ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 3, March 2019

Developing a Method for Reduction of Password Guessing Attacks Using Graphical Password & Sound Signature

Papiya Biswas[1], Mohua Biswas[2], Ankita Singh [3]

Assistant Professor, Department of Electronics & Telecommunication Engineering, SVERI's COE, Pandharpur, Solapur University Solapur, Maharashtra, India[1]

Assistant Professor, Department of Electronics & Telecommunication Engineering, SVERI's COE, Pandharpur, Solapur University Solapur, Maharashtra, India[2]

Assistant Professor, Department of Electronics & Telecommunication Engineering, SVERI's COE, Pandharpur, Solapur University Solapur, Maharashtra, India[3]

ABSTRACT: The central idea of the work on the subject matter is to lessen the password guessing attack in a computer protection technique by developing graphical passwords for which pixels are selected from pictures having some unique sound effects coupled with a password. In a computer protection technique, human-computer communication relies on good authentication of the method. For the attackers, impressive passwords are easy to guess. For this reason, research workers of present days preferred the technique in which graphical pictures are used as passwords. Human brain recalls picture better than textual character. Recent certification methods go through many weak points. Therefore, graphical passwords are developed using pictures or representation of pictures.

KEYWORDS: Certification, graphical password, pictures, guessing attack, persuasive cued click points, sound signature

I. INTRODUCTION

In a computer system, human-computer communication [4] is reflected as the most uncovered area and its security relies on proper certification by the users. Human constraints are measured to be the unprotected bond in a computer protection technique. The foundation of human-computer communication is based on (a) authentication (b) security operations and (c) developing protected methods. The most universal tradition for a user in a computer certification method is to select a user name and a text password. The exposure of computer certification method is familiar. In spite of the vulnerabilities, the typical mental attitude of the users is to have short password which is normally a character comprising of either a letter(s) or a number(s) that are easy to keep in mind. Some users are also not aware as to how intruders are likely to attack. Such passwords are more likely to get hacked and can be easily cracked by intruders through several offensive ways. Biometric passwords and tokens are also used to prevent the intruders and hackers to hit the method, although these two techniques involve some extra hardware which is expensive. Alternate to all these techniques is to make use of graphical passwords. According to Psychologists, human brainis capable of identifying pictures rather than texts. Application of graphical password has two main advantages. Firstly, it is simple and easy to keep in mind and secondly, it turns out to be difficult to figure out. In case of a graphical password, users click on pictures instead of typing alphanumeric characters. A picture and audio based certification of a user will verify the users through an order of pictures having some unique audio effects coupled with a password.

DOI: 10.15680/IJIRCCE.2019. 0703005

II. Related work

Problems with textual characters: Textual password is the most accepted user certification method but it has protection and usability setbacks. The trend of a common human is to make unforgettable passwords, as well-built system assigned passwords are complex to remember [8]. When a password is chosen and discovered, the client has to be competent to keep in mind to log on. But if a password is not used regularly, it may be forgotten. A review has shown that most of the users tend to pick small password or passwords that can be remembered effortlessly. But such passwords can be easily cracked by attackers. Some users select complicated passwords which are not easy to remember as well as unbreakable. The other negative side with textual password is that many users cannot remember a number of passwords for different certifications. They have a tendency to make use of the similar password for various accounts. Also clients may have a number of passwords for computers and websites. Huge numeral of passwords improves interference and may lead to confusion.

Biometric based authentication techniques: Biometric based authentication techniques, such as fingerprints, iris scan, facial recognition also a number of other known or innovative biometrics [11] [12] such as gait and smell, are not approved to the full extent. The major shortcoming of Biometric based approach is a system which is costly and the detection process can be slow and often undependable [2].

Token based authentication techniques: A security token is a visible device that can be easy to accept. This can be a bankcard, a smartcard having passwords, PIN to guard a missing or stolen token. The disadvantage of a metal key is that, if it gets stolen, it allows its claimant to go into the house. There is a specific advantage of a tangible purpose used as an authenticator, because if it is lost, the owner can have proof of this and can act accordingly [2].

PassPoint Technique: Previously a technique was used in this system to enter click points on image which is called PassPoint (PP) technique. Pass Point technique allows a user to enter maximum twelve click points on each image. But more click points on an image consumes more memory. One great disadvantage of this technique is shoulder surfing attack which cannot be overcome and user cannot easily recall more click points. To overcome these drawbacks, a technique called Cued Click Point (CCP) is used. It permits user to go through one click point on each picture and also allows sequence of five images to set as a password. A CCP technique is used only at the login time. While login into system if a user clicks on wrong click point it leads a user to incorrect path. It means if an attacker tries to login into an e-mail account of a user and if he misplaces a one click point then the sequence of images set as a password are changed and in place of correct sequence images, random images will be displayed. This change in sequence is recognized only by an authorized user and not by an attacker and finally a failed login attempt results.

