Grenze International Journal of Engineering and Technology, July 2015

Secure Authentication using Hybrid Graphical Passwords

[1]Shalaka Jadhav and [2]Abhay Kolhe
[1, 2]Computer Department, MPSTME, Narsee Monjee Institute Of Management Studies, Vile Parle(W)
Mumbai, Maharashtra 400056, India

***Abstract*— Passwords are used to restrict access to data. A user can gain access to a password protected file only by entering the correct password. Generally users prefer to use short passwords or those which are easy to remember. Such passwords definitely save time while logging in but are prone to various kinds of attacks. If an attacker is able to break the password then he will gain unauthorised access to someone's private data. To solve this problem researchers have come up with various techniques to strengthen the authentication system. One of those methods is based on graphical passwords. Graphical password techniques have been introduced as an alternative to the conventional textual password techniques. The password techniques presented in this paper will see a transition from textual passwords to graphical passwords. Simple textual characters will be treated as graphical forms. The users need to understand the graphical password system and the password entry mechanism.**

***Index Terms*— Graphical Passwords, Brute Force, Shoulder Surfing, Memory Ability, Session.**

I. Introduction

Authentication is required to secure a system. Usually passwords are used for authentication. Since textual passwords are prone to various kinds of attacks we use graphical passwords. Researchers have introduced many graphical password schemes which enhance security, are easy to remember and take minimal time to log in.

Haichang Gao, Xiyang Liu & Ruyi Dai (2009) stated that it is well known that people can memorise pictorial information better than textual information. So if passwords are created out of pictures, it would reduce the chaos of long complex textual passwords. Some pure graphical passwords are also vulnerable to shoulder surfing attacks. To prevent any breach of security, hybrid graphical passwords have been introduced. These would retain the characteristics of textual passwords and introduce new graphical features.

In these graphical password schemes the passwords are generated from an N x N grid. Here the value of “N” can be decided by the user. This grid will be filled by alphanumeric and special characters. Using these characters a pattern would have to be visualised. The user will just select the appropriate regions by clicking on it as explained by I. Jermyn, A. Mayer, M. Reiter & A. Rubein (1999). Thus a new graphical password would be created.

To secure the passwords various encryption techniques or one way hash functions can be used as explained

Grenze ID: 01.GIJET.1.2.513

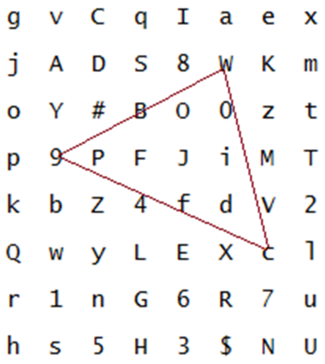
by Wei-Chi Ku & Maw-Jinn Tsaur (2005). In this way the computational load can be reduced. Care has to be taken to maintain the integrity of data and any attempt of unauthorised modification should be detected by the server.

The rest of the paper is organised as follows: Related work has been described in Section II, Proposed system is explained in Section III, Analysis on the proposed system is done in Section IV, Conclusion is given in Section V and References are mentioned in Section VI.

II. RELATED WORK

This section deals with the various existing graphical password strategies. Researchers have introduced both, pure graphical password schemes and hybrid graphical password schemes. Zhao and Li (2007) have described a triangle based graphical password scheme. It generates a randomised N x N gird consisting of alphabets A-Z and a-z, numbers 0-9 and special characters. The user selects a primary textual password. Using this password on the randomised grid, a new graphical password is generated.

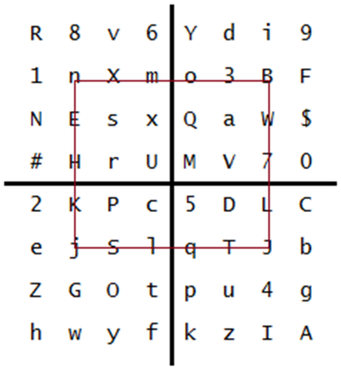
The user has to consider every three consecutive characters of his textual password and visualise a triangle on the randomised grid. Once the virtual triangle is formed, the user has to click inside that triangle or enter a character present inside that triangle. An example is shown in Fig. 1. This method has a few limitations. If the three characters fall in the same row or column, then the triangle cannot be formed. Thus the graphical password cannot be generated.



