A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme

Prof. G.N.Tikhe[1], Miss. Pradnya M. Thakre[2], Miss. Kajal G. Telrandhe[3]
[123]*(Department of Information Technology, Datta Meghe college of Engg. and Research, Wardha/RTMNU, India)*

Abstract–Today's World is Information and computer world, We Are surrounded by Different types of Computer Applications. Form Mobile Phones to Computer systems we are now depend on computer application in manythings. We use Computer to share many things, to get connected with friend and family, to perform banking operation, and much more. When it comes to net Banking or sharing of information, we need the way of protecting this data and information from the attacker. In one way, this is done by providing the authentication to the user using username and password. Information and computer security is supported largely by textual or alpha numeric passwords which are the principle part of the authentication process. The most textual as well as alpha numeric and latter graphical password are endangered and unprotected to shoulder-surfing attacks, hidden camera and spyware attacks, or by brute-force attack. In this paper, we proposed a new system providing the security for authenticating the user. It prevents user from attackers by providing the two stage validation i.e. one is by textual Graphical password and another is by sending the OTP to registered mobile number.

Keywords: Brute-force, DAS, graphical password, OTP, shoulder-surfing, spyware, textual-graphical passwords, S3PAS, etc.

I. INTRODUCTION

Text based password is widely used method for providing the authentication to user. As this method is widely used, more of with less protection of this method have been found. Most of the user keeps their Passwords short and one which can be easy to remember, but it makes easy for attackers to breakthe system or any user account. Because maximum user uses the password like their names, birth dates, pet names,etc. which is very easy to guess and hack there accounts. Also the textual password can easily get hack by shoulder-surfing or spyware attacks. To make it tough for attackers and to resist brute-force search and dictionary attacks, we need to make random and long password. But unfortunately, in many cases such passwords are really hard to remember and inconvenient for user. Furthermore, textual password is not more secure and vulnerable to shoulder-surfing, hidden-camera and spyware attacks, etc. And now a day we need more security to our all accounts whether it is social networking or any bank account. For that we have to choose efficient password authentication scheme.

Under consideration the fact that human mind can recall the image or picture more easily than complex and long text. A new method ware introduces, **a graphical password authentication schemes.** In addition, the Graphical password schemes provide higher level of security and more

Authentications styles. As text based is with less protection to direct attacks, this becomes hard in the graphical password. Attacker cannot hack users account easily. It gives quite more security than textual passwords, due to these advantages; there is a growing interest in graphical password authentication scheme.

Though, the oldest graphical passwords are more from perfect. Typically, system requirements and communication costs for graphical passwords are higher than text-based passwords. Along with this the more important drawback in the current graphics based password scheme is that they are secure than textual passwords to shoulder-surfing attacks but its cost is high in case of installation, maintenance, etc. To address the above problem, in this paper we have proposed and discuss a new textual graphical password system named, **Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication System (S3PAS),** which continues without stopping integrates the textual and graphical passwords. In which we are using the textual as well as graphical password system. This will definitely increase the security of the system.

S3PAS system has the following salient features:-

I]this is secured to the Shoulder-surfing, hidden-camera and spyware resistant, even the attacker watches or camera record the victim entering the password, password won't be stolen.
II] Exactly match the related password and can go beyond. S3PAS can coexist with text passwords without changing the existing user profiles. Further, it can add more graphical pass-icons and refined rules to further enhance the security level.
III] It is robust against brute-force attacks.
IV] It supports both keyboard and mouse as input devices.
V]More secure than conventional text and alpha numeric password authentication scheme.

II. RELATED WORK

In the 1960's, as the first multi-user operating system waregrown and it uses by many applications,to provide the solution to a security issue, Textual-alpha-numeric passwords were first introduced. But because of computer revolution this password authentication system was not capable to provide enough security to the user.

So, a Graphical password scheme ware designed by Blonder, where the password is created as user selects different location on the image and that locations or points are stored as his password. At the time of authentication user has to select the same location on the image. The Image helps the user to recall the password and that's why it was easier that the traditional text based password. Then the Blonder's idea is extended in the "Pass-Point" system. "Pass-Point" system eliminates the predefined boundaries of graphical passwords and allowing arbitrary images to be used. The result of this elimination was, user can click anywhere on the image to create his/her password. A tolerance around each pixel chosen by user is calculated. In order to be authenticated, the user must click within the tolerance of the chosen pixels.After that the Real User Corporation developed a new technique called "Pass-face", based on the assumption that human can remember the faces of human than any other picture. The working of "Pass -face" or the basic idea behind the technique is as follows. A user has to select four faces from the database as their future password. At the time of authentication, user is presented with a grid of nine faces, one from his/her password and eight decoy faces. User will select the know face and this procedure will be followed several rounds. The user is authenticating if he/she will correctly identifies all the faces.

