AUTHENTICATION SCHEMES FOR SESSION PASSWORD USING COLOR AND SPECIAL CHARACTERS

Rohit Jagtap[1], Vaibhav Ahirrao[2], Vinayak Kadam[3], Nilesh Aher[4]

[1,2,3,4].Department of Computer Engineering,
Purandar College of Engineering,Pune,Maharashtra

Abstract-- ***Generally user select password that is easy. This happens with both graphical and text based passwords. Users wish to choose memorable password it means that the passwords tend to follow patterns that are easier for attackers to guess. While such problem can be solved by not allow user to choice .usually leads to guessing issues since users cannot easily remember such random passwords. A literature survey shows that text-based passwords suffer with both security problems. As per the security requirement consideration we used two algorithm approaches.***

Keywords: session password, pair based approach, hybrid based approach, security schemes.

1. INTRODUCTION

Textual password is a very simple password scheme. It was used in old days. The textual password is easy to trace so system access easily. Because user give the password that are easy to remember, like pet name, birth date, mobile number etc. So textual password scheme is unreliable. For more security practices a new technology is invented that is Graphical password. It uses a very expensive system like a biometrics, thumb recognition, speech recognition, digital signature etc .But it was a very expensive so it is not affordable for user. Both the textual password and Graphical password having some drawbacks hence to remove such drawbacks the newely security scheme is implemented or invented that is session password. It is very secure compares to remaining systems.

2. LITERATURE SURVEY

2.1 BIOMETRICS

The biometric is one of the techniques for identification.It uses physiological or behavioral characteristics like retina scan, fingerprint scan as well as facial recognition or sound recognition to identify the user.But this technique is expensive.

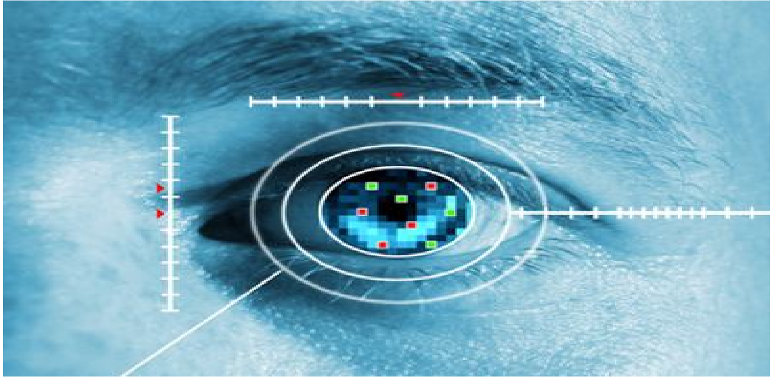


Figure 2.1: Retina scan

2.2 GRAPHICAL PASSWORD

The graphical password is most commonly used in authentication purpose. In this system, the user selects a certain number of images from a set of random pictures during registration

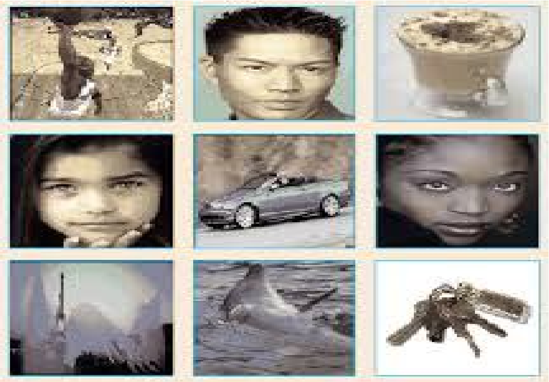


Figure 2.2:Example of pass faces

Later, during login the user has to identify the pre selected images for authentication from a set of images as shown in figure 2. This system is vulnerable to shoulder-surfing.

2.3 DIGITAL SIGNATURE

A digital signature is done by digital pen or any digital equipment.It is move to storage device by using some storing media.Once it is store in the database next time when login, the parameters can be check and if matching, the successfully login is granted.

Figure 2.3: Digital signature

The drawback of this technology is that a every user is not familier with digital equipment.If you forget the parameter of signature then user cannot get the access to the system.

2.4 VOICE RECOGNITION

Voice recognition refers to the recognition of human speech by computers and then performing a voice initiated program or function. The challenge that is handled so easily by the human brain, of interpreting speech amidst all accents, pitch, tone, articulation, nasality, vocalizations and pronunciation is a challenge when a computer tries to do it.

