Graphical Password System Using Moveable Frames

S Pandikumar, Manoj C

ABSTRACT

By using standard alphanumeric passwords, attackers can easily compromise password systems through shoulder surfing or dictionary attacks. Unfortunately, the continuity of threats has been the motivator for the development of an alternative to alphanumeric password authentication systems, namely graphical passwords, which do not use alpha numeric characters, but instead images. This paper looks at the development and classification of graphical passwords. Graphical passwords can be classified into two major classes recognitional based and recall based. The pros and cons of relying on each method of graphical password authentication system are explained and an overview of the newer research and development in graphical passwords related to shoulder surfing attacks is presented. Finally, a novel password system is presented that utilizes a combination of the textual password and graphical images in order to develop an operationally secure password authentication system. The proposed password system will allow the users to register a textual password and graphical password with a movable frames grid and subsequently into a defined graphical image and produce an authentication response. Experimental results on the proposed system show that although user-friendly methods of authentication can be incorporated it will improve the security of graphical authentication against shoulder surfing attacks. Future studies in graphical passwords will also aim to determine whether these graphical passwords can also effectively secure alternate forms of user identification in different applications.

Key Terms - Graphical Password Authentication, Movable Frame Scheme, Shoulder Surfing Resistance, Recognition-based Authentication, Recall-based Authentication, Image-based Password Security, AES-Rijndael Encryption, Banking Security Systems, User Authentication.

1. INTRODUCTION

Standard password schemes are text-based and are subject to a whole variety of attacks including, shoulder surfing or dictionary attacks [1]. As more users and organizations are aware of these attacks, that are following rapidly suit and examining the security of their own schemes. Password authentication schemes should promote less predictable and more robust passwords that are still memorable and secure [2]. Alphanumeric usernames and passwords are predominantly the norm for user authentication; while one downside of using this mechanism to authenticate someone is that passwords could just be guessed [3]. It is easy to overlook that if a password is not easy for anyone to guess, it is equally perhaps difficult to remember [4].

Alphanumeric passwords also face the vulnerability of dictionary attacks. Because of the difficulty associated with remembering random character strings, the vast majority of users will often using a normal word or a name, not knowing that their password can be brute-forced several million times, and humans can remember images much better than text. This weakness has been leveraged to propose graphical password schemes as a viable alternative to text-based systems [5].

Graphical passwords schemes make use of pictures rather than alphanumeric characters. A user has to remember a number of pictures to log in successfully. The apparent downside of such a scheme is having a massive dictionary of unique images to remember, but if the number of possible images is large enough, the potential password space of a graphical password scheme seems to offer stronger resistance against dictionary attacks. Another downside is that graphical passwords tend often to be vulnerable to shoulder

surfing attacks [5]. Shoulder surfing is when an adversary tries to guess a password by looking directly at the user logging in.

2. LITERATURE REVIEW

previous sections have shown a solution based on text-based graphical passwords whose using Déjà vu and Moveable Frame schema literally changed the format of Déjà vu by employing text-based images rather than only graphics. The main aim of our study has two objectives; the primary objective is to avert shoulder surfing, by limiting the searching time of the pass-images to the login body page [5].

Text-based passwords have some overall significant relevance in developing access control based on the owners of the privileged entity. On the contrary, text-based authentication models, also have their own disadvantages. For example, users generally prefer to get authenticated by the fastest and easiest means (credentials) often neglecting security; security experts typically favor more stringent and dogmatic text rules. Experiments also indicate that images are more memorable than letters, numbers and symbols. One of the more common attacks on graphical authentication systems that bad actors tend to use is shoulder surfing. Indeed, shoulder surfing is considered the biggest disadvantage of graphical passwords [6].

In this paper, we have offered to suggest a method that combines a and recognition in graphical user-authentication and Zero knowledge protocol to withhold the user's input when attempting to login into the given system. This method has inhibited the shoulder surfing attack of a hacking attack on people logging into a graphical user-authentication system. the observation is that after hackers failed to see the full stem on one attempt, the user didn't experience any other adverse observations, in that there was no sign the hacker had pursued this login. So, in summary, propose the method offer by Steve Anderson (2006) using a Zero Knowledge Protocol and recognition based graphical user authentication.

They provided a solution paper that invented a simple text-based shoulder surfing resistant graphical password which allows a user to easily and securely complete the login process with being aware of shoulder surfing attacks. The operation of the proposed scheme is simple enough for users who are already familiar with text passwords. A user can effectively login onto the system with its seated on its own desk without having a keyboard or on-screen keyboard to type on. As a final point, they evaluated the resistances of their newly proposed scheme to accidental login and shoulder surfing [7].
The paper describes a new method called a scalable shoulder surfing resistant textual formula base password authentication system (S3TFPAS). S3TFPAS combines the textual password and formula to create a strong random password using a simple common interface. The S3TFPAS provides a very complex and secure authentication with a much lesser cognitive load. S3TFPAS can be resistant to shoulder surfing, brute-force attack, hidden cam, and dictionary attack due to dynamic random passwords [8].

