Journal of Signal and Image Processing
ISSN: 0976-8882 & E-ISSN: 0976-8890, Volume 3, Issue 1, 2012, pp.-68-70.
Available online at http://www.bioinfo.in/contents.php?id=48

AUTHENTICATION SCHEMES FOR SESSION PASSWORDS USING COLOR AND GRAY-SCALE IMAGES

GAJBHIYE S.K.[1]* AND ULHE P.[2]

[1]Department of Information Technology, SDCE, Wardha, MS, India.
[2]Department of Computer Engineering, SDCE, Wardha, MS, India.
*Corresponding Author: Email-

Received: February 21, 2012; Accepted: March 15, 2012

Abstract- The most common method used for authentication is Textual passwords. But textual passwords are vulnerable to eves dropping, dictionary attacks, social engineering and shoulder surfing. Graphical passwords are introduced as alternative techniques to textual passwords. Most of the graphical schemes are vulnerable to shoulder surfing. To address this problem, text can be combined with images or colors to generate session passwords for authentication. Session passwords can be used only once and every time a new password is generated. In this paper, we proposed a scheme related to the grayscale images which will be advantageous as compared to many of the well known formats. Here we are going to use Visual secret sharing (VSS) scheme for security of grayscale images And to generate session passwords using text, colors and grayscale images.

In this paper, two new authentication schemes are proposed. These schemes authenticate the user by session passwords which are used only once. Once the session is terminated, the session password is no longer useful. 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 and colors for generating session passwords.

Keywords- visual secret sharing (VSS), grayscale images Authentication, session passwords, shoulder surfing.

Citation: Gajbhiye S.K. and Ulhe P. (2012) Authentication Schemes for Session Passwords using Color and Gray-scale Images. Journal of Signal and Image Processing, ISSN: 0976-8882 & E-ISSN: 0976-8890, Volume 3, Issue 1, pp.-68-70.

Introduction

The most common method used for authentication is textual password. The vulnerabilities of this method like eves dropping, dictionary attack, social engineering and shoulder surfing are well known. Random and lengthy passwords can make the system secure. But the main problem is the difficulty of remembering those passwords. Studies have shown that users tend to pick short passwords or passwords that are easy to remember. Unfortunately, these passwords can be easily guessed or cracked. The alternative techniques are graphical passwords and biometrics. But these two techniques have their own disadvantages. Biometrics, such as finger prints, iris scan or facial recognition have been introduced but not yet widely adopted.

The major drawback of this approach is that such systems can be expensive and the identification process can be slow. There are many graphical password schemes that are proposed in the last decade. But most of them suffer from shoulder surfing which is becoming quite a big problem. There are graphical passwords schemes that have been proposed which are resistant to shoulder -surfing but they have their own drawbacks like usability issues or taking more time for user to login or having tolerance levels. Personal Digital Assistants are being used by the people to store their personal and confidential information like passwords and PIN numbers. Authentication should be provided for the usage of these devices.

In this paper, two new authentication schemes are proposed . These schemes authenticate the user by session passwords which are used only once. Once the session is terminated, the session password is no longer useful. For every loginprocess, 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 and colors for generating session passwords.

This paper is organized as follows: In section II related methods and materials are discussed ; in section III Results & Discussions are introduced. In the next Section ,we give some experimental results and comparisons. Lastly, we conclude the paper.

Materials and methods

Dhamija and Perrig [1] proposed a graphical authentication scheme where the user has to identify the pre-defined images to prove user's authenticity. In this system, the user selects a certain number of images from a set of random pictures during registration. Later, during login the user has to identify the pre selected images for authentication from a set of images as shown in figure 1. This system is vulnerable to shoulder-surfing.

