Authentication Schemes for Session Passwords using Color and Images

Himanshu Choudhary[1], Vartika Joshi[2], Vinay Kumar Satsangi[3], Vinita Chauhan[4]

[1,2,3,]*Research Scholar, Dept. of Computer Science & Engg. IMS Engineering college.*
[4]*Assistant Professor, Dept. of Computer Science & Engg. IMS Engineering college,(U.P.),India*

---***---

Abstract - *Authentication is the first and the most important step in information security. It use to authenticate the user identity. Where user need to memorize their password and remember at login time. Normally user use textual password to provide security, but textual passwords are vulnerable to many cyber-attacks, Such as - dictionary attacks, shoulder surfing etc. Graphical password schemes are used to overcome these problems. A Session password is a new technique based on the graphical password in which we using combination of text, color and images to solve the problem of security. Every time session password can be used to create password for user authentication, by this technique we can overcomes the attacks like shoulder surfing, dictionary attacks. We can use this method for PDAs (Personal Digital Assistants).*

***Key words*: Authentication, Security, Cyber-attacks, Shoulder Surfing, Dictionary attacks.**

1. INTRODUCTION

Now a day, Textual password is most common method used for authentication. But there is vulnerabilities of this method such as- eves dropping, dictionary attack, social engineering and shoulder surfing are well known. Normally we use random and lengthy passwords to make the system secure. But the main problem is the difficulty of remembering those passwords. If we use short password or passwords that are easy to remember, such passwords can be easily guessed or cracked. There are alternative techniques like graphical passwords and biometrics. Biometrics, such as finger prints, iris scan or facial recognition has been introduced but these make system to costly and not easy to adopt. The drawback of this approach is that such systems can be expensive and the identification process can be slow. In other hand, there are many graphical password schemes that are proposed in the last decade. But most of them facing shoulder surfing attacks, which is quite a big problem. There are graphical passwords schemes that have been proposed which are resistant to shoulder-surfing attacks but they have their others problems like usability issues and having tolerance levels (taking so much time for user to login). These schemes authenticate the user by session passwords. Session passwords are passwords that are used only once. The session password is no longer useful if session is terminated. For every login process, users input different passwords. The session passwords provide better security against dictionary and brute force attacks as password changes for every session. The proposed authentication schemes use text, colors and images for generating session passwords. We can use this method for PDAs (Personal Digital Assistants). This authentication system is used for authenticate user to access the website or ant window application as PDA.

2. RELATED WORK

Word-based passwords introduced in the early years are subjected to various attacks as mentioned in the former section. Besides this, many graphical authentication schemes have been evolved based on the requirements and the pitfalls associated with the prior existing authentication methods. Let we have a brief description on the various prevailing & proposed graphical authentication methods.

Blonder [5] state on graphical password technique, in which the password is generated by allowing the user to click on different positions on an image. During authentication, the user has to click on the estimated areas of those locations. Later, this idea was prolonged by 'pass-point system 'where the predefined boundaries are excluded and arbitrary images are supported. Everytime, for constructing password, the user can click over any region on the image. A tolerance around each chosen pixel is evaluated. To be authenticated, the user has to click within the tolerance level of the pixels chosen.

Syukri [6] generate a scheme in which authentication is carried out by sketching out the user signature. This scheme involves two levels, registration and verification. While registering, the user draws his signature using mouse, then system extracts the signature area. During the verification level, it acquires the user signature as input, performs normalization and finally extracts the parameters of the signature. But this scheme is associated with several disadvantages such as forgery of signatures, inconvenience while drawing with mouse, difficulty in sketching the signature in the same perimeters at the time of registration. There is another, a new graphical authentication method has been designed by Dhamija and Perrig[1]. This method, while creating the password allows the user to select certain number of pictures from a set of random images. Then, during login, the user has to recognize the preselected portraits from the set of images. But this method is liable to shoulder-surfing.

Passface[7] is an approach proposed by the Real User Corporation in which the user is allowed to choose four images of human faces from the face database as their password. While in verification phase, the user is provided with a grid of nine faces, one already chosen during the registration and eight decoy faces. The user identifies the selected face and clicks anywhere over it. Four times this course of action will repeat, and the user is ascertained as genuine if he recognizes all faces accurately.

A new innovative authentication scheme is proposed by Jansen [8, 9] for mobile devices. While creating the password, the user chooses a theme of snapshots in thumbnail size and the sequence of those snapshots is fixed as password. As each thumbnail is associated with numerical value, the sequence of images form numerical password. The only drawback with this method is that the password space is not large, as no of images is limited to 30.

To overcome shoulder-surfing challenge, many methods have been proposed. One of such technique is designed by Man, et al[10].In this system, the user selects many portraits as the pass objects. Each pass object is allotted an inimitable code. During the verification process, the user has to input those unique codes of the pass objects in the login interfaces presented by the system. Through the scheme resists the unvisible camera, the user has to memorize all pass object codes. In this way, many other graphical authentication schemes and their drawbacks are presented in a latest survey paper [11].

3. PROJECT WORK

The project working in this paper is entirely based on the session passwords. The main objective of this project is to provide security to the confidential website and web application in computing devices through session passwords. First it will be checked that the user is already registered or not. If yes, then it will go for the step of login, but if user is not registered then first he will go through registration and then to the login step. At the verification phase this password will be verified. It includes 3 phases: Textual Phase, Color Phase(Rating the color between 0-9), Image Phase(choosing the selected images). The process of figuring out the validate person is accomplished in the following manner:

3.1 Registration

On running the application, a login form turn up, allowing the user to enter the username and password. The form provide three buttons-register, login, close. If the user is already a registered one, then clicking on the "login "button would advance him to the first phase of login as a textual password. If the user is not a registered member, then on doing the above action would generate a message box conveying "username doesn't exist". Thus, in order to make use of the application, the person must register itself.

