Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 6, Issue. 6, June 2017, pg.394 – 400

Graphical Password Authentication

Towseef Akram[1], Vakeel Ahmad[2], Israrul Haq[3], Monisa Nazir[4]

[1]Student, Computer Science Engineering, SSM College of Engineering & Technology, Kashmir, India
haqisrar999@gmail.com
[2]Student, Computer Science Engineering, SSM College of Engineering & Technology, Kashmir, India
ervakeel3774@gmail.com
[3]Student, Computer Science Engineering, SSM College of Engineering &Technology, Kashmir, India
towseefakram786@gmail.com
[4]Assistant Professor, Computer Science Engineering, SSM College of Engineering & Technology, Kashmir, India
monisanazir.ssm@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 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 disadvantages. For e.g, users tend to choose passwords that can be easily guessed. On the other hand, if a password is difficult to guess, then it is often difficult to remember. To overcome this problem of low security, Authentication methods are developed by researchers that use images as password. In this research paper, we conduct a comprehensive survey of the existing graphical password techniques and provide a possible theory of our own. Graphical password schemes have been proposed as a possible alternative to text-based schemes, by the fact that humans can remember pictures better than text; Pictures are generally easier to be remembered or recognized than text.*

1. INTRODUCTION

Password is a secret that is used for authentication. Passwords are the commonly used method for identifying users in computer and communication systems. It is supposed to be known only to the user. 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).

Human factors are often considered the weakest point in a computer security system. Patrick, et [1] point out there are three major areas where human-computer interaction is important: security operations, developing

secure systems, authentication. Here we focus on authentication problem . User authentication is one of the important and fundamental component in most computer security systems. Biometrics is one of the important authentication methods used to tackle the problems associated with traditional username-passwords. But here we will deal with another alternative: using image as passwords.

According to a recent computer world 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 difficult to guess or break are often difficult 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 divided into three major categories based on the type of 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 mix 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 remembers 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. 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, Wieden beck 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. Wieden beck 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 Pass Points was a usable authentication scheme.

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

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 thumb nail 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.

3.2 Cued Click Points

Cued Click Points (CCP) is a proposed alternative to Pass Points. 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.

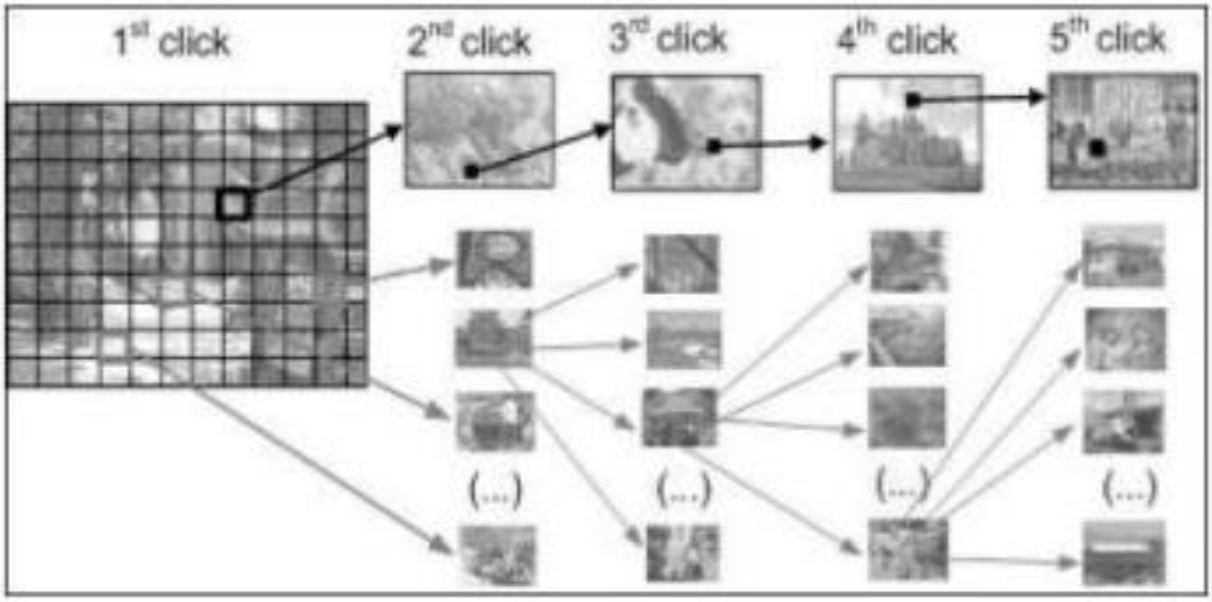

Fig 1: CCP passwords can be regarded as a choice-dependent path of images

C. Implementation and Discussion

The proposed system was implemented using PHP, CSS, JavaScript and Macromedia flash 2008(Action Script 2). This Graphical Password can be implemented in authenticating several systems and websites. The implementation has few focuses:

- Password: Contain image as reference & encryption algorithm.
- Grids: Contains unique grid values and grid clicking related methods.
- Login: Contains username, images, Graphical password and related methods.
- SSR shield: Contains shield for Shoulder surfing.

