VOLUME-8, ISSUE-4, APRIL-2019 • PRINT ISSN No 2277 - 8160

Original Research Paper

Engineering

SECURE GRAPHICAL PASSWORD USING CLUED CLICK POINT

Mayur Chincholkar	Department of computer science and engineering P.R.Pote college,Amravat,Indiai
Heena Shaha*	Sant Gadge Baba Amravati University, Amravati,India *Corresponding Author
Hrishikesh Gosavi	Department of computer science and engineering P.R.Pote college,Amravat,Indiai
Manoj Thombare	Department of computer science and engineering P.R.Pote college,Amravat,Indiai
Kanchan Gomase	Department of computer science and engineering P.R.Pote college,Amravat,Indiai
Atul Jamnekar	Prof. Department of computer science and engineering P.R.Pote college, Amravat,Indiai
Dr. chetan Shelke	Department of computer science and engineering P.R.Pote college, Amravat,Indiai

ABSTRACT

In current era, most Internet applications still establish user authentication with traditional text based passwords. Designing a secure as well as a user friendly password-based method has been on the agenda of security researchers for a long time. On one hand, there are password manager programs which facilitate generating site-specific strong passwords from a single user password to eliminate the memory burden due to multiple passwords. We proposed different level of authentication such as textual authentication, image authentication and audio authentication, for providing better security for the applications. In textual Phase user will choose the username and password while making the registration. During registration user must input the registered username and password, if it match with the database then user can login to system. In image authentication model, we take image as input from user at time of registration and inserting cued point, cued point is selected part of image which is selected by user. At the time of login user should have to select image and select the part of image which he/she inserting at the time of registration w called it cued points. If this all information is match exactly then and only then user is authenticate and he/she eligible to login successfully

KEYWORDS : Graphical Passwords, Authentication, gateways, Cued Points.

I. INTRODUCTION

In this project, we propose a new graphical password scheme for accessing web accounts called "Secure Web Account Access through Recognition Based Graphical Password by Watermarking". Various graphical password schemes have been proposed as alternatives to text-based passwords. Research and experience have shown that text-based passwords are fraught with both usability and security problems that make them less than desirable solutions. Psychology studies have revealed that the human brain is better at

recognizing and recalling images than text. Graphical passwords are intended to capitalize on this human characteristic in hopes that by reducing the memory burden on users, coupled with a larger full password space offered by images, more secure passwords can be produced and users will not resort to unsafe practices in order to cope. Human factors are often considered the weakest link in a computer security system. Patrick, et al. point out that there are three major areas where human computer interaction is important: authentication, security operations, and developing secure systems. Here we focus on the authentication problem. The most common computer authentication method is for a user to submit a user name and a text password. The vulnerabilities of this method have been well known. One of the main problems is the difficulty of remembering passwords. Studies have shown that users tend to pick short passwords or passwords that are easy to remember. Unfortunately, these passwords can also be easily guessed or broken. According to a recent Computerworld news article, the security team at a large company ran a network password cracker and within 30 seconds, they identified about 80% of the passwords. On the other hand, passwords that are hard to guess or break are often hard to remember. Studies showed that since user can only remember a limited number of passwords, they tend to write them down or will use the same passwords for different accounts. To address the problems with traditional username password

II. BACKGROUND

In the literature, several techniques have been proposed to reduce the limitations of the traditional alphanumerical password. One of the proposed

solution is to use an easy to remember long phrases (passphrase) rather than a single word. Another proposed solution is to use graphical passwords, in which graphics (images) are used instead of alphanumerical passwords. This can be achieved by asking the user to select regions from an image rather than typing characters as in alphanumeric password approaches. R. Dhamija and Perrig proposed a graphical authentication scheme based on the Hash Visualization technique. In their system, 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 preselected images in order to be authenticated. results showed that 90% of all participants succeeded in the authentication using this technique, while only 70% succeeded using text-based passwords and PINS. The average log-in time, however, is longer than the traditional approach. A weakness of this system is that the server needs to store the seeds of the portfolio images of each user in plain text. Also, the process of selecting a set of pictures from the picture database can be tedious and time consuming for the user.

