International Journal of Recent Trends in Engineering & Research (IJRTER)
Conference on Electronics, Information and Communication Systems (CELICS'18)
Special Issue; March - 2018 [ISSN: 2455-1457]
DOI : 10.23883/IJRTER.CONF.02180328.008.D09QI

Graphical Password Authentication System Based On Persuasive Cued Click-Points

V.Sunilanandh,
Asst.Prof / Department of CSE,
Annai Vailankanni College of Engineering.

Abstract **- The main goal for authentication systems is to support users in selecting better passwords. Users often use easily memorable passwords that are easy for attackers to guessing attack, but strong system assigned password is difficult for users to remember. Graphical password generally uses an image or representation of image as password. Human brain is better in remembering picture than remembering a textual character. There are various graphical password schemes or graphical password software in the market. However, not much research has been done to analyze graphical passwords that are still immature. Hence, this project work is based on persuasive cued clicks points (PCCP). The major goal of this work is to protect against guessing attacks as well as encouraging users to select more random and difficult passwords to be guessed by an attacker. Well known security threats like brute force attacks and dictionary attacks can be successfully abolished using this method.**

Key Terms - **Authentication, graphical passwords, guessing attacks, computer security.**

1. INTRODUCTION

There has been a great deal for graphical passwords since two decades due to the fact that primitive method suffered from an innumerable number of attacks which could be imposed easily. The progress of taxonomy of the authentication methods is discussed in this section. To start with, the most common computer authentication method that makes use of text passwords is focused. Despite the vulnerabilities, it's the user's natural tendency that they will always prefer to go for short passwords for ease of remembrance and also lack of awareness about how attackers are likely to attack. These types of passwords are broken mercilessly by intruders by several simple means such as, masquerading, eavesdropping and other means like dictionary attacks, shoulder surfing attacks, social engineering attacks, etc. To mitigate the problems with traditional methods, recent methods have been proposed using graphical points as passwords. Since then, many other graphical password schemes have been proposed. The desirable quality associated with graphical passwords is that, psychologically humans can remember graphical password far better than text and hence is the best alternative which is proposed in this paper. There is a rapid and growing interest in graphical passwords since they are infinite in number, thus providing more resistance to any attack launched by intruders. The major aim of this work is to reduce the guessing attacks as well as encouraging the users to select random and difficult passwords that cannot be guessed.

Special Issue; March - 2018 [ISSN: 2455-1457]
DOI : 10.23883/IJRTER.CONF.02180328.008.D09QI

2. RELATED WORK

In [1], Sonia Chiasson and Elizabeth Stobertto have proposed a password authentication system that encourages using strong passwords while maintaining memorability. It says that this authentication schemes allow user's choice while influencing users toward stronger passwords. It is easier to follow this system's suggestions for a secure password. In [2], Paul C. van Oorschot, Amirali Salehi-Abari have proposed a system
where the password consists of a sequence of random images in which the user can select one click-point per image. In addition, the user is asked to select a sound signature corresponding to each click point. This sound signature is
used to help the user in recalling the click point on an image. This system showed very good performance in terms of speed, accuracy and ease of use. In [3], S. Chiasson, R. Biddle and P. van Oorschot have proposed a system that uses persuasion to influence user's choice in click-based graphical passwords while encouraging them to select more random, and hence more secure, click-points. In this approach, persuasion to the Cued Click-Points graphical password scheme is introduced, as it reduces hotspots while still maintaining its usability. In [9], S. Man, D. Hong, and M. Mathews have proposed a system where the users click on one point per image for a sequence of images. The next image is based on the previous click-point. They presented the results of an initial user study which revealed positive results. The performance was found to be good in terms of speed, accuracy and minimized number of errors. Users preferred CCP to Pass Points since selecting and remembering only one point per image was easier and additionally the sound signature helps considerably in recalling the click points. It also suggested that CCP provides greater security than PassPoints because the number of images increases the workload for the attackers.

3. 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 their information. Online password guessing attacks have been known since the days of the Internet. There is a small academic literature on the prevention techniques. This method deals with guessing attacks like brute force attacks and dictionary attacks. This work proposes a click-based graphical password system. The various phases involved in conducting this experiment are:

i. User enrollment
ii. Graphical password generation
iii. Secure password storage
iv. Database maintenance

DOI : 10.23883/IJRTER.CONF.02180328.008.D09QI

A user, new to the system, will create a new account by entering his details. A profile with the user name will be created along with a password of his choice (graphical password). From each image selected by the user, user clicks one or more points of interest in each image.The co-ordinates of the points from all images will then be collected/ filtered. Thus the password is generated using these click points. The co-ordinates in the pattern clicked and the number of strokes along with the image is redirected to the database. During authentication phase, the user has to enter the same password as in the enrollment phase. Database maintenance is achieved by using SQL server. Fig.1. shows the registration process of the user for graphical cued password management. Fig.2. shows the process flow diagram for log-in process for a user who already has an account.