Movie character identification: According to Jitao Sang, face identification of different characters in movies has attracted interest amongst researchers for studies and cause to various remarkable applications. It is a complex problem because of large variation in the outward appearance of each character [7].

III. Proposed System

We propose a latest click-based graphical password procedure called Persuasive Cued Click Points (PCCP) along with sound signature which allows the user to choose an audio file at run-time or use his voice for creating sound file. The main objective is to lessen the password guessing attack in a computer protection technique by developing graphical passwords for which pixels are selected from pictures having some unique sound effects coupled with a password. This method of generating a password, even if time consuming, will be difficult to guess.

IV. Implementation

Graphical passwords were first implemented by Blonder [6]. Since then numerous other graphical password methods have been implemented. A graphical password is a authorizationtechnique which works by choosing pictures, in an correct sequence present in a graphical user interface (GUI). Due to this reason, graphical-password approach is occasionally known as graphical user authentication (GUA). Graphical password is a simple system where a user presents a user ID and a password to the method. If the user ID and key match by the one stored in the system, then the user is authentic.To deal with the matter of hotspots, Persuasive Cued Click Points were implemented. In the case of CCP, a password includes five click points, one each of five pictures. During password formation, main part of the picture remains fainted except for a small view port area which is randomly placed on the picture. Users must pick a click-point inside the view port. If they are not able to pick a point in the present view port, they may press the jumbled up button to randomly relocate the view port. The view port directs users to pick more random passwords that are less likely to include hotspots. A user who is strong-minded to get to a certain click-point may still jumbled up until the view port shifts to the precise location, but this is a time consuming and more tedious process. Persuasive technology is used to inspire interest and influence the individuals to perform in a strong manner. A certification method which uses persuasive technology should direct and encourage users to pick stronger passwords, but not force system-created passwords. Cued Click-Points (CCP) was proposed to lessen patterns and to reduce the efficacy of hotspots for attackers. Instead of five click-points on one picture, CCP uses one click-point on five different pictures. Occurrence of next picture is based on the position of the earlier entered click-point, creating a path through a picture set.Users go for their pictures merely to the extent that their click-point determines the next picture.

In sound signature, we make use of sound clips for certification. While registering the new user, one audio clip is to be picked and played and thus saves its stop time in System Database. When user logs in, an appropriate audio clip and its stop time are to be picked, then the system verifies whether the audio clip and stop time are similar or not. If wrong, then error will be shown and if it is right, then it will accept the data.

V. FLOW DIAGRAM

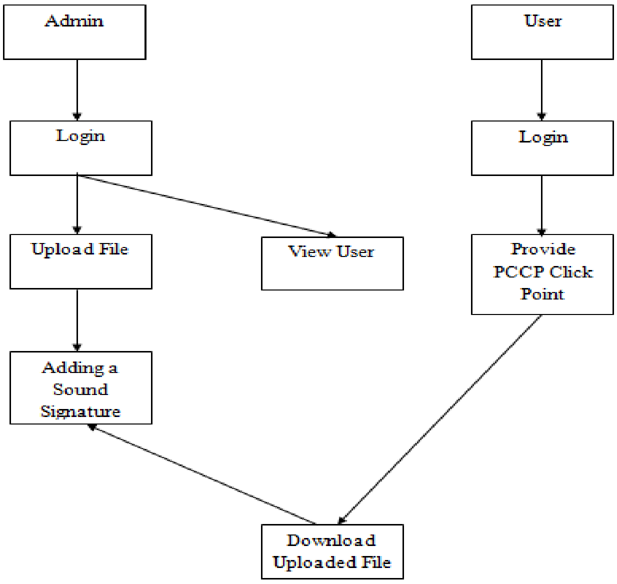
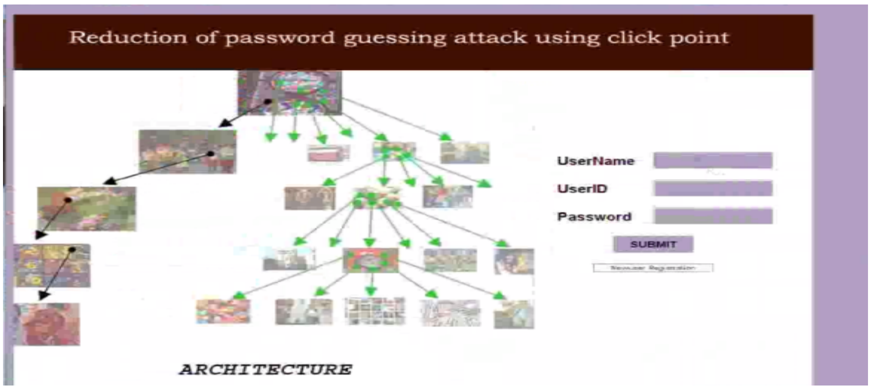


Fig. 1. Flow Diagram

The administrator first logs on to the system and uploads the file (application) for end users. Then the end users log on to the system to pick out their desired graphical passwords along with sound signature and the same can be used for downloading the file and performing other tasks on the system.

VI. Results



Reduction of password guessing attack using click point

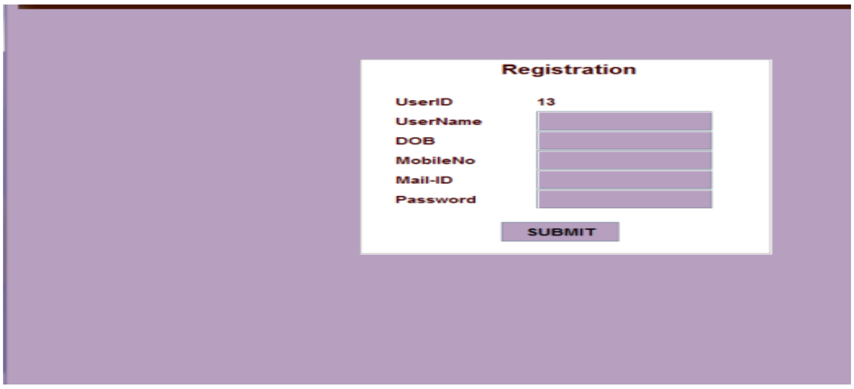
UserName

UserID

Password

Fig.2. New User Registration

Initially the user is opened with a screen and the option to either login with existing user details like UserName, UserID and Password or to register a new account in order to gain access to the system. After selecting the register button, the user is navigated to the second stage of the registration process.

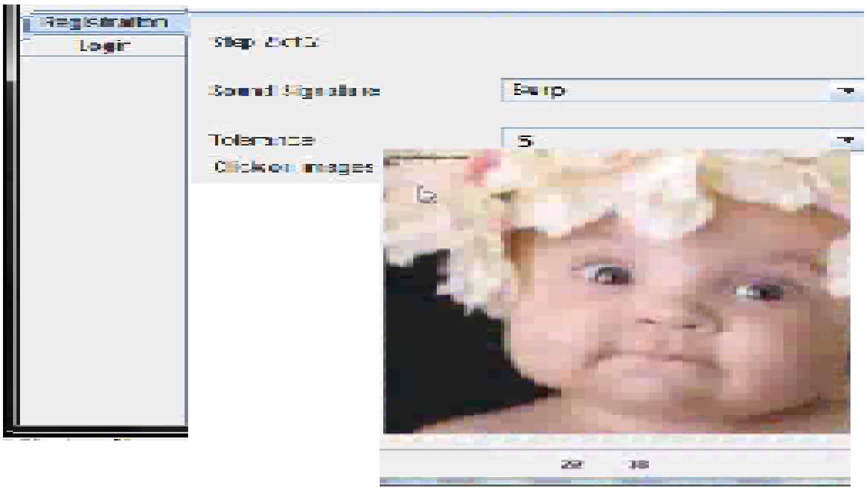


Registration

UserID	13
UserName	
DOB	
MobileNo	
Mail-ID	
Password	

Fig.3. Information related to new user

Initially the user is opened with a screen and the option to either login with existing user details like UserName, UserID and Password or to register a new account in order to gain access to the system. After selecting the register button, the user is navigated to the second stage of the registration process.



Step 2of3

Sound Signature Beep

Tolerance 5

Click on images

Fig.4. Sound Selection

In the second stage of the registration, the user is supposed to fill the details in order to create a password. The user is required to click on the desired picture along with sound signature which will then navigate then to that last stage of the registration process.