III. PROPOSED WORK

To overcome the drawbacks of the existing system, the proposed system has been evolved. In this project, however, we have focus on another alternative: using pictures as passwords. Graphical password schemes have been proposed as a possible alternative to text-based schemes, motivated partially by the fact that humans can remember pictures better than text; psychological studies supports such assumption. Pictures are generally easier to be remembered or recognized than text. In addition, if the number of possible pictures is sufficiently large, the possible password space of a graphical password scheme may exceed that of text based schemes and thus presumably offer better resistance to dictionary attacks. Because of these (presumed) advantages, there is a growing interest in graphical password. In addition to workstation and web log-in applications, graphical passwords have also been applied to

ATM machines and mobile devices. The efficient reports can be generated by using this proposed system.

Fig.3.1. Data flow diagram for Authentication

Textual Authentication: In this Phase user will choose the username and password while making the registration. During registration user must input the registered username and password, if it match with the database then user can login to system.

Image & Cued Point authentication: In this project we design multilevel authentication for file sharing system, there are two main models for image authentication and audio authentication. In image authentication model, we take image as input from user at time of registration and inserting cued point, cued point is selected part of image which is selected by user. At which he/she inserting at the time of registration w called it cued points. If this all information is match exactly then and only then user is authenticate and he/she eligible to login successfully.

Audio authentication: In this module, we take audio file as input at time of registration from user and also take the time duration of recording audio file. At time of login if user authenticate from previous level then audio authentication phase will open. User should have to select audio file which he/she uploaded at time registration and inserting the time duration of audio file. If all data is exactly match then user authenticate for audio level, user is eligible to login next proses.

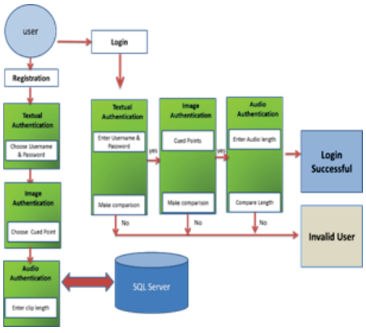

Fig. 3.2 Data flow diagram for System Architectures.

Textual Authentication: In this Phase user will choose the username and password while making the registration. During registration user must input the registered username and password, if it match with the database then user can login to system.

Image & Cued Point authentication: In this project we design multilevel authentication for file sharing system, there are two main models for image authentication and audio authentication. In image authentication model, we take image as input from user at time of registration and inserting cued point, cued point is selected part of image which is selected by user. At the time of login user should have to select image and select the part of image which he/she inserting at the time of registration w called it cued points. If this all information is match exactly then and only then user is authenticate and he/she eligible to login successfully.

Audio authentication: In this module, we take audio file as input at time of registration from user and also take the time duration of recording audio file. At time of login if user authenticate from previous level then audio authentication phase will open. User should have to select audio file which he/she uploaded at time registration and inserting the time duration of audio file. If all data is exactly match then user authenticate for audio level, user is eligible to login next proses. .

IV. Advantages and Disadvantages:

ADVANTAGES:

- It is trouble-free to use. It is a relatively fast approach to manage events. Is highly reliable, approximate result rom user.
- Best user Interface. Efficient reports.
- The system is very effective and convenient to us.
- It reduces the use of manpower to a great extent. The system is secured and gives only authorized access. It saves cost and time. In this project we are using pictures as passwords.
- Humans can remember pictures better than text. Pictures are generally easier to be remembered or recognized than text.
- In addition, if the number of possible pictures is sufficiently large, the possible password space of a graphical password scheme may exceed that of text based schemes and thus presumably offer better resistance to dictionary attacks. Because of these (presumed) advantages, there is a growing interest in graphical password.