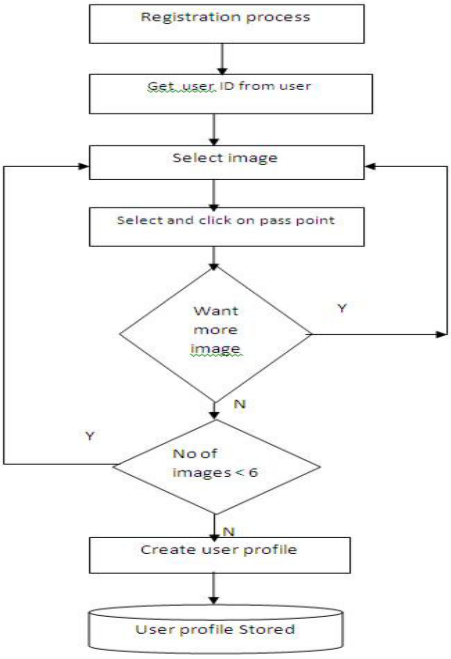


Fig.1. Registration process flow

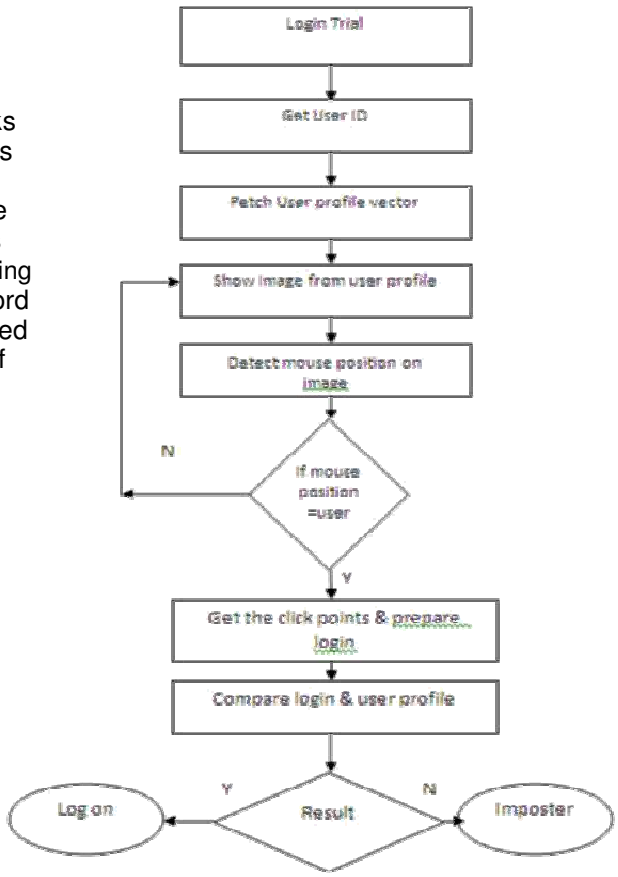


Fig.2. Existing user process flow

4. EXPERIMENTAL RESULTS

The graphical password authentication system is developed using Visual studio 2008, ASP.net with C# program. All the experiments are performed on a PC with Intel Pentium III Xeon 2.8GHz CPU, 2GB RAM with Windows XP professional Edition. The compiling environment which is used for program development is Microsoft Visual Studio 2008. The database used for this experiment is SQL server.

Fig.3. User details management page controlled by admin

Fig.3. shows how the user details are managed by the administrator. Fig.4. shows a sample password enrollment phase by clicking on the image area of interest to generate co-

DOI : 10.23883/IJRTER.CONF.02180328.008.D09QI

ordinates. Thus, the user can select more co- ordinates on one or more images which represent the graphical password.

