Reduction of Password Guessing Attacks using Click Point

Papiya Biswas
ETC Department
SVERI's C.O.E Pandharpur,
Solapur University, India

M.M.Patil
ETC Department
SVERI's C.O.E Pandharpur,
Solapur University, India

Mohua Biswas
ETC Department
SVERI's C.O.E Pandharpur,
Solapur University, India

ABSTRACT
The main aim of the work on the subject is to reduce password guessing attack in a computer security system by creating graphical passwords for which pixels are chosen from images. In a computer security system, human-computer interaction depends on proper authentication of the system. For the attackers, memorable passwords are easy to guess. Hence, researchers of modern days have opted for an alternative method wherein graphical pictures are used as passwords. Human brain recollects picture better than textual character. Hence, graphical passwords are created using images or representation of images.

Keywords
Authentication, Persuasive Cued Click Point, Graphical Password, Images, Guessing Attack, User Security.

1. INTRODUCTION
In a computer system, human-computer interaction [5] is considered as the most exposed area and its security depends on proper authentication by the users. Human parameters are considered to be the powerless link in a computer security system. The essentials of human-computer interaction are: (a) authentication (b) security operations and (c) developing secure systems. The most common practice for a user in a computer authentication system is to select a user name and a text password. The vulnerabilities of computer authentication method are well known. Despite the vulnerabilities, the expected mental attitude of the users is to have short passwords which are normally alphanumeric and easy to remember. Users are also unaware about how attackers tend to attack. Such passwords are more prone to get hacked and can be easily cracked by intruders through several means such as masquerading, Eaves dropping and other rude means i.e. dictionary attacks, shoulder surfing attacks, social engineering attacks.

Biometric passwords and tokens are also used to prevent the intruders and hackers to attack the system, but these two methods require some additional hardwares which are costly.

So an alternative to all these methods is the use of graphical passwords. According to Psychologists, human brain can recognize images better than the text. Use of graphical password has the following two main advantages: firstly, it is easy to remember and secondly, it becomes difficult to guess or hack. For a graphical password, users click on images rather than typing alphanumeric characters.

2. RELATED WORK
Problems with textual characters: Textual passwords are the most popular user authentication method but have security and usability problems. The common human tendency is to create memorable passwords, as strong system assigned passwords are difficult to remember [10]. Once a password is selected and learned, the user must be able to remember it to log on. But if a password is not used frequently, it may be forgotten. A survey has shown that most of the users tend to select short password or passwords that are easy to remember. But such passwords can be easily guessed or broken by attackers. Some users select long passwords which are difficult to remember as well as hard to guess or break. The other drawback with textual password is that many users cannot remember a number of passwords for different authentications. They tend to use the same password for different accounts. Moreover users may have a number of passwords for computers, networks and websites. Large number of passwords increase interference and may lead to confusion.

Biometric based authentication techniques: Biometric based authentication techniques, such as fingerprints, iris scan, facial recognition as well as some other more known or futuristic biometrics [17] [18] such as gait and smell, are not adopted to the full extent. The major drawback of Biometric based approach is that such a system is costly and the identification process can be slow and often undependable [2].

Token based authentication techniques: A security token is a physical device that can be easily carried. This can be a bankcard, a smartcard containing passwords, PIN to protect a lost or stolen token. The drawback of a metal key is that, if it gets lost, it enables its finder to enter the house. There is a distinct advantage of a physical object used as an authenticator, because if it is lost, the owner can have proof of this and can act accordingly [2].

Multiple password interference in text: The problems relating to the utility and security of multiple passwords are largely not evaluated. However, we know that people generally have difficulty in remembering multiple passwords. This reduces security since users reuse the same password for different systems as they try to login [7].

Movie character identification: According to Jitao Sang, self-regulating face identification of characters in movies has drawn significant research interests and led to many interesting applications. It is a difficult problem due to the large variation in the outward appearance of each character [9].

Image based registration & authentication system: Here the genuine system uses image based passwords and combines image registration and notification interfaces [1].

Human selection of mnemonic phrase-based passwords: In this paper, users will select memory related expressions that are commonly available on the Internet [4].

A persuasive cued click-point based authentication mechanism with dynamic user blocks: In this system, the size of the portal area is set by the user, depending upon his/her present requirement, with the help of dynamic user blocks [12].

An effective secure environment using graphical password authentication scheme: In the graphical password system, the images should be sufficiently large so that images can be cut into many sub-blocks to meet the users to set their passwords [13].

A proficient multilevel graphical authentication system: In this paper, a genuine graphical password system consists of a sequence of 'n' images and the user have to select the click points connected with one of the 'n' image in correct sequence for successful login [14].

