Pair & Hybrid Based Authentication Technique using PBKDF2

Priyanka Kedar, Vrunda Bhusari
Computer Department & University Pune,
India

Abstract— Everyone used the text password method for authentication. Authentication is used for information security. For authentication user name and password is used by the user. Authentication means, it is the process of identifying the user which is based on user name and the password. But takes passwords are susceptible to attackers , dictionary attacks, shoulder surfing and social Engineering. Text password are having number of problems so graphical password is introduced. In graphical   password, it has a shoulder surfing problem. In each session for authentication a new password is generated by combining text with images or colors. For this system two techniques are using to generate the session password by using text and colors. These techniques are opposed to shoulder surfing attack. PDA(Personal Digital Assistant) is the application of this system.

Keywords— Authentication, session password, shoulder surfing, PDA, Dictionary Attack.

I.   INTRODUCTION

   The common method is used for authentication is the text password method. In this method user enter user name and password. But in this method there are n number of problems because text passwords are easy to remember and simple. But vulnerable for eves-droppers for access. So, there are dictionary attacks, shoulder surfing , brute force and social engineering attack. Session passwords are complex and lengthy , it can make the system secure. But, this password can be easily breake because all these passwords are short password, simple and easy to remember[1]. Another technology for password is a graphical password, biometrics but both are having different disadvantages. There are number of methods for biometrics such as finger print, iris scan, facial recognition, signature. But major disadvantage of biometrics is that these systems can be costly. For graphical password there are number of methods used in last decades. In graphical password there is also a big problem for shoulder surfing. Many people are using PDA's to store confidential and personal data like PIN number, passwords. For authentication there are 3 main categories as token based, Biometric based and knowledge based authentication. Knowledge based authentication method is widely used for authentication which include both text based and picture based password[2][6][9].
.

II.   RELATED WORK

   Dhamjia & perrig[2] proposed a graphical authentication scheme. . At the time of Registration user has to select number of images from set of random pictures. After at the time of Login, user has to identify the images that pr-selected at the time of registration. This system is susceptible to shoulder surfing.
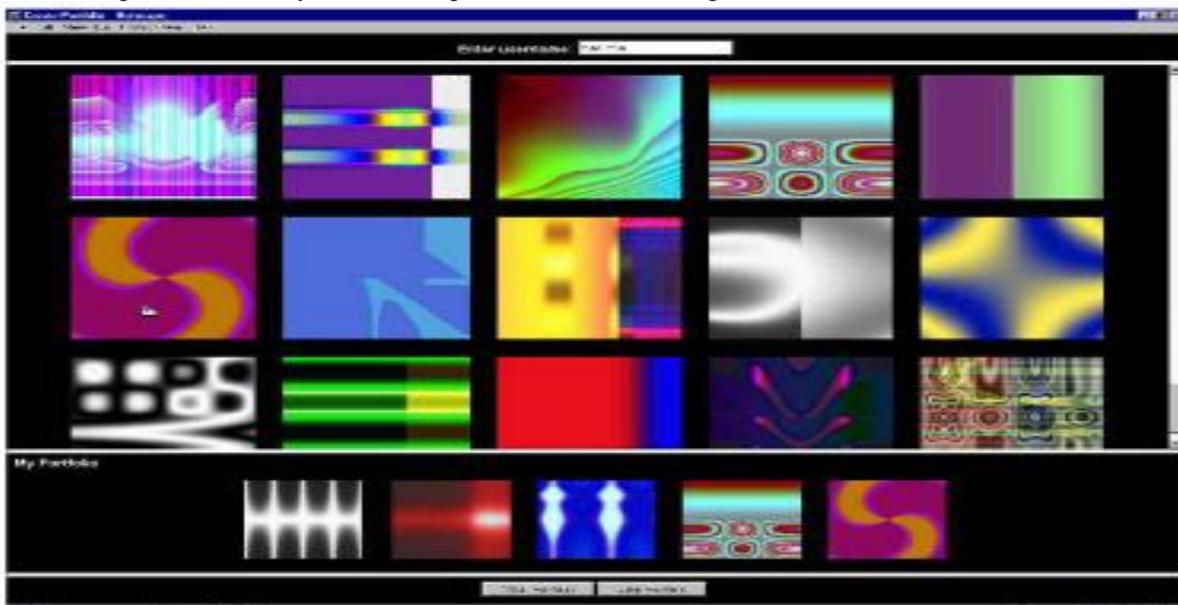

