International Journal On Engineering Technology and Sciences – IJETS™
ISSN (P): 2349-3968, ISSN (O): 2349-3976
Volume 2 Issue 2, February 2015

OVERCOME PASSWORD HACKING THROUGH GRAPHICAL PASSWORD AUTHENTICATION

Dr.C.Kumar Charliepaul [1]
Principal
A.S.L Pauls College of Engg & Tech, Coimbatore .
charliepaul1970@gmail.com

Abstract— *a 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 (GUI). The most common computer authentication method is to use alphanumerical usernames and passwords. This method has been shown to have significant drawbacks. For example, user tends to pick a password that can be easily guessed .On the other hand, if a password is hard to guess, and then it is often hard to remember. In this paper, we conduct a comprehensive survey of the existing graphical password techniques and proposed a new technique. We discuss the strengths and limitations of each method and point out the future research directions in this area. And also major design and implementation issues are clearly explained. The main advantage of this method is it is difficult to hack. For example, .If there are 100 images on each of the 8 pages in a 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 the built-in delay of only 0.1 second following the selection of each image until the selection of the next page, it would take millions of years to break into the system by hitting it with random image sequences .therefore hacking by random combination is impossible.*

Keywords — *graphical password, authentication, hack, network security.*

INTRODUCTION

Authentication is the process to allow users to confirm his or her identity to a Web application. Human factors are often considered the weakest link in a computer security system. Point out that there are three major areas where human-computer interaction is important: authentication, security operations, and developing secure systems. Here we focus on the authentication problem. A password is a form of secret authentication data that is used to control access to a resource. The password is kept secret from those not allowed access, and those wishing to gain access are tested on whether or not they know the password and are granted or denied access accordingly. The use of passwords goes back to ancient times. They would only allow a person in if they knew the password. In modern times, passwords are used to control access to protected computer operating systems, mobile phones, ATMs machines, etc. A typical computer user may require passwords for many purposes: logging in to computer accounts, retrieving email from servers, accessing files, databases, networks, web sites, and even reading the morning newspaper online.

The password is a very good and strong authentication method still used up to now but because of the huge advance in the uses of computer in many applications as data transfer, sharing data, login to emails or internet, some drawbacks of conventional password appears like stolen the password, forgetting the password, week password, etc so a big necessity to have a strong authentication way is needed to secure all our application as possible, so a researches come out with advanced password called graphical password where they tried to improve the security and avoid the weakness of conventional password. Graphical password have been proposed as a possible alternative to text based, motivated particularly by the fact that humans can

remember pictures better than text. Psychological studies have shown that people can remember pictures better than text (R.N Shepard 1987). Pictures are generally easier to be remembered or recognized than text, especially photos, which are even easier to be remembered than random pictures (Xiaoyuav Suo 2009).

OVERVIEW OF THE AUTHENTICATION METHODS

Current authentication methods can be divided into three main areas:

1. Token based authentication
2. Biometric based authentication
3. Knowledge based authentication

Token based techniques, such as key cards, bank cards and smart cards are widely used. Many token based authentication systems also use knowledge based techniques to enhance security. For example, ATM cards are generally used together with a PIN number. Biometric based authentication techniques, such as fingerprints, iris scan, or facial recognition, are not yet widely adopted. The major drawback of this approach is that such systems can be expensive, and the identification process can be slow and often unreliable. However, this type of technique provides the highest level of security. Knowledge based techniques are the most widely used authentication technique and include both text-based and picture-based passwords. The picture-based techniques can be further divided into two categories: recognition-based and recall-based graphical techniques. Using recognition-based techniques, a user is presented with a set of images and the user passes the authentication by recognizing and identifying the images he or she selected during the registration stage. Using recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage.

RECOGNITIONBASED TECHNIQUES

Dhamija and Perrig proposed a graphical authentication scheme based on thee Hash Visualization technique. In their system, the user is asked to select a certain number of images from a set of random pictures generated by a program. Later, the use r will be required to identify the pre selected images in order to be authenticated. The results showed that 90% of all participants succeeded in the authentication using this technique, while only 70% succeeded using text-based passwords and PINS. The average log-in time, however, is longer than the traditional approach. A weakness of this system is that the server needs to store the seeds of the portfolio images of each user in plain text. Also, the process of selecting a set of pictures from the picture database can be tedious and time consuming for the user.

