increases spammer’s operating cost and thus helps reduce spam emails. For an email service provider that deploys CaRP, a spam bot cannot log into an email account even if it knows the password. Instead, human involvement is compulsory to access an account. If CaRP is combined with a policy to throttle the number of emails sent to new recipients per login session, a spam boot can send only a limited number of emails before asking human assistance for login, leading to reduced outbound spam traffic. In determining clickable points, the distance between any pair of clickable points in a character must exceed a threshold so that they are perceptually distinguishable and their tolerance regions do not overlap on CaRP images. In addition, variation should also be taken into consideration.

This variation in selecting clickable points ensures that a clickable point is context-dependent: a similarly structured point may or may not be a clickable point, depending on the character that the point lies in. Character recognition is required in locating clickable points on a Text Points image although the clickable points are known for each character. This is a task beyond a bots' capability. A password is a sequence of clickable points. A character can typically contribute multiple clickable points. Therefore Text Points has a much larger password space than Click Text. Text Points images look identical to Click Text images and are generated in the same way except that the locations of all the clickable points are checked to ensure that none of them is occluded or its tolerance region overlaps another clickable point's, to generate another image if the check fails.

A. Click Text

Click Text is a recognition-based CaRP scheme built on top of text Captcha. Its alphabet comprises characters without any visually-confusing characters. For example, Letter "O" and digit "0" may cause confusion in CaRP images, and thus one character should be excluded from the alphabet. A Click Text password is a sequence of characters in the alphabet, e.g. ρ ="AB#9CD87", which is similar to a text password. A Click Text image is generated by the underlying Captcha engine as if a Captcha image were generated except that all the alphabet characters should appear in the image. During generation, each character's location is tracked to produce ground truth for the location of the character in the generated image.

B. Click Based Graphical Password

Graphical Password or Captcha Zoon is a Captcha scheme which uses 3D models of horse and dog to generate 2D animals with different textures, colours, lightings and poses, and arranges them on a cluttered background. A user clicks all the horses in a challenge image to pass the test. Click password is a recognition-based CaRP scheme built on top of Captcha Zoo, with an alphabet of similar animals such as dog, horse, pig, etc. Its password is a sequence of animal names such as ρ = "Turkey, Cat, Horse, Dog" For each animal, one or more 3D models are built. The Captcha generation process is applied to generate Click Animal images: 3D models are used to generate 2D animals by applying different views, textures, colours, lightning effects, and optionally distortions.

C. Graphical Password Grid

The number of similar animals is much less than the number of available characters. Graphical Password grid has a smaller alphabet, and thus a smaller password space, then Click Text. CaRP should have a sufficiently-large effective password space to resist human guessing attacks. Graphical grid's password space can be increased by combining it with a grid- based graphical password, with the grid depending on the size of the selected animal.DAS is a candidate but requires drawing on the grid. To be consistent with Click Animal, to change from drawing to clicking: Click-A-Secret (CAS*)* wherein a user clicks the grid cells in her password. Animal Grid is a combination of Click Animal and CAS. After an animal is selected, an image of $n \times n$ grid appears, with the grid-cell size equalling the bounding rectangle of the selected animal. Each grid-cell is labelled to help users identify. A user can select zero to multiple grid- cells matching her password. Therefore a password is a sequence of animals interleaving with grid-cells, e.g., ρ = "Dog, Grid_2_, Grid_1_; Cat, Horse, Grid_3_", where Grid_1_ means the grid-cell indexed as 1, and grid-cells after an animal means that the grid is determined by the bounding rectangle of the animal.

D. PGRP

The proposed PGRP scheme is more restrictive against attackers than commonly used countermeasures. At the same time, PGRP requires answering fewer ATTs for all legitimate users, including those who occasionally require multiple protocol (PS protocol) based on Atts to protect against online password guessing attacks. It reduces the number of ATTs that legitimate users must correctly answer so that a user with a valid browser cookie (indicating that the user has previously logged in successfully) will rarely be prompted to answer an ATTs. A deterministic function (Ask ATTs()) of the entered user credentials is used to decide whether to ask the user an ATTs. A secure non-deterministic key hash function as Ask ATTS() so that each username is associated with one key that should be changed whenever the corresponding password is changed.

GRAPHICAL PASSWORD TECHNIQUES

In this project we used four graphical password techniques to avoid the automatic password guessing attack.

