Textual and Graphical Password Authentication Scheme Resistant to Shoulder Surfing

Roshni Rajavat
K.J.Somaiya COE
Vidyavihar, Mumbai

Bhavna Gala
K.J.Somaiya COE
Vidyavihar, Mumbai

Asmita Redekar
K.J.Somaiya COE
Vidyavihar, Mumbai

ABSTRACT

Authentication is a process that ensures a user's identity. User's identity can be verified by user name and password. The textual passwords are the most widely used passwords for authentication. There is a common trend among users to choose short length passwords which are easy to memorize. However, textual passwords are vulnerable to various attacks that include shoulder-surfing, brute force attack, hidden camera and spyware attacks. So to overcome the issues related to textual passwords we propose an authentication scheme called Textual Graphical Password Authentication Scheme Resistant to Shoulder Surfing. This scheme combines both text as well as graphics which are capable of resisting shoulder surfing, brute force attack, hidden camera and spyware attack. The specialty of Textual Graphical Password Authentication Scheme Resistant to Shoulder Surfing is its user friendliness which allows the user to migrate from the current authentication scheme to our proposed scheme.

General Terms

Authentication, technique, shoulder-surfing, clicks and single set scheme.

Keywords

Hacking, brute force attack, graphical password and authorization.

1. INTRODUCTION

Authentication requires a user to enter user name and password for authorization. The length of the password is usually chosen to be short by the user for easy remembering this increases the chance of the password to be hacked by the attacker. Long length password cannot solve the drawback of short passwords because users tend to forget their own passwords [1].

Graphical passwords can be considered as an alternative to textual passwords. Humans can recognize and remember images easily over text [2]. However, the graphical passwords are not economically viable as compared to text based. Unfortunately, graphical passwords are more vulnerable to shoulder surfing attacks as compared to textual passwords.

To overcome the weakness of text as well as graphical passwords we propose an authentication scheme called Textual Graphical Password Authentication Scheme Resistant to Shoulder Surfing which is a combined approach of text as well as graphical passwords.

The advantages of Textual Graphical Password Authentication Scheme Resistant to Shoulder Surfing are: It secures the password even if attacker sees or camera records the password during authentication process. The scheme is user friendly. The input can be given through keyboard as well as mouse which make it more adaptable. It supports client-server environment and its main advantage is it's resistant to brute force attack, shoulder surfing.

2. RELATED WORK

The existing authentication scheme uses text as well as graphics but lacks the security factor. The existing authentication schemes are not immune to shoulder surfing and brute force attack .The various existing authentication schemes are as follows:

2.1 Pass Point System

The textual alpha-numeric password came into existence in 1960's for security in multi user environment. For security reasons Blonder proposed the graphical password scheme which allows the user to set a particular image as his password and click on specified positions in the given image for authentication. The pass point system elaborated on Blonder's idea and allowed the user to click on arbitrary position rather than click on specified locations [3].In this technique user is asked to click on several positions in the given image to get authenticated. The image helps the user to recognize his set password [4, 5]. The user is authenticated when he clicks on accurate position and within the tolerance of the pixels.

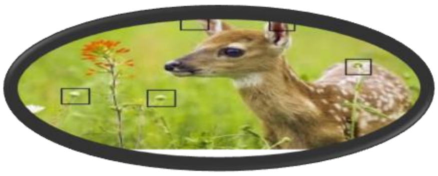


Figure 1: Pass point image

2.2 Pass Face Technique

Graphical password technique has been proposed as an alternative to text based techniques. Graphical password techniques can be categorized into two schemes which are Recognition based and Recall-based graphical techniques. The pass face technique fall into recognition based technique in this technique user is given a face database and user has to click on given faces to get authenticated. The pass face technique [6] was developed by Real User Corporation in this technique user has to select faces from a given face database to get authenticated. Here, User has to select four faces from a given face database to set his password.