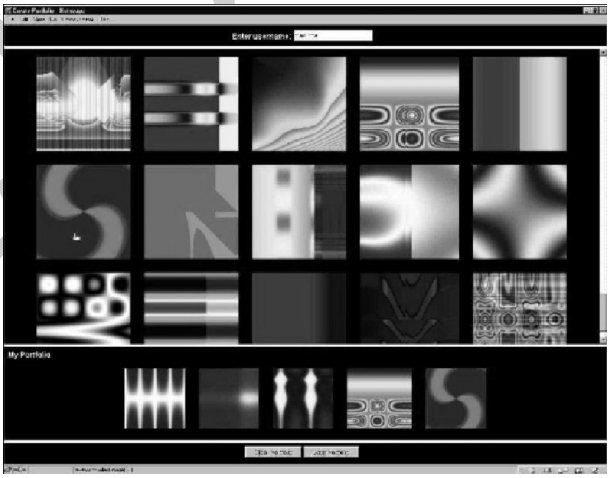

Fig 1 Random images used by Dhamij and Perrig

Sobrado and Birget developed graphical password technique that deals with the shoulder surfing problem. In the first scheme, the system will display a number of pass-objects (pre-selected by user) among many other objects. To be authenticated, a user needs to recognize pass-objects and click inside the convex hull formed by all the pass-objects. In order to make the password hard to guess, Sobrado and Birget suggested using 1000 objects, which makes the display very crowded and the objects almost

indistinguishable, but using fewer objects may lead to a smaller password space, since the resulting convex hull can be large. In their second algorithm, a user moves a frame (and the objects within it) until the pass object on the frame lines up with the other two pass-objects. The authors also suggest repeating the process a few more times to minimize the likelihood of logging in by randomly clicking or rotating. The main drawback of these algorithms is that the log in process can be slow.

Fig 2 A shoulder-surfing resistant graphical password scheme

Man, et al. proposed another shoulder-surfing resistant algorithm. In this algorithm, a user selects a number of pictures as pass-objects. Each pass-object has several variants and each variant is assigned a unique code. During authentication, the user is challenged with several scenes. Each scene contains several pass-objects (each in the form of a randomly chosen variant) and many decoy-objects. The user has to type in a string with the unique codes corresponding to the pass-object variants present in the scene as well as a code indicating the relative location of the pass-objects in reference to a pair of eyes. The argument is that it is very hard to crack this kind of password even if the whole authentication process is recorded on video because where is no mouse click to give away the pass-object information. However, this method still requires users to memorize the alphanumeric code for each pass-object variant. Hong, et al. later extended this approach to allow the user to assign their own codes to pass-object variants. However, this method still forces the user to memorize many text strings and therefore suffer from the many drawbacks of text-based password.

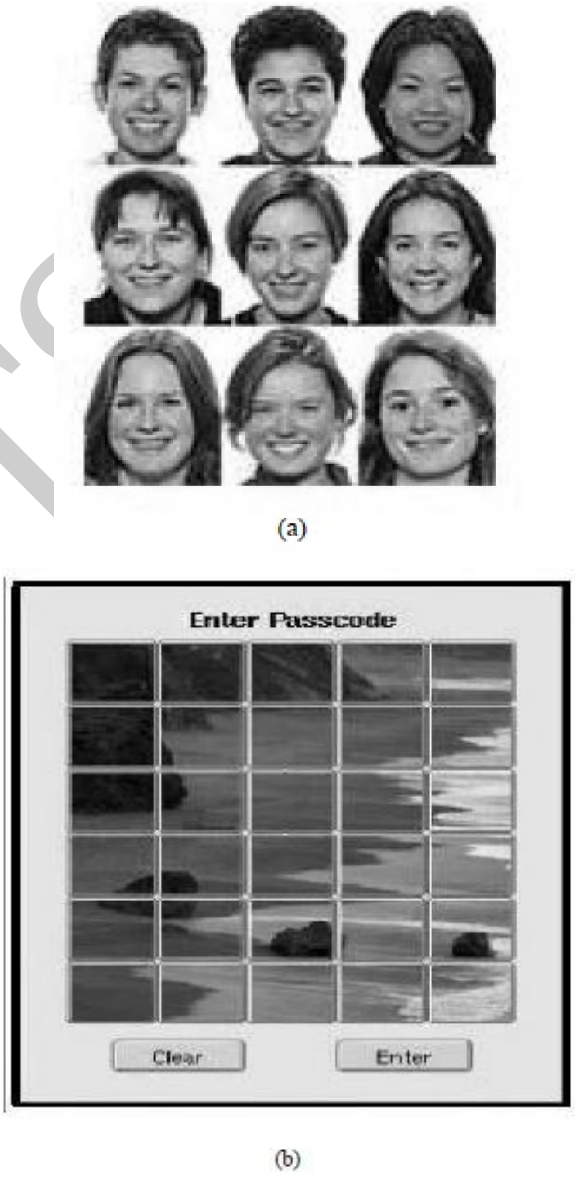

Fig 3(a) An example of pass faces, (b) Password mechanism

Jansen et al proposed a graphical password mechanism for mobile device .during the enrollment stage, a user selects a theme (e.g. sea, cat, etc.) which consists of thumbnail photos and then registers a sequence of images as a password .During the authentication, the user must enter the registered images in the correct sequence. One drawback of this technique is that since the number of thumb nail images is limited to 30, the password space is small. Each thumbnail image is assigned a numerical value, and the sequence of selection will generate a numerical password. The result showed that the image sequence length was generally shorter than the textural password length. To address this problem, two pictures can be combined to compose a new alphabet element, thus expanding the image alphabet size.

