SECURITY SYSTEM for SESSION PASSWORD USING COLOR RATINGS and CHECK BOX GRID

Mr. Diney Wankhede[1],Mr. Ankit Ambekar[2] , Mr. Viplav Gangawane[3]
Mr. Amit Yeligeti[4], Mrs.Reena Mahe[5]

Department of Information Technology,
Atharva College of Engineering, Malad(West),
Mumbai, India.

[1]diney.12323@gmail.com,[2]ankitambekar08@gmail.com,[3]vipz24g@gmail.com,[4]amityeligeti@gmail.com

Abstract— **Text passwords, smartcards, digital certificates, graphical passwords, textual passwords, image passwords and the most extensively used biometric authentication are mechanisms presently used for authentication. But these systems are vulnerable to eavesdropping, dictionary attacks, social engineering and shoulder surfing; also the cost for biometric systems is a major concern. To address these problems, we are using color rating system to generate session passwords. Session passwords can be used only once and in each session a new password is generated. The approach is to improve the security of these systems relies on recognition-based, rather than recall-based authentication. This method is suitable for PDA's (Personal Digital Assistance).Importantly, introducing an efficient method of using check boxes in the grid so as to solve the problem of multiple values in the grid faced by existing systems.**

Keywords— **PDA's, Session passwords, recognition-based, color ratings, brute force attack, and dictionary attack.**

I. INTRODUCTION

The central component of currently deployed security infrastructures is user authentication. There are three main techniques for user authentication, classified as: Knowledge based, token-based, and systems based on biometrics.

Nowadays knowledge-based schemes are mainly used for user authentication systems. Despite their wide usage, passwords and PINs have number of shortcomings. These passwords are generally simple and easy to remember hence they are vulnerable to attacks.

Random and lengthy passwords can make the system secure, but the main problem is the difficulty of remembering those passwords. The users tend to pick short passwords or passwords that are easy to remember. But problem with these passwords is that it can be easily guessed or cracked. Graphical passwords and biometrics is an alternative method for authentication. Graphical passwords have disadvantages mentioned in the later part of the paper. Biometrics, such as finger prints, iris scan or facial recognition has been introduced but they may be very expensive.

In this paper we focus on authentication based on session passwords. A new authentication schemes is proposed for PDAs. Personal Digital Assistants are being used by the people to store their personal and confidential information like passwords and PIN numbers which needs high security. Hence providing authentication is very important for such devices.

This system uses combination of recognition-based and token based method of authentication in which the user is authenticated by session passwords. Session passwords are passwords that are used only once. Once the session is terminated, the session password is no longer valid. 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 scheme uses pre-defined color ratings for generating session passwords and check box grid for selection of the password with respect to the ratings.

II. EXISTING SYSTEMS

There are basically two types of authentication and it is worth understanding the two types and determining which one really matches the systems requirement. User authentication is the process whereby the identity of an evading user is confirmed. Entity authentication is a process used to restrict unauthorized entities/users from accessing information that is considered restricted or confidential. It is an authentication technique which is designed to let one entity prove the identity of another entity. The term entity may refer to a person, a process, a client, or a server.

Computer security is dependent on the proper design, management, and application of authentication systems.

© 2014 JCT. ALL RIGHTS RESERVED

Authentication mechanisms uses the term 'Identity' for building secure systems. Existing systems of authentication uses three main credentials which can be used to authenticate any type of system.

A. Something The User Knows:

The password security system [2] is the most common method of authentication. Passwords can be pure alphabetical, numerical, alpha-numeric and it may also contain special characters. Large number of systems use password based authentication.

Fig. 1 Password login system in Windows

Passport number, mother's maiden name, last 4 digits of your social security, credit card numbers are examples of passwords that are set by user generally. Systems such as online accounts of banks use passwords for authentication. PIN numbers used for operating ATM machines is also an example of password authentication. Passwords are generally pretty weak. Same passwords may be used in more than one place. If the user has ability to remember the password, the computer can easily guess those passwords. There are various attacks like brute force attack which can often crack all the types of passwords.

