International Journal of Advance Research and Innovation
Vol. 3(1), Jan-Mar 2015, pp. 28-33
Doi: 10.51976/ijari.311505

Article Info
Received: 21 Jan 2015 | Revised Submission: 15 Feb 2015 | Accepted: 28 Feb 2015 | Available Online: 15 Mar 2015

User Privileged CAPTCHA as Graphical Password for Multistage Authentication

M. Anitha and G. Saranya***

ABSTRACT

Nowadays, user authentication is one of the important topics in information security. In today's world the password security is very important. For password protection various techniques are available. Cued Click Points are a click-based graphical password scheme, a cued-recall graphical password technique. Users Click on one point per image for a sequence of images. The next image is based on the previous click-point. The passwords which are easy to memorize are chosen by the users and it becomes easy for attackers to guess it, but the passwords assigned by the strong system are difficult for users to remember. Many current systems have low level security, and even then users often devise insecure coping strategies in order to compensate for memorability and usability problems. Alternatives such as tokens or biometrics raise other issues such as privacy and loss. Various graphical password mechanisms have received considerable attention in response. In this paper describes CAPTCHA authentication is clearly a practical problem. In a new security primitive based on hard AI problems, namely, a novel family of graphical password systems built on top of Captcha technology is call Captcha as graphical passwords.

Keywords: *Re-Captcha; User Personalisation; Graphical; Passwords; Authentication.*

1.0 Introduction

Security has unique usability challenges because the need for security often means that standard human-computer-interaction approaches cannot be directly applied. An important usability goal for authentication systems is to support users in selecting better passwords. Users often create memorable passwords that are easy for attackers to guess, but strong system-assigned passwords are difficult for users to remember. So researchers of modern days have gone for alternative methods wherein graphical pictures are used as passwords. Graphical passwords essentially use images or representation of images as passwords. Human brain is good in remembering picture than textual character. There are various graphical password schemes or graphical password software in the market. However, very little research has been done to analyze graphical passwords that are still immature. There for, this project work merges persuasive cued click points and password guessing resistant protocol. The major goal of this work is to reduce the guessing attacks as well as encouraging users to select more random, and difficult passwords to guess. Well known security threats like brute force attacks and dictionary attacks can be successfully abolished using this method. There has been a great deal of hype for graphical passwords since two decade due to the fact that primitive's methods suffered from an innumerable number of attacks which could be imposed easily. Here we will progress down the taxonomy of authentication methods. To start with we focus on the most common computer authentication method that makes use of text passwords. Despite the vulnerabilities, it"s the user natural tendency of the users that they will always prefer to go for short passwords for ease of remembrance and also lack of awareness. About how attackers tend to attacks. Unfortunately, these passwords are broken mercilessly by intruders by several simple means such as masquerading, Eaves dropping and other rude means say dictionary attacks, shoulder surfing attacks, social engineering attacks.

**Corresponding Author: Department of Computer Science Engineering, Sir Issac Newton College of Engineering and Technology, Nagapattinam, Tamil Nadu, India (E-mail: anithamurugaiyan91@gmail.com)*
***Department of Computer Science Engineering, Sir Issac Newton College of Engineering and Technology, Nagapattinam, Tamil Nadu, India*

To mitigate the problems with traditional methods, advanced methods have been proposed using graphical as passwords. The idea of graphical passwords first described by Greg Blonder (1996). For Blonder, graphical password shaves a predetermined image that the sequence and the tap regions selected are interpreted as the graphical password. Since then, many other graphical password schemes have been proposed. The desirable quality associated with graphical passwords is that psychologically humans can remember graphical far better than text and hence is the best alternative being proposed. There is a rapid and growing interest in graphical passwords for they are more or infinite in numbers thus providing more resistance. The major goal of this work is to reduce the guessing attacks as well as encouraging users to select more random, and difficult passwords to guess.