Figure 2: Face database

2.3 Draw a Secret

This technique was developed by Jermyn et al in 1999 [7].This technique is also known as DAS Scheme. In this technique user is allowed to draw any shape, picture or any character as password to get authenticated. This scheme increases troubles for hacker while hacking the password. The DAS technique is implemented using following aspects. In this scheme suppose user draws any shape as password this shape or picture is 2 dimensional grid of size G*G [8, 9, 10] as Fig. shown that each cell in the grid is represented with (x, y) coordinates. The value of selected grid first stored temporary when user select exact coordinates then user get authenticated. For example, in the following image user made curve like shape as password.

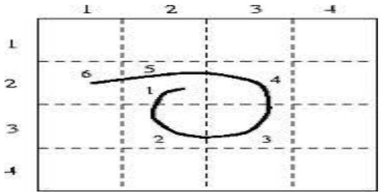


Figure 3: Draw a secret

2.4 Drawbacks of current Authentication Techniques

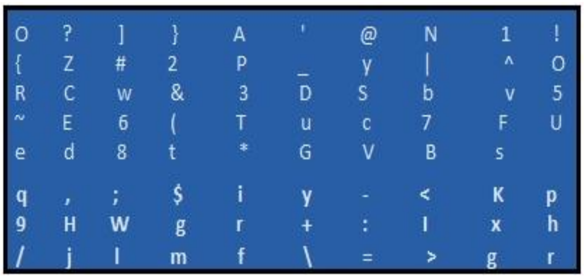
Traditional alpha-numeric passwords are text based these passwords are effortlessly hacked by the hacker and these passwords are easily vulnerable to Shoulder-Surfing, Brute Force, Hidden camera & Spyware attacks [11, 12]. Shoulder-Surfing means when user enters password attacker watches from behind, all of the above explained techniques are easily vulnerable to Shoulder-Surfing. While clicking on given image anyone can easily notice where the user is exactly clicking because the size of the image is big enough to click on exact position. Since large size of image increases the chances of password getting hacked. Brute Force attack means constant attempts of different combination of passwords to hack the password, this attack is also possible due to size of given image there is enough space where in user try to match original password by clicking on several positions on given image. So to overcome with these weaknesses of current authentication schemes we proposed Textual Graphical Password Authentication Scheme Resistant to Shoulder Surfing.

3. PROPOSED SCHEME

We propose a Textual Graphical Password Authentication Scheme Resistant to Shoulder Surfing which is a basic Single Set Scheme. To increase the level of security and to prevent Brute force attack we shall introduce the SMS module.

3.1 Single Set Scheme

In this scheme, the system generates a login image which displays a set of printable characters which consist of upper case (A-Z) and lower case (a-z) alphabets, numbers (0-9), and all printable special characters. These set of characters are randomly scattered on the login image.



O	?	]	}	A	'	@	N	1	!
{	Z	#	2	P	_	y	|	^	O
R	C	w	&	3	D	S	b	v	5
~	E	6	(	T	u	c	7	F	U
e	d	8	t	*	G	V	B	s	
q	,	;	$	i	y	-	<	K	p
9	H	W	g	r	+	:	I	x	h
/	j	l	m	f	\	=	>	g	r

Figure 4: Login image

To login user should find all his original password characters in the login image and click inside the invisible triangle which is also called as password triangle. This password triangle is created using 3 original password characters. The user can select any character which is present inside the invisible triangle or on the border of password triangle. These selected characters are known as session characters and all such session characters makes session password. Therefore in this scheme there are two types of passwords i.e. original password and session password.

The original password is set by the user while registering in the system and session password is created when user makes clicks inside the password triangle during login. Session password changes every time when the user tries to login. This is due to a technique called “Change Image Technology”, system generates a new login image every time user tries to login. This helps in securing original password from being hacked.

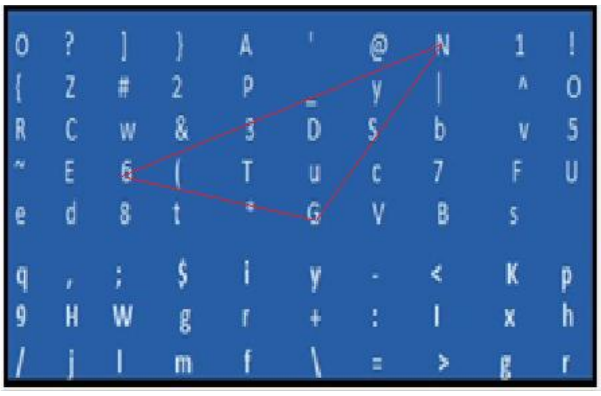
There can be a possibility that out of three password triangle characters two are same then in such case the password triangle cannot be formed so we need to consider a line instead of the triangle and click on that invisible line.