Another Method Called "Draw a secret (DAS)" proposed by the Jermyn, et al. allow user to draw their unique password. 2D grid is used as input which allow user to draw the simple picture and it was used for the verification. All the coordinates of the picture consist of the picture as password is stored in the database. During Authentication process, the user is asked to re-draw the same picture on the 2D grid. Then this Coordinate is matches with the one stored in database. If both of this is matches then the user is authenticate, otherwise not.

III. S3PAS SYSTEM

S3PAS is designed on the client server architecture, as most password authentication system. The S3Pas system generates the login image on client and then transmits the image specification to the server instead of entire image pixel by pixel. This reduces the communication between more parties and authentication time.

3.1. Notations:

To support the demonstration and investigation, we define the following notations to be used throughout the paper.

- T: The set of all the available password icons in a password scheme.
- |T |: The number of icons in the set of T (size of set T).

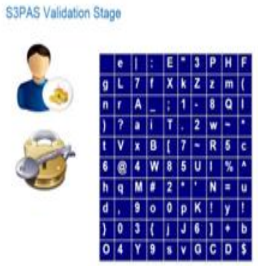
- T _: The set contains all the combinations consisting

Of the elements in T.T _ is called “password space” in a certain password scheme.

- K: An element in the set of T_. It is chosen by the user as a password, usually a string or a special orderof several icons.
- |k |:The length of the user’s password k.

3.2. Single Set Scheme:

S3PAS schemes include several variants, which are designed for different environment and for different security requirements. The Single-Set scheme is the basic S3PAS scheme. In this scheme, the available password icons set T is the set of all the printable characters just like the conventional textual password system, and |T | = 99. There is a string k which is user’s password previously chosen and memorized by the user, which is named “original password” i.e. S3PAS password. We use two different passwords in this system, one is simple login password and another is S3PAS password. The S3PAS or original password is use for four stage validation process. The characters in k are called “original pass-characters”. Initially, the system randomly scatters the set T in the login image as shown in Figure 1(a).



S3PAS Validation Stage

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

Figure 1(a): S3PAS Login Interface

To login, the user must find all the character from his original pass-character from the login image,and then make a triangle by making some click inside the image which is called "pass-triangle” created by 3 original pass characters from his/her S3PAS password string and has to follow a certain click-rule. Alternatively, the user can input/type a textual character chosen from inside or on the border of the pass triangle area instead of clicking by mouse. Such character is called “session pass-character”. The final input could be either several session pass-clicks or several session pass-characters. This is the user's "session Passwords".

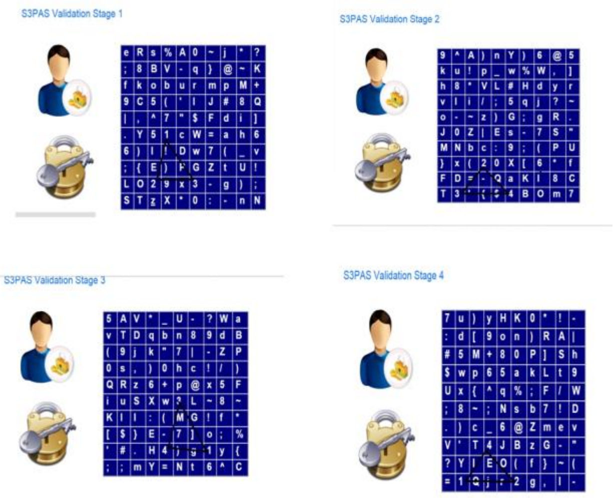
The click-rule for single-set scheme is as follows. For

The user’s password string K,we number the first character in Kas k1, k2, k3, k4, etc. Then we have k1, k2, k3. . . kn−1, kn, n = |K|. To login, users have to find out k1, k2, k3, ….., kn−1, kn in the login image. Then the first click must be inside the pass-triangle formed by k1, k2 and k3. The second click must be inside the pass-triangle formed by k2, k3 and k4. Recursively, the i-th click must be inside the pass-triangle formed bykimod|K|,k(i+1)mod|K| and k(i+2)mod|K|, i = 1 . . . n. This is the “basic click-rule.”

To show the login process, let us take an example:

Without loss of generality, we assume that the user XYZ has original password Kis “1234”. Since the length of the password is, |K| = 4, based on the basic click-rule, XYZ has to click four times correctly in the right sequence to be authenticated. The four combinations of password in order are “123”, “234”, “341” and “412”. The login procedure consists of the following four steps and is also shown in Figure 2.