2.0 Requirements of Authentication

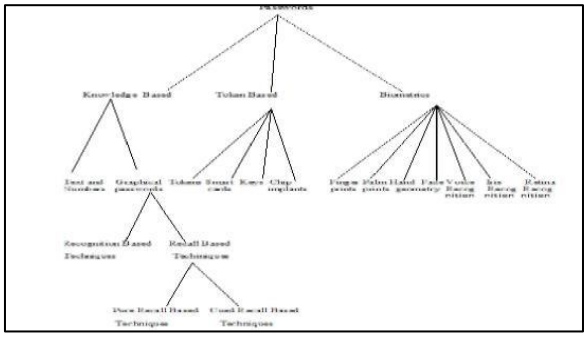
Authentication technology on the Internet is typically used to give users access to their accounts. Thus the requirements for the authentication technology are driven by the requirements of the services to which they enable access. As the service provider is the party that ultimately makes the decision which authentication technology to deploy we will list some common requirements from a service provider's perspective.

The first requirement is availability. Web based services should be accessible from a number of machines that can in general only be expected to have standard available tools, in particular a web browser. The second criterion is robustness and reliability, i.e. a legitimate user should always succeed in logging into his account. The next criterion is user friendliness. Internet services strive to provide a good user experience and many of them try to encourage usage. Another key requirement from the service provider perspectiveis that authentication technology should have low costs to implement and operate. The following Figure 1: is the depiction of current authentication methods

2.1 Token based authentication

The traditional user name password or personal identification number (PIN) based authentication scheme is an example of the Token Based. For example, Smart Cards, a driver's license, credit card, a university ID card etc. It allows users to enter their user name/ password in order to obtain a token which allows them to fetch a specific resource- without using their user name and password. Once their token has been obtained, then the user can offer the token-which offers access to a specific resource for a time period- to the remote site.

Fig 1: Authentication Methods



2.2 Biometrics based authentication

Biometrics is the study of automated methods for uniquely recognizing human beings based upon one or more intrinsic physical or behavioral traits. It is based on "something you are". It uses physiological or behavioral characteristics like facial or fingerprint scans and iris or voice recognition to identify users.

2.3 Knowledge based authentication

Knowledge based authentication are the most extensively used authentication techniques and include both text based and picture based passwords KBA is based on "something You Know to identify you". The major drawback of token- based and biometric- based authentication methods are expensive and requires special devices. Graphical-based password methods have been proposed as a potential alternative to text-based techniques, supported partially by the fact that humans can remember images better than text Psychologists have confirmed that in both recognition and recall scenarios, the images are more memorable than text.

Therefore, graphical- based authentication mechanisms have higher usability than other authentication techniques In general, the graphical password methods can be classified into two categories: Recognition-based and Recall-based graphical techniques.

3.0 Existing System

Previous research recognized the weaknesses of knowledge-based authentication schemes (in particular password-based computer logins). So far, however, most of the proposed solutions have been based on technical fixes or on educating users.

Neither of these address the fundamental problem of knowledge-based authentication systems, which is that the authentication task is based on precise recall of the secret knowledge. Since people are much better at recognizing previously seen images than at precisely recalling pass phrases from memory, we employ a recognition-based approach for authentication.

The examine the requirements of a recognition-based system and propose, in which the replace the precise recall of pass phrases with the recognition of previously seen images.

This system has the advantage that the authentication task is more reliable, easier and fun to use. In addition, the system prevents users from choosing weak passwords and makes it difficult for users to write passwords down and to communicate them to others.

Results indicate that image authentication systems have potential applications, especially where text input is hard (e.g., PDAs or ATMs), for infrequently used passwords or in situations where passwords must be frequently changed.

Since the error recovery rate was significantly higher for images, compared to passwords and PINS, such a system may be useful in environments where high availability, of a password is paramount and where the difficulty to communicate passwords to others is desired. Further study is required to determine how user performance and error rate will vary with frequency of use, over longer time periods and with large or multiple portfolios.

Many improvements can be made to strengthen the system against attack and to improve its usability. For example, we are exploring ways to mask or distort portfolio images, such that users will be able to recognize their images, while leaking information about the portfolio to observers.

We are also exploring authentication schemes that take advantage of other innate human abilities. Hackers recognize that humans are often the weakest link in system security and exploit this using social engineering tactic.

Yet designers do not always include human limitations in their evaluation of system security. Systems should not only be evaluated theoretically, but by how secure they are in common practice.