An exceptional case may be that all the three password triangle characters are same then there can be neither a triangle formation nor a line so the user has to consider a virtual circle centered on that character.

3.2 The algorithm for login into the system using Single Set Scheme

For example consider: Let the original password be N6G2, The length of password is 4 so there are 4 combination N6G, 6G2, G2N and 2N6.

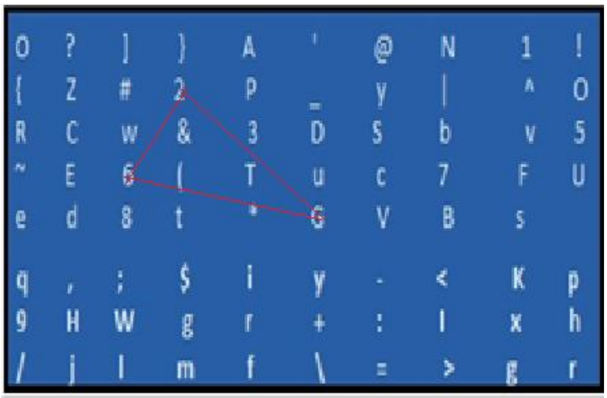
Step 1: The user will find the original password characters “N”,”6”,”G” and click inside the invisible password triangle made by these characters.



0	?	]	}	A	'	@	N	1	!
{	Z	#	2	P	_	y	|	^	O
R	C	w	&	3	D	S	b	v	5
~	E	6	(	T	u	c	7	F	U
e	d	8	t	*	G	V	B	s	
q	,	;	$	i	y	-	<	K	p
9	H	W	g	r	+	:	I	x	h
/	j	l	m	f	\	=	>	g	r

Figure 5: Step 1

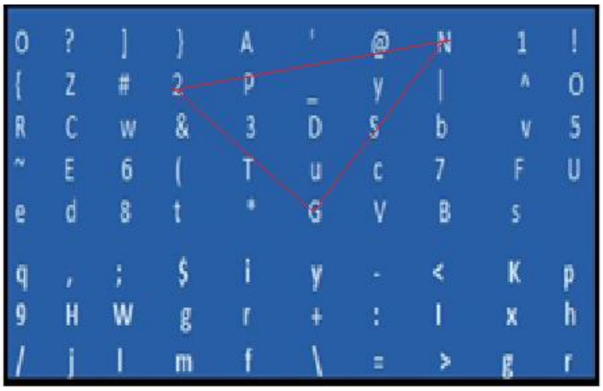
Step 2: The user will find the original password characters “6”,”G”,”2” and click inside the invisible password triangle made by these characters.



0	?	]	}	A	'	@	N	1	!
{	Z	#	2	P	_	y	|	^	O
R	C	w	&	3	D	S	b	v	5
~	E	6	(	T	u	c	7	F	U
e	d	8	t	*	G	V	B	s	
q	,	;	$	i	y	-	<	K	p
9	H	W	g	r	+	:	I	x	h
/	j	l	m	f	\	=	>	g	r

Figure 6: Step 2

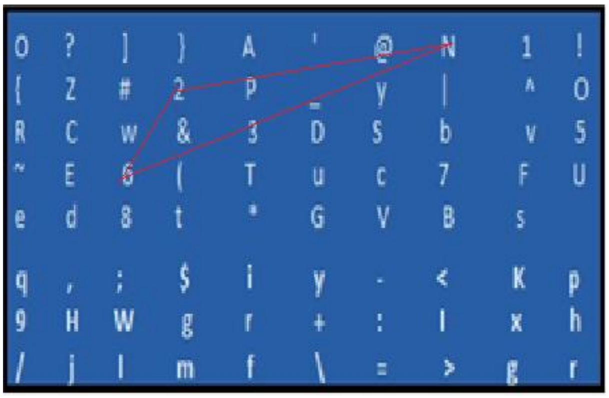
Step 3: The user will find the original password characters “G”,”2”,”N” and click inside the invisible password triangle made by these characters.



