Shoulder Surfing Proof Secure Authentication Algorithm Using Textual Passwords

P Aditya Kiran, Dr. A Sri Krishna

Abstract—: Authentication is the basic requirement of information security. Many real life applications require the identity of a user. Strong text based password scheme which are difficult to memorize provides certain degree of security. It has motivated graphical authentication as an alternative to the text-based authentication. The graphical implementation has a disadvantage of user selecting the wrong order. It was observed that the selection of images and the rule that controls the choice of the images were critical in the implementation of the system. The paper proposes a new method which is the enhancement of the login and password system. The system is more secure and vulnerable to shoulder surfing. The system has been tested with various passwords by novice users.

Index Terms— Information Security, Authentication, Passwords, Attacks, Shoulder Surfing

1 Introduction

In recent years, computer and network security has been formulated as technical problem. A key area in security is authentication which allows the users access to given system or resource. A password is a form of secret authentication that allows to control access to a resource. The use of password goes back to ancient times when soldiers guarding a location by exchanging a password and then allow a person who know the password [1]. In modern times these passwords are used to control access to mobile phones, auto teller machines (ATM) and to protect computer Operating System [8]. A typical computer user may require passwords for many purposes such as login to computer accounts, retrieving email from servers, accessing to databases, network, and websites and even reading a newspaper online.

Some drawbacks of novel passwords are;

(i) People may (forget them) not remember them.
(ii) They are weak and hence can be easily stolen.

Graphical passwords were an alternative to the text based passwords. Psychological studies have shown that people can remember pictures better than text [2]. In graphical password, the problem arises because passwords are expected to have two fundamental requirements namely;

a. Password should be easy to remember.
b. Password should be secured.

The graphical password authentication scheme was new and several drawbacks were identified [3] [6].

- Users were fascinated by the pictures drawn by other users, so frequently common pictures were used for passwords.
- The users tend to select weak passwords which are vulnerable to graphical dictionary attacks.
- Not all users were familiar to use mouse as an input device.
- The memorization and usability of some of the algorithms were difficult.
- In some case the passwords are easily guessable or predictable.

Malicious attackers frequently infect user PC by virus, malware and other hacking program and try to steal users' private information such as user ID, password etc. Furthermore, malicious attackers' secondary attack (extortion to user critical private information) is to use seized user information. In addition, the additional damage such as identity theft is performed through the seized user information. Attack methods involve phishing, Key logging, Sniffing; keyboard hooking etc. Among these entire attacks, keyboard hooking attack is one of the common attacks to seize user information. In this method, the entered values through keyboard (e.g. user ID, password etc.) are seized by the attacker while using the web service. Typical well known attack methods are COM hooking, memory hooking [9]. In addition, recent spotlight introduces Shoulder-Surfing-Attack (SSA). The attack method is such that, while the user enters password, the attackers observe the data over the shoulder of the user and memorize it. Shoulder-surfing-attack is known as high-risk attack stealing personal information.

To have a more stringent password composition rules or to have strong password, many users have resorted to alternate passwords such as password phrases and keyboard pattern for their password [4] [5]. These methods addresses brute force methods but could not solve the dictionary attack and Shoulder Surfing Attacks.

This paper proposes a new efficient password authentