International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 06 | June 2020 www.irjet.net p-ISSN: 2395-0072

Review on the Graphical User Authentication System

Ashish Rasal[1], Vicky Prasad[2], Ketan Bhujbal[3], Saurabh Ubale[4], Mr. D.S. Thosar[5]

[1-4]Last Year Computer Engineering Student S.V.I.T. Chincholi, Nashik
[5]Assistant Professor, Department of Computer Engineering S.V.I.T. Chincholi, Nashik

---

Abstract - *A graphical password is an authentication system that works on selecting the user from images, presenting them in some order, in a graphical user interface (GUI). Due to this, the graphical-password system is called graphical user authentication (GUA). The most common computer authentication method is to use an alphanumeric username and password. This method has been shown to cause significant damage. For example, users select passwords that can be easily guessed. On the other hand, if a password is difficult to guess, it is often difficult to remember it. To overcome this problem of low security, authentic methods are developed by researchers who use images as passwords. In this research paper, we conduct an extensive survey of existing graphical password techniques and provide our possible theories. Graphical password schemes have been proposed as a possible alternative to text-based schemes because humans can remember images better than text; Pictures are generally easier to remember or recognize than text.*

Key Words: Graphical Password, Security, Persuasive Cued Clicks, Pattern Detection, Authentication

1. INTRODUCTION

A password is a secret used for authentication. Passwords are a commonly used method of identifying users in computers and communications systems. It is known only to the user. A graphical password approach is an authentication system that works on selecting the user from images, presenting them in a specific order, 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 al. Indicate that there are three major areas where human-computer interaction is important: security operations, developing secure systems, authentication. Here we focus on the authentication problem. User authentication is one of the important and fundamental components in most computer security systems. Bio-Matrix is one of the important authentication methods used to deal with problems associated with traditional username-passwords. But here we will deal with another option: using an image as a password[3].

Graphical methods of creating passwords provide a predefined depiction of the image. In this image, the selected chain and tap area are taken as graphical passwords. Graphical methods of password creation became popular since then. Linked to the company of graphical methods of password creation, which is that it is easier for humans to remember graphically than text. Therefore the graphical method is the best option that has been proposed so far. The most important objective of this work is to select more random and complex passwords for guessing attacks and hearty users.

2. LITERATURE SURVEY

A comprehensive survey of existing graphical password techniques is performed. These techniques are classified into four types: recognition-based, pure recall-based, cared-recall based and hybrid approaches. Here the strengths and drawbacks of each method are analyzed. This survey will be particularly useful for researchers who are interested in developing new graphical password algorithms as well as industry practitioners who are interested in implementing graphical password techniques. Promotion of password authentication system with the help of images is proposed. This paper mainly focuses on the concept of graphical password system. This is supported by click points for authentication purpose. The basic concept of this system is simply the user's interaction with a sequence of images. The basic goal of this system is to achieve high security with simple technology to be used by a user and difficult to guess by a hacker. The graphical password authentication system is the best option for text passwords. Click point (CP) is the best option for older graphical password systems. CP is a combination of five click points on particular images. In this paper, CP has been combined with new technologies such as mobile phones and e-mail[2].

A novel authentication system called pass matrix is proposed based on graphical passwords to resist shoulder surfing attacks. Operate horizontal and vertical bars with a one-time valid login indicator and covering the entire scope of pass-images, the pass matrix provides no indication for attackers to detect or narrow passwords, even they Many conduct camera-based attacks. A pass matrix prototype was implemented on Android and real user experiments were carried out to evaluate its recall and usability. From the experimental results, the proposed system achieves better resistance to shoulder surfing attacks while maintaining usability.

3. SYSTEM OBJECTIVE

To validate the end user for authentication we usually prefer to adopt the knowledge-based authentication.

- To support the users in selecting better and safe passwords.
- To provide a security to the system.
- To reduce the guessing attacks and assign a strong password to the system.
- To select more random, and difficult passwords to guess.

4. SYSTEM ARCHITECTURE

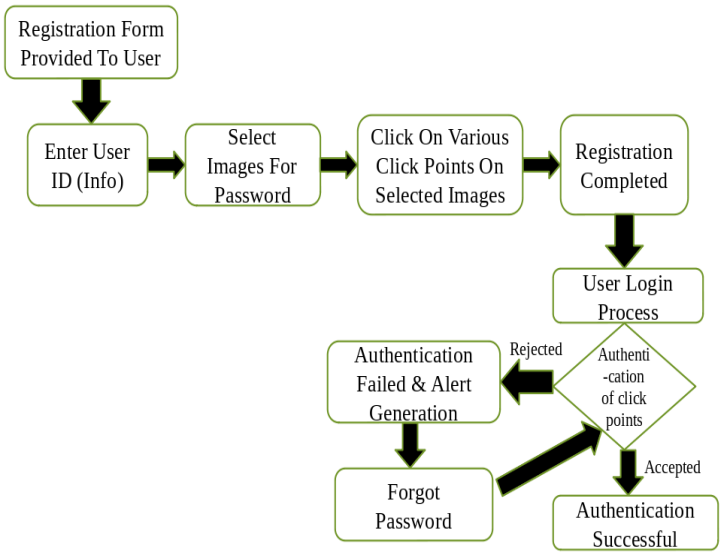

Fig1-System architecture

This process can be done by using the algorithms the algorithms are:

1. Sign Up

This feature allows all users including servicemen or product vendors can register their details along with credentials.

2. Login

This feature allows all types of users a secure authentication mechanism in order to get access to the system.

3. PCP password creations:

- Layer 1:- 1st password is set on image through clicking event check attribute height, width, and size and image name.

- Layer 2:- 2nd password is set on image through cropping image with X and Y axis checking.

- Layer 3:- 3rd password is set on select point around images like if we select three point it will be triangle around image. If four it will be a cube (this will check points and shape and also X and Y axis) click point plays a vital role for password protection, the graphical password are more protected and are better than the alphanumeric passwords. One most important factor with the graphical passwords is they are very easy to memorize for the user and more protected as well. Online password guessing attacks are more common these days and so the use of more protected password system is needed which brings us to graphical passwords.

5. CONCLUSION

The last decade has shown a growing interest in using graphical passwords as an alternative to traditional text-based passwords. In this paper, we have done a comprehensive survey of existing graphical password techniques. Although the main use of this system is that it is better to remember graphical passwords than human text-based passwords, existing human studies are very limited and there is not yet convincing evidence to support this argument. Our study suggests that it is more difficult to hack graphical passwords using traditional attack methods such as brute force search, dictionary attack, or spyware. Overall, current graphical password techniques are still immature. Much research and user studies are required for graphical password techniques to achieve high levels of maturity and usability.

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 13thUsenix 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