B. Something The User Has:

Existing systems provides security by various entities such as the tokens, smartcards and digital certificates.
Smart Cards have features like unpowered processors, small storage capacity, tamper resistant which provide security for online and offline systems using the physical card.

Fig. 2 Example of a smart card

Digital Certificates [2] is a method used by websites for the authentication of trusted applications or users. A certificate makes an association between a user identity/job/attribute and a private key. It contains public key information which has a validity period and is signed by some certificate authority (CA). The identity may have been vetted by a registration authority (RA) and issued by CA for some purpose. Verisign is in the business of issuing certificates

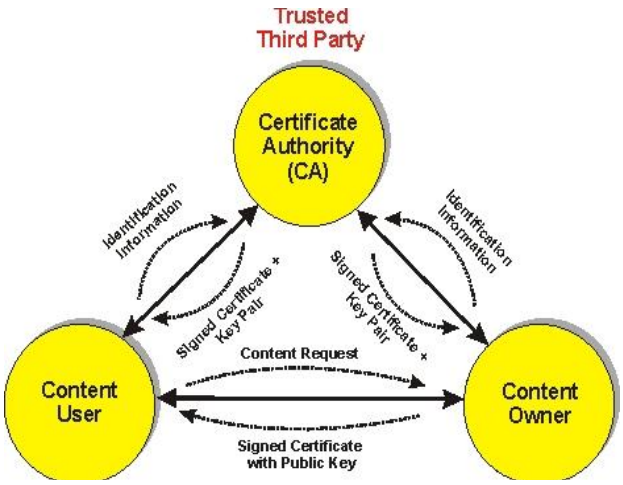

Fig. 3 Digital Certificate Mechanism

C. Something The User Is:

The most widely used system for authentication is biometric authentication systems [10]. This system measures the physical characteristics of the user. Fingerprint, face recognition, retina scanners, voice, signature and DNA are examples of this type of authentication. This method can be extremely accurate and fast. It can be classified on the basis of physiological and behavioral characteristics.

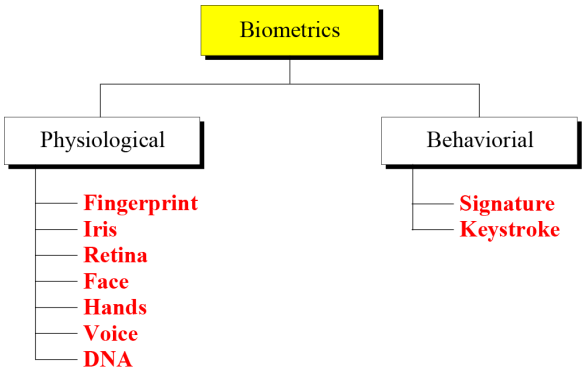

Fig. 4 Classification of Biometric Authentication

Active biometrics authentication is the one in which the user has to say the pass phrase in the microphone, the computer identifies the user from its stored database and authenticates the user by voice identification.

© 2014 JCT. ALL RIGHTS RESERVED

Passive biometrics recognizes the finger prints or scans the retina. Type of biometric authentication is used as per the requirement of the system.

Fig. 5 Examples of Biometric Authentication

D. Other Methods of Authentication:

Authentication by graphical pictures [1] is one method in which pre selected images needs to be selected from a set of images during the login phase. Drawing a secret [3] or digital signature [4] are methods which uses similar types of 2D grid on which a pattern has to be drawn to login the system. Pattern recognition techniques are used in digital signatures.

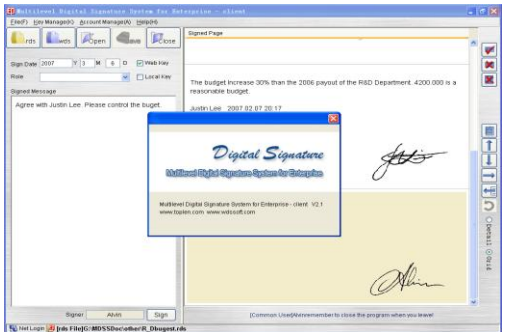

Fig. 6 Example of digital signature

III. SHORT COMING OF EXISTING SYSTEMS

The existing systems have number of disadvantages. The simple passwords or PIN's can easily be cracked by dictionary attacks or the brute force attacks. The smart cards system has a physical entity hence is prone to thefts and is risky for confidentiality systems. The graphical method of authentication is prone shoulder surfing while pass face requires lots of remembering work and can be cracked by brute force attacks.

