Volume 5, Issue 2, February 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Graphical Password Authentication Using Sound Signature

Manal Vartak, Rahul Kute, Akshay Jadhav, Parth Makwana

B.E. Information Technology

India

Abstract—It's a new technology which has continued to provide commercial, good quality security solutions, made-to-order to protect our client's products and documents against counterfeiting and fraud. Graphical authentication is proposed to be the alternate for textual passwords since it could be simple for users to remember.

Keywords— Graphical Passwords, AES, Image Authentication, Sound Signature, Recognition.

I. INTRODUCTION

Users employ passwords as a kind of authentication to properly identify themselves on any computer or communications network. Graphical passwords provide one such substitute for traditional passwords approaches. The essential premise is pictures are much easier to remember or recognize than text. Many different patterns could have been proposed for users to develop pictures or drawings instead of entering text letters [2-7].The predictability problem can be solved by disallowing user choice and assigning passwords for people, this usually gets to usability issues since users cannot easily remember such random passwords.

- ❖ Authentication- Creates that the user is who they say they are.
- ❖ Authorization- The process used to decide if the authenticated person is allowed to access specific information or functions.
- ❖ Access Controls-Restriction of access-includes authentication & authorization.

Mostly user select password that is estimated. This happens with both graphical and text passwords. Users tend to choose easily remembered password, unfortunately it means that the passwords tend to follow expected patterns that are easier for attackers to predict. While the expectedness problem can be solved by disallowing user choice and assigning passwords to users, this usually leads to usability problems since users cannot easily remember such random passwords. Number of graphical password systems has been developed; Study shows that text-based passwords suffer with both security and usability problems.

According to a recent news research, a security team at a company ran a network password cracker and within 30 seconds and they identified about 80% of the passwords. It is known that the human brain is better at recognizing and recalling images than text, graphical passwords exploit this human distinctive. In addition sound signature is provided for better recalling the pictures while entering the password.

1.1. OBJECTIVES

The objectives for this paper is to Examine the existing password systems and suggest a new graphical password system which would increase the security and also help in smoothening the system working.

this focuses on security of data and keeps info about the resources which are used and therefore concentrates on complete optimization of graphical password system, along with increasing the security by addition of sound signature into the graphical password system.

1.2. SCOPE

- ❖ Provide human friendly passwords while increasing the security level.
- ❖ On average-million of years to break into systems.
- ❖ Dictionary attacks are infeasible.
- ❖ Its more secure the text password.
- ❖ Easy recalling of Password.
- ❖ Graphical Password Provide a way of making more human friendly password.

II. LITERATURE SURVEY

Literature review for this project will review the existing graphical password schemes and on the selection of the most appropriate development tools.

There are two schemes which are used in Graphical Password Authentication which are as follows

- Recognition Based Techniques in which, the user is asked to select a certain number of images from a set of random pictures generated by a program . Later, the user will be required to identify the images in the sequences in order to be authenticated. The results showed that 90% of all users succeeded in the authentication using this technique, while only 70% succeeded using the traditional text-based passwords.

- Recall Based Techniques in which a user is asked to draw a simple image on a 2D grid. The coordinates of the grid which are used by picture are stored in order of drawing. During authentication, re-drawing scheme is provided for the user. If the drawing matches the same grids in the same order, then the user is authenticated.

III. DIAGRAMS

3.1 Block Diagram for System Architecture

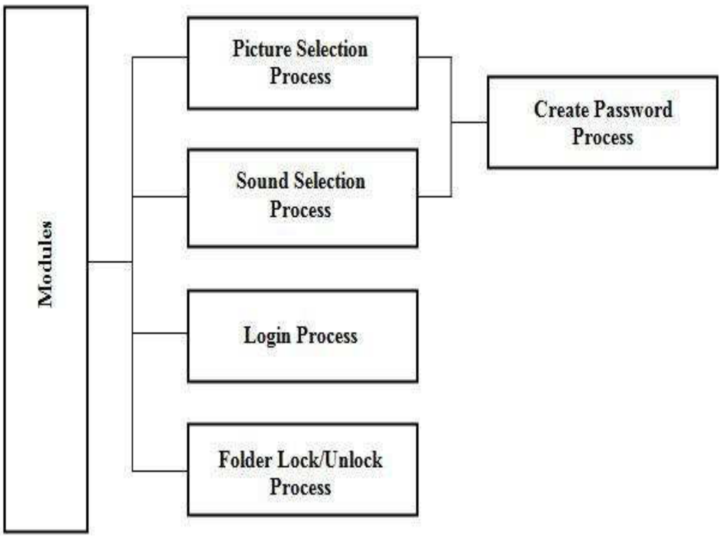
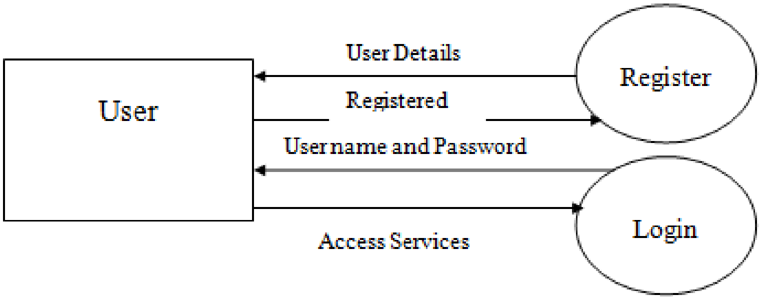