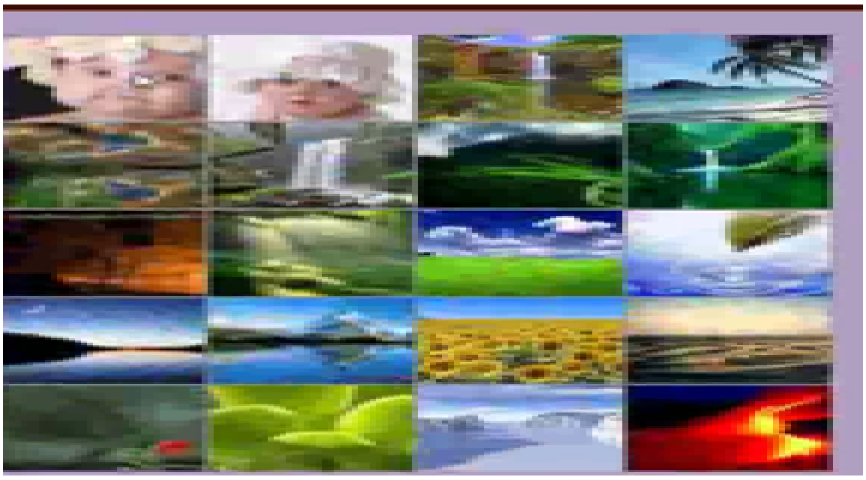


Fig.5. List of pictures

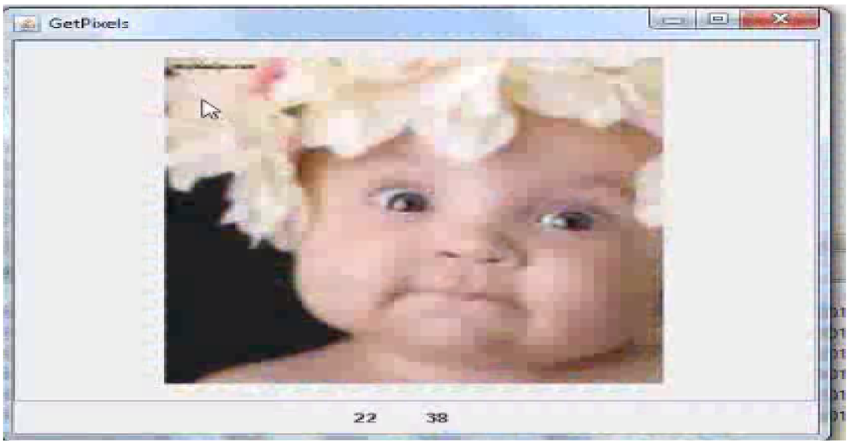


Fig.6. Selecting pixels from the image

In the third stage of the registration process, a screen with a randomly picked image is shown. Users need to choose an image of their choice. The user is requested to choose five different images and then select pixels from the images by clicking on one particular point to make up their password and submit it to the system. This step acts as a memory prompt to help the users better remembers their selected password.

VII.CONCLUSIONS

We have proposed a novelapproach we have proposed uses sound signature and graphical password click points. Through this project we would like to introduce a novel password selection system which will be both cost efficient and secure. This system lets client to pick pixels from the images as passwords along with text. The main idea in creating this project is to diminish the password guessing attack by hackers and intruders.

REFERENCES

1. SrinathAkula, VeerabhadramDevisetty, “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. 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. 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.
5. AmiraliSalehi-Abari, Julie Thorpe, and P.C. van Oorschot, “On purely automated attacks and click- based graphical passwords”, December 8- 12, 2008.
6. Sonia Chiasson, Alain Forget, Robert Biddle, P.C. van Oorschot, “User interface design aspects security: patterns in click-based graphical passwords”, April 9, 2009.
7. Jitao Sang, ChangshengXu, Senior Member, “Robust face-name graph matching for movie character identification”, 2010 IEEE.
8. 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.
9. 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.
10. International Journal of Research in Engineering & Advanced Technology’ “A persuasive cued click-point based authentication mechanism with dynamic user blocks”, Volume 1, Issue 1 March, 2013.
11. Xiongwu Xia, Lawrence O’Gorman, “Innovations in fingerprint capture devices”, Veridicom Inc. 31 Scotto Pl, Dayton, NJ 08810, USA Received21 December 2001.
12. S. Pankanti, R. M. Bolle, A. Jain, “Biometrics: the future of identification, special issue of Computer”, Vol. 33, no. 2, Feb. 2000.
13. Cynthia Kuo, Sasha Romano sky, Lorrie Faith Cranor, “Human selection of mnemonic phrase-based passwords”, 2006, July 12.
14. 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.