Increasing the security of gaze-based cued-recall graphical passwords using saliency masks: In this paper, authors present a novel gaze-based authentication scheme that provides a list of images [15].

3. PROPOSED SYSTEM

We propose a new click-based graphical password technique called Persuasive Cued Click Points (PCCP). The main objective is to reduce the guessing of passwords by intruders. As the name suggests, this application uses graphical passwords along with alphanumeric characters that allow users to select pixels from images which are to be used as passwords. This method of creating a password, though time consuming, will be difficult to guess.

4. GRAPHICAL PASSWORDS

Graphical passwords were first described by Blonder [8]. Since then many other graphical password systems have been proposed. A graphical password in an authentication system works by selecting images, in a specific order, present in a graphical user interface (GUI). For this reason, graphical-password approach is sometimes called graphical user authentication (GUA). Graphical password is a simple system where a user presents a user ID and a password to the system. If the user ID and password match with the one stored in the system, then the user is authentic.

5. PERSUASIVE CUED CLICK POINTS

To address the issue of hotspots, Persuasive Cued Click Points were proposed. In the case of CCP, a password consists of five click points, one each of five images. During password creation major part of the image remain dimmed except for a small view port area which is randomly positioned on the image. Users must select a click-point within the view port. If they are unable to select a point in the present view port, they may press the shuffle button to randomly reposition the view port. The view port guides users to select more random passwords that are less likely to include hotspots. A user who is determined to reach a certain click-point may still shuffle until the view port moves to the specific location, but this is a time consuming and more tedious process. Persuasive technology is used to stimulate interest and influence the people to behave in a strong manner. An authentication system which applies persuasive technology should guide and encourage users to select stronger passwords, but not impose system-generated passwords. Cued Click-Points (CCP) was designed to reduce patterns and to reduce the usefulness of hotspots for attackers. Rather than five click-points on one image, CCP uses one click-point on five different images. The next image displayed is based on the location of the previously entered click-point, creating a path through an image set. Users select their images only to the extent that their click-point determines the next image.

6. FLOW DIAGRAM

Data Flow Diagram (Figure 1) is a simple graphical description of something that can be used to represent a system in terms of the input data to the system. Various types of operations have been carried out on these data and the output data is then generated by the system. The diagram helps to show how information is used to produce the functions that are required by the current system.

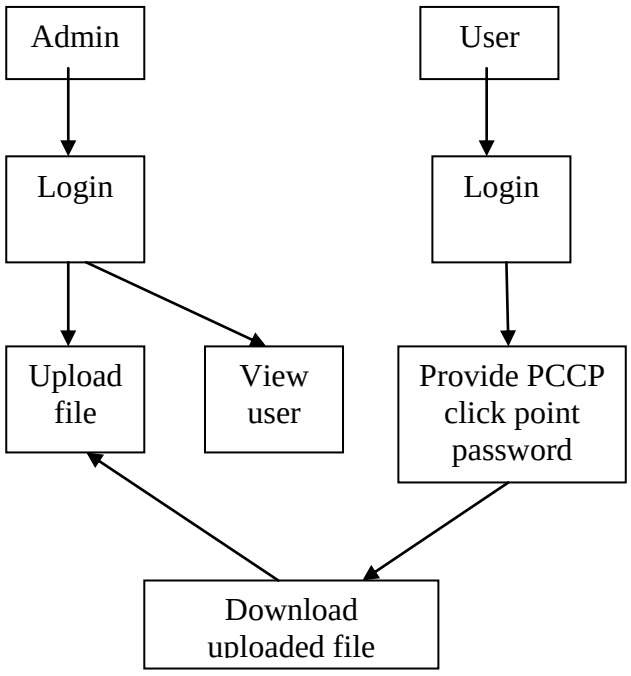

Figure 1: Flow Diagram

The administrator first logs on to the system and uploads the file (application) for end users. After that the end users log on to the system to select their required graphical passwords and

can use the same for downloading the file and perform other tasks on the system.

7. REGISTRATION PROCESS

The process flow starts from registering user ID. On completion of all the user details, the user proceeds to the next stage for selecting pixels from the images by clicking on a point. On completion of all the above procedures, user profile vector will be created.

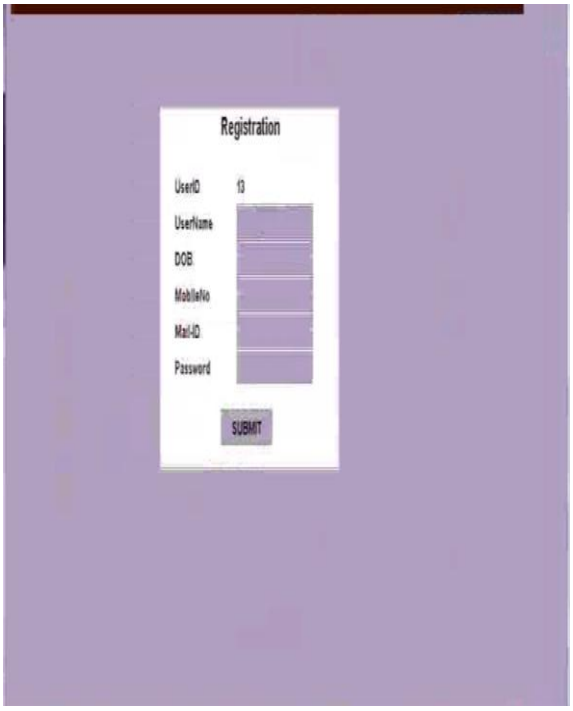

Figure 2: Registration Process

Figure 3: A sequence of images to form a password

Figure 4: Selecting pixels from the images

8. CONCLUSION

Through this project we would like to present a new password selection system which will be both cost efficient and secure. This system allows user to select pixels from the images as passwords along with text. The main idea in creating this project is to reduce the password guessing attack by hackers and intruders.

9. REFERENCES

[1] Srinath Akula, Veerabhadram Devisetty, **Image based registration and authentication system**, Department of Computer Science St. Cloud State University, St. Cloud, MN 56301.

[2] L. O'Gorman, **Comparing passwords, tokens, and biometrics for user authentication**, Proc. IEEE, vol. 91, no. 12, pp. 2019-2020, Dec. 2003.

[3] A. Jain, A. Ross, and S. Pankanti, **Biometrics: a tool for information security,** IEEE Trans. Information Forensics and Security (TIFS), vol. 1, no. 2, pp. 125-143, June 2006.

[4] Cynthia Kuo, Sasha Romano sky, Lorrie Faith Cranor, **Human selection of mnemonic phrase-based passwords,** 2006, July 12.

[5] S.Chiasson, A. Forget, R. Biddle and P. van Oorschot, **Influencing users towards better passwords: persuasive cued click- point**s, Proc. British HCI Group Ann. Conf. People and Computers: Culture, Creativity, Interaction, Sept. 2008.

[6] Amirali Salehi-Abari, Julie Thorpe, and P.C. van Oorschot, **On purely automated attacks and click-based graphical passwords**, December 8- 12, 2008.

[7] Sonia Chiasson1, Alain Forget1, Elizabeth Stobert2, P.C. van **Oorschot1**, Robert Biddle1 1School of Computer Science, **Multiple password interference in text passwords and click-based graphical passwords,** Department of Psychology Carleton University, Ottawa, Canada, November 2009.

[8] Sonia Chiasson, Alain Forget, Robert Biddle, P.C. van Oorschot, **User interface design aspects security: patterns in click-based graphical passwords**, April 9, 2009.

[9] Jitao Sang, Changsheng Xu, Senior Member, **Robust face-name graph matching for movie character identification**, **2010** IEEE.

[10] 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.

[11] Sonia Chiasson, Member, IEEE, Elizabeth Stobert, Alain Forget, Robert Biddle, Member, IEEE and P. C. van Oorschot, **Persuasive cued click points: design, implementation and evaluation of a knowledge-based authentication mechanism**, **25th** October, 2011.

[12] International Journal of Research in Engineering & Advanced Technology, **A persuasive cued click-point based authentication mechanism with dynamic user block**s, Volume 1, Issue 1 March, 2013.

[13] K.Semmangaiselvi1,T.Vamsidhar2,KothaHariChandana, B. Krishna Priya and E. Nalina, **An effective secure environment using graphical password authentication scheme**, Volume 2 Issue 2 Feb 2013.

[14] Aswathy Nair, Theresa Rani Joseph, Jenny Maria Johny**, A proficient multilevel graphical authentication system**, IJSETR Volume 2, No 6, June 2013.

[15] Andreas Bulling, Florian Alt, Albrecht Schmidt**, Increasing the security of gaze-based cued-recall graphical passwords using saliency masks**, CHI'12, May 5–10, 2012, Austin, Texas, USA.

[16] Alireza Pirayesh Sabzevar, Angelos Stavrou, **Universal multi-factor authentication using graphical passwords**, Computer Science Department, George Mason University.

[17] Xiongwu Xia, Lawrence O'Gorman **Innovations in fingerprint capture devices**, Veridicom Inc. 31 Scotto Pl, Dayton, NJ 08810, USA Received21 December 2001.

[18] S. Pankanti, R. M. Bolle, A. Jain, **Biometrics: the future of identification**, special issue of Computer, Vol. 33, no. 2, Feb. 2000.