4.0 Problem Analysis

4.1 Text based passwords

Here we briefly exam some of the possible techniques for breaking graphical passwords and try to do a comparison with text-based passwords

4.2 Dictionary attacks

Since recognition based graphical passwords involve mouse input instead of keyboard input, it will be impractical to carry out dictionary attacks against this type of graphical passwords. For some recall based graphical passwords, it is possible to use a dictionary attack but an automated dictionary attack will be much more complex than a text based dictionary attack. More research is needed in this area Overall; we believe graphical passwords are less vulnerable to dictionary attacks than text-based passwords

4.3 Guessing

Unfortunately, it seems that graphical passwords are often predictable, a serious problem typically associated with text-based passwords. More research efforts are needed to understand the nature of graphical passwords created by real world users.

4.4 Shoulder surfing

Like text based passwords, most of the graphical passwords are vulnerable to shoulder surfing. At this point, only a few recognition-based techniques are designed to Resist shoulder-surfing.

4.5 Spyware

Except for a few exceptions, key logging or key listening spy ware cannot be used to break graphical passwords. It is not clear whether "mouse tracking" spy ware will be an effective tool against graphical passwords. However, mouse motion alone is not enough to break graphical passwords. Such information has to be correlated with application

information, such as window position and size, as well as timing information.

4.6 Social engineering

Comparing to text based password, it is less convenient for a user to give away graphical passwords to another person. For example, it is very difficult to give away graphical passwords over the phone. Setting up a phasing web site to obtain Graphical passwords would be more time consuming

5.0 Proposed System

Now-a-days, all business, government, and academic organizations are investing a lot of money, time and computer memory for the security of information. Online password guessing attacks have been known since the early days of the Internet, there is little academic literature on prevention techniques. This project deals with guessing attacks like brute force attacks and dictionary attacks.

This project proposes a click-based graphical password system. During password creation, there is a small view port area that is randomly positioned on the image. Users must Select a click-point within the view port.

If they are unable or unwilling to select a point in the current view port, they may press the Shuffle button to randomly reposition the view port. The view port guides users to select more random passwords that are less likely to include hotspots. Therefore this works encouraging users to select more random, and difficult passwords to guess. Brute force and dictionary attacks on password-only remote login services are now widespread and ever increasing. Enabling convenient login for legitimate users while preventing such attacks is a difficult problem. Automated Turing Test, continue to be an effective, easy-to-deploy approach to identify automated malicious login attempts with reasonable cost of inconvenience to users.

This project proposes a new Password Guessing Resistant Protocol (PGRP), derived revisiting prior proposals designed to restrict such attacks. While PGRP limits the total number of login attempts from unknown remote hosts, legitimate users in most cases can make several failed login attempts before being challenged with an ATT. This proposed system also provides protection against key logger spy ware. Since, computer mouse issued rather than the keyboard to enter our graphical password this protects the password from key loggers.

6.0 Related Works

6.1 Re-captcha

Captcha as CAPTCHA or Captcha is a type of challenge-response test used in computing to ensure that the response is not generated by a computer. Re-Captcha is a popular captcha system that uses successful decoding to helps digitise books for online use. This validation is typically used in contact forms and registration forms to fight against spam bots.

To use it, you'll only need to include the Re-Captcha API, and get an API key on the website. Re-Captcha technology works together with the Re-Captcha library available on web server, so no need use it in a network which is not connected to the internet. You need to get API keys before using and pass it. Websites that use forms will need to be secured from spamming by "Spam-Bots".

Spam-Bots will visit your site and fill out forms that are not secured. This can result in comment spamming in forums, spam emails being sent from your server, and other spam related activities.

The "Recaptcha" that allows us to add an image with a special code to web forms. This requires the person filling in and submitting the form to type the code correctly before the form can be submitted.

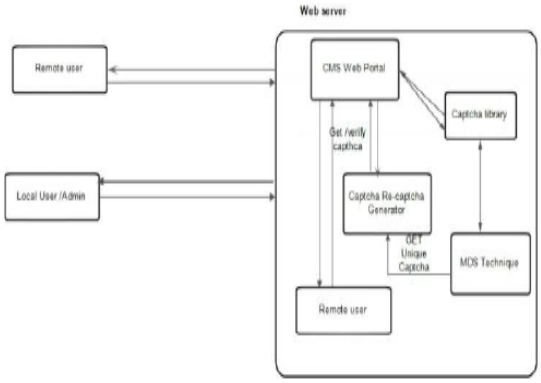
When setting up web forms in Content Management Systems like social networks, and any other potential information portal like Drupal, Wordpress, Joomla, Moodle, and others, application will need to have 2 keys created for your Re-CAPTCHA to work. Re-Captcha requires a public and a private key in order for the code to function in your web forms.