Consequently, on clicking the "register "button on the login form would display phase 1 window allowing the user to enter its personal information and username and text-password. On click of submit button data will safe then it proceed to phase 2. In Phase 2 (Color Phase), there is displaying four color (Red, Blue, Green, Yellow) and user need to rate the color in between (0-9). On click of submit button data will safe then it proceed to phase 3. In Phase 3 (Image Phase) there displaying 9 image grid with of 3X3 matrix, user need to choose 4 image among them and arrange in sequence. On click of submit button data will safe and then new user successfully get register and move to login page.

3.2 Authentication Process

On running the application, a login form turn up, allowing the user to enter the username and password. The form provide three buttons-register, login, close. If the user is already a registered one, then clicking on "login "button after filling username and password block. System will check the given data from database, if username exist then proceed to Phase 2(color phase) otherwise generate a message box conveying "username doesn't exist". In Phase 2 (Color Phase), there is displaying four color (Red, Blue, Green, Yellow) and user need to rate the color in between (0-9) value must be same as user gave while register. System will check the given data from database, if data match then proceed to Phase 3(image phase) otherwise generate a message box conveying " value is not match ". In Phase 3 (Image Phase) there displaying 9 image grid with of 3X3 matrix, user need to choose 4 image among them and arrange in sequence, chosen image and their sequence must b same as he choose while register. System will check the given data from database, if data match then generate a message box conveying "user successfully identify" otherwise generate a message box conveying "user is not identify " and move to login page.

4. SECURITY ANALYSIS AND PERFORMANCE EVALUATION

Every time, the session password changes as the interface changes. This technique is resistant to shoulder surfing. Due to dynamic passwords, dictionary attack is not applicable. In PDAs hidden camera attacks are not applicable because it is difficult to capture the interface in the PDAs.

Dictionary Attack: [12], This directly attacks towards on textual passwords. In this type of attack, hacker uses the set of dictionary words and authenticate by trying one word after one. The Dictionary attacks fails towards our authentication systems because session passwords are used for every login.

Shoulder Surfing:[13] These techniques are Shoulder Surfing Resistant. Using Pair based scheme, resistance is provided by the fact that secret password created during registration phase and remains hidden so the session password cannot be enough to find secret pass in one session. In hybrid textual scheme, the randomized colors hide the password. The ratings of the session password decide in this scheme,. But with session password you can't find the ratings of colors. It is resistant to shoulder surfing even by knowing session password, the complexity is 84 .

Guessing:[11] Guessing can't be a threat to the pair based because it is hard to guess secret pass and it is 364.The hybrid textual scheme is dependent on user selection of the colors and the ratings. If we follow the general order for the colors by the user , then there is a possibility of breaking the system.

Brute force attack:[12] These techniques are particularly resistant to brute force due to use of the session passwords. The use of these possibility of the traditional brute force attack negligible.

Complexity : The Complexity for Pair-Based Authentication Scheme is to be carried over the secret pass. The complexity is 368, for a secret pass of length 8. The complexity depends on colors and ratings in the case of the Hybrid Textual Authentication Scheme. The complexity is 8! if ratings are unique ,otherwise it is 8.

5. CONCLUSIONS

These techniques generate session passwords for user identifying. These technique are resistant to dictionary attack, brute force attack and shoulder-surfing. This technique use grid for generation session passwords. For the hybrid textual scheme, ratings should be given to colors, based on these ratings and the grid displayed during login, session passwords are generated. Hence, this scheme is quite new to the users and the proposed authentication techniques should be verified extensive.

6. REFERENCES

[1] R. Dhamija, and A. Perrig. "DéjàVu: A User Study Using Images for Authentication". In 9th USENIX Security Symposium, 2000.

[2] H. Zhao and X. Li, "S3PAS: A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme," in 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW 07), vol. 2. Canada, 2007, pp. 467- 472.

[3] Haichang Gao, Zhongjie Ren, Xiuling Chang, Xiyang Liu Uwe Aickelin, "A New Graphical Password Scheme Resistant to Shoulder-Surfing.

[4] M Sreelatha, M Shashi, M Anirudh, MD Sultan Ahamer,V Manoj Kumar "Authentication Schemes for Session Passwords using Color and Images", International Journal of Network Security & Its Applications (IJNSA),Vol.3, No.3,May2011.

[5] G. E. Blonder. Graphical passwords. *United States Patent 5559961*, 1996.

[6] 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. 403-441.

[7] Real User Corporation: Passfaces. www.passfaces.com

[8] W. Jansen, "Authenticating Mobile Device User through Image Selection," in Data Security, 2004.

[9] W. Jansen, "Authenticating Users on Handheld Devices "in Proceedings of Canadian Information Technology Security Symposium, 2003.

[10] 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

[11] X. Suo, Y. Zhu and G. Owen, "Graphical Passwords: A Survey". In Proc. ACSAC'05.

[12] Jermyn, I., Mayer A., Monrose, F., Reiter, M., and Rubin., "Thed esign and analysis of graphical passwords"in Proceedings of USENIX Security Symposium, August 1999.

BIOGRAPHIES

A Student and research scholar and dedicated towards the work assigned, and hardworking.

A Student and research scholar very persistence and peer learning

A Student and research scholar, good problem solving skills and having leadership quality.

Faculty incharge for industry interaction and department magazine and assistant professor in computer Science & Engg. Dept.,IMS Engineering College Ghaziabad.