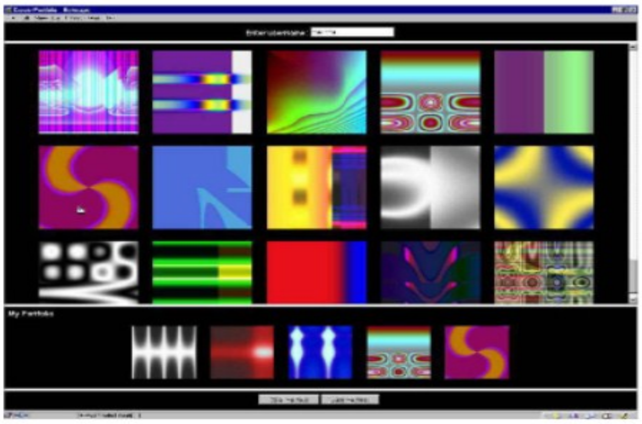


Fig. 1- Random images used by Dhamija and Perrig

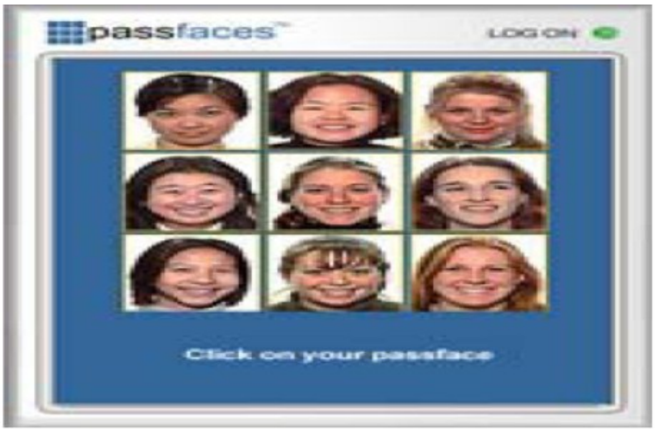
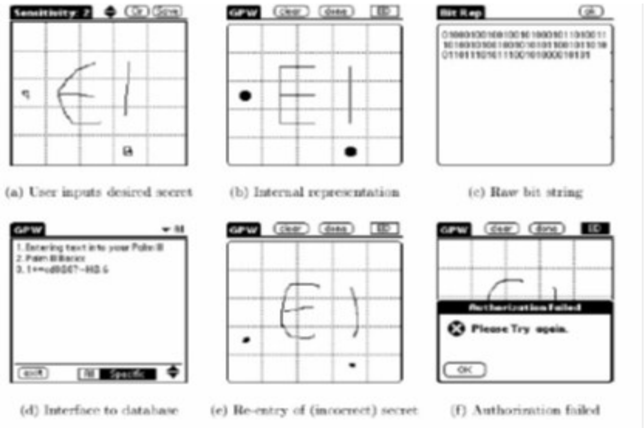


Fig. 2-

Example of Passfaces

A comparative study conducted by Brostoff and Sasse [14] in which 34 subjects involved in the test showed that, the Passfaces password is easier to remember compared to textual passwords. Results also showed that Passfaces took a much longer login time than textual passwords. Empirical and comparative studies by Davis et al. [15] showed that, in Passfaces the user's choice is highly affected by race, the gender of the user and the attractiveness of the faces. This will make the Passfaces password somewhat predictable.

Jermyn, et al. [3] proposed a new technique called "Draw- a-Secret" (DAS) as shown in figure 3 where the user is required to re-draw the pre-defined picture on a 2D grid. If the drawing touches the same grids in the same sequence, then the user is authenticated. This authentication scheme is vulnerable to shoulder surfing.



(a) User inputs desired secret (b) Internal representation (c) Raw bit string

(d) Interface to database (e) Re-entry of (incorrect) secret (f) Authorization failed

Fig. 3- DAS technique by Jermyn

Syukri [4] developed a technique where authentication is done by drawing user signature using a mouse as shown in figure 4. This technique included two stages, registration and verification. At the time of registration stage the user draws his signature with a mouse, after that the system extracts the signature area. In the verification stage it takes the user signature as input and does the normalization and then extracts the parameters of the signature.

The disadvantage of this technique is the forgery of signatures. Drawing with mouse is not familiar to many people, it is difficult to draw the signature in the same perimeters at the time of registration.

To overcome the shoulder-surfing problem,many techniques are proposed. Zhao and Li [13] proposed a shoulder-surfing resistant scheme "S3PAS". The main idea of the scheme is as follows. In the login stage, they must find their original text passwords in the login image and click inside the invisible triangle region. The system integrates both graphical and textual password scheme and has high level security. Man, et al [14] proposed another shoulder-surfing resistant technique. In this scheme, a user chooses many images as the pass-objects. The pass-objects have variants and each of them is assigned to a unique code.