3. METHODOLOGY

We adopted the banking sector scenario to implement the Graphical Password System. We adopted a Graphical User interface for Banking sector; we created one graphical password technique for banking sector. The banking sector requires an extensive level of authentication to confirm a user's identity. However, our system can also be adapted to be used in any high security required areas, military sectors, Government sector etc.

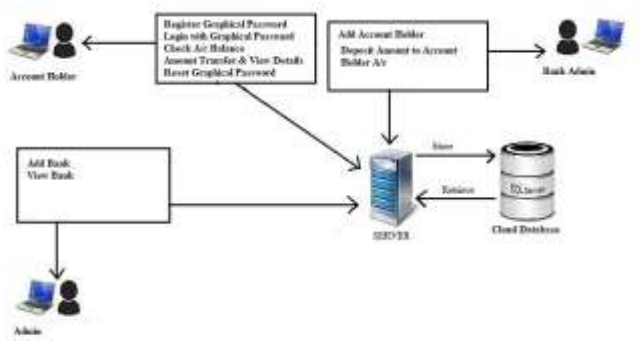

Figure 1: System Architecture of Graphical Password System Using Movable Frames

The architecture of Graphical Password System Using Movable Frames is shown in the above figure; there are three modules admin, Bank administrator and Account holder. New user can register providing user details which were stored to database. The system would then create the image grid, and then the user would select their password from that image grid. The images selected will then be stored in the database. The authenticated user can login to application by entering the graphical password that had provided previously. The image grid will be in horizontal movement in the login page by a movable frame schema.

4. PROBLEM STATEMENT

The proposed system employs a Graphical interface which has a visual display that uses a grid of graphical images for identification and authentication. The working of the system is well defined and clear and includes registration, login phase and change password. In the Registration phase, the user will first have to enter the account number and password (which has been already been sent to the user's mail once he/she is added by the bank admin). Upon entering this information, the screen will display a grid, in which 9 random Graphical images will be displayed to the user, where he/she will pick 5 images using a mouse click and set the graphical password. After the graphical password is set, we are going to consider the images chosen as ID's and the images are separated by commas. The ID is encrypted using the AES-Rijndael Algorithm and stored in the database, giving multi-level security. During the Login phase, the user must first enter his / her account number and password. Once the user enters his / her account number and password, they will be sent to the page to give their Access key which is emailed to him / her once it is encrypted, after the 5 chosen images. When the Access key is entered, the graphical images ID will be decrypted and the user must log in by selecting 5 images chosen during the registration phase. The access key or the graphical password only has 3 attempts. If the user exceeds the 3 attempts, the account will be blocked and the user will not be able to perform any transactions on the account. The user can reset password if forgot password by entering the account number and password and the steps are the same as during the registration phase.

Admin

Login: Administrator will have a unique id and password; administrator will login and will have the following functions.

Manage Bank: Admin will have the option to add bank details

Bank Admin

Login: Bank Admin will have a unique id and password; Bank Admin will login and will have the following functions.

Manage Account Holder: Bank administrator will have the option to add Account holder, have the unique Account No and give the password to Account holder.

Manage Account Holder Amount Deposit: Bank Administrator will have the option to deposit to account

holder account.

Account Holder

Registering graphical password: Account holder will finally register the graphical password by choosing 5 images out of 9-images, The account holder input account number, account holder uses to registered 5 images as graphical password. The selected Graphical Password images Id's will be encrypted by AES Rijndael algorithm and will generate Access Key that will be emailed to Account The account holder and will be stored in cloud DB for secure purpose.

Logging In: Account Holder will use unique Account No. and Password, Account Holder will be redirected to graphical password page, Account holder will chose Graphical password images. holder. The account holder has 3 attempts to choose right graphical password images. If account holder fails to choose the graphical password images after 3 attempts than graphical password option will be blocked. The account holder will have to Reset Graphical password to unblocking or activating by choosing 5 new set of graphical password images.

Reset Graphical Password: An account holder may reset the graphical password by selecting 5 images out of 9 images made available, enter account number to set id's of images as graphical password. The account holder chosen Graphical Password Images Id's are encrypted and generates access key which will be sent through Mail and also will be updated to cloud DB for secure purpose. Check Account Balance: An account holder can see the details of the deposit and also can check are also account balance details. Amount Transfer: An account can transfer the amount to other registered account holder in the application, and view the transfer amount detail.