1. XYZ finds his/her pass-characters “1”, “2” and “3”, then clicks inside the pass-triangle or input a session pass character inside ∆123 (e.g., “P”, which is completely lie inside the triangle).
2. XYZ finds his/her pass-characters “2”, “3” and “4”, then clicks inside the pass-triangle or input a session pass character inside ∆234 (e.g., “D”, which is completely lie inside the triangle).
3. XYZ finds his/her pass-characters “3”, “4” and “1”, then clicks inside the pass-triangle or input a session pass character inside ∆341 (e.g., “5”, which is completely lie inside the triangle).
4. XYZ finds his/her pass-characters “4”, “1” and “2”, then clicks inside the pass-triangle or input a session pass character inside ∆412 (e.g., “2”, which is completely lie inside the triangle).



S3PAS Validation Stage 1

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

S3PAS Validation Stage 2

9	^	A	)	n	Y	)	6	@	5
k	u	!	p	_	w	%	W	,	]
h	8	*	V	L	#	H	d	y	r
v	I	i	/	;	5	q	j	?	~
o	-	~	z	)	G	;	g	R	.
J	0	Z	|	E	s	-	7	S	"
M	N	b	c	:	9	;	(	P	U
}	x	(	2	0	X	[	6	*	f
F	D	=	-	Q	a	K	I	8	C
T	3	*	{	$	4	B	O	m	7

S3PAS Validation Stage 3

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

S3PAS Validation Stage 4

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

Figure 2: S3PAS Login Process

In this example, XYZ’s original password is“1234”,andhis/her session password is four clicks in sequence or textual password “PD52”. Cause we create session password for each stage. He has to click four times inside the invisible pass-triangles or input the session passwords “PD52” to be authenticated. User will get access if and only if all these four stages are valid clicks inside the triangle. Due to this we can resist attacker to hack our account.

Two special cases need to be considered. If the two of those three pass-characters are the same, or even all of the three are identical, they cannot construct a triangle. To address this problem, S3PAS requires that if two of the three characters are the same, users have to click in the invisible line formed by the two different characters. Similarly, if all of the three characters are the same, users have to click inside a certain circle area centeraround to this character.

IV. ANALYSIS AND DISCUSSION

4.1. Shoulder Surfing Resistant:

Most textual and graphical password authentication schemes are vulnerable to shoulder-surfing and get easily hacked by attacker. However, our S3PAS scheme offers perfect resistance to shoulder-surfing, hidden-camera and spyware attacks. Often an attacker observes or records one click on the screen from the user, the attacker cannot gain enough information of the user’s password. Cause we made a password authentication scheme in four different stages. And this shows that a shoulder-surfing attack is physically infeasible.Whether the attacker knows our login password we can protect our account by another original password i.e. S3PAS password.

4.2. Random Click Attack and Triangle

Area Approximation Analysis:

In S3PAS schemes, users have to find out their pass characters provided in original password (K) and then click inside the pass-triangle areas. However, attackers have the chance to click the right areas just by random-click even though they do not really know the password. This kind of attack is called “random-click attack.” Toresist random-click attack, users are required to click several times followed by some click-rule like the basicS3PAS scheme. Recall the example shown in Section 3;if the password is “A1B3”, the user has to click four timesto login.

The problem is that whether four-character passwordis long enough to resist the random-click attack? Ifthe attacker is “lucky”enough,he/she might be able to clickinside the correct triangle regions correctly just by randomclicks.If the area of the circle is large,wecan observe that the size of the pass-triangle areagreatly affects S3PAS’s security level. If the size of everypass-triangle area is too large, attackers are able to click insidethe right areas with higher probabilities just by random clicks. To evaluate and maintainthe security level of S3PAS system, we should find out the expected averagesize of the pass-triangle areas. It is an important measure of S3PAS’ssystem security level.

