Integrated Intelligent Research (IIR)
International Journal of Computing Algorithm
Volume: 03 Issue: 03 December 2014 Pages: 273-276
ISSN: 2278-2397

A Novel Crave-Char Based Password Entry System Resistant to Shoulder-Surfing

A.R.Johnson Durai[1], V.Vinayan[2]
St. Joseph's College of Arts and Science (Autonomous), Cuddalore
Email: duraiar@gmail.com, vinay@vinai.in

Abstract - Authentication is the process of allowing an authorized user to access a computer system. The commonly used system of authentication is the traditional Text password-based authentication mechanism. Though the traditional alpha-numeric driven text password entry system is well known for its higher state of security, it even experiences some drawbacks. To replace the traditional schemes and overcome their shortcomings, alternative solutions like graphical password schemes have been introduced. The graphical password systems are less prone to dictionary attacks and are easy to use visually. However, these graphical password schemes suffer from a potential drawback of being more vulnerable to shoulder surfing attacks when compared to conventional text driven passwords. In this paper, we propose a text-graphic password entry system which protects the user's password from being observed by attackers and prone to shoulder surfing and spyware attacks.

Keywords: Attackers, Authentication, Security, Shoulder-Surfing Attack.

I. INTRODUCTION

Authentication is one of the most essential processes which are highly necessary for every Security System. Authentication involves the user to enter the password. For every successful entry of the correct password for a specific user, He/She is allowed to access the Computer System. When this kind of process is carried out by the user, there are possibilities of the user's password being stolen by attackers using various attacks like Shoulder-Surfing, Screen Capturing Attacks. Each and every time it is not possible for the user to be aware of attackers. In order to protect the user's password from the attacker, I have prepared a Text-Graphic based Password Entry System which helps the user to be authenticated in a secure manner. In this paper, I have explained a Security Solution to prevent Shoulder-Surfing Attacks. In the first section, I have provided a brief description about Shoulder-Surfing Attacks. In the second section, I have covered some of the related works that have already been carried out in the area of Shoulder-Surfing. The Third section, explains my core Security Solution methodology. The performance and experimental analysis of my system is explained in section 4. In section 5, certain constraints and utilities of my Password Entry System are listed.

A. *Shoulder-surfing attack*

Shoulder-Surfing is using direct observation techniques, such as, looking over someone's shoulder to get information. Shoulder-Surfing is an effective way to get information be it in a user's home while he works on his personal computer or in a public place which is more prone to Shoulder-Surfing attack. Shoulder-Surfing can also be done even from a long distance with the aid of binoculars or other vision-enhancing devices. The increase in number of laptop and personal digital assistant (PDA) usage has greatly increased the danger of unauthorized observation of authentication procedures. The users have become more prone to password theft due to such kind of sneaking. Especially when users are moving around, it is more difficult for them to keep a strict vigilance on their surroundings. They could be easily trapped by someone who is viewing the traveller's authentication information. One should remain cautious of his/her surroundings if his/her authentication methods are prone to Shoulder-Surfing.

B. *Methods to reduce Shoulder-Surfing Attack*

Shoulder-Surfing certainly is not the most technical form of identity theft, but many have used this method to commit major fraudulent issues. The first step in the prevention of Shoulder-Surfing is in understanding that this problem does exist. There are certain precautions which may be taken by the user on a small scale while authenticating in any system, that are presently not using any prevention techniques to control Shoulder-Surfing. Shielding keypad from view by using body or cupping by hand while typing passwords is obviously one such method. One should experiment and create best password. It is advisable to use mixtures of numbers and letters rather than single, simple words for passwords. One should never carry important letters or statements from banks or building societies. These documents, along with credit or debit card can be a treat to a robber. It is not a direct solution to Shoulder-Surfing, but doing so can be a bit handy when it comes to protecting customers from revealing their personal information to strangers.