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

Figure 1: Triangle based password generation using three consecutive characters from primary password

Rao and Yalamanchili (2012) have described a rectangle based method. It has a similar randomised N x N grid consisting of alphabets, numbers and special characters. The grid is divided into quadrants. The user has to consider pairs of consecutive characters of the textual password and locate the pair on the grid and find its mirror coordinate characters across the axes. An example is shown in Fig. 2. Thus four characters forming a closed figure will be visualised. The user has to click inside this closed figure. After repeating these steps for the entire textual password a new graphical password will be generated.



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

Figure 2: Rectangle based password generation using pairs of characters from primary password

Gao, Chen and Wang (2008) have described a graphical password strategy that not only enhances the strength of the password but also removes the restrictions on the user. It uses the neighbourhood grid concept. Every stroke would be represented by the number given in the neighbourhood grid. Pen-up and pen-down actions are represented by ‘5’. After following every stroke a coded string is generated. This string is the graphical password. A similar sketching concept has been used by Yuxin Meng (2012), where initially the user has to select an image from a pool of images. The next step involves password sketching on a grid. The stroke sequence to be followed is shown in Fig. 3.

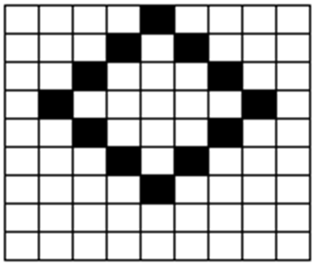
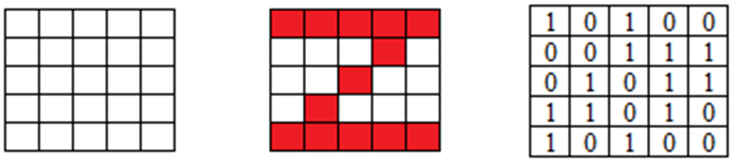


Figure 3: Password generation using neighbourhood grid concept

Zheng and Liu (2009) have described a stroke based textual scheme. The user has to select a stroke and sketch it on an N x N grid. This grid will be filled with a set of characters. A vector will be generated containing those characters covered by the stroke. This vector is the generated graphical password. An example is shown in Fig. 4.



1	0	1	0	0
0	0	1	1	1
0	1	0	1	1
1	1	0	1	0
1	0	1	0	0

Figure 4: Stroke based password generation

The vector generated for the grid used in Fig. 4 will be [1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0].

III. Proposed System

A. Description

This section describes a hybrid graphical password scheme. It works on an N x N grid consisting of alphabets, numbers and special characters. In this technique the user will select a primary textual password. The basic idea of using graphical passwords is that the user never has to enter his primary password. The user has to visualise accurate patterns and enter the new graphical password accordingly. Thus the primary password remains secure.

To make the password more secure, the grid is randomised. This ensures that the characters are always placed in different cells. If the grid itself keeps changing at every run, the generated graphical password also keeps changing. So even if an attacker is able to capture the entered password it would be of no use at consequent login sessions.

This technique uses an N x N grid as shown in Fig. 5. Depending on the value of ‘N’, the set of password icons would be decided. In the grid shown in Fig. 5, the diagonals are left blank. These blank diagonals would act as dividers of the four regions.