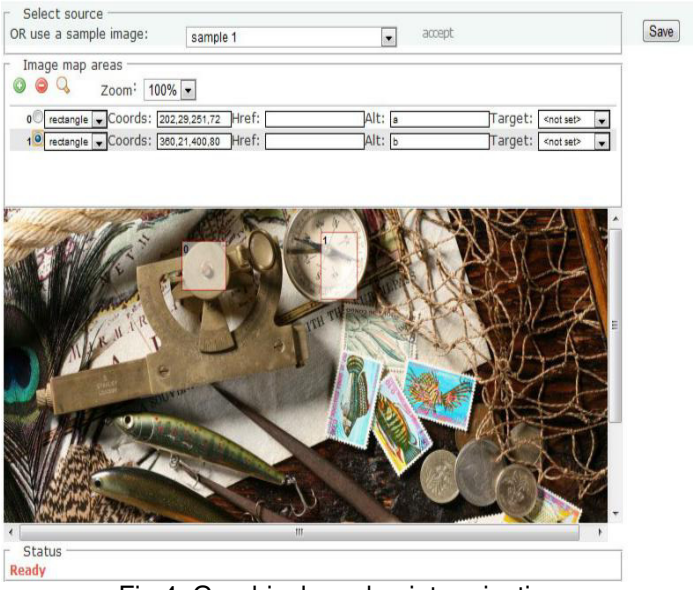
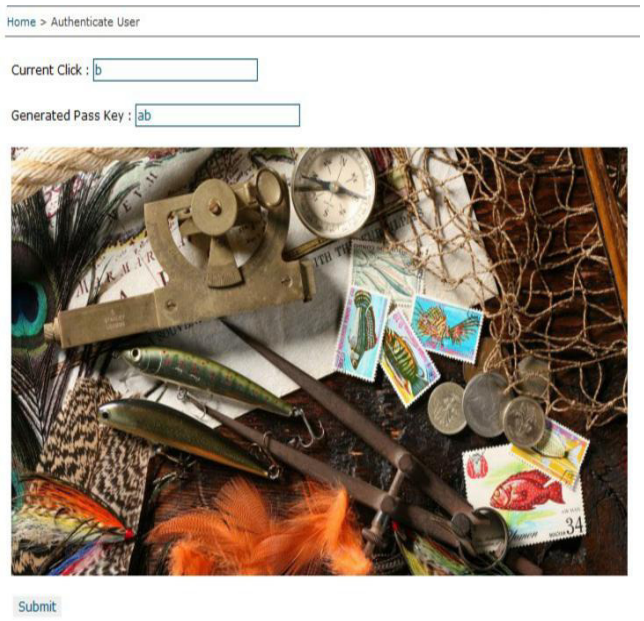


Fig.4. Graphical cued point projection

Fig.5. shows the authentication phase, where an already enrolled user enters his/her graphical password by selecting on the same points/ co-ordinates which was selected during the enrollment phase. If the clicked points, matches with the ones selected during enrollment, the user will be authenticated. Else, the user will be rejected.



DOI : 10.23883/IJRTER.CONF.02180328.008.D09QI

5.1. **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 perform 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 and it can be believed that graphical passwords are less vulnerable to dictionary attacks than text-based passwords.

5.2. **Guessing attacks**

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.

5.3. **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.

5.4. **Spy ware**

Except for 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.

6. CONCLUSION

In this paper, a click-based graphical password system is proposed. During password creation, there is a small size view port area that is randomly positioned on the image. Users select a click-point within the view port area. The view port guides users to select many random passwords that are less likely to include hotspots. This proposed system also provides protection against spyware. This paper, therefore, proposes an authentication system that protects the passwords against guessing attacks and encourages the users to select more random and difficult passwords that cannot be guessed by an attacker.

Fig.5. Authentication of user

5. DISCUSSION

Special Issue; March - 2018 [ISSN: 2455-1457]
DOI : 10.23883/IJRTER.CONF.02180328.008.D09QI

REFERENCES

[1] Sonia Chiasson, Elizabeth Stobert, "Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism", IEEE Transactions on Dependable and Secure Computing, Vol. 9, No. 2, March/April 2012.

Special Issue; March - 2018 [ISSN: 2455-1457]
DOI : 10.23883/IJRTER.CONF.02180328.008.D09QI

[2] Paul C. van Oorschot, Amirali Salehi-Abari, "Purely Automated Attacks on PassPoints-Style Graphical Passwords", IEEE Transactions on Information Forensics and Security, Vol. 5, No. 3, September 2010.
[3] S. Chiasson, R. Biddle, and P. van Oorschot, "A Second Look at the Usability of Click-Based Graphical Passwords", Proc. ACM Symp. Usable Privacy and Security (SOUPS), July 2007.
[4] R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in Proceedings of 9th USENIX Security Symposium, 2000.
[5] S. Akula and V. Devisetty, "Image Based Registration and Authentication System," in Proceedings of Midwes Instruction and Computing Symposium, 2004.
[6] L. Sobrado and J.-C. Birget, "Graphical passwords," The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4, 2002.
[7] Sonia Chiasson, Alain Forget , Robert Biddle, P. C. van Oorschot, "User interface design affects security: patterns in click-based graphical passwords", Springer-Verlag 2009.
[8] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A.D. Rubin, "The Design and Analysis of Graphical Passwords," in Proceedings of the 8th USENIX Security Symposium, 1999.
[9] S. Man, D. Hong, and M. Mathews, "A shoulder surfing resistant graphical password scheme," in Proceedings of International conference on security and management. Las Vegas, NV, 2003.
[10] A. Adams and M. A. Sasse, "Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures," *Communications of the ACM*, vol. 42,