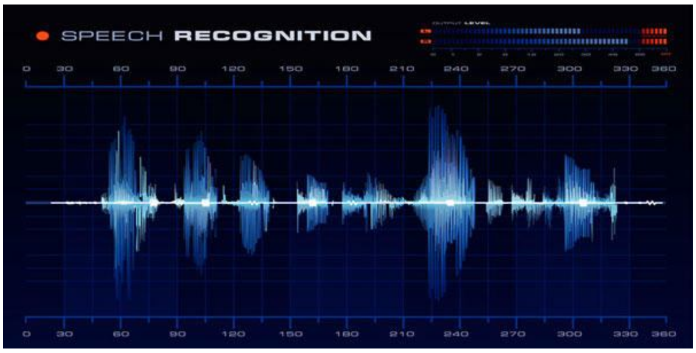


Figure 2.4 :Voice recognition

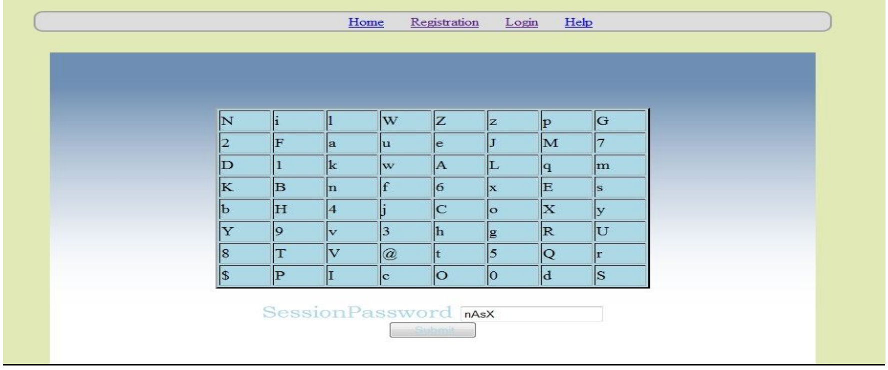
Moreover, the natural voice generation process in humans is a non-linear process which is not only under conscious control but is subject to variations based on factors as diverse as gender, upbringing or the emotional condition. This pattern is further distorted by the presence of noise and echoes in the surrounding environment.

3. NEW AUTHENTICATION SCHEMES

Authentication technique consists of 3 phases: registration phase, login phase and verification phase. During registration, user enters his password in first method or rates the colors in the second method. During login phase, the user has to enter the password based on the interface displayed on the screen. The system verifies the password entered by comparing with content of the password generated during registration.

3.1 PAIR BASED AUTHENTICATION SCHEMES

During registration user submits his password. Minimum length of the password is 8 and it can be called as secret pass. The secret pass should contain even number of characters.Session passwords are generated based on this secret pass. During the login phase, when the user enters his username an interface consisting of a grid is displayed. The grid is of size 8 x 8 and it consists of alphabets and numbers. These are randomly placed on the grid and the interface changes every time.



N	i	l	W	Z	z	p	G
2	F	a	u	e	J	M	7
D	1	k	w	A	L	q	m
K	B	n	f	6	x	E	s
b	H	4	j	C	o	X	y
Y	9	v	3	h	g	R	U
8	T	V	@	t	5	Q	r
$	P	I	c	O	0	d	S

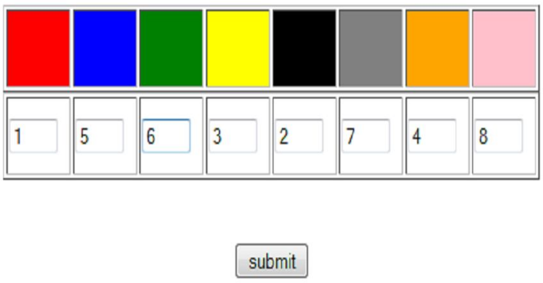
SessionPassword nAsX

Figure:3.1 Pair based approach

Figure 3.1 shows the login interface. User has to enter the password depending upon the secret pass. User has to consider his secret pass in terms of pairs. The session password consists of alphabets, digits ana special characters.The first letter in the pair is used to select the row and the second letter is used to select the column. The intersection letter is part of the session password. This is repeated for all pairs of secret pass. Fig 3.1 shows that x is the intersection symbol for the pair “xn”. The password entered by the user is verified by the server to authenticate the user. If the password is correct, the user is allowed to enter in to the system.