Draw-a-Secret and Digital signatures are again vulnerable to shoulder surfing and it is difficult to exact sequence of the signature every time. Even a slight difference in the signature will be detected and hence causes error in authentication. Moreover these techniques are also not advisable as it needs special hardware and using the mouse every time for drawing may not be easy for everyone. Graphical Curve technique is resistant to shoulder surfing but at some point may be cracked by brute force attack as the grid size is of limited number of rows and columns. If the grid size is to be increased it will turn out to be difficult for the user to remember the exact sequence of the images and in turn will result in failure to authenticate.

Biometric Authentication is widely used but is most expensive method of authentication as the instruments required for scan the physical characteristics are expensive.

IV. TASK COMPLETION TIME

Based on study [1], we found out that it took longer for users to create image passwords than to create textual passwords and PINS. Photo registry took longer to create than Random Art registries, because people spent more time browsing and looking at each image. Users also required more time to login with image portfolios compared to passwords and PINs. Users took slightly longer to login using Random Art compared to photos, suggesting that people can recognize photographic images more quickly than abstract images.

TABLE I
AVERAGE SECONDS TO CREATE/LOGIN [1]

Phase	PIN	PASSWORD	ART	PHOTO
Create	15	25	45	60
Login	15	18	32	27
Login (after one week)	27	24	36	31

V. NECESSITY OF HIGHLY SECURED SYSTEM

Authentication is the act of confirming the truth of an attribute of user. This might involve confirming the identity of a person or software program, tracing the origins of an artifact, or ensuring that a product is what it claims to be.

In this paper, we are mainly concerned with user authentication. The proposed system is suggested for Personal Digital Assistance's. This device consists for highly confidentially information such as bank passwords, PINs, credit card numbers, passwords of websites logins etc. One cannot simply rely on the existing systems of authentication as due to their shortcomings. Accuracy in accessing the PDA at all time with ease is essential. The proposed system here provides us with secure system of authentication which uses color rating and checkbox grid. This authentication system provides us with high security for login. The user only needs to remember the ratings given to colors and according to the password pattern needs to check in the checkboxes as described in the further part of the paper. This security system may also be used in scientific labs or military stations which grant access only to registered users.

© 2014 JCT. ALL RIGHTS RESERVED

VI. PROPOSED SYSTEM OF AUTHENTICATION

In the new system, we use recognition based techniques. Recognition of the colors during the login phase as per the ratings given during the registration phase is the basis of the proposed system [9]. At the initial state, the user should rate the colors according to personal choice. Here, the user needs to create an account by entering a username and password. The user should rate colors from 1 to 8 as per own choice. For the ease of remembering the ratings the user can make own acronym. For example he can remember it by making a mnemonic such as 'RLYOGIPB'. Here in the fig.7, it stands for Red, Lime, Yellow, Olive, Gray, Indigo, Pink, and Black. User can also give same rating to two or more colors. Initially, during the login phase, when the user enters his username an interface is displayed based on the colors selected by the user.

Fig. 7 Color rating at creation phase

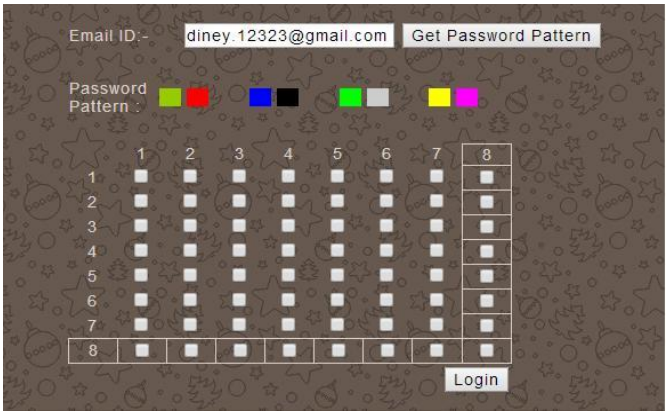

Fig. 8 Checkbox Grid Generation

While logging in the initial interface consists of grid of size 8*8. This grid consists of checkboxes placed in grid cells. The login interface contains strips of colors grouped in pairs which are termed as the password pattern. The color strip consists of 4 pairs of colors. We need to enter the rating of each pair by selecting it from grid. Depending on the ratings given to colors, we obtain the session password.