Fig 3.1: System Architecture

3.2 Data Flow Diagrams (Level 0 and 1)



3.2.1 DFD for Login System (Level 0)

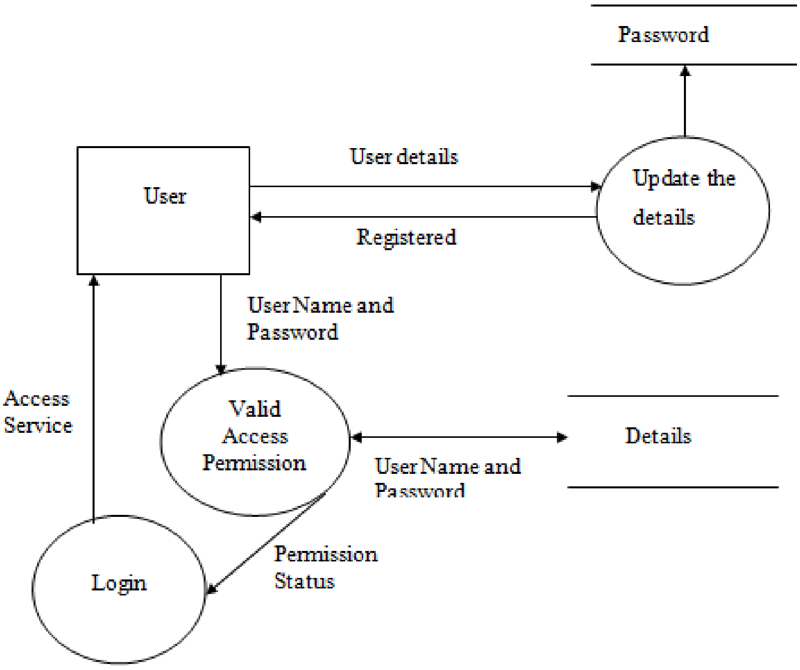


Fig 3.2.2 DFD for Login System (Level 1)

IV. METHODOLOGY

An authentication system which applies Persuasive Technology should guide and encourage users to select more secure passwords, but not impose system-created passwords. To be operational, the users must not ignore the persuasive elements and the resulting passwords must be memorable. The proposed system accomplishes this by making the task of selecting a weak password more tedious and time-consuming. The goal is to encourage compliance by making the less secure task more time consuming and awkward. A sound signature is added to this system in order to help the user in recalling an image during login phase. During registration phase, user is asked to select a sound signature or music. That is, during login phase, if the user clicks the appropriate image then the sound that the user selected during registration phase will be played.

V. OTHER RECOMMENDATIONS

The system we proposed are better than the traditional password and is more feasible, reliable and flexible. Also this system is more flexible for password recalling and recovering system through OTP[One Time Password] by using the GSM Modem. For password recalling sound signature is provided which increase the password remembrance. This technology is has been efficiently developed by using the existing algorithm Dhamija and Perrig algorithm. In future the system security can be increased by increasing the levels of the Password which are easy to implement through this technology. This can make the password more complex for guessing and not easily crackable. Also the are various password recalling and recognition algorithm which can be used for better security purpose.

VI. DISCUSSION & CONCLUSION

We have proposed a novel approach which uses sound signature and graphical password which are sequence of images. Previously developed system never used this approach this system is helpful when user is logging after every single cycle. In future systems other patterns may be used for security purpose like touch of smells, video graphical click point, study shows that these patterns are very useful in secure login the associated objects like images, text and video clip.

The use of graphical images and sound signatures strengthens the security system by almost removing the chances of getting penetrated. This application can be used for providing security to any application by placing this application over any application which is needed to be secured and whose security system is to be enhanced. The application here can be used by any organization or industry that needs to handle intimate data. The application ensures that only a legitimate user who can provide the right SQL user password, graphical password and there sequence and along with the right sound file for verification will be able to access the application protected by this security system.

This system can further be enhanced by providing a more user friendly and easy access for genuine users by providing them with the facility to use sound signature first and on its authentication system generates the approximate graphical password which must be further corrected by the legitimate user. Thus helps genuine users in recollecting graphical password and stops any kind of false trails of illegitimate users. The scope of the project can be further improved by using various techniques like Sudoku. The passwords can be changed every minute, thus making the user free from remembering passwords. He does not have to register on each and every website. Passwords are automatically generated and changed every time the user has to login.

REFERENCES

[1] Increase the remembrance of the password using graphical password with a support of sound signature(ISSN: 2348-4748, Volume 1, Issue 4, April 2014)

[2] Birget, J.C., D. Hong, and N. Memon. Graphical Passwords Based on Robust Discretization. IEEE Trans. Info. Forensics and Security, 1(3), September 2006.

[3] Davis, D., F. Monrose, and M.K. Reiter. On User Choice in Graphical Password Schemes.13th SENIX Security Symposium, 2004.

[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] Birget, J., Brodskiy, A., Memon, N., Waters, J., Wiedenbeck, S., Authentication using graphical passwords: basic results", ACM International Conference Proceeding Series, Vol. 93, 2005

[6] "Authentication using graphical passwords: Effects of tolerance and image choice," in 1st Symposium on Usable Privacy and Security (SOUPS), July 2005.

[7] A. De Angeli, L. Coventry, G. Johnson, and K. Renaud. "Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems", International Journal of Human-Computer Studies, 63(1-2):128-152, 2005.