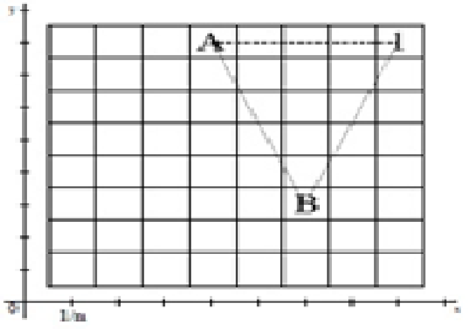


Figure 3: Analysis of Triangle Area

Consider the basic S3PAS authentication scheme. Without loss of generality,we divide the login image region into n∗n grids. Weassume that each character in the set T, which consists of allthe 99 available password characters, is placed randomly inthe centre of every grid. If we consider 10*10 grid then we can use total 99 different variables inside the grid. In which we can place all the T elements randomly. In addition, we assume the lengthof the border of the login image is L. The three vertices ofa pass-triangle hold coordinates: (X1, Y1), (X2, Y2), and(X3, Y3). X1, Y1, X2, Y2, X3, Y3 are independent witheach other. Each of them is distributed uniformly betweenL/n and L as shown in Figure 3.

The area of a triangle is given by,

$$S = \frac{1}{2}\left|(X_1 - X_2)(Y_1 - Y_3) - (X_1 - X_3)(Y_1 - Y_2)\right| \tag{1}$$

The expected average triangle area is,

$$E(S) = \sum_{f=1}^{n}\sum_{g=1}^{n}\sum_{h=1}^{n}\sum_{i=1}^{n}\sum_{j=1}^{n}\sum_{k=1}^{n}\frac{1}{2}\left|\left(\frac{f}{n}-\frac{g}{n}\right)\left(\frac{i}{n}-\frac{k}{n}\right)-\left(\frac{f}{n}-\frac{h}{n}\right)\left(\frac{i}{n}-\frac{j}{n}\right)\right|\frac{1}{n^{6}} \qquad (2)$$

In the basic S3PAS scheme, we have 99 printable characters.As an example, 10 ∗10 grids are able to containall the characters. Setting n = 10 in equation (2), we obtain,E(S) = 0.7554300L_2 ≈ 0.076L_2. Based on E(S),we know that the success probability using the randomclickattack is given by P(S) = 0.076L_2/L_2 = 0.076.For a password K, the probability to get authentication justby random-clicks is 0.076$_{|K|}$. Recall theformer example,the length of the password is four. For attackers, theProbability of click the right area for all the four times isP(S)$_{|k|}$ = 0.076$_4$ ≈ 0.0000334.This probability is pretty low. It is extremely hard / tough forattacker to get such a good“luck” to get authentication justby doing random-clicks. Attackers are forced to use brute-forcesearch attack to break the password. That is, they hope to try manytimes, so that even though the probability to break the systemfor one time is pretty low, they can get the authenticationby large number of tries. We will show later howS3PAS resists the brute-force search attack.Let us go back to the expected average triangle areaE(S) in basic S3PAS scheme. Since the value of E(S)determines the scheme’s security level, we should try to reducethe value of E(S). From equation (2), we observethat the parameter n is an important factor affecting E(S).To show the relationship between E(S) and n, we calculateseveral E(S) value according to different n. We get thefollowing results as shown in Table 1.

N	Triangle area
2	.04687500L^2
3	0.06401463L^2
4	0.06994629 L^2
5	0.07246848 L^2
6	0.07379544 L^2
7	0.07453787 L^2
8	0.07501316 L^2
9	0.07532504 L^2
10	0.07554300 L^2
....	....

Table 1: The Area of Pass-Triangle as per the Grid Number n

The table reveals a direct relation between the grids Number n and the triangle area; thus, we have the following conjecture. (i.e. an opinion or conclusion formed on the basis of incomplete information.)

Conjecture: (i.e. an opinion or conclusion formed on the basis of incomplete information.)*As the grid number* n *increases, the expectedaverage area of a randomly-placed pass-trianglealso increases; when n approaches infinity* (n → ∞),*the expected average area of a triangle approaches a limitvalue*.Based on the conjecture, to achieve the best securitylevel, we should make the average size of the triangles assmall as possible; thus, we should choose the smallest gridnumber that is large enough to host the set of all characters inT.

4.3. Brute Force Search Resistant:

In S3PAS authentication systems, there are two kinds of passwords, the original password and another is dynamic session password generated during each login validation stage.Therefore, there are mainly two ways to brute-force search attack onS3PAS's passwords: one is brute-force search attacks on original passwordand another is brute-force search attacks on session password.

4.3.1. Brute Force Search Original Passwords Resistant:

The main method used previously to defend brute-forcesearch attacks towards the passwords is to have a sufficiently largepassword space. Text-based passwords have a passwordspace of T(|T | = 94). Our basic S3PAS scheme hasbeen shown to provide a password space similar to textbasedpasswords. However, S3PAS schemes can provide amuch larger password space by using the enhanced graphicalS3PAS scheme.Moreover, it is much more difficult to carry out bruteforceattacks against textual-graphical passwords than textbasedpasswords. The attack programs need to automatically generate accurate mouse motion to imitate human inputs,which is particularly difficult for S3PAS. People canrecognize a login image in less than one second, whereascomputers spend a considerable amount of time processingmillions of bytes of information regardless of whether thelogin image is a face, a landscape, or a meaningless shape.