II. RELATED WORKS

There have been some counter measures used in a few products to prevent peeping attack. Few research proposals pertaining to it have also been proposed. But a fully functional solution which could be Shoulder-Surfing has not been deployed yet. One of the schemes proposed is that of pass faces shown in Fig.1 [1]. It is a challenge response scheme. A user chooses a set of images as his password. While authentication a user needs to select the chosen images in the serial order of his selection. When one picture is selected a new set of images for subsequent selection appears. In this method a user can authenticate by going through several rounds of image selection (which is actually equivalent to the password length). This method is prone to Shoulder-Surfing attack because one can easily view the position of the mouse cursor while authentication and the picture can be noted. Here the Pass faces are arranged in a similar fashion and challenge response

International Journal of Computing Algorithm
Volume: 03 Issue: 03 December 2014 Pages: 273-276
ISSN: 2278-2397

scheme is carried out. A user enters the coordinates of a particular Pass face rather than choosing it directly.

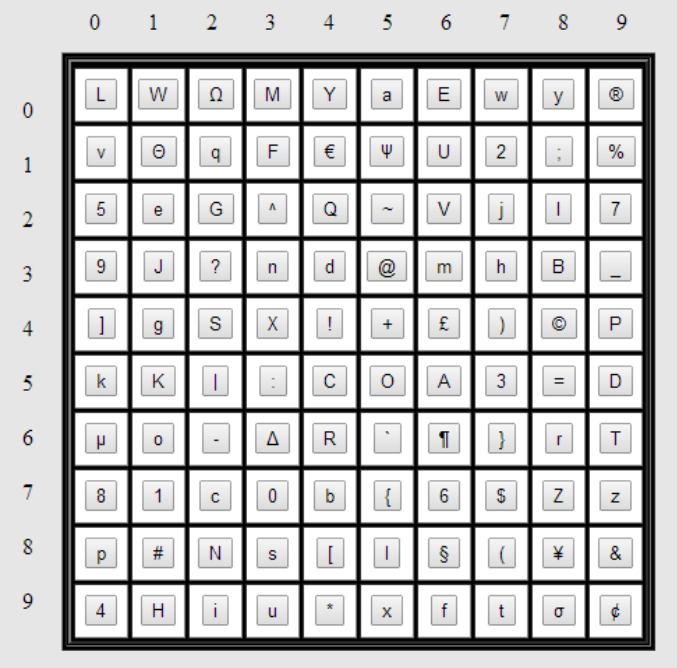

Figure 1. Pass faces

2) Divyans Mahansaria etal [2] describes A Fast and Secure Software Solution that Counters Shoulder-Surfing Attack.
In this Software Solution, when user click the password field a popup box appears.

	1	2	3	4	5	6
1	A	O	E	N	I	T
2	9	2	H	J	K	Q
3	6	0	Y	S	3	L
4	U	V	7	B	W	P
5	C	M	8	4	R	F
6	X	Z	D	1	G	5
7	!	@	#	$	%	:
8	&	*	(	)	?	“

Fig 2. Software Solution Method

It contains 8*6 order matrix (i.e. 8 rows and 6 columns) as shown Fig.2. The rows are numbered using the numbers from 1 to 8 and columns are numbered using the numbers from 1 to 6. The elements of the matrix will be randomly generated set of alphabets, numerals and symbols without repetition of any alphabet, numerals and symbols in the matrix. In the Password field, the user needs to type the position of the character. Let us suppose, for example, the password corresponding to the username “SECURITY” is “1DEI*2DTA#3. In this case, the user enters “SECURITY” in the ‘username field’. In the password field, the user will enter the position of the character (For ‘1’ – Position is 64 i.e. 6th row & 4th column, for ‘D’ – position is 63 i.e., 6th row & 3rd column). The user will enter 6463131582226316 as his password position. The last three characters of the password the user will enter the usual characters of the password without using position from the matrix (i.e. 6463131582226316A#3). In this solution, the login time will increase than usual. For example, password length is 10 then the user need to type 17 characters (14 characters indicate the original password). Therefore the user takes more time to authenticate.

III.CRAVE-CHAR BASED PASSWORD ENTRY SYSTEM

In the system, I have introduced a grid with 100 blocks with index of two sides. Left and Top sides of the Grid are indexed from 0 to 9. Totally the Grid constitutes of 100 blocks which contain alphabets, numbers, symbols and other web-supportive special characters. When the cursor is clicked on the Password field, then this set of blocks will appear. These blocks are named here as Pass Blocks. This helps to type your Password in a secure manner. The elements of the Pass Blocks will be a randomly generated set of alphabets, numerals and symbols without repetition. At the time of every login, these Pass blocks are randomly generated. The entire 26 English alphabets (both Upper and Lower Case), 10 numerals (0-9) and 38 chosen symbols will fill the Pass blocks as per the arrangement shown in the Fig.3.