Security Analysis

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

Dictionary Attack

These are attacks directed towards textual passwords. Here in this 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

These techniques are Shoulder Surfing Resistant. In Pair based scheme, resistance is provided by the fact that secret pass created during registration phase remains.

Results and Discussion

There are six main security features that are used on existing graphical password schemes. The features are shown in Table 2. The possible attack method is not classified as the security feature, it is only for the guidance and supporting reason of why the security features is needed. The possible attack method is divided into six types of attacks which are brute force, dictionary, guessing, spyware, shoulder-surfing and social engineering. These are the current active attack methods in graphical authentication environment.

From Table 2, it can be concluded that all of the existing schemes are vulnerable to brute force, guessing and shoulder-surfing attack. As we can see, the Draw-A-Secret (DAS) scheme is the only scheme that is capable of defending against brute force attack. This is because DAS provides the largest password space compared to other schemes [23]. The Pict-OLock scheme has a strong resistance to guessing.This scheme used the image variation where a same imageis displayed in different colors. Overall, the existing schemes have strong security mechanisms to counter dictionary, spyware and social engineering attacks. In order to protect against brute force and guessing, the scheme needs to provide a large password space. The larger the password space, the harder for brute force and guessing to succeed.

As depicted in Table 2, seven schemes provide a large size of password space to their scheme. To increase the security of graphical authentication, seven schemes used randomly assigned image and decoy images features. The purpose of using these features is mainly to defend against shouldersurfing attacks. As we can see, almost all of the schemes using these features are less susceptible to shoulder-surfing attacks. A total of four schemes used the hash visualization function. In order to strengthen the security of the selected password, some of these schemes combined hash and salt functions. Among all of these recognition and recall based security features, we will select the large password space, hash function and decoy images features to protect against the possible attack methods in graphical authentication environment. The repeat verifications, randomly assign images and image variation will not be used in the development of our scheme. As we can see, by repeating the process of verification it will make the authentication process slower which will affect scheme usability.

We conducted the user study of the proposed techniques with 10 participants for each technique. As the techniques are new, first the participants were briefed about the techniques. They were given demonstrations for better understanding purpose. Then each user was requested to login. After that, the usability study was conducted with the students in two sessions. The sessions were conducted in time frame of one week.

Conclusion

In this paper, two authentication techniques based on text and colors are proposed for PDAs. These techniques generate session passwords and are resistant to dictionary attack, brute force attack and shoulder-surfing. Both the techniques use grid for session passwords generation. Pair based technique requires no special type of registration, during login time based on the grid displayed a session password is generated. For hybrid textual scheme, ratings should be given to colors, based on these ratings and the grid displayed during login, session passwords are generated. However these schemes are completely new to the users and the proposed authentication techniques should be verified extensively for usability and effectiveness.

Acknowledgement

The authors would like to thank University of Technology Malaysia (UTM) and Ministry of Higher Education Malaysia (MOHE) for funding this work and the involving research.

References

[1] Dhamija R. and Perrig A. (2000) 9*th USENIX Security Symposium*.

[2] Real User Corporation: Passfaces. *www.passfaces.com*.

[3] Jansen W. (2004) *Data Security*.

[4] Jansen W. (2003) *Proceedings of Canadian Information Technology Security Symposium*.

[5] Weinshall D. and Kirkpatrick S. (2004) *Conference on Human Factors in Computing Systems (CHI)*. Vienna, Austria: ACM, 1399-1402.

[6] Goldberg J., Hagman J. and Sazawal V. (2002) *CHI* '02 *extended abstracts on Human Factors in Computer Systems*.

[7] Zhao H. and Li X. (2007) 21*st International Conference on Advanced Information Networking and Applications Workshops (AINAW)*, 2, 467-472.

[8] Man S., Hong D. and Mathews M. (1998) *Third Australasian Conference on Information Security and Privacy (ACISP)*: (1438), 403-441.

[9] Suo X., Zhu Y. and Owen G. (2005) *ACSAC*.

[10]Zheng Z., Liu X., Yin L. and Liu Z. (2010) *Journal of Computers*, 5(5).

[11]Passlogix, site *http://www.passlogix.com*.

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

[13]Wiedenbeck S., Waters J., Birget J.C., Brodskiy A. and Memon N. (2005) *International J. of Human-Computer Studies* 63, 102-127.