www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 2 Issue 9 September 2013 Page No. 2765-2769

Graphical Password or Graphical User Authentication as Effective Password Provider

Khundrakpam Johnson Singh, Usham Sanjota Chanu

Johnkh34@gmail.com, chanu06atcs012@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). For this reason, the graphical-password approach is sometimes called graphical user authentication (GUA). The most common computer authentication method is to use alphanumerical usernames and passwords. This method has been shown to have significant drawbacks. For example, users tend to pick passwords that can be easily guessed. On the other hand, if a password is hard to guess, then it is often hard to remember. Graphical passwords are an alternative to alphanumeric passwords in which users click on images to authenticate themselves rather than type alphanumeric strings.*

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. Because of these (presumed) advantages, there is a growing interest in graphical password. In addition to workstation and web log-in applications, graphical passwords have also been applied to ATM machines and mobile devices.

Keywords: Password, graphical user interface, secure, reliable, usability.

1. INTRODUCTION

Human factors are often considered the weakest link in a computer security system. Patrick, et al. [1] point out that there are three major areas where human-computer interaction is important: authentication, security operations, and developing secure systems. According to a recent Computerworld news article, the security team at a large company ran a network password cracker and within 30 seconds, they identified about 80% of the passwords. On the other hand, passwords that are hard to guess or break are often hard to remember. Studies showed that since user can only remember a limited number of passwords, they tend to write them down or will use the same passwords for different accounts. To address the problems with traditional username-password authentication, alternative authentication methods, such as biometrics [2, 7], have been used. In this paper, however, we will focus on another alternative: using pictures as passwords. 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. Because of these (presumed) advantages, there is a growing interest in graphical password.

2. EXISTING SYSTEM

Graphical password schemes can be grouped into three general categories based on the type of cognitive activity required to remember the password: recognition, recall, and cued recall. Recognition is the easiest for human memory whereas pure recall is most difficult since the information must be accessed from memory with no triggers. Cued recall falls somewhere between these two as it offers a cue which should establish context and trigger the stored memory.

Among existing graphical passwords, CCP most closely resembles aspects of Passfaces [3], Story, and PassPoints [3]. Conceptually, CCP is a blend of the three; in terms of implementation, it is most similar to PassPoints. It also avoids the complex user training requirements found in a number of graphical password proposals, such as that of Weinshall [4].

Passfaces is a graphical password scheme based primarily on recognizing human faces. During password creation, users select a number of images from a larger set. To log in, users must identify one of their pre-selected images from amongst several decoys. Users must correctly respond to a number of these challenges for each login. Davis et al [5]. implemented their own version called Faces and conducted a long-term user study. Results showed that users could accurately remember their images but that user-chosen passwords were predictable to the point of being insecure.

Davis et al. proposed an alternative scheme, Story that used everyday images instead of faces and required that users select their images in the correct order. Users were encouraged to create a story as a memory aid. It fared somewhat worse than

Faces for memorability, but user choices were much less predictable.

The idea of click-based graphical passwords originated with Blonder who proposed a scheme where a password consisted of a series of clicks on predefined regions of an image. Later, Wiedenbeck et al proposed PassPoints, wherein passwords could be composed of several (e.g., 8) points anywhere on an image. They also proposed a "robust discretization" scheme, with three overlapping grids, allowing for login attempts that were approximately correct to be accepted and converting the entered password into a cryptographic verification key.

Wiedenbeck et al. examined the usability of PassPoints in three separate in-lab user studies to compare text passwords to PassPoints, test whether the choice of image impacted usability, and determine the minimum size of the tolerance square. The overall conclusion was that PassPoints was a usable authentication scheme.

We recently conducted two user studies on a PassPoints-style system. Our initial lab study revisited the original usability claims, explored usability of such passwords on a wider range of images and gathered information about users' password choices. Next, we conducted a large-scale field study that examined click-based graphical passwords in practice.

Intuitively, it seems obvious that some areas of an image are more attractive to users as click-points. If this phenomenon is too strong, the likelihood that attackers can guess a password significantly increases. If attackers learn which images are being used, they can select a set of likely hotspots through image processing tools or by observing a small set of users on the target image and then building an attack dictionary based on those points.

3. PROPOSED SYSTEM

Graphical passwords allow users to click on certain areas of the screen that are then converted by the computer to be used for authentications.