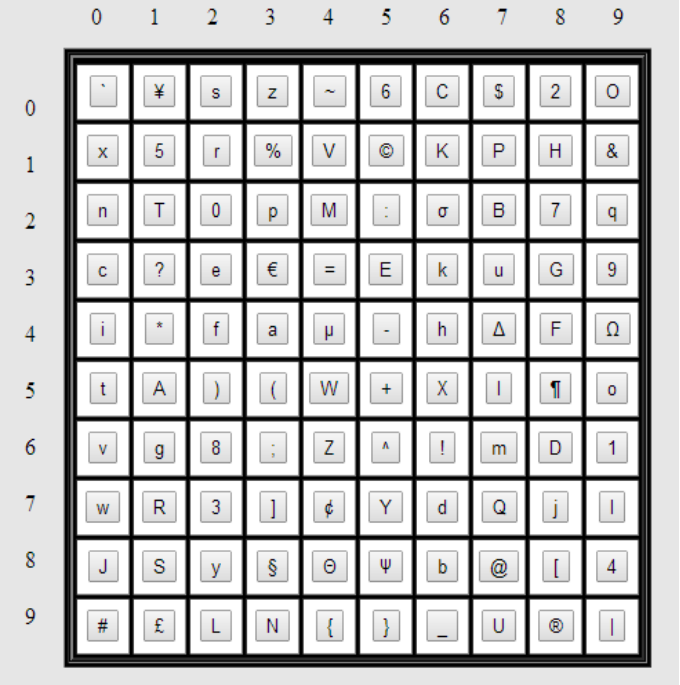

Figure 3. Pass Blocks

The difference between the previous systems of password entry and my own password entry system is, an additional attribute called Crave (favourite) Character. This Crave Character i.e the user’s favourite number (0 – 9), which he/she has to choose at the time of User Registration, helps the user to choose alternate password characters from a range of characters. This range of characters is characterized by the index shown in the grid which represents the favourite character chosen by the User.

International Journal of Computing Algorithm
Volume: 03 Issue: 03 December 2014 Pages: 273-276
ISSN: 2278-2397

Let us take the randomly generated grid shown in Fig.4 for experimentation. The grid consists of 100 pass blocks with varying characters. The user's selection of password from the generated block according to their constant password and favourable character is explained below. Let us consider, the username is "VINAY", the corresponding password is "2014" and the Crave Character chosen by the user at the time of registration is "5".

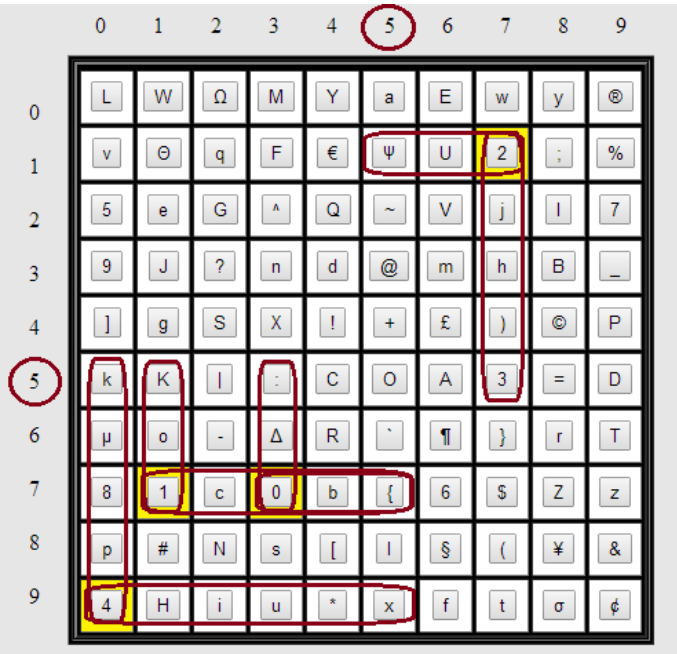

Figure4. Experimental Pass Blocks

The user types his username "VINAY" in username field. In the password field, the user types the pass character from the Pass Blocks based on illustration below.