0	?	]	}	A	'	@	N	1	!
{	Z	#	2	P	_	y	|	^	O
R	C	w	&	3	D	S	b	v	5
~	E	6	(	T	u	c	7	F	U
e	d	8	t	*	G	V	B	s	
q	,	;	$	i	y	-	<	K	p
9	H	W	g	r	+	:	I	x	h
/	j	l	m	f	\	=	>	g	r

Figure 7: Step 3

Step 4: The user will find the original password characters “2”,”N”,”6” and click inside the invisible password triangle made by these characters.



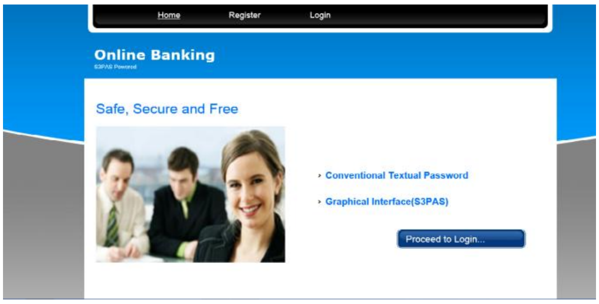
0	?	]	}	A	'	@	N	1	!
{	Z	#	2	P	_	y	|	^	O
R	C	w	&	3	D	S	b	v	5
~	E	6	(	T	u	c	7	F	U
e	d	8	t	*	G	V	B	s	
q	,	;	$	i	y	-	<	K	p
9	H	W	g	r	+	:	I	x	h
/	j	l	m	f	\	=	>	g	r

Figure 8: Step 4

4. EXPERIMENTAL DETAILS

4.1 Graphical User Interface

We have considered online banking system for implementing our scheme. The GUI of our system is shown in the figure below.



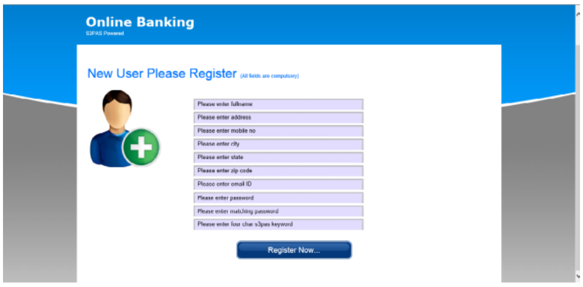
Online Banking
S3PAS Powered

Safe, Secure and Free

Figure 9: Home image

4.2 Registration Form

The new user is required to register to the online banking application by filling the registration form .The registration form includes fields like name of user , city, address and personal details. The user needs to set two types of password i.e. first password is used to access login image of our system which is known as login access password and the other password is the original password of our proposed scheme.



Online Banking
S3PAS Powered

New User Please Register (All fields are compulsory)

Please enter fullname
Please enter address
Please enter mobile no
Please enter city
Please enter state
Please enter zip code
Please enter email ID
Please enter password
Please enter matching password
Please enter four char s3pas keyword

Figure 10: Registration form image

4.3 Login Image

To access login image of our online banking system, the user needs to enter user name and the login access password as shown in figure below.

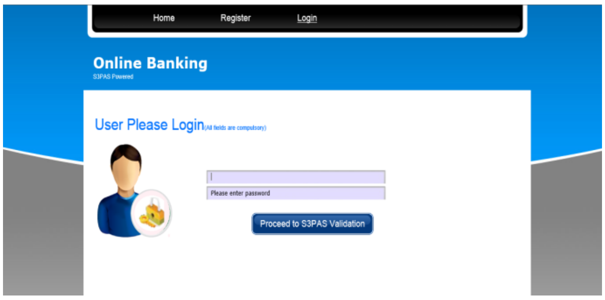
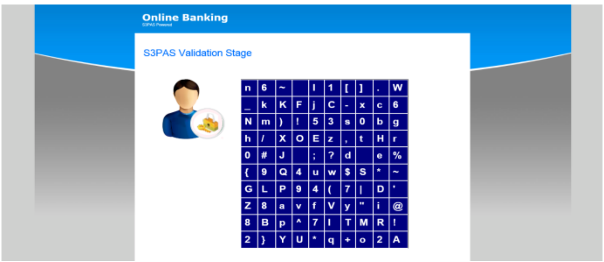

