International Journal of Engineering and Technical Research (IJETR)
ISSN: 2321-0869, Volume-2, Issue-3, March 2014

Comparison of Various Persuasive Cued Click Points for Image Applications

S.Manimurugan, Nadhiya Nazeer Khan, Sona Ann Sam

***Abstract*— One of the main problems that people today are facing is the security issues due to the use of textual or alphanumeric passwords. People always have the tendency to create simple, easy to remember passwords which can easily make an attacker to hack a computer system. So, in order to enhance the security of the system, we concentrate in this paper on different graphical password strategies. Most often access to computer systems are based on the alphanumeric passwords. long and random-appearing passwords may cause difficulty among users. For making more memorable and secure Graphical passwords have been designed. Rather than using alphanumeric characters, here images are used. More secure graphical password systems called Pass Points are designed. Comparisons were made on alphanumeric passwords and different graphical password strategies. Attacks such as brute force attack and dictionary attacks can be successfully avoided through this technique. A dictionary search can often hit on a password and allow a hacker to gain entry into a system in seconds.**

***IndexTerms*—Attacks, Authentication, Graphical Passwords, Security**

I. INTRODUCTION

Graphical Password is a type of authentication system in which user select the images in a specific manner. It is presented in a Graphical User Interface (GUI),so this approach is sometimes called graphical user authentication. Two categories for image based technique are Recognition-based technique and Recall-based graphical technique. In Recognition-based technique, a user is given with a set of images and the user gives the authentication by recognizing and identifying the images he or she selected during the registration stage. In recall- based techniques, a user is asked to recreate something that he or she created or selected earlier during the registration stage. Persuasive Cued Click Points is an efficient technique in which use of textual passwords can be avoided by making click points in images. It has an alternative feature of maintaining usability. Authentication is a process of confirmation of a person identity. There are mainly three different types of authentication. They are Token-based Authentication which includes credit cards, smart cards etc, Biometric Authentication such as fingerprints, iris scan etc, and Knowledge-based Authentication which include both textual based and picture based passwords[1][2]. A password authentication system should encourage strong passwords while maintaining memorability. Through this approach, we should enhance users towards a more secure system. Rather than increasing the difficulty for a user for selecting a textual password, it is easier to follow the systems suggestions for a secure passwords feature. This feature replaces alphanumerical passwords for general-purpose user authentication. The alphanumerical passwords can be hacked easily. So, the attackers can easily guess the text passwords of the system. So, we introduce graphical passwords instead of textual passwords in order to maintain system security. The graphical passwords are hard to guess by the attacker and easy to remember for the users[5][3]. So the password authentication system should encourage the graphical password selection while maintaining the memorability as well as usability of the user. Graphical Password is a type of authentication system in which user select the images in a specific manner [2][4]. It is presented in a Graphical User Interface (GUI),so this approach is sometimes called graphical user authentication.

Manuscript received March 19, 2014.
S.Manimurugan, Computer Science, M.G University/ Peermade, India.
Nadhiya Nazeer Khan, Computer Science, M.G University/ Peermade, India.
Sona Ann Sam Computer Science, M.G University/ Peermade, India.

II. COMPARISON OF DIFFERENT PERSUASIVE CUED CLICK POINTS FOR IMAGE APPLICATION

Persuasive Technology was first developed by Fogg [2] as technology to motivate and help people to behave in a specific manner. Persuasive Technology is an efficient computing systems designed to change people's behaviour towards authentication systems. An authentication system that applies Persuasive Technology should encourage the users to select stronger passwords. To be effective, the users do not ignore the persuasive elements and the resulting passwords must be easy to remember. Our proposed system accomplishes this by making the task of selecting memorable and more secure passwords through graphical password strategy.

A. Alphanumerical Password Strategy

Creating memorable passwords [3] using currently existing approaches are easy for attackers to guess. Also, it is very difficult for users to remember strong system-assigned passwords. Despite all possible issues, it is the natural tendency of users to go for short passwords for the purpose of remembering it in a better way. Users often lack awareness about how attackers will attack their passwords. Through Eaves dropping, dictionary attacks and social engineering attacks intruders will break the passwords easily.[9][10]

B. Graphical Password Strategy

Cued Click Points (CCP) was a new graphical password technique in which user selects one click point on each image rather than multiple click points on single image. During password creation, user has to select the sequence of the images and a click point for each image [3][5]. This data is stored on a server. The stored data will authenticate users as they enter graphical password. Persuasive Technology was first developed by Fogg, as a technology to motivate and inspire people to behave in a specific way. An authentication system which applies Persuasive Technology should guide and encourage users to select stronger passwords. To be effective, passwords must be memorable [1][5].In this system since click-points are randomly distributed the formation of hotspots are minimized. Our hypotheses were:

1. There will be less chance for selecting click-points that fall into known hotspots.
2. The click-point are randomly dispersed and will not form new hotspots.
3. Users will feel that their passwords are more secure with PCCP and more efficient

