A Study of Various Passwords Authentication Techniques

Aakansha Gokhale
Dept.of Computer Engineering,
Saraswati College of Engineering, Kharghar,
Navi Mumbai, Maharashtra, India

Vijaya Waghmare
Dept.of Computer Engineering,
Saraswati College of Engineering, Kharghar,
Navi Mumbai, Maharashtra, India

ABSTRACT
Information and computer security is supported by passwords. Password is the principal part of authentication process. The traditional authentication method is to use text-based password which is also called alphanumeric password. But it has significant drawbacks. So to overcome vulnerabilities of this traditional password scheme a graphical password scheme is developed. But major drawback of graphical scheme is it is vulnerable to shoulder surfing attack and also sometimes to spyware attack. So alternative technique to graphical password a Captcha technique is developed. The major advantage of Captcha is that it can not be identified by bots. Captcha gives the protection from unwanted bots. Also there are some limitations of Captcha, and to overcome those after Captcha for more robust security a new technique is developed which is CaRP (Captcha as gRaphical Passwords).This paper will explore all the passwords techniques for security.

General Terms
Information Security, Password Techniques.

Keywords
Captcha, CaRP, Graphical password, Text-based password.

1. INTRODUCTION
Nowadays information security is important factor in security program and for this security convenient method is authentication [1]. Authentication is a process of verifying the identity of a particular person. The most popular method is password authentication.

In this, traditional method used is textual (alphanumeric) passwords. These types of passwords are strings of letters and digits .But there are several deficiencies in these textual passwords.

In this technique passwords used are short and simple which are easy to remember [2]. So textual passwords can be personal names of family members, dictionary words, birth-date, pet name, phone number etc. and vulnerable to various attacks like dictionary attack, easy to guess, key-loggers, shoulder surfing, ,social engineering, spyware attack, hidden camera etc[3][4].

Also nowadays users require the passwords for personal computers, social networks, email and more, and for all these systems, to remember easily the users can use the same password which reduces security [5].

So in this way if textual passwords are kept difficult then they are difficult to remember and if kept easy then they are easy to guess.

So alternative to textual password, a technique proposed is graphical password [6].

In this technique the images or shapes are used because people can remember images easily than text; the psychological studies support such assumption [7]. It is easy for human beings to remember the places they visit, things they have seen and faces of different people.

In addition, if images used in graphical password technique are large enough, the password space of a graphical password technique may exceed as compare to text-based password and thus can offer resistance to all possible attacks of text-based password.

In such way graphical passwords are difficult to guess and easy to remember.

But also there are some drawbacks of graphical passwords, such as password registration and log-in process require much more storage space than text based passwords, vulnerable to shoulder surfing attacks.

So after graphical password one more security technique was developed which is known as CAPTCHA (Completely Automated Public Turing-test to tell Computers and Humans Apart).

Captcha is a type of challenge-response test used in computing to ensure that the response is generated by a human and not by a computer.

It generates the test which is human solvable but difficult for computer programs.

And when Captcha is combined with graphical passwords a new innovative technique developed is CaRP.

2. LITERATURE SURVEY
2.1 Graphical Password Techniques
These techniques are developed to overcome the limitations of text-based passwords. Graphical passwords consist of recognizing the images or sometimes to recognize the image and click the particular points or area on image rather than typing the characters like text-based password. In this way, the problems that arise from the text-based passwords are reduced.

Graphical password techniques were originally described by Blonder [8].

Graphical password techniques are categorized as follows:

2.1.1 Recognition Based System
In this system, for registration the user has to select the certain number of images from a set of random images in an order as a password, and for authentication the user has to identify (recognize) those images in a same order.

There are three schemes under this system:

2.1.1.1 Dhamija and Perrig Scheme [9]

In this scheme, during registration the user has to pick the several pictures according to choice from a set of random pictures in a sequence and during authentication the user has to identify those same pictures in a sequential manner.