The figure 7 and figure 8 shows login phase having the color grid and checkbox grid of 8 * 8 having 8 row and 8 columns. The first color of every pair in color grid represents row and second represents column of the checkbox grid. The session password is generated by selecting the appropriate checkbox according to the password pattern i.e. the intersection of the row and column of the grid. The session password is not displayed externally; it is developed in the bank end and passed for authentication. Thus four pairs give us four checks in the checkbox grid which is the session password. For next login the pattern is being changed.

In the figure, the first pair of colors has olive and red colors. If the olive color rating is 4 and red color rating is 1. So the first check for generating the session password is 4th row and 1st column. We keep a grid of check boxes wherein we directly select the appropriate boxes for the ease of use. Using the checkboxes also allows us to avoid the problem of same digits in multiple boxes. There can be an error generated due to same digits at multiple places. Avoiding the use of checkboxes may not result in accurate result at all times. Hence using the checkbox grid is essential for the accuracy in logging in. The same method is followed for other pairs of colors. Using this grid will also help in speeding up the process as the user just needs to click on the intersecting checkbox directly the password gets registered internally. For every login, both the color grid and the checkbox grid get randomizes so the session password changes for every session maintaining the security of the system.

VII. CONCLUSION

Thus, we have described the high security authentication system which works accurately at all time. This technique generates session passwords and is resistant to dictionary attack, brute force attack, shoulder-surfing and eavesdropping. This system is developed specifically for Personal Digital Assistance (PDA's) which uses grid of checkboxes for session passwords generation. The vital addition to the existing system is that of using checkboxes in the grid which will facilitate the system to work precisely and accurately at all time. For this technique, ratings should be given to colors during the registration phase, depending on these ratings and the grid generated during login phase, and finally session passwords should be selected from the grid according to pairs of color. However this system is new and for more accurate results at every login phase checkboxes with values should be used in the 8*8 grid.

ACKNOWLEDGEMENT

The authors would like to thank project guide Prof. Reena Mahe Atharva College of Engineering, ,Mumbai and H.O.D. (I.T) Prof. Jyoti Chinchole Atharva College of Engineering, Mumbai (India).for their guidelines and involving in research.

REFERENCES

[1] R. Dhamija, and A. Perrig. "Déjà Vu: A User Study Using Images for Authentication". In 9th USENIX Security Symposium, 2000.
[2]http://ix.cs.uoregon.edu/~butler/teaching/11W/cis533/slides/cis533-authentication.
[3] Jermyn, I., Mayer A., Monrose, F., Reiter, M., and Rubin., "The design and analysis of graphical
passwords" in Proceedings of USENIX Security Symposium, August 1999.

© 2014 JCT. ALL RIGHTS RESERVED

[4] 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.
[5] Haichang Gao, Zhongjie Ren, Xiuling Chang, Xiyang Liu Uwe Aickelin, "A New Graphical Password Scheme
Resistant to Shoulder-Surfing"
[6] Passlogix, site http://www.passlogix.com.
[7] G. E. Blonder, "Graphical passwords," in *Lucent Technologies, Inc., Murray Hill, NJ*, U. S. Patent,
Ed. United States, 1996.
[8] Gajbhiye s.k.1 and Ulhe p.2 "authentication schemes for session passwords using color and gray-scale images" from Journal of signal and image processing.
[9] "Authentication Mechanisim For Session Passwords By Imposing Color With Text" K.Nivetha1, M. Muthumeena2, R. Srinivasan3
[10] The Mc Graw Hill's 'Cryptography and Network Security' by Behrouz Forouzan.

© 2014 JCT. ALL RIGHTS RESERVED