In this user login process (Fig 1), user enters the user ID as same as that of the registration. Then images are displayed normally. Repeat the sequence of clicks in the correct order. After done with all these above procedure, user can successfully login. This procedure can be explained as follows [6][7].A user after entering a valid user name and password can access their profile, given as user profile vector. Then the user can select appropriate image in a correct manner as that of the images selected during the registration. If the number of images becomes equal to that of the user profile, then the login vector and user vector are compared. If it is correct, login will be done successfully

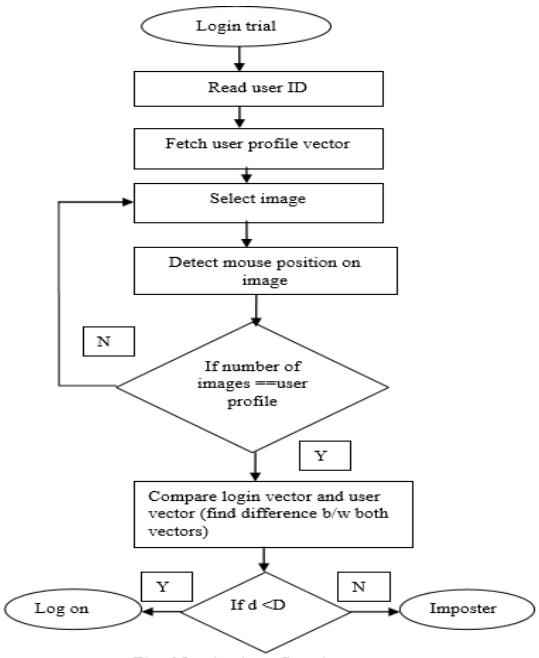

Fig1 .user login process

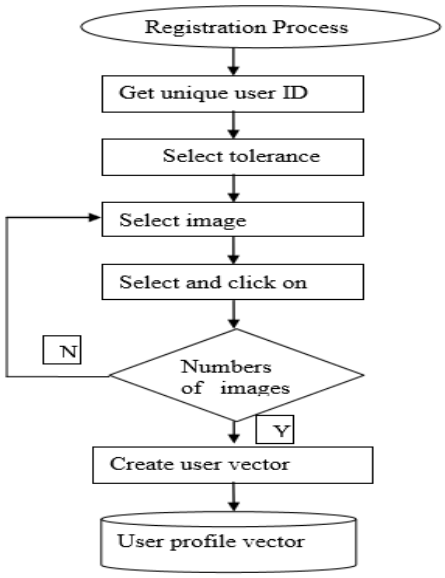

Fig 2:user registration process

In this User Registration Process, as shown in (Fig2)[1][7],after completing the registration details of a particular user, he/she will be provided with a valid username and password. Note that only a properly registered user will get username and password. After that the user is supposed to select images and make appropriate click points as per his/her likes. If the number of selected images is correct, he/she can create a user vector. After done with all procedures, user profile is provided to the user. This covers the user registration process of Graphical Password Strategies.

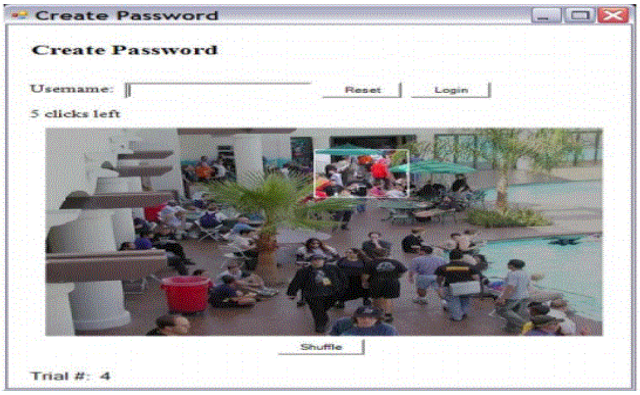

Fig 3:Password interface during PCCP Creation. The viewport highlights part of the image.

Fig 3: shows , except for a randomly positioned viewport, the images were slightly shaded when users created a password. The viewport's size was intended to offer a variety of distinct points but still cover only an acceptably small fraction of all possible points. Users were required to select a click-point within this highlighted viewport and could not click outside of this viewport. If they were unable or couldn't able to select a click-point in this region, they could press the "shuffle" button to reposition the viewport randomly. users are allowed to shuffle as often when they wanted, this can slowed the password creation process.[8] The only during password creation the viewport and shuffle buttons are created. [2][6], The images were displayed accurately,and

users were allowed to click anywhere during password confirmation and login.

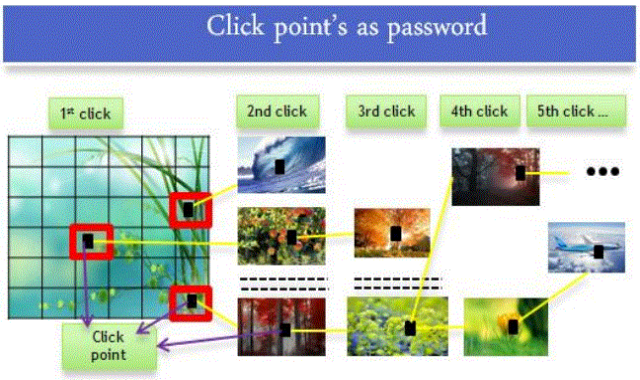

Fig 4: user can select one click point for each image in CCP.Current click- point determines the next image.