5. RESULTS

Figure 2 depicts the home page of Graphical Password System for online banking which consists of Login, Account Register and Reset Password.

Figure 3: Account Holder registration page

Figure3 depicts the Account Holder registration page where Account holder registers themselves to the system by selecting images as password and with account id which is provided by Bank Admin.

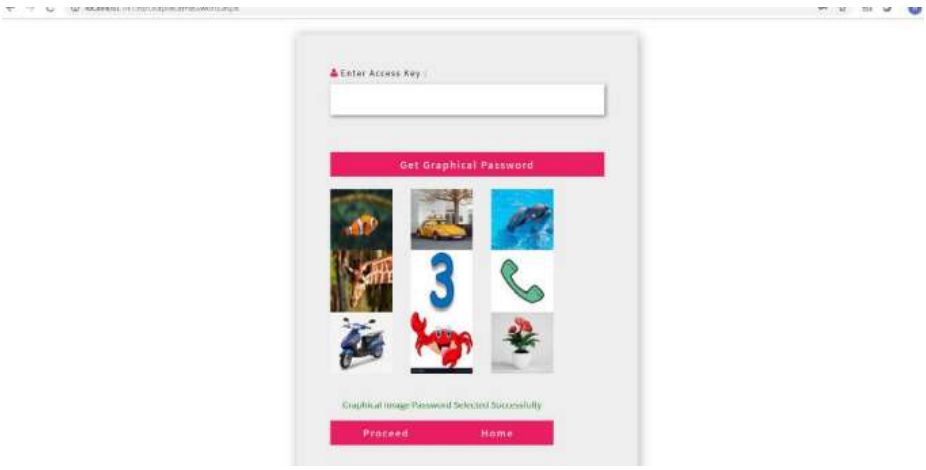

Figure 4: Account Holder login page
Figure 4 depicts the Account Holder login page where account holder will select his/her graphical password of 5 images to login to the system.

6. CONCLUSION

Graphical Password Systems utilize photographs or images in place of alphanumeric characters. The user must remember many images to login successfully. The obvious disadvantage of such a scheme is there is a large dictionary of such unique images in memory, however, if the number of possible images is sufficiently large, the potential password space of a graphical password does provide some added protection against dictionary attacks. Password authentication system, will lead to a less predictable and strong password yet still password that could be remembered reasonably and in a way that password has security. The correct login rate for multiple images with movable frame is 15% high then text password schemes, then they are better protection against shoulder surfing. Proposed system, gets away from the problem with remembering strings or random characters. Images are much easier to remember than passwords based on text. Our system is currently secure and hard to guess at graphical password.

7. REFERENCES

[1] Suo, Xiaoyuan, Ying Zhu, and G. Scott Owen. "Graphical passwords: A survey." Computer security applications conference, 21st annual. IEEE,2020.

[2] Noor Ashitah Abu Othman, Muhammad Akmal Abdul Rahman, Anis Shobirin Abdullah Sani, Fakariah Hani Mohd Ali "Directional Based Graphical Authentication Method with Shoulder Surfing Resistant", IEEE, 2021.

[3] Basak Bilgi, Bulent Tugrul, "A Shoulder- Surfing Resistant Graphical Authentication Method", IEEE, 2019.

[4] R. Sudha, M. Shanmuganathan, "An Improved Graphical Authentication System to Resist the Shoulder Surfing Attack", IEEE,2020.

[5] Sobrado, Leonardo, and Jean-Camille Birget. "Graphical passwords."The Rutgers Scholar, an electronic Bulletin for undergraduate research 2019.

[6] Khandelwal, Ankesh, Shashank Singh, and Niraj Satnalika. "User Authentication by Secured Graphical Password Implementation. "International Journal of Computer Applications pp 115- 120, 2018.

[7] Ugochukwu, Ejike Ekeke Kingsley, and Yusmadi Yah Jusoh. "A review on the graphical user authentication algorithm: recognition-based and recall-based." International Journal of Information Processing and Management 4.3 pp 238-252., 2021.

[8] Shah, Amish, et al. "Shoulder-surfing Resistant Graphical Password System." Procedia Computer Science 45, 2019.

[9] Dhamija, Rachna, and Adrian Perrig. "Deja Vu-A User Study: Using Images for Authentication." USENIX Security Symposium. Vol. 9.

[10] K. Gilhooly, "Biometrics: Getting Back to Business", in Computerworld, (May, 2019).

[11] R. N. Shepard, "Recognition memory for words, sentences, and pictures," Journal of Verbal Learning and Verbal Behavior, vol. 6, pp. 156-163.

[12] Real User Corporation, Passfaces TM "http//: www.realuser.com," Accessed on June2019.-