2.1.1.2 Passface Scheme [10]

In this scheme, human faces are used as password. This is based on an assumption that human can remember the human faces easily. In this, a grid of nine human faces is used. In this nine faces one is known to the user and remaining are decoys. The user has to recognize that known face among the nine faces. And this is continued until all the four faces are identified.

2.1.1.3 Sobrado and Birget Scheme [11]

In this scheme system display a number of pass-objects (pre-selected by user) among other objects, user click inside the convex hull bounded by pass-objects.

2.1.2 Recall-Based System

In this system a user is asked to reproduce something that he created or selected earlier during the registration stage.

There are three techniques under this system:

2.1.2.1 Draw-A-Secret (DAS) Scheme [12]

Here user will draw a simple picture on 2D grid. The coordinates of a grids are occupied by the picture are stored in the order of the drawing. During authentication, the user will be told to re-draw the picture. If the drawing touches the same sequence, then the user is authenticated.

2.1.2.2 Signature Scheme

Here authentication is conducted by having the user drawing their signature using mouse.

2.1.2.3 Pass-point Scheme

Here user will click on any place on an image to create a password. A tolerance around each chosen pixel is calculated. In order to be authenticated, user must click within the tolerances in the correct sequence.

Benefits:

- Graphical password schemes provide a way of making more user-friendly passwords.
- Here the security of the system is very high.
- Like textual passwords, the dictionary attacks and brute force attacks are not possible with graphical passwords.
- Spyware attack: Key logging or key listening spyware cannot be used to break graphical passwords.
- Social engineering: To give away graphical passwords to another person is difficult as compared to text based password.e.g. it is very difficult to give away graphical passwords over phone.
- Setting up the phishing website to obtain graphical passwords would be more time consuming.

Limitations:

- Password registration and log-in process take too long.
- Require much more storage space than text based passwords.
- Shoulder surfing: As name implies, shoulder surfing means watching over people's shoulders as they process information. Because of their graphic nature, nearly all graphical password schemes are vulnerable to shoulder surfing.

2.2 Captcha

To overcome the drawbacks of textual password the graphical password schemes were developed. But these schemes are vulnerable to spyware attacks. Spyware is software that gathers information about computer's use and relays that information to third party [13]. Spyware has become one of the most common security threats to computer systems. Password collection by spywares has rapidly increased.

So to resist the spyware attack, a new technique is developed known as Captcha

Captcha is a program that generates and grades tests that are human solvable, but beyond the capabilities of current computer programs [14].The strength of Captcha is in resisting automatic adversarial attacks.

Captcha is used to test whether the user is computer or a human by creating a task easy for humans but difficult for machines.

It is based on hard AI problems which can not be solved with any greater accuracy than what is known to the AI community.

Captcha is now a standard security mechanism for addressing malicious Internet bot programs [15] and major web sites such as Google, Yahoo and Microsoft all have their own Captchas,

Captcha mainly include 3 types: text-based, image-based and sound-based.

The AI knowledge is advanced if Captchas are broken.

The Captcha can be described as a picture contains distorted letters to ensure that the user is a human not bots. These pictures can not be read by bots because Captcha is resistant to OCR (Optical Character Recognition)

Benefits:

- Distinguishes between a human and a machine.
- Makes online polls more legitimate.
- Reduces spam and viruses.
- Makes online shopping safer.
- Diminishes abuse of free email account services.

Limitations:

- Sometimes very difficult to read.
- Are not compatible with users with disabilities
- Time-consuming to decipher.
- Technical difficulties with certain internet browsers.
- May greatly enhance Artificial Intelligence.

Applications:

Captchas are used in various web applications to identify human users and to restrict access to them.

- Online polls
- Protecting web registration

- Search engine bots
- E-Ticketing
- Email spam
- Preventing dictionary attacks
- As a tool to verify digitized books
- Improved Artificial Intelligence(AI) technology

2.3 Captcha as gRaphical Password (CaRP) technique:

Captcha has also some limitations. So new security primitive based on hard AI problem is developed which is a combination of Captcha and gRaphical passwords. It is called as CaRP (Captcha as gRaphical Passwords). CaRP is a click-based graphical password 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 in CaRP scheme every time new image is generated. CaRP is built on the both text Captcha and image-recognition Captcha.