Picture Password

A series of steps are carried out in the proposed system, these steps provide:
User is presented with a grid of pictures (photographs) or segments of a single picture, user clicks on a sequence of pictures each segment of the picture grid is associated with a value matrix.
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 techniques 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.

3.1 Recognition Based 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.

We proposed a graphical password mechanism for mobile devices. During the enrolment 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 thumbnail 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.

3.2 Cued Click Points

Cued Click Points (CCP) is a proposed alternative to PassPoints. In CCP, users click one point on each of c = 8 images rather than on five points on one image. It offers cued-recall and introduces visual cues that instantly alert valid users if they have made a mistake when entering their latest click-point (at which point they can cancel their attempt and retry from the beginning). It also makes attacks based on hotspot analysis more challenging, as we discuss later. As shown in Figure 1, each click results in showing a next-image, in effect leading users down a "path" as they click on their sequence of points. A wrong click leads down an incorrect path, with an explicit indication of authentication failure only after the final click. Users can choose their images only to the extent that their click-point dictates the next image. If they dislike the resulting images, they could create a new password involving different click-points to get different images.

We envision that CCP fits into an authentication model where a user has a client device (which displays the images) to access an online server (which authenticates the user). We assume that the images are stored server-side with client communication through SSL/TLS.

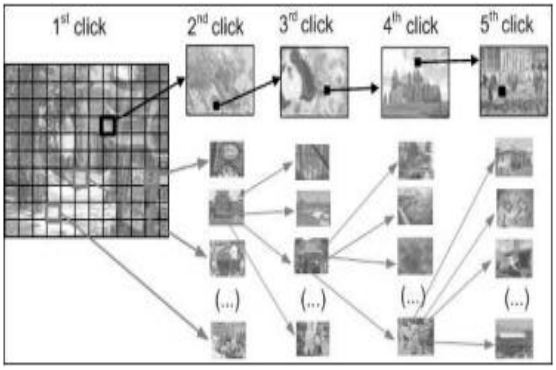

Fig 1: CCP passwords can be regarded as a choice-dependent path of images

4. MAJOR DESIGN AND IMPLEMENTATION ISSUES OF GRAPHICAL PASSWORDS

4.1 Usability

One of the main arguments for graphical passwords is that pictures are easier to remember than text strings. Preliminary user studies presented in some research papers seem to support this. However, current user studies are still very limited, involving only a small number of users. We still do not have convincing evidence demonstrating that graphical passwords are easier to remember than text based passwords.

A major complaint among the users of graphical passwords is that the password registration and log-in process take too long, especially in recognition-based approaches. For example, during the registration stage, a user has to pick images from a large set of selections. During authentication stage, a user has to scan many images to identify a few pass-images. Users may find this process long and tedious. Because of this and also because most users are not familiar with the graphical passwords, they often find graphical passwords less convenient than text based passwords.

4.2 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.

4.3 Storage and Communication

Graphical passwords require much more storage space than text based passwords. Tens of thousands of pictures may have to be maintained in a centralized database. Network transfer delay is also a concern for graphical passwords, especially for recognition-based techniques in which a large number of pictures may need to be displayed for each round of verification.

5. MODULE DESCRIPTION

There are mainly three modules, they are:

5.1 Module for Select from stored images

In such a scheme the user chooses several locations in an image to create a password. To log in the user must click on or close to those locations. There are multiple rounds of images (8 images). In an implementation of this scheme the image had predefined click objects or regions that were outlined by thick boundaries. The users chose the password from these objects and logged in using them.

5.2 Module for Finding Coordinates and Range

The user must recognize and click anywhere on the previously chosen image regions (ranges). This procedure is repeated with different target and different images, for a total of 8 images. Only if the user chooses all 8 correct regions, will he or she successfully log in.

5.3 Module for Password Generation

To log in the users must click within the region of their chosen click points. Their memory is cued by the image as they enter their password. The system or the user could provide the image. The main requirement is that it be a complex image that is visually rich enough to have many potentially memorable click places. Without artificial predefined boundaries, more intricate images, such as natural scenes, can be used.