3.1 HYBRID TEXTUAL AUTHENTICATION SCHEMES

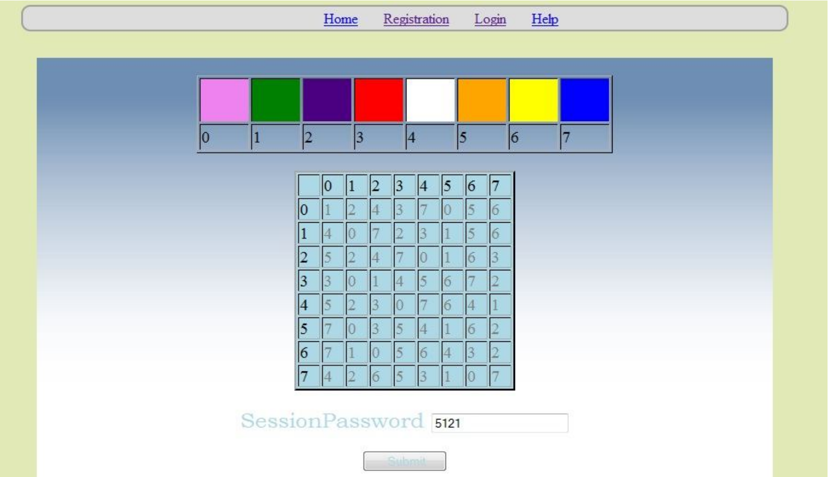
During registration, user should rate colors as shown in figure 9.



🟥	🟦	🟩	🟨	⬛	▨	🟧	▨
1	5	6	3	2	7	4	8

Figure 3.2: Registration phase

The User should rate colors from 1 to 8 and he can remember it as “RLYOBGIP”. Same rating can be given to different colors. During the login phase, when the user enters his username an interface is displayed based on the colors selected by the user. The login interface consists of grid of size 8×8. This grid contains digits 1-8 placed randomly in grid cells. The interface also contains strips of colors as shown in figure 10. The color grid consists of 4 pairs of colors. Each pair of color represents the row and the column of the grid.



🟪	🟩	🟪	🟥	⬜	🟧	🟨	🟦
0	1	2	3	4	5	6	7

	0	1	2	3	4	5	6	7
0	1	2	4	3	7	0	5	6
1	4	0	7	2	3	1	5	6
2	5	2	4	7	0	1	6	3
3	3	0	1	4	5	6	7	2
4	5	2	3	0	7	6	4	1
5	7	0	3	5	4	1	6	2
6	7	1	0	5	6	4	3	2
7	4	2	6	5	3	1	0	7

SessionPassword 5121

Figure 3.3: Login interface

Figure 3.2 shows the login interface having the color grid and number grid of 8 x 8 having numbers 1 to 8 randomly placed in the grid. Depending on the ratings given to colors, we get the session password. As discussed above, the first color of every pair in color grid represents row and second represents column of the number grid. The number in the intersection of the row and column of the grid is part of the session password. Consider the figure 9 ratings and figure 3.2 login interface for demonstration. The first pair has red and yellow colors. The red color rating is 1 and yellow color rating is 3. So the first letter of session password is 1st row and 3rd column intersecting element i.e **5**. The same method is followed for other pairs of colors. For figure 3.3 the password is “ **5121”.**”.

4. Conclusion and future implementation.

Textual password and Graphical password is easy to remember password scheme hence some security we have to provide a two secure algorithms implemented that is Pair based approach and Hybrid based approach. In that selecting the rating of color and also selecting the intersection of the password stream .Its a very secure such interface not easy to understand for new person or attacker.We have also use the Encryption standard like AES standard. In future in authentication approach first column second row can be implementing and also first row and last column also implement.

5. References

[1] 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.

[2] Haichang Gao, Zhongjie Ren, Xiuling Chang,Xiyang Liu Uwe Aickelin, “A New Graphical Password Scheme Resistant To Shoulder Surfing.

[3] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy and N. Memon, “PassPoints: Design and longitudinal valuation of a graphical password system”, International Journal of Human-Computer Studies, vol. 63, **(2005)**, pp. 102-127.

[4] D. Weinshall, “Cognitive Authentication Schemes Safe against Spyware”, (Short Paper), IEEE Symposium on Security and Privacy, **(2006)**.

[5] S. Chiasson, R. Biddle and P. C. van Oorschot, “A Second Look at the Usability of Click-based Graphical Passwords”, ACM SOUPS, **(2007)**.

[6] L. F. Cranor and S. Garfinkel, “Security and Usability”, O’Reilly Media, **(2005)**.

[7] R. N. Shepard, "Recognition memory for words, sentences, and pictures", Journal of Verbal Learning and Verbal Behavior, vol. 6, **(1967)**, pp. 156-163.

[8] A. Perrig and D. Song, "Hash Visualization: A New Technique to Improve Real-World Security", in Proceedings of the 1999 International Workshop on Cryptographic Techniques and E-Commerce, **(1999)**.

[10] D. Weinshall and S. Kirkpatrick, "Passwords You’ll Never Forget, but Can’t Recall", in Proceedings of Conference on Human Factors in Computing Systems (CHI). Vienna, Austria: ACM, **(2004)**, pp. 1399-1402.