DISADVANTAGES:

- The proposed work is for seen to have significant uses in application. This work helps us to provide the significant input to get desired output avoiding ambiguity. But it has some limitations like,
- It takes more time to recognize image and audio if any noise present. We have to apply filter for filtering noise.
- If any noise is present in audio file it may causes of generation of incorrect encryption key.

V. RESULT AND CONCLUSION:

The basic aim of this research study authentication technique for personal authentication traditional text based passwords, graphical, audio method and improvement in authentication and authorization to provide a better security. We proposed different level of authentication such as textual authentication, image authentication and audio authentication, for providing better security for the applications. In textual Phase user will choose the username and password while making the registration. During registration user must input the registered username and password, if it match with the database then user can login to system. In image authentication model, we take image as input from user at time of registration and inserting cued point, cued point is selected part of image which is selected by user. At the time of login user should have to select image and select the part of image which he/she inserting at the time of registration w called it cued points.

VI. FUTURE SCOPE:

Various graphical password schemes have been proposed as alternatives to text-based passwords. Research and experience have shown that text-based passwords are fraught with both usability and security problems that make them less than desirable solutions. This application requires correct feed on input into the respective field. Suppose the wrong inputs are entered, the application resist to work.

REFERENCES

1. Sonia Chiasson,, Elizabeth Stobert, Alain Forget, Robert Biddle, and Paul C. van Oorschot," Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism" Transactions on Dependable and Secure Computing, Volume: 9 , Issue: 2 , March-April 2012 .
2. Ushir Kishori Narhar, Ram B. Joshi" Highly Secure Authentication Scheme", 2015 International Conference on Computing Communication Control and Automation, 26-27 Feb. 2015.
3. Varun Kumar, M. K. Gupta, Ashish Chaturvedi, 4Anuj Bhardwaj, Manu Pratap Singh," Click to Zoominside Graphical Authentication", International Conference on Digital Image Processing,7-9 March 2009.

4. Gi-Chul Yang,"PassPositions: A Secure and UserFriendly Graphical Password Scheme", 4th International Conference on Computer Applications and Information Processing Technology (CAIPT),8-10 Aug. 2017. [5] Ali Mohamed Eljetlawi, Norafida Ithnin. " Graphical Password: Prototype Usability Survey" International Conference on Advanced Computer Theory and Engineering, 20-22 Dec. 2008. [6]Andrea Bianchi, Ian Oakley, and Hyoungshick Kim." PassBYOP: Bring Your Own Picture for Securing Graphical Passwords", IEEE Transactions on Human-Machine Systems (Volume: 46 , Issue: 3 , June 2016).
5. S.Chiasson, R. Biddle, and P. van Oorschot, "Asecond look at the usability of click-based graphical passwords," in Proc. 3rd Symp. Usable Privacy Security, 2007, pp. 1–12.
6. S. Chiasson, P. C. van Oorschot, and R. Biddle, "Graphical password authentication using cued click points," in Proc. 12th Eur. Symp. Res. Comput. Security, 2007, pp. 359–374.
7. S. Chiasson, A. Forget, R. Biddle, and P. C. Oorschot, "User interface design affects security: Patterns in click-based graphical passwords, Int. J. Inf. Security, vol. 8, no. 6, pp. 387–398, 2009.
8. S. Chiasson, E. Stobert, A. Forget, R. Biddle, and P. C. Van Oorschot, "Persuasive cued click-points: Design, implementation, and evaluation of a knowledge-based authentication mechanism," IEEE Trans. Dependable Secure Comput., vol. 9, no. 2, pp. 222–235, Mar./Apr. 2012.
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. 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.
11. J. Thorpe and P. C. v. Oorschot, "Graphical Dictionaries and the Memorable Space of Graphical Passwords," in Proceedings of the 13th USENIX Security Symposium. San Deigo, USA: USENIX, 2004.
12. A. F. Syukri, E. Okamoto, and M. Mambo, "A User Identification System Using Signature Written with Mouse," in Third Australasian Conference on Information Security and Privacy (ACISP): Springer Verlag Lecture Notes in Computer Science (1438), 1998, pp. 403-44