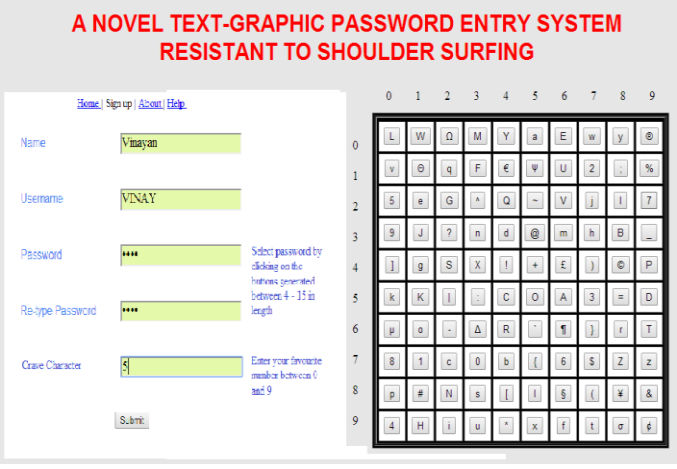

Figure5. Range of Selection for Password

In this method of Crave-Char based password entry, the password characters are matched with the possible paths to traverse the Crave-Char number position from the current position of the Password Character. In the above Illustration, the crave-char is '5'. So, the user is in need to traverse to the 5th column and 5th row in the generated grid. The user is free to select any character in between the current password character position and the position '5' on both sides. The possible set of characters for the above illustration is tabulated below.

Password Character	Possible Characters
'2'	U, Ψ, j, h,), 3
'0'	B, {, :, Δ
'1'	C, 0, b, {, o, K
'4'	H, i, u, *, x, p, 8, μ

Figure 6. Alternate password Characters

IV.MATHEMATICAL AND PERFORMANCE ANALYSIS

In the suggested grid, there are absolutely 100 Pass Blocks. Therefore the entire Blocks can be arranged in (100!) = (9.3326215444 x 10^{157}) Ways (approx.). In this Entry System, we have assigned the password length as minimum of 5 characters and maximum of 15 characters. Thus, total possible combinations of choosing a password length 'L' is C= ((100) ^L) where C is equal to the number of Combinations & 5<=L<=15 thus for password length equal to 5 characters, the total choice of ((100) ^5) = 10000000000 Ways. (approx.) and for password length which is equal to 15 characters, the total choice of (100 ^25) ways. This analysis shows that wide range of arrangements possible in the Pass Blocks and thus making it very difficult to break the security.

V.SIMULATION

A user starts the system to logon. If the users don't have the account and he or she need to create the account by click the Signup shown in fig 7. The user provide the require details for

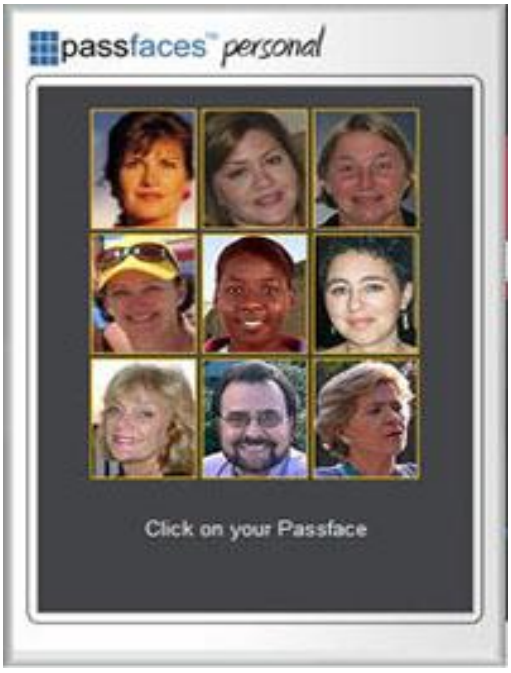

Figure 7.Signup snapshot

International Journal of Computing Algorithm
Volume: 03 Issue: 03 December 2014 Pages: 273-276
ISSN: 2278-2397

Sign-up and click submit button to create account.
After creating account, the user starts to login. To logon the user need to enter the username and password. The username is entered as usual. While entering the password, a new scheme introduced. The matrix like structure appears that is Pass Blocks which contain alphabets, numerals and symbols shown in fig. 4. The user has to find out the corresponding Pass character of his/her password from Pass Blocks and provide the Pass Characters as his/her password in the password field. Then 'Submit' is clicked for verification of the correctness of the provided username & password.
A comparison between the entered username & password and the already existing username & password in the database is made. If there exits such an account, then the login becomes successful.
If the authentication information is incorrect, then the login error message appears. Once again the user needs to type the username & password.