Fig. 1 Images used by Dhamjia & perrig

yukri[3] developed a new authentication scheme by user drawing the signature using mouse. This technique uses the two stages, registration and verification. During the registration stages the user draw his signature with a mouse. System extract the signature area after drawing the signature. In verification stage system takes the input of user signature and extract the parameters of the signature, which draw at the time of registration stage
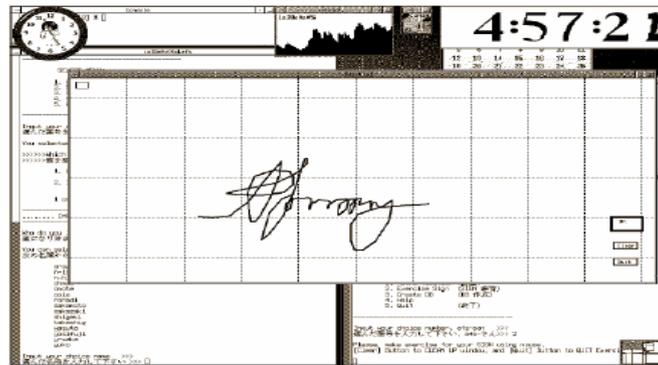
Fig. 2 Signature technique by Sukri

.
Jermyn[4] introduced a authentication technique called as " Draw_a_Secret"(DAS). In this technique user has to draw the signature by using mouse. Here user is needed to redraw the secret picture on a grid & if that drawing signature touches the same sequence that means user is authenticated person. This technique is vulnerable to shoulder surfing.

Fig. 3 DAS technique by Jermyn

Wiedenback[5] introduced a graphical password scheme because there are number of problems on shoulder surfing. In this technique user has to remember pass object & click in the convex hull formed of the pass objects.

Fig. 4 Example of convex hull

Haichang[6] described a new shoulder surfing resistant technique. As shown in the figure here user is needed to draw a curve across the password images orderly rather than clicking on them directly because to confuse to attaker.

Fig. 5 Shoulder surfing technique

III.   PROJECT WORK

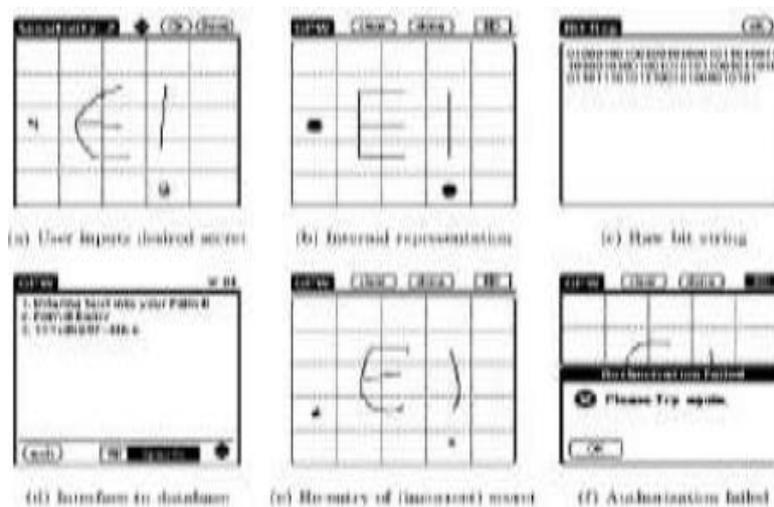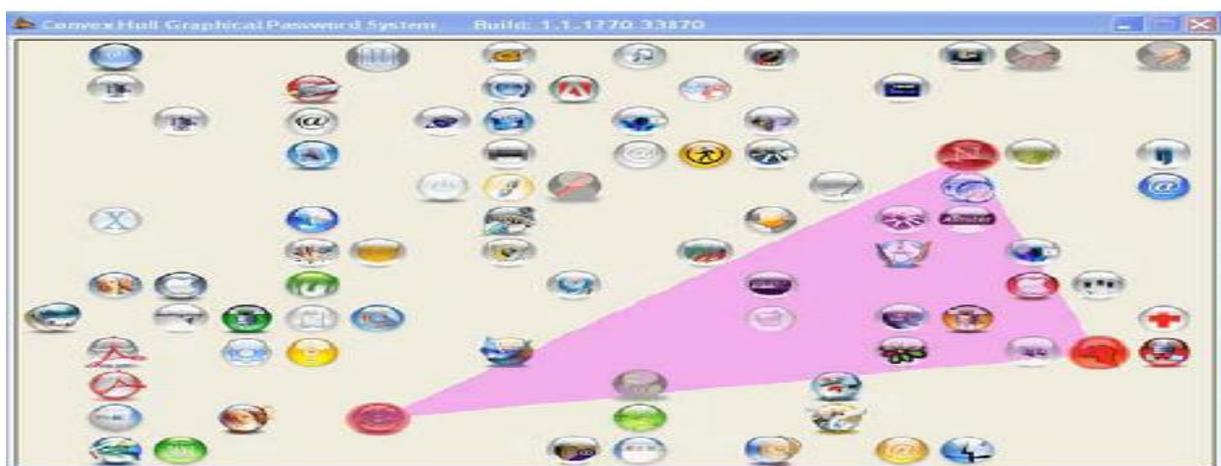In this technique there are 3 phases : Registration phase, login phase and verification phase.First check user is already registered or not if there is no registration then he will go through the registration else he will go for login phase. Main functionality of this system is to provide security to the confidential data, folders, files in computing devices through session password. During registration phase user enter his password in this phase or rate the colors in second phase. During login phase the user has to enter password based on the interface displayed on the screen.