These are free to get from Google if you have a Gmail account. The following will explain how to get a free Re-Captcha key from Google.

6.2 User profile personalization

In Web portal, as the amount of information available causes information overloading, the demand for personalized approaches for information access increases. Personalized systems address the overload problem by building, managing, and representing information customized for individual users

Fig 2: User Protrre Personalization Architecture



This customization may take the form of filtering out irrelevant information and/or identifying additional information of likely interest for the user. Research into personalization is ongoing in the fields of information retrieval, artificial intelligence, and data mining, among others. Purpose of personalisation, reside at individuality and uniqueness on user profile information. While setting security using captcha image, user may wish to personalize their profile based on their vision. Anyhow the update information should be kept in privacy and utilized at authentication time of image captcha verification. To avoid repletion of captcha image this will collapse and make confusion when intruder try to do shoulder surfing atacks

7.0 Conclusion and Future Work

A major advantage of Persuasive cued click point scheme is its large password space over alphanumeric passwords. There is a growing interest for Graphical passwords since they are better than Text based passwords, although the main argument for graphical passwords is that people are better at memorizing graphical passwords than text-based passwords. Online password guessing attacks on password-only systems have been observed for decade's .Present-day attackers targeting such systems are empowered by having control of thousand to million node bonnets. In previous ATT-based login protocols, there exists a security-usability trade-off with respect to the number of free failed login attempts versus user login convenience. In contrast, PGRP is more restrictive against brute force and dictionary attacks while safely allowing a large number of free failed attempts for legitimate users. PGRP is apparently more effective in preventing password guessing attacks , it also offers more convenient login experience, e.g., fewer ATT challenges for legitimate users. PGRP appears suitable for organizations of both small and large number of user accounts. The past decade has seen a growing interest in using graphical passwords as an alternative to the traditional text-based passwords. To address this problem, some researchers have developed authentication methods that use pictures as passwords. In this project, conducted a comprehensive survey of existing graphical password techniques. The current graphical password techniques can be classified into two categories recognition-based and recall-based techniques. Although the main argument for graphical passwords is that people are better at memorizing graphical passwords than text-based passwords, the existing user studies are very limited and there is not yet convincing evidence to support this argument

References

[1] C. Adams et al., Pass-Go: A proposal to improve the usability of graphical passwords, Int. J. Netw. Security, 7(2), 2008, 273-292

[2] U. Aickelin et al., Against spyware using CAPTCHA in graphical password scheme' in Proc. IEEE Int. Conf. Adv. Inf. Netw. Appl., 2010, 1-9

[3] Biddle .R et al., Influencing users towards better passwords: Persuasive cued click-points' in Proc. Brit. HCI Group Annu. Conf. 1, 2008, 121-130.

[4] R. Dai et al., A new graphical password scheme against spyware by using CAPTCHA' in Proc. Symp. Usable Privacy Security, 2009, 760-767

[5] A. E. Dirik et al., Modeling user choice in the pass points graphical password scheme, in Proc. Symp. Usable Privacy Security, 2007, 20-28

[6] P. Dunphy et al., Do background images improve Draw a Secret graphical passwords, in Proc. ACM CCS, 2007, 1-12

[7] P. Golle et al., Machine learning attacks against the Asirra CAPTCHA, in Proc. ACM CCS, 2008, 535-542.

[8] E. Kirda et al., Secure input for web applications Cued Click Point Technique for Graphical Password Authentication' in Proc. ACSAC, 2007, 375-384

[9] M. Motoyama et al., Re: CAPTCHAs-Understanding CAPTCHA solving services in an Economic Context' in Proc. USENTX Security, 2010, 23-28

[10] M. Moy et al., Distortion estimation techniques in solving visual CAPTCHAs, in Proc. Soc. Conf. Comput. Vis. Pattern Recognit, 2004, 23- 28