If ‘N’ is odd: -

$$\text{Total no. of password icons} = (N-1)^2 \qquad (1)$$

If ‘N’ is even: -

$$\text{Total no. of password icons} = \{(N-1)^2 - 1\} \qquad (2)$$

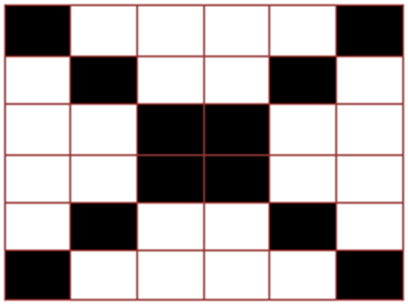


Figure 5: Password Grid for the proposed system with diagonals as separators

B. Password Entry Mechanism

The graphical password would be entered in ‘m’ rounds. Here ‘m’ is the length of user’s primary textual password. For every character in the primary password, four inputs will be made. If a character is found in a region then ‘Y’ or ‘y’ would entered. If the character is not present in a region then ‘N’ or ‘n’ would be entered.

We will begin with the first character in the primary password; check in which region it lies. If it lies in the right region then the four inputs to be made will be “NYNN” or “nynn”. The order to be followed is clockwise starting from top region.

After one round is completed, the grid is reset. We will have a new randomised grid. This is done to ensure that an attacker is unable to keep track of the password characters. Similarly the procedure will be carried out for all the characters of the primary password. Once all ‘m’ rounds are done we will have a matrix of dimension ‘m’ by 4. This matrix will be compared to the correct input sequence. If they match then the user will be granted access.

Example

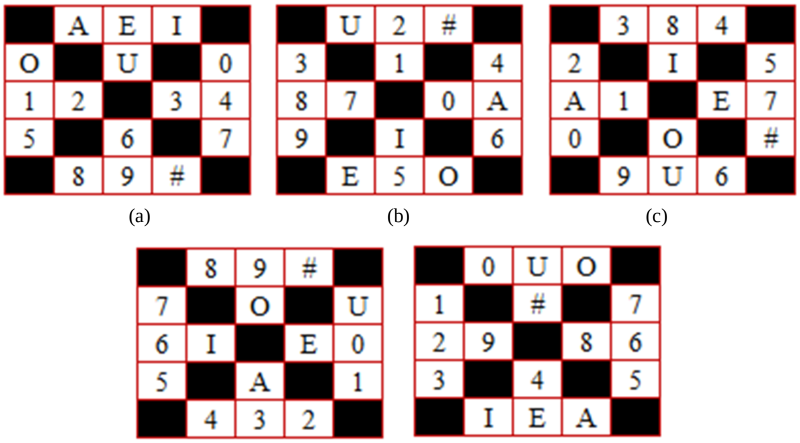
N = 5

Set of Password Icons = {‘A’, ‘E’, ‘I’, ‘O’, ‘U’, ‘0’, ‘1’, ‘2’, ‘3’, ‘4’, ‘5’, ‘6’, ‘7’, ‘8’, ‘9’, ‘#’}

Primary Textual Password = “A15#E”

Since the length of textual password = 5, there will be five rounds as shown in Fig. 6.

m = 5



■	A	E	I	■
O	■	U	■	0
1	2	■	3	4
5	■	6	■	7
■	8	9	#	■

(a)

■	U	2	#	■
3	■	1	■	4
8	7	■	0	A
9	■	I	■	6
■	E	5	O	■

(b)

■	3	8	4	■
2	■	I	■	5
A	1	■	E	7
0	■	O	■	#
■	9	U	6	■

(c)

■	8	9	#	■
7	■	O	■	U
6	I	■	E	0
5	■	A	■	1
■	4	3	2	■

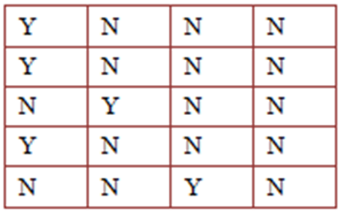
(d)

■	0	U	O	■
1	■	#	■	7
2	9	■	8	6
3	■	4	■	5
■	I	E	A	■

(e)

Figure 6: Rounds of password set procedure

The password matrix should be: -



Y	N	N	N
Y	N	N	N
N	Y	N	N
Y	N	N	N
N	N	Y	N

Figure 7: Password Matrix

If the user enters the correct sequence authentication would be successful. If the correct sequence of inputs is not entered, then the user will not be granted access. Here the count as well as the position of input is important.