Home
Register
Login
Online Banking
S3PAS Powered
User Please Login(All fields are compulsory)
Please enter password
Proceed to S3PAS Validation

Figure 11: Login page

After completion of the above process the login image will be displayed as shown in the figure below.

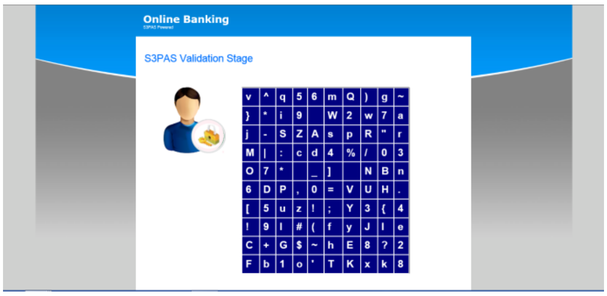


n	6	~		I	1	[	]	.	W
_	k	K	F	j	C	-	x	c	6
N	m	)	!	5	3	s	0	b	g
h	/	X	O	E	z	,	t	H	r
0	#	J		;	?	d		e	%
{	9	Q	4	u	w	$	S	*	~
G	L	P	9	4	(	7	|	D	'
Z	8	a	v	f	V	y	"	i	@
8	B	p	^	7	I	T	M	R	!
2	}	Y	U	*	q	+	o	2	A

Figure 12: Login image

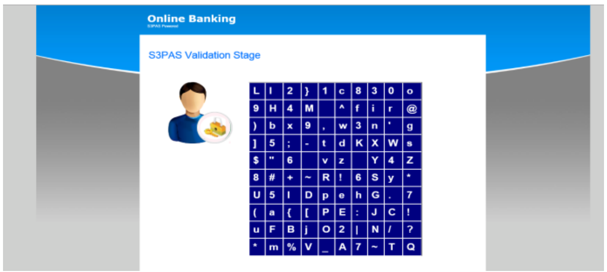
4.4 Change Image Technology

The main feature of our system is "Change Image Technology". This technique makes our system more secure. In this technique the login image changes every time when the user logs in to the system and also if the user fails to click inside the pass triangle correctly. The different login images are shown below.



v	^	q	5	6	m	Q	)	g	~
}	*	i	9		W	2	w	7	a
j	-	S	Z	A	s	p	R	"	r
M	|	:	c	d	4	%	/	0	3
O	7	*		_	]		N	B	n
6	D	P	,	0	=	V	U	H	.
[	5	u	z	!	;	Y	3	{	4
!	9	I	#	(	f	y	J	I	e
C	+	G	$	~	h	E	8	?	2
F	b	1	o	'	T	K	x	k	8

Figure 13: Login image



L	I	2	}	1	c	8	3	0	o
9	H	4	M		^	f	i	r	@
)	b	x	9	,	w	3	n	'	g
]	5	;	-	t	d	K	X	W	s
$	"	6		v	z		Y	4	Z
8	#	+	~	R	!	6	S	y	*
U	5	I	D	p	e	h	G	.	7
(	a	{	[	P	E	:	J	C	!
u	F	B	j	O	2	|	N	/	?
*	m	%	V	_	A	7	~	T	Q

Figure 14: Changed Login image

4.5 Evaluation of algorithms

Here the comparison of the three algorithms are done. Depending on the comparison we have used the single set scheme for our system.

Table 1. Comparison of the algorithms

Single set scheme	**Three set scheme**	**Rule based scheme**
Login image is small in size.	Login image is large in size	Login image size is small.
No load on client.	No load on client.	Load on client.
Simple to implement	Difficult to implement	Difficult to implement

5. FUTURE WORK

The future improvement of our system can be the use of one time passwords (OTP). After successfully completing all the login steps, a unique code will be send to the user's mobile phone, after entering this unique code user will be successfully logged-in.This will provide double authentication and will secure users account.