A. Recognition-Based CaRP

ClickText is a recognition-based CaRP scheme built on top of text Captcha. Its alphabet comprises characters without any visually-confusing characters. For example, Letter "O" and digit "0" may cause confusion in CaRP images, and thus one character should be excluded from the alphabet. A ClickText password is a sequence of characters in the alphabet.

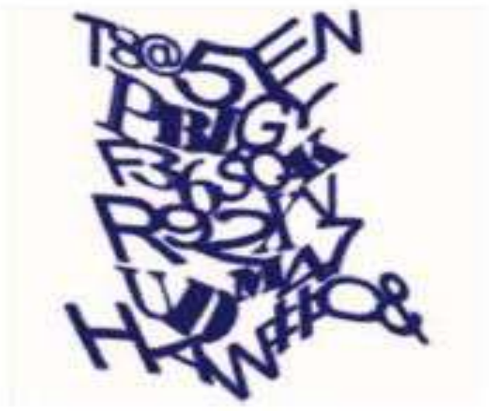

Fig 2: Recognition-Based CaRP

A Click Text image is generated by the underlying Captcha engine as if a Captcha image were generated except that all the alphabet characters should appear in the image. During generation, each character's location is tracked to produce ground truth for the object-dependent, It has the advantage that a correct animal should be clicked in order for the clicked grid- authentication server relies on the ground truth to identify the characters corresponding to user-clicked points.

B. Dimensional-Based Click Animal Captcha

Captcha scheme which uses 3D models of horse and dog to generate 2D animals with different textures, colors, lightings and poses, and arranges them on a cluttered background. A user clicks all the horses in a challenge image to pass the test. Click Animal is a recognition-based CaRP scheme built on top of Captcha Zoo, with an alphabet of similar animals such as dog, horse, pig, etc…The Captcha generation process is applied to generate Click Animal images. The resulting 2D animals are then arranged on a cluttered background such as grassland. Some animals may be occluded by other animals in the image, but their core parts are not occluded in order for humans to identify each of them

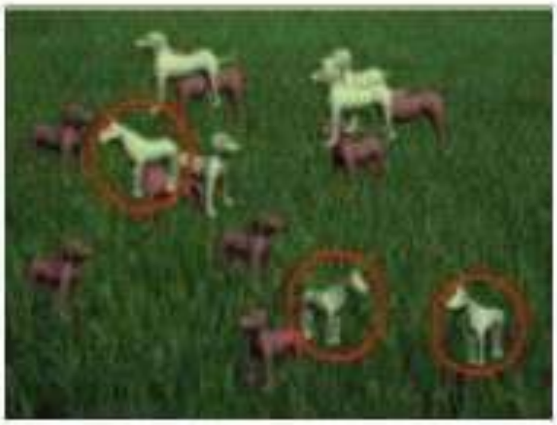

Fig 3: Dimensional-Based Click Animal Captcha

C. Graphical Password Grid

Animal Grid's password space can be increased by combining it with a grid-based graphical password, with the grid depending on the size of the selected animal. Click-A-Secret (CAS) wherein a user clicks the grid cells in her password. Animal Grid is a combination of Click Animal and CAS. The number of grid-cells in a grid should be much larger than the cell(s) on the follow-up grid to be correct. If a wrong animal is clicked, the follow-up grid is wrong.

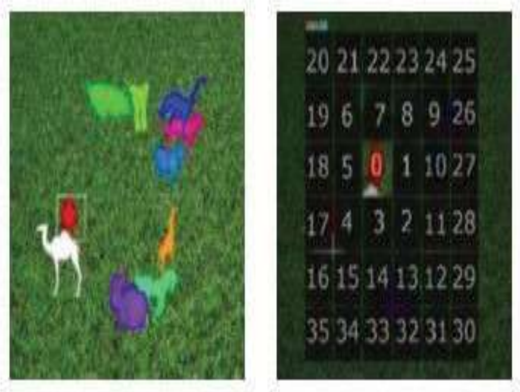

Fig 4: Graphical Password Grid

D. Data Accessing and Authentication

Authentication Systems for managing passwords should ensure the quality of this authentication method. This could include log-on methods enforce use of individual user-IDs and associated passwords, and set or change password methods enforce choice of strong passwords. In authentication, the user or computer has to prove its identity to the server or client. In this technique authentication by a server entails the use of a user name and password, this authentication process is use to find the trusted user. Successfully pass authentication level like captcha and access the data from the Server. The Server verifies the user authentication level and produces the data from the data storage. The user click wrong format in this captcha to exit the entire application.