Captcha is an independent entity, used together with text or graphical password.

CaRP is both a Captcha and a graphical password scheme which are intrinsically combined into a single entity.

CaRP: An Overview

In CaRP, a new image is generated for every login attempt even for the same user. CaRP uses an alphabet of visual objects (e.g., alphanumerical characters, similar animals) to generate a CaRP image, which is also a Captcha challenge.

A major difference between CaRP images and Captcha images is that all the visual objects in the alphabet should appear in a CaRP image to allow a user to input any password but not necessarily in a Captcha image. Many Captcha schemes can be converted to CaRP schemes.

CaRP Schemes: These are classified into two categories:

2.3.1 Recognition-Based CaRP

In this scheme a password is a sequence of visual objects in the alphabet. As per view of traditional recognition-based graphical passwords, recognition-based CaRP seems to have access to an infinite number of different visual objects.

There are 3 techniques under this scheme:

2.3.1.1 CilckText

Figure 1: A ClickText image

It is a recognition-based CaRP scheme. It based on text Captcha. Its alphabet consists of characters and these are without any visually confusing characters. The ClickText image has mostly 33 characters. These characters are randomly arranged on 2D space. Here the password is a sequence of characters e.g. =“# 9CABTCD”. It is same as text password. The ClickText image is generated by the Captcha engine and almost all the characters should appear in the image. The user is authenticated according to user-clicked points on the ClickText image by authentication server.

The ClickText image is different from normal text Captcha. In text Captcha user has to type the characters from left to right sequentially and in ClickText user has to click the characters in password. In the above example user has to click the characters in the order as ‘#’, ‘9’, ‘C’, ‘B’, ‘T’, ‘C’, and ‘D’. If this orders for given password example is followed by user, then user is an authorized user. The ClickText image is shown in Figure1.

2.3.1.2 ClickAnimal

It is also a recognition-based CaRP scheme. This scheme is based on Captcha Zoo [16] Here an alphabet consists of similar animals e.g. dog, horse, pig etc. For every animal 3D model is used. By using a Captcha generation process, ClickAnimal images are generated. Here 3D models are used to generate 2D animals by using different views, colors, textures, lightning effects and if require distortions. The resulting 2D animals are placed on cluttered background. In the 2D model of ClickAnimal image, sometimes it is possible that some animals may be covered by other animals in the image, but their core parts are not covered so that humans can easily identify them but it is difficult for bot to identify such covered images as shown in Figure 2. Here the password is a sequence of animal names such as p=“Cat, Dog, Horse, Turkey” etc. The ClickAnimal has a smaller alphabet and so the password space required is also less as compare to ClickText as number of similar animals is less than the number of available characters.

Figure 2: A ClickAnimal image.

2.3.1.3 AnimalGrid

To resist the human guessing attack the password space should be sufficiently large for CaRP scheme. So here in AnimalGrid CaRP scheme the password space is increased by combining it with the grid depending on the size of the selected animal.

AnimalGrid is a combination of ClickAnimal and CAS (Click-A-Secret). In CAS, a user clicks the grid cells in a password. In this AnimalGrid for authentication a ClickAnimal image is displayed first. After an animal is selected an image of n*n grid appears, with the grid-cell size equaling the bounding rectangle of the selected animal. All grid cells are labeled to help users identify. As shown in Figure 3, when the red turkey in the left image was selected a 6*6 grid is generated.

In this scheme password is a sequence of animals interleaving with grid cells. Here password must begin with animal name. E.g. p=“Cat, Horse, Grid (3), Dog, Grid (2), Grid (1)”.Where Grid (3) means the grid-cell indexed as 3 and grid cells after an animal name means the grid is determined by the bounding rectangle of animal.