6. CONCLUSION

To overcome the issues related to security and to have safe data transfer we have proposed Textual Graphical Password Authentication Scheme Resistant to Shoulder Surfing. This system strikes a balance between being easy to use and provide security .The user need not be an expert to use this scheme. The most common and the easiest way of hacking users password is through shoulder surfing and our scheme nearly resist shoulder surfing. The probability of password getting hacked is ≈ 0.0000334 which is very minute. The programming language used is PHP and MYSQL. Our system can also be used in applications where security is a must like in military where confidential data needs to be transferred or for websites that require online transactions. Our systems key feature is the Change Image Technology which prevents the brute force attack and shoulder surfing by changing the image for each session and for each authentication stage which makes the password difficult to crack. Also the length of the password is four which is easy for users to remember. Thus our proposed system fulfills all the requirements of security.

7. ACKNOWLEDGMENTS

We would like to thank the mentor of our college Ms Sheetal Pereira and all the people and anonymous referees who contributed to improve our paper in some way. The authors thank everyone for their suggestions

8. REFERENCES

[1] A. Adams and M. A. Sasse, "Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures", Communications of the ACM, 42:41–46, 1999.

[2] R. N. Shepard, "Recognition memory for words, sentences and pictures", Journal of Verbal Learning and Verbal Behavior, 6:156–163, 1967.

[3] G. E. Blonder, "Graphical passwords", United States Patent 5559961, 1996.

[4] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: Basic results", in Human-Computer Interaction International (HCII 2005), Las Vegas, NV, 2005.

[5] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords:

Effects of tolerance and image choice", in Symposium on Usable Privacy and Security (SOUPS), Carnegie Mellon University, Pittsburgh, 2005.

[6] R. U. Corporation, "How the pass face system works", 2005.

[7] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "In proceedings of the design and analysis of graphical passwords", in the 8th USENIX Security Symposium, 1999.

[8] A.P. Sabzevar, A. Stavrou, "Universal Multi-factor authentication using graphical passwords," in: IEEE International Conference on Signal Image Technology and Internet Based Systems, 2008, SITIS "08, Nov. 30 2008–Dec. 3 2008, pp. 625–632.

[9] D. Nali and J. Thorpe, "Analyzing user choice in graphical passwords", in Technical Report, School of Information Technology and Engineering, University of Ottawa, Canada, May 27 2004.

[10] J. Thorpe and P. C. v. Oorschot, "Graphical dictionaries and the memorable space of graphical passwords", in Proceedings of the 13th USENIX Security Symposium, San Deigo, CA, 2004.

[11] Haichang Gao, Xiyang Liu, Sidong Wang, Honggang Liu, Ruyi Dai, "Design and analysis of a graphical password scheme," 2009 Fourth International Conference on Innovative Computing, Information and Control, ICICIC, 7–9 Dec. 2009, pp. 675–678.

[12] A.P. Sabzevar, A. Stavrou, "Universal Multi-factor authentication using graphical passwords," in: IEEE International Conference on Signal Image Technology and Internet Based Systems, 2008, SITIS 08, Nov. 30 2008–Dec. 3 2008, pp. 625–632.

[13] D. Hong, S. Man, B. Hawes, and M. Mathews, "A password scheme strongly resistant to spyware", in Proceedings of International conference on security and management, Las Vergas, NV, 2002.

[14] S. Man, D. Hong, and M. Mathews, "A shoulder surfing resistant graphical password scheme", in Proceedings of International conference on security and management, Las Vegas, NV, 2003.

[15] Huanyu Zhao and Xiaolin Li, " S3PAS:A Scalable Shoulder-Surfing Textual- Graphical Password Authentication Scheme", in Scalable Software Systems Laboratory, Department of Computer Science, Oklahoma State University, Stillwater, OK, USA, May 21 2007.

[16] R. N. Shepard, "Recognition memory for words, sentences and pictures", Journal of Verbal Learning and Verbal Behavior, 6:156–163, 1967.