6. RESULTS

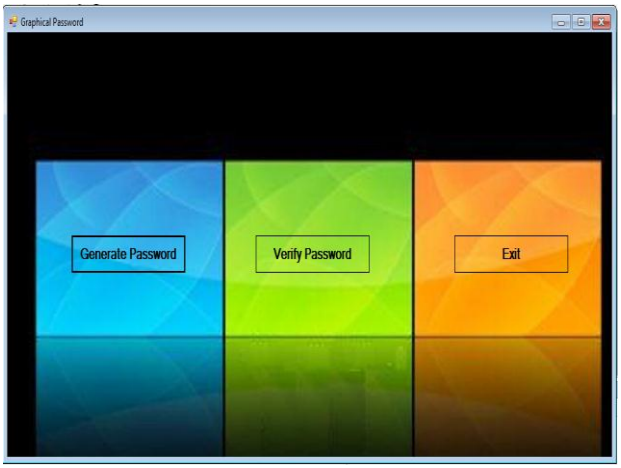

Fig.2: Main Module for password generation

The main module consist of three sub modules namely Generate password, Verify Password and Exit.

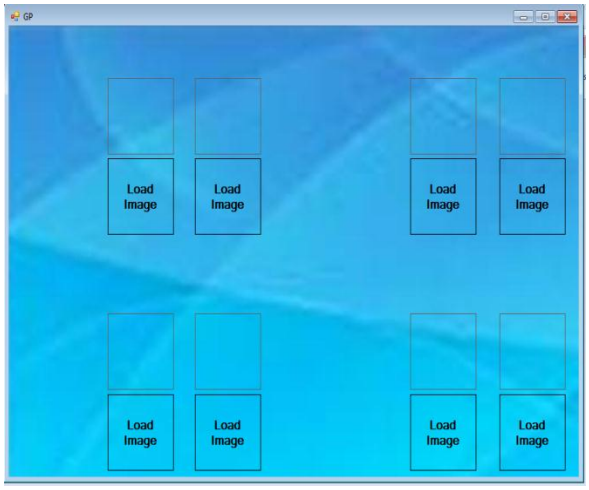

Fig.3: Module for picture selection

The Generate password module consists of 8 grids for loading the picture from a database. This module helps in loading the picture in an order sequence, may be vertically or horizontally. The 8 grids for picture selection can be extended according to the user's demand.

This module also contains the addition of user Id for authentication. The selection of the picture along with the proper sequence of its selection gives a secure password.

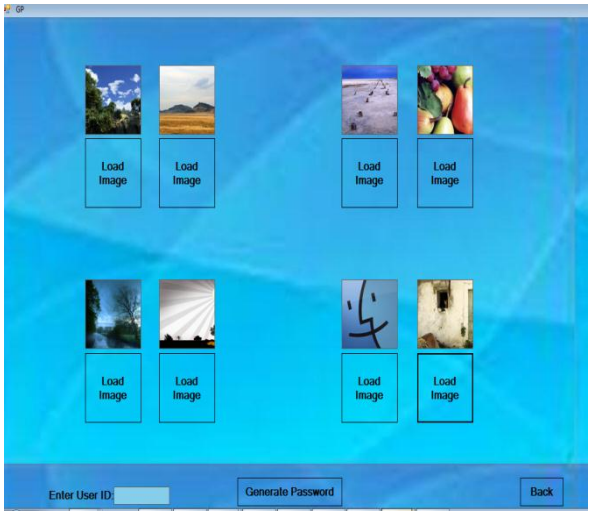

Fig.4: Selected image from a database

After the selection of the picture, enter a user Id. In our model we enter 12345 as a user Id and click on each picture (at a particular point of the picture). Then we can generate the password by clicking the Generate Password button. The database will store the coordinates of each click on the pictures we have taken.

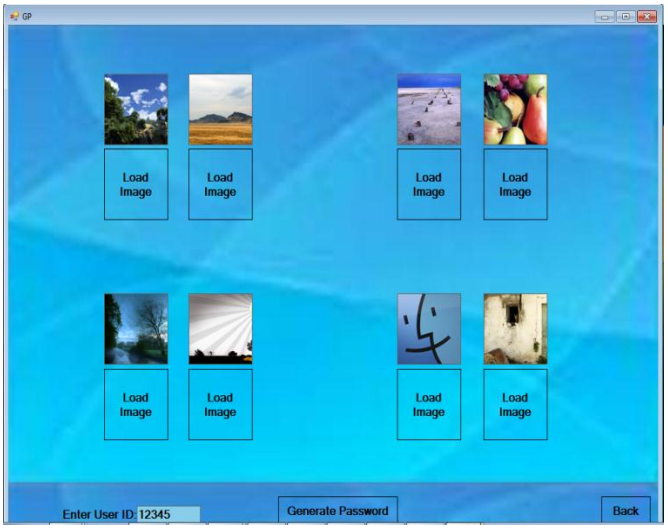

Fig.5: Enter a user Id

The last step is to verify the password we have created. In order to do this we again load the same picture from the database in the same order we taken earlier. Then entering the user Id we have taken, we start clicking the picture with the help of the mouse.