RECALL BASED

A. Reproduce a drawing

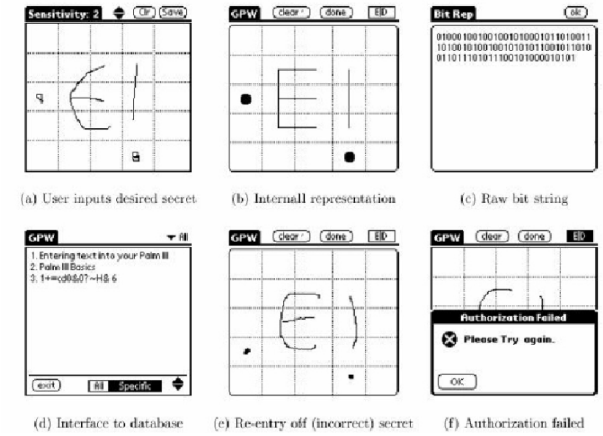

Fig 4 A graphical password scheme proposed by Jansen, et al

Jermyn, et al. proposed a technique, called "Draw - a -secret (DAS)", which allows the user to draw their unique password .A user is asked to draw a simple picture on a 2D grid. The coordinates of the grids occupied by the picture are stored in the order of the drawing. During authentication, the user is asked to redraw the picture. If the drawing touches the same grids in the same sequence, then the user is authenticated. Jermyn, et al. suggested that given reasonable-length passwords in a 5 X 5 grid, the full password space of DAS is larger than that of the text based password.

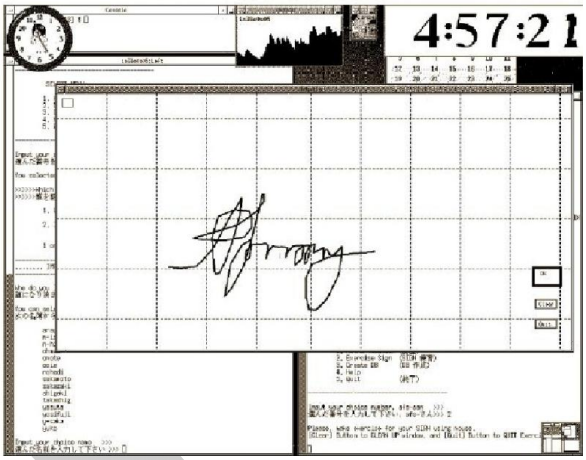

Fig 5 draw –a-secret (das) technique proposed by Jermyn, et al

NEW TECHNIQUE FOR GRAPHICAL PASSWORD AUTHENTICATION

Here we are proposing a new algorithm of authentication using graphical images. When a user tries to register over a network we will ask him or her to select a theme or sequence of pictures from already given image frame. The local host downloads an image frame which contains various themes of sequence of pictures which act as passwords, these are given by server. Since any image is made of pixels we have its gray level concentration. In this way the image will be distorted and can't be in original form. So it is not easy for hacker to reproduce the original form of image. For example, the user will select an image from database as a password, then encrypt the password and stored in the database for login user will again asked to pickup an image from database. Then s ever reproduces the encrypted image and the image compared to original if it matches user will allow surfing on website.

International Journal On Engineering Technology and Sciences – IJETS™
ISSN (P): 2349-3968, ISSN (O): 2349-3976
Volume 2 Issue 2, February 2015

DESIGN AND IMPLEMENTATION OF GRAPHICAL PASSWORD

To make sure that this project will be done a Hardware and Software requirements are needed as follows. The Software needed to develop the new scheme is:

1. Delphi programming language.
2. Windows operating system (XP/7).

The Hardware needed to develop the new scheme will have these specifications because the Graphical Password schemes need to deal with pictures or photos which need more memory and storing space where these requirements are:

1. PC with high performance processor
2. DDR Memory minimum 1GB.
3. HDD for large data stored

For example we can implement authentication of graphical password method for our college TCENET. The login interface designed to login to the system for both the existing user and new user.