Here the correct animal should be clicked for the correct follow up grid. If wrong animal is clicked, the follow up grid is wrong.

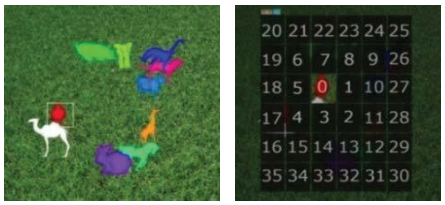

Figure 3: A ClickAnimal image (left) and 6 × 6 grid (right) determined by red turkey's bounding rectangle.

2.3.2 Recognition-Recall CaRP

This scheme combines the tasks of both recognition based and cued-recall and retains the advantages of both. The advantage of recognition-based is of being easy for human memory and the advantage of cued-recall is a password space.

In this type, the 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 object and thus can be uniquely identified by humans. No matter how the object appears in CaRP images.

For authentication first user has to identify the object and then click the invariant points on the object matching the password. A user has to click within the acceptable tolerance range of the invariant point (password point) [17].

There are two techniques under this scheme:

2.3.2.1 TextPoint

In this scheme, characters contain invariant points. As shown in Figure 4 the character A has some invariant points. It offers a cue to memorize and locate its invariant points. For TextPoints a set of internal invariant points of characters is selected to form a set of clickable points. If the distance of point to the closest boundary of the object exceeds a threshold then that point is said to be internal point. This internality ensures that a clickable point should not be covered by a neighboring character and its tolerance region should not overlap with any tolerance region of a neighboring character's clickable points on the image generated by the underlying Captcha engine.

In TextPoints image although the clickable points are known for each character, character recognition is required for locating clickable points.

This is beyond the bot's capability.

In TextPoints, a password is a sequence of clickable points on a character. A character can have multiple clickable points. Therefore TextPoints has a much larger space than ClickText.

Figure 4: The character image for TextPoints scheme with some invariant points (red crosses) of 'A'.

2.3.2.2 TextPoints4CR

In the CaRP schemes studied up to now, for authentication, the coordinates of user clicked-points are sent directly to authentication server. But for complex challenge-response protocol, instead, a response is sent to the authentication server. So here TextPoints can be modified to fit challenge-response authentication. This variation is called TextPoints for challenge-response or TextPoints4CR.

In TextPoints CaRP scheme, the authentication server stores a salt and password hash value for each account, but in TextPoints4CR the server stores a password for each account.

Also another difference is that each character can appear multiple times in TextPoints CaRP scheme but in a TextPoints4CR each character appears only once. This is because in a TextPoints4CR the client and server both generate the same sequence of discretized grid-cells independently.

So as compare to TextPoints a TextPoints4CR is robust because of no repetition of characters in a shared secret i.e. Password.

In this way, in TextPoints4CR the server stores the passwords directly instead of their hash values and passwords are encrypted with a master key. This master key knows to server and a password is decrypted only when its associated account attempts to log-in.

Benefits:

- CaRP offers protection against Automatic Online Guessing Attacks on passwords.
- It also offers protection against Relay Attacks.
- It offers security against Human Guessing Attacks.
- It offers protection against Shoulder Surfing Attack.
- It offers security against spam emails sent from a Web email service.

Limitations:

- CaRP scheme is vulnerable to phishing attack because user-clicked points are sent to the a authentication server.
- Also CaRP is vulnerable if both the image and user-clicked points can be captured.(if client is compromised).

Applications:

- CaRP can be useful for touch-screen devices where typing a password is difficult.
- CaRP is also useful for secure internet applications such as e-business, e-commerce, e-banking etc.
- CaRP is used to reduce the spam emails. For the email service provider which uses CaRP, a spam bot can not log into an email account even if it knows the password.

3. CONCLUSION AND FUTURE WORK

In this paper, we have studied various password techniques such as textual password, graphical password, Captcha password and CaRP. The best alternative for textual password is a graphical password. The graphical password can reduce the burden of human memory as humans tend to remember graphics and images better.