If the same Id is taken and if have clicked at the points where we have already clicked (approximately around +10 and – 10 of the co-ordinates of the clicked points) then the password is verified. On the other hand if one of the picture sequences is improper or the wrong picture has been selected or even the wrong Id is entered then the password will not valid.

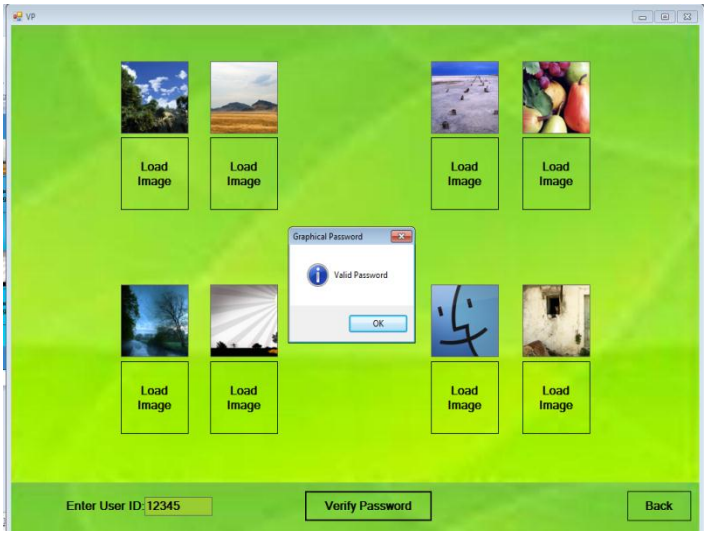

Fig.6: Verifying password and user Id

7. CONCLUSION

The past decade has seen a growing interest in using graphical passwords as an alternative to the traditional text-based passwords. In this paper, we have conducted a comprehensive survey of existing graphical password 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. 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.

We are interested in studying the process of consolidation of graphical passwords in memory more fully and in investigating the time to input graphical passwords when the user has become highly skilled. This automation did not occur in our studies because of the focus on memorability, which dictated intermittent use over time.

8. REFERENCE

[1]. A. S. Patrick, A. C. Long, and S. Flinn, "HCI and Security Systems," presented at CHI, Extended Abstracts (Workshops). Ft. Lauderdale, Florida, USA., 2003.

[2]. K. Gilhooly, "Biometrics: Getting Back to Business," in *Computerworld*, *May 09*, 2005.

[3]. A. Jain, L. Hong, and S. Pankanti, "Biometric identification," *Communications of the ACM*, vol. 33, pp. 168-176, 2000.

[4]. D. Weinshall and S. Kirkpatrick, "Passwords You'll Never Forget, but Can't Recall," in Proceedings of Conference on Human Factors in Computing Systems (CHI). Vienna, Austria: ACM, 2004, pp. 1399-1402

[5]. D. Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical password schemes," in Proceedings of the 13th Usenix Security Symposium. San Diego, CA, 2004.

[6]. A. Jain, L. Hong, and S. Pankanti, "Biometric identification," Communications of the ACM, vol. 33, pp. 168-176, 2000.

BIOGRAPHIES

KHUNDRAKPAM JOHNSON SINGH completed his B.E degree in computer science and engineering from KBNCE in 2010, completed M.Tech from Dayananda Sagar College of Engineering, Bangalore and now working as an Assistant Professor in National Institute of Technology, Manipur in Computer Science and Engineering department. Khundrakpam Johnson Singh is the main author and may be reached at johnkh@gmail.com.

USHAM SANJOTA CHANU completed her B.E degree in computer science and engineering from ICFAI, Tripura in 2010, completed M.Tech from SJBIT, Bangalore and now working as an Assistant Professor in Channabasaveshwara Institute of Technology, Tumkur in Computer Science and Engineering department. Usham Sanjota Chanu may be reached at chanu06atcs012@gmail.com