Fig 4: shows that other than using five click-points in one image, CCP uses one click-point on five different images. Based on the location of the previously entered click-point the next image is displayed. Users select their images, based on these click-point ,it determines the next image.

III. ALPHANUMERICAL PASSWORD SYSTEMS VERSUS GRAPHICAL PASSWORD SYSTEMS

No	Alphanumerical Password Systems	Graphical Password Systems
1	Enables the use of system assigned strong password, which are difficult for users to remember.	Enables the use of images which are easier for human brain to remember.
2	Possibility of guessing attacks	no possibility of guessing attacks
3	Not secure because of its poor usability	secure and highly usable
4	It is widely used.	It is not widely used. Often used to protect secure data's such as in banking systems

Graphical passwords are better in all terms than that of a textual passwords, textual passwords enable us to use strong system assigned passwords which are difficult for a user to remember and the passwords that opted by the user will be very easy for an attacker to break. Possibility of guessing the attacks are more, it is no more secure due to its poor vulnerability, but they are widely used, so the security of the system is affected. The user's should be encouraged to select the graphical password strategy which are easy to remember and more secure, the possibility of guessing these type of password's are very less and it provide more security. it is widely used in the banking system due to its security . Brute force attack and dictionary attacks are not affected in graphical password strategy.

IV. CONCLUSION

An important goal in authentication systems is to help user's select better passwords and thus increase the security. We strongly believe that users can be persuaded to select stronger passwords through user interface design. As an example, we compared various Persuasive Cued Click-Points (PCCP) and alphanumeric passwords and conducted a usability study to evaluate its effectiveness. PCCP encourages and helps users in selecting click-based graphical passwords. A key feature of PCCP is that it helps people to select random click points and hence reduce the hotspots. It is better than other authentication systems in terms of it security and usability.it also avoids Brute force attacks and other dictionary attacks. A major threat today people are facing is the integrity and security of data in order to keep the security of the systems we propose graphical password strategies which is better than textual passwords. .

ACKNOWLEDGEMENT

We would like to extend our gratitude to the reference authors, as well as reviewer of our paper.

REFERENCES

[1] S. Chiasson, R. Biddle, and P. van Oorschot. A second look at the usability of click-based graphical passwords. *In 3rd Symposium on Usable Privacy and Security (SOUPS)*, July 2007.

[2] S. Chiasson, A. Forget, R. Biddle, and P. van Oorschot, "Influencing Users towards Better Passwords: Persuasive Cued Click- Points," *Proc. British HCI Group Ann. Conf. People and Computers*: Culture, Creativity, Interaction, Sept. 2008.

[3] S. Chiasson, A. Forget, E. Stobert, P. van Oorschot, and R. Bddle, "Multiple Password Interference in Text sand Click-Based Graphical Passwords," *Proc. ACM Conf. Computer and Comm. Security CCS*), Nov. 2009.

[4] E. Stobert, A. Forget, S. Chiasson, P. van Oorschot, and R.Biddle, "Exploring Usability Effects of Increasing Security in Click-Based Graphical Passwords," *Proc. Ann. Computer Security Applications Conf.* (ACSAC), 2010.

[5] S. Chiasson, A. Forget, R. Biddle, and P.C. van Oorschot, "User Interface Design Affects Security: Patterns in Click-Based Graphical Passwords," *Int"l J. Information Security*, vol. 8, no. 6, pp. 387- 398, 2009.

[6] Suo, Xiaoyuan, "A Design and Analysis of Graphical Password" (2006). Computer Science Theses. Paper 27. A. C. L. Andrew S. Patrick, Scott Flinn, "HCI and Security Systems," in *CHI, Extended Abstracts (Workshops)*. Ft. Lauderdale, Florida, USA, 2003.

[7] Persuasive Cued Click-Points:"Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism" Sonia Chiasson, Member, IEEE, Elizabeth Stobert, Student Member, IEEE, Alain Forget, Robert Biddle, Member, IEEE, and Paul C. van Oorschot, Member, IEEE.*IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING*, VOL. 9, NO. 2, MARCH/APRIL 2012

[8] "A Graphical Password Based System for Small Mobile Devices", IJCSI *International Journal of Computer Science Issues*, Vol. 8, Issue 5, No 2, September 2011, Wazir Zada Khan, Mohammed Y Aalsalem and Yang Xiang.

[9] P. C. van Oorschot, A. Salehi-Abari, and J. Thorpe." Purely automated attacks on passpoints-style graphical password". *IEEEE Trans. Info. Forensics and security*, vol. 5, no. 3, pp. 393-405, 2011

[10] "Enhanced Knowledge Based Authentication Using Iterative Session Parameters", Ali Alkhalifah, Geoff D.Skinner, World Academy of Science, Engineering and Technology 47 2010.