C. Possible Improvements

An alternative can be considered for entering the password. A ‘y’ input can be replaced by left mouse click and ‘n’ input can be replaced by right mouse click. This way it becomes easier to input password and it also takes lesser time. It also becomes difficult for the attacker to keep track of the mouse clicks. Password entry by mouse clicks is faster than entry by keyboard. Also it is more difficult to capture for any possible attack. The user simply has to click on the accurate regions with the corresponding mouse click. The user will click left mouse button for character match and right mouse button for character mismatch.

IV. ANALYSIS

A. Usability

Since this method is a transition from textual passwords to hybrid graphical passwords, it is user friendly. It involved conventional characters that the users are familiar with. The users only need to remember the sequence of password entry, i.e. clockwise, starting from top region.

B. Time taken to login

Once the user understands the idea behind this method, it will become easier to simply enter the password matrix. Depending on the length of primary password it would take 15 – 20 seconds to be authenticated. Password entry by mouse clicks is faster than that by keyboard. Thus it will take less time to login.

C. Memory ability

This method does not involve any complex procedure. The user has to remember the sequence of password entry. Then he just needs to click ‘Y’ or ‘N’ to complete the password matrix or click left or right mouse button accordingly.

D. Resistance to attacks

Randomised grid is used to generate the password. This ensures that all characters appear in different cells in consequent runs. Thus it is nearly impossible to predict the password by brute force attack. Since the grid resets after every round the attacker cannot find any intersecting region where a character might lie. It also ensures that a password once generated will not be the same for the next session. Thus it prevents shoulder surfing attack.

V. CONCLUSION

Thus a secure and user-friendly technique for authentication using hybrid graphical passwords has been proposed. It serves the purpose of enhancing more security and at the same time eases the restrictions on the users. The users do not have to worry about anyone spying during logging in as the passwords would be different for every login session. The proposed technique is user friendly. It is easy to understand and can be adapted on existing systems. It takes less time to login and is able to resist various kinds of attacks like brute force, shoulder surfing and random click attacks. Since the proposed technique is a transition from conventional textual passwords to hybrid graphical passwords, the users will find it easier to adapt to such a system. The randomised nature of the password grid ensures that an attacker will not be able to capture the original password by any form of spyware and any random click attack will be blocked by grid reset feature.

REFERENCES

[1] Haichang Gao, X. Guo, X. Chen, L. Wang & X. Liu (2008). "Yet Another Graphical Password Strategy", *Annual Computer Security Applications Conference*, 121-129.

[2] Haichang Gao, Xiyang Liu & Ruyi Dai (2009). "Analysis and Evaluation of Colour Login Graphical Password Scheme", *Fifth International Conference on Image and Graphics*, 722-727.

[3] I. Jermyn, A. Mayer, M. Reiter & A. Rubein (1999). "The Design and Analysis of Graphical Passwords", *Proceedings of the 8th USENIX Security Symposium*, Volume: 8, 1-14.

[4] Wei-Chi Ku & Maw-Jinn Tsaur (2005). "A Remote User Authentication Scheme using Strong Graphical Passwords", *Proceedings of IEEE Conference on Local Computer Networks*, 351-357.

[5] Yuxin Meng (2012). "Designing Click-Draw based Graphical Password Scheme for Better Authentication", *IEEE Seventh International Conference on Networking, Architecture and Storage*, 39-48.

[6] M. Kameswara Rao & Sushma Yalamanchili (2012). "Novel Shoulder-Surfing Resistant Authentication Scheme using Text-Graphical Passwords", *International Journal of Information and Network Security*, Volume: 1, No. 3, 163-170.

[7] Huanyu Zhao & Xiaolin Li (2007). "A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme", *Advanced Information Networking and Applications Workshops*, Volume: 2, 467-472.

[8] Z. Zheng, X. Liu, L. Yin & Z. Liu (2009). "A Stroke Based Textual Password Authentication Scheme", *First International Workshop on Education Technology and Computer Science*, Volume: 3, 90-95.