E. Password Guessing Resistance Protocol

All remote hosts must correctly answer an CAPTCHA challenge prior to being informed whether access is granted or the login attempt is unsuccessful: (i) when the number of failed login attempts for a given username is very small; and (ii) when the remote host has successfully logged in using the same username in the past (however, such a host must pass an CAPTCHA challenge if it generates more failed login attempts than a pre- specified threshold). PGRP uses either IP addresses, cookies, or both to identify machines from which users have been successfully authenticated. Thedecision to require a CaRP challenge upon receiving incorrect credentials is based on the received cookie (if any) and or the remote host's IP address. In addition, if the number of failed login attempts for a specific username is below a threshold, the user is not required to answer an CaRP challenge even if the login attempt is from a new machine for the first time (whether the provided username-password pair is correct or incorrect).

CONCLUSION AND FUTURE WORK

CaRP is both a Captcha and a graphical password scheme. The notion of CaRP introduces a new family of graphical passwords, which adopts a new approach to counter online guessing attacks: a new CaRP image, which is also a Captcha challenge, is used for every login attempt to make trials of an online guessing attack computationally independent of each other. A password of CaRP can be found only probabilistically by automatic online guessing attacks including brute-force attacks, a desired security property that other graphical password schemes lack. Hotspots in CaRP images can no longer be exploited to mount automatic online guessing attacks, an inherent vulnerability in many graphical password systems. CaRP forces adversaries to resort to significantly less efficient and much more costly human-based attacks. In addition to offering protection from online guessing attacks, CaRP is also resistant to Captcha relay attacks, and, if combined with dual-view technologies, shoulder-surfing attacks. CaRP can also help reduce spam emails sent from a Web email service. Our usability study of two CaRP schemes we have implemented is encouraging. For example, more participants considered AnimalGrid and ClickText easier to use than PassPoints and a combination of text password and Captcha. Both AnimalGrid and ClickText had better password memorability than the conventional text passwords. On the other hand, the usability of CaRP can be further improved by using images of different levels of difficulty based on the login history of the user and the machine used to log in.

REFERENCES

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

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

3. Bonneau.J(Jun. 2012), “The science of guessing: Analyzing an anonymized corpus of 70 million passwords,” in Proc. IEEE Symp. Security Privacy, , pp. 20–25.

4.Chellapilla.K, Larson.K, Simard.L, and Czerwinski.M(2005), “Computers beat humans at single character recognition in reading-based human interaction proofs,” in Proc. 2nd Conf. Email Anti- Spam, pp. 1–3.

5.Chiasson.S, van Oorschot.P.C, and Biddle.R(2007), “Graphical password authentication using cued click points,” in Proc. ESORICS,pp. 359–374.

6.Chiasson.S, Forget.A, Biddle.R(2008), and van Oorschot.P.C, “Influencing users towards better passwords: Persuasive cued click-points,” in Proc. Brit. HCI Group Annu. Conf. People Comput., Culture, Creativity, Interaction, vol. 1, pp. 121–130.

7.Dirik.E, Memon.N, and Birget(2007), “Modeling user choice in the passpoints graphical password scheme,” in Proc. Symp. Usable Privacy Security, pp.
20–28.

8. Davis.D, Monrose.F, and Reiter.M(2004), “On user choice in graphical password schemes,” in Proc. USENIX Security, pp. 1–11.

9. Dunphy.P and Yan.J(2007), “Do background images improve ‘Draw a Secret’ graphical passwords,” in Proc. ACM CCS, pp. 1–12.

10. Elson.J, Douceur.J.R, Howell.J, and Saul.J(2007), “Asirra: A CAPTCHA that exploits interest-aligned manual image categorization,” in Proc. ACM CCS, pp. 366–374.

11.Gao.H, Liu.X, Wang.S, and Dai.R(2009), “A new graphical password scheme against spyware by using CAPTCHA,” in Proc. Symp. Usable Privacy Security, pp. 760–767.

12. Golle.P(2008), “Machine learning attacks against the Asirra CAPTCHA,” in Proc. ACM CCS, pp.
535–542.

13.Golofit.K(2007), “Click passwords under investigation,” in Proc. ESORICS,
pp. 343–358.

15.Joshi.N (2009, Nov. 29). Koobface Worm Asks for CAPTCHA [Online]. Available: http://blogs.mcafee.com/mcafee-labs/koobface-worm-asksfor

● ● ●