4.3.2. Brute Force Search Session Passwords Resistant:

S3PAS scheme is also efficient in resisting attacks on thesession passwords. The primary cause is that we choose and accept "change image" technology. If a user fails in clicking thecorrect areas i.e. inside the triangle, or a user inputs wrong session passwords forI (e.g., I = 10) times, the client automatically changesthe session login image. By doing this, there is no wayfor attackers to adopt brute-force search attack to break the sessionpassword because the session password will dynamicallychange after changing the image. As a result, all theAttempts toward the previous image become useless. Theattacker has to start a new search in the new image. Therefore,we argue that "change image" techniquemakes S3PASimmune to the brute-force search towards the session passwords.Furthermore, the system might be broken once by chanceunder a tiny probability using brute-force attacks towardssession password like any password system, but the attackerscannot obtain the original secret passwords to completelybreak the system.

V. CONCLUSION

We proposed a scalable shoulder-surfing resistant passwordauthentication system (S3PAS) to provide better security to users information system by using textual as well as graphical passwords. S3PAS provides desirablefeatures of a secure authentication system and being immune/resistto shoulder-surfing attacks, hidden-camera, brute-force attacks, spyware attacks, etc.Further, S3PAS is that it seamlessly matchesthe conventional text-based passwords and can adapt to various lengths of textual passwords, which requireszero efforts from users to migrate their existing passwords toS3PAS. However, there are still some minor drawbacks inthis system similar to other conventional textual and some graphical password authentication systems.The major issues in S3PAS schemes include slightly many and confusing aspects and longer login processes, because if the original password of the user is 4 digits (n=4) then he/she has to go through 4 different validation stages. Our further plan is to designa simpler and easier version of S3PAS with a little lower safetylevel to ease its adoption.Future work should consider higher security mechanisms,and reducing time consumption.

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] G. E. Blonder, Graphical passwords,*United States Patent, 5559961*, 1996.

[3] R. U. Corporation. How the passface system works, 2005.

[4] 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.

[5] 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 8thUSENIX Security Symposium*, 1999.

[6]S.Man, D. Hong, and M. Mathews, A shouldersurfing resistantgraphical password scheme, In *in Proceedings of International conference on security and management*, Las Vegas, NV, 2003.

[7]D. Nali and J. Thorpe, Analyzing user choice ingraphical passwords, In*Technical Report*,Schoolof Information Technology and Engineering, University of Ottawa, Canada, May 27 2004.

[8]R.N. Shepard, Recognitionmemoryforwords, sentences and pictures.*Journal of Verbal Learning and Verbal Behavior*, 6:156-163, 1967.

[9] L.Sobrado and J. C. Birget, Graphicalpasswords. *The Rutgers Scholar, an Electronic Bulletin for Undergraduate Research*, 4, 2002.

[10]X.Suo,Y.Zhu,andG.S. Owen, Graphicalpasswords:A survey, In *21st Annual Computer Security Applications Conference (ACSAC 2005)*, Tucson, AZ, 2005.

[11] J.ThorpeandP.C.v.Oorschot,Graphicaldictionariesandthememorablespaceofgraphical passwords, In *in Proceedings of the 13th USENIX Security Symposium*, San Diego, CA, 2004.

[12]J.ThorpeandP.C.v. Oorschot, Towards securedesignchoicesforimplementinggraphical passwords, In*inProceedings of the 20th Annual Computer Security ApplicationsConference*, Tucson,Arizona, 2004.

[13]S.Wiedenbeck,J.Waters,J.C.Birget,A.Brodskiy,andN. Memon, Authenticationusinggraphicalpasswords:Basic results, In*HumanComputerInteraction International(HCII2005)*,Las Vegas, NV, 2005.

[14]S.Wiedenbeck, J.Waters,J.C.Birget,A.Brodskiy,andN. Memon, Authenticationusinggraphical passwords:Effectsof toleranceandimagechoice.In*SymposiumonUsablePrivacyand Security (SOUPS)*,Carnegie Mellon University, Pittsburgh, 2005.

[15S.Wiedenbeck,J.Waters,J.C.Birget,A.Brodskiy,andN.Memon,Passpoints:Designandlongitudinalevaluationofagraphicalpasswordsystem, *InternationalJournalofHumanComputerStudies*, 63, 2005.