A. Pair-Based authentication scheme

At the time of registration user submit his password and minimum length of password character is 8 and it should contain even numbers is called as secret pass[8][9]. By using secret pass session password is generated. At the time of login phase user enter his username and the grid is displayed. The grid size of 8x8 and it consist of alphabets, Special characters and numbers. At any session that are placed randomly on the grid.Depending upon the secret pass, the password entered by the user. Pair of secret pass has to consider by user so session password consist of alphabets, special characters and digits.

W	O	U	a	j	X	n	L
i	C	r	y	@	D	_	q
K	t	T	&	B	z	b	M
w	s	3	c	Y	2	J	u
V	o	Z	e	4	m	k	N
p	Q	h	1	A	9	d	O
5	v	x	E	I	H	g	l
F	f	6	G	R	S	7	P

| | LOGIN |

Fig. 6 Login Grid with Intersection character

For secret pass user has to consider the password in terms of pairs. From the pair, user has to select the 1st letter from the row and 2nd letter from the column. Select the intersection point of the row and the column , this is the part of the session pass. In this way repeat this procedure for all the pairs of session pass. When user enter the password that is verified by the server to authenticate the user. If the password is valid then n users are authenticated and enter in to the system.

B. Hybrid textual authentication scheme

At the time of registration phase user should rate the colours from 1 to 8 colours from the color grid which is called as hybrid textual password. For different colours we can give the same rating.

During login phase, user enter his user name, an interface is displayed which is based on colours which are selected by user. In login phase grid of size 8x8 & it contains digits 1to 8 paced randomly in grid cells. Grid has 4 pair of colours and each pair of colour represent row & column of grid. In this phase user will get the session password based on the ratings given to colours. Session password is the intersection of the row and column of the grid. Here colour grid get randomizes so the session password changes for every section.

Fig. 7 Colour rating

IV. CONCLUSION

In this technique user generate the session password by using two authentication scheme based on text and colors. For PDA's this technique opposed to dictionary attack, brute force, shoulder surfing. This technique can be verified usability and effectiveness.

V. FUTURE SCOPE

This technique can be used to develop any windows application or external authen -tication to connect the application to a database. PBKDF2 can be used for cryptography of session password.

REFERENCES

[1] G. E. Blonder, "Graphical passwords," in *Lucent Technologies, Inc., Murray Hill, NJ*, U. S. Patent, Ed. United States, 1996.

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

[3] 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.

[4] 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.

[5] S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy, N. Memon, "Design and longitudinal evaluation of a graphical password system". International J. of Human-Computer Studies 63 (2005) 102-127.

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

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

[8] S.Balaji, Lakshmi.A, V.Revanth, M.Saragini, V.Venkateswara Reddy "Authentication Techniques For Engendering Session Passwords With Colors And Text" Advances in Information Technology and Management Vol. 1, No. 2, 2012.

[9] 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