VI.CERTAIN CONSTRAINTS IN THIS ENTRY SYSTEM

The proposed mechanism of Password entry system is a new one so users need to be educated about the new password entry method. The login time will increased than usual. But keeping the high performance and other benefits in mind, we compensate on the time taken for initial logon.

VII.CONCLUSION

Unfortunately, today's standard methods for password input are subject to a variety of attacks based on observation, from casual sneaking, to many other forms of attacks. The Password Entry System can be very useful in controlling "Shoulder-Surfing". My Entry scheme can be used while initial logon after booting of a computer, during authentication which may be required before using particular software, opening important documents etc. With necessary changes the same scheme can also be employed to ATM machines and other forms of electronic which requires authentication before giving access to its users. It could also be used in websites wherever a username & password is initially required for authentication. Thus we see that the High Secure Password Entry System find its usage in a wide variety of different applications.

REFERENCES

[1] Real User Cooperation : www.passfaces.com
[2] Divyans Mahansaria, Samarpan Shyam, Anup Samuel, and Ravi Teja "A Fast and Secure Software Solution [SS7.0] that Counters Shoulder Surfing Attack," Proceedings of the 13th IASTED International Conference November 2-4 2009, Cambridge, MA,USA.
[3] William Stallings, "Cryptography and Network Security," 4th Edition. Publisher–Pearson Education Inc.
[4] Wade Trappe, Lawrence C Washington, "Introduction to Cryptography with coding theory", 2nd Ed, Pearson, 2007.
[5] Bogdan Hoanca, Kenrick Mock, "Screen Oriented technique for reducing the incidence of shoulder surfing," Security and Management 2005.
[6] S.Wiedenbeck, J.Waters, L.Sobrado, and J.C.Birget, "Design and Evaluation of a Shoulder-Surfing Resistant Graphical Password Scheme," Proc. of Advanced Visual Interface (AVI2006), pp.23-26, May (2006).
[7] Behzad Malek, Mauricio Orozco and Abdulmotaleb El Saddik, "Novel Shoulder-Surfing Resistant Haptic-based Graphical Password," Proc. of the EuroHaptics 2006 conference, July 3-6 Paris, France.
[8] S.Bindu, Raj Mohammed "A Novel Cognition based graphical Authentication Scheme which is resistant to shoulder surfing attack", Proceedings ICIP 08, I.K. International, Bangalore, August, 2008.
[9] Arash Habibi Lashkari, Dr. Omar Bin Zakaria, Samaneh Farmand, and Dr. Rosli Saleh "Shoulder Surfing Attack in Graphical Password Authentication," (IJCSIS) International Journal of Computer Science and Information Security, Vol. 6, No. 2, 2009.
[10] Haichang Gao, Zhongjie Ren, Xiuling Chang, Xiyang Liu, Uwe Aickelin, "A New Graphical Password Scheme Resistant to Shoulder-Surfing," cw, pp.194-199, 2010 International Conference on Cyberworlds, 2010.
[11] Tetsuji TAKADA "fakePointer: An authentication scheme for improving Security against Peeping attacks using video Cameras". UBICOMM08, Sept. 29-Oct.4 2008 Page(s):395 – 400.Publisher – IEEE Computer Society.
[12] Huanyu Zhao and Xiaolin Li, 2007, "S3PAS: A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme", 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW).
[13] Paul Dunphy, James Nicholson, Patrick Oliver,2008, "Securing passfaces for description", Proceedings of the 4th symposium on Usable privacy and security, ACM.
[14] Xiaoyuan Suo, Ying Zhu G. Scott. Owen, 2005, "Graphical passwords: a survey", 21st Annual Computer Security Applications Conference.
Furkan, Tari, A. Ant Ozok, Stephen H. Holden, 2006, "A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords", Proceedings of the second symposium on Usable privacy and security, ACM.