As shown in the figure below researchers are trying to stabilize the goal in text based system. However, the text based approach is not able to achieve the goal because as the password strength increases usability

decreases. Our main aim is to achieve this goal. In which the usability as well as the security of the system is maintained in such a way that we don't need to compromise on either of these constraints.

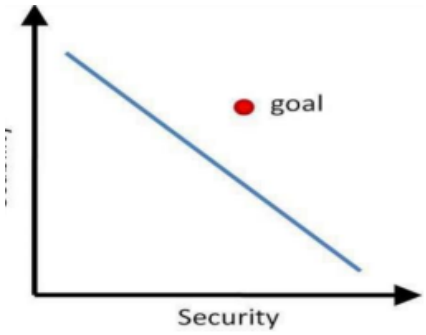

Fig.2: Usability VS Security

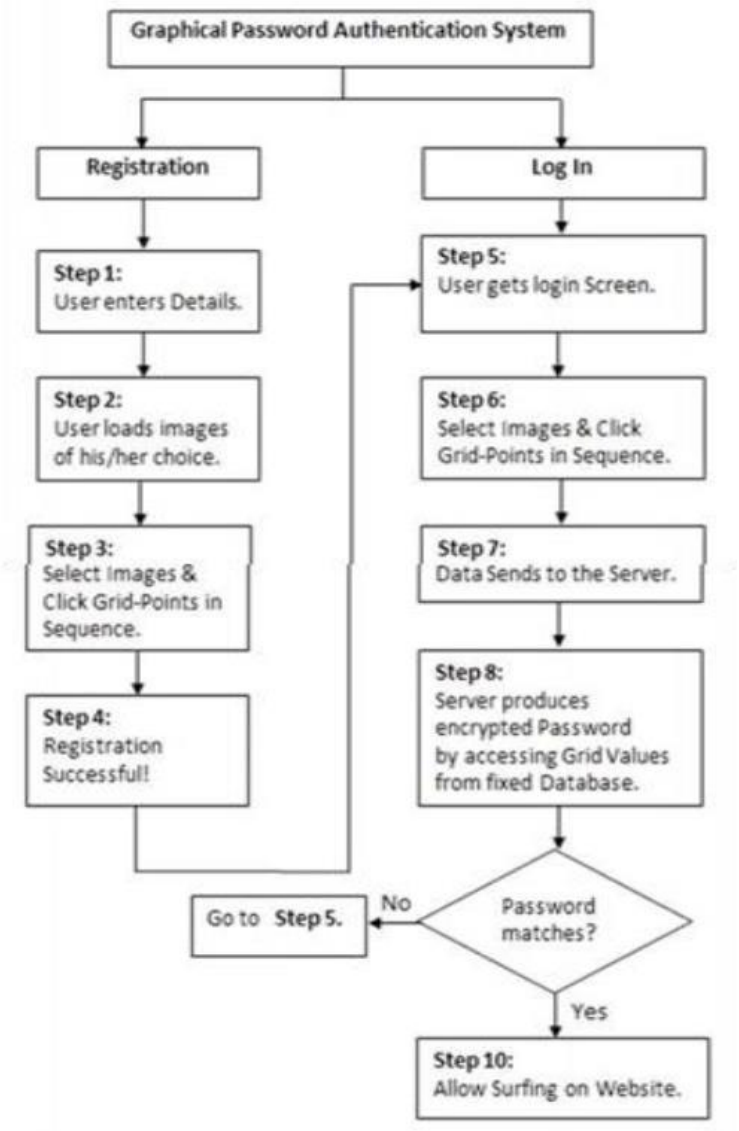

FIG 3. FLOW GRAPH

4. ADVANTAGES:

- Graphical passwords schemes provide a way of making more human friendly passwords.
- Here the security of the system is very high.
- Dictionary attacks and brute force search are infeasible.

5. CONCLUSION:

The past decade has shown 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 use 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. 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]. 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 *Computer world, 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:

Towseef Akram is pursuing B.E Degree from SSM College of Engineering & Technology in Computer Science Engineering from University of Kashmir, J&K, India. His field of interest is ASP.Net & SQL.

Vakeel Ahmad is pursuing B.E Degree from SSM College of Engineering &Technology in Computer Science Engineering from University of Kashmir, J&K, India. His field of interest is ASP.Net &SQL.

Israrul Haq is pursuing B.E Degree from SSM College of Engineering &Technology in Computer Science Engineering from University of Kashmir, J&K, India. His field of interest is ASP.Net &SQL

Monisa Nazir, is the Assistant Professor at SSM College of Engineering & Technology in The Department of Computer Science Engineering. Her field of interest is signal analysis and operating system.