Fig 7 login interface

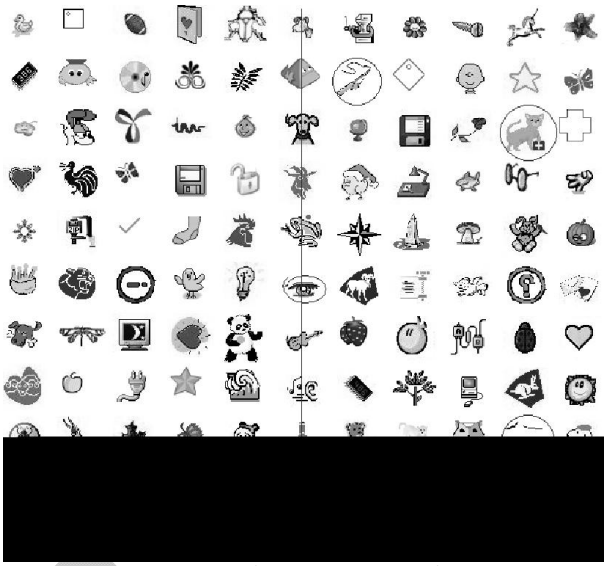

Fig 8 Choosing password

SECURITY

Very little research has been done to study the difficulty of cracking graphical passwords. Because graphical passwords are not widely used in practice, there is no report on real cases of breaking graphical passwords. Here we briefly exam some of the possible techniques for breaking graphical passwords and try to do a comparison with text-based passwords.

BRUTE FORCE SEARCH

The main defense against brute force search is to have a sufficiently large password space. Text-based passwords have a password space of 94^N, where N is the length of the password, 94 is the number of Printable characters excluding SPACE. Some graphical password techniques have been shown to provide a password space similar to or larger than that of text-based passwords. Recognition based graphical passwords tend to have smaller password spaces than the recall based methods. It is more difficult to carry out a brute force attack against graphical passwords than text-based passwords. The attack programs need to automatically generate accurate mouse motion to

imitate human input, which is particularly difficult for recall based graphical passwords. Overall, we believe a graphical password is less vulnerable to brute force attacks than a text-based password.

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.

SHOULDER SURFING PROBLEM AND ITS SOLUTIONS

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. None of the recall-based based techniques are considered should-surfing resistant. To overcome this shoulder surfing problem, we implement a new idea when we move our mouse over the password selection area, then the mouse pointer becomes small dot point .and another method is to rearrange the images randomly in the password selection image so that shoulder surfing problem can be reduced.

RELIABILITY

The major design issue for recall-based methods is the reliability and accuracy of user input recognition. In this type of method, the error tolerances have to be set carefully overly high tolerances may lead to many false positives while overly low tolerances may lead to many false negatives. In addition, the more error tolerant the program, the more vulnerable it is to attacks.

ADVANTAGE OF GRAPHICAL PASSWORD OVER TEXT BASED PASSWORDS

Graphical passwords may offer better security than text based password because many people in attempt to memorize text based passwords, use plain words(rather than 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 a 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 the built-in delay of only 0.1 second following the selection of each image until the selection of the next page, it would take millions of years to break into the system by hitting it with random image sequences therefore hacking by random combination is impossible.

CONCLUSION

The past decade has seen a growing interest in using graphical passwords as an alternative to the traditional text-based passwords .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. Our preliminary analysis suggests that it is more difficult to break graphical passwords using the traditional attack methods such as brute force search, dictionary attack, or spyware. However, since there is not yet wide deployment of graphical password systems, the vulnerabilities

of graphical passwords are still not fully understood. Overall, the current graphical password techniques are still immature. Much more research and user studies are needed for graphical password techniques to achieve higher levels of maturity and usefulness

REFERENCES

[1] S. Patrick, A. C. Long, and S. Flinn, "HCI and Security Systems," presented at CHI, Extended Abstracts (Workshops). Ft. Lauderdale, Florida, USA., 2007.

[2] BOWER, G. H., KARLIN, M. B., AND DUECK, A. 1975. Comprehension and memory for pictures. Memory and Cognition 3, 216-220.

[3] ATTNEAVE, F. 1955. Symmetry, Information and Memory Patterns. American Journal of Psychology 68, 209-222.

[4] BLONDER, G. 1996. Graphical passwords. United States Patent 5559961.

[5] FELDMEIER, D. AND KARN, P. 1989. UNIX password security-Ten years later. In Proceedings of the 19th International Conference on Advances in Cryptology (CRYPTO '89).

Author Biography: -

Kumar Charlie Paul, Principal of A.S.L Pauls College of Engineering & Technology. Had did many National and International Conferences and published many papers in journals. He also guided many students for their Ph.D project works. Having more than 23 years of experience in teaching field.