The graphical password techniques are classified into two categories: recognition-based and recall-based techniques. Overall it is more difficult to break graphical passwords using various attacks like brute force attack, dictionary attack, social engineering etc.

But graphical passwords are vulnerable to shoulder surfing and spyware attack. So the best alternative to graphical scheme is Captcha technique. Captcha can be recognized by humans and not by bots. But there are also some limitations for Captcha and for more robust security a new technique is developed which is called CaRP which is combination of Captcha and graphical password. It is relying on hard AI problems. CaRP is also classified as Recognition-Based CaRP and Recognition-Recall CaRP.

We have discussed both the categories. The Recognition-Based CaRP includes ClickText, ClickAnimal and AnimalGrid techniques and the Recognition-Recall CaRP includes TextPoints and TextPoints4CR techniques.

In all these techniques every time a new image is generated and so all the techniques are resistant to shoulder surfing attack and secure than graphical password techniques.

Also for attackers to hack CaRP more incentives are required as compare to Captcha as CaRP does not rely on any specific scheme.

At present all the CaRP techniques are more secure as compare to other password techniques. But also CaRP has a scope for refinements.

So to increase a security the difficulty level of images can be increased at every login attempt and this level is based on the machine used to login and on the login history of the user.

Another scope of improvement here is some CaRP techniques can be made two-way or three-way for authentication.

E.g. If AnimalGrid and ClickText are combined then it will become three-way authentication technique.

4. REFERENCES

[1] K. Renaud. “Evaluating authentication mechanisms”. In L. Cranor and S. Garnkel, editors, Security and Usability: Designing Secure Systems That PeopleCanUse, chapter 6, pp.103-128. O'Reilly Media, 2005.

[2] A. Adams and M. A. Sasse. “Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures”. Communications of the ACM, 42:41-46, 1999.

[3] D. Feldmeier and P. Karn. “UNIX Password Security-Ten Years Later”. In Crypto'89, August 1989.

[4] R. Morris and K. Thompson. “Password Security: A Case History”. Communications of the ACM,22(11):594-597, 1979.

[5] D. Florencio and C. Herley. “A large-scale study of WWW password habits”. In 16th ACM International World Wide Web Conference (WWW), May 2007.

[6] A. Adams, M. A. Sasse, and P. Lunt. “Making passwords secure and usable”. In HCI 97: Proceedings of HCI on People and Computers, pp.1-19, London, UK, 1997. Springer-Verlag.

[7] Xiaoyuan Suo, Ying Zhu, G. Scott. Owen, “Graphical Passwords: A Survey”, Department of Computer Science Georgia State University

[8] Blonder G. (1996) In Lucent Technologies, Inc., Murray Hill, NJ, United States Patent 5559961.

[9] R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in Proceedings of 9 USENIX Security Symposiums, 2000.

[10] Real User Corporation (2007) Passfaces T M , http//:www.realuser.com.

[11] L. Sobrado and J.C. Birget, "Graphical passwords," The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4, 2002

[12] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A.D. Rubin, "The Design and Analysis of Graphical Passwords," in Proceedings of the 8th USENIX Security Symposium, 1999.

[13] S. Sariou, S.D. Gribble, and H.M. Levy. Measurement and Analysis of Spyware in a University Environment. In Proceedings of the ACM/USENIX Symposium on Networked Systems Design and Implementation (NSDI), San Francisco CA, 2004

[14] D. Weinshall. Cognitive Authentication Schemes Safe Against Spyware. In Symposium on Security and Privacy, 2006.

[15] J. Yan and A.S. El.Ahmad. Usability of CAPTCHAs - Or, Usability issues in CAPTCHA design. In the 4th Symposium on Usable Privacy and Security, Pittsburgh, USA, July 2008.

[16] R. Lin, S.-Y. Huang, G. B. Bell, and Y.-K. Lee, “A new CAPTCHA interface design for mobile devices,” in Proc. 12th Austral. User Inter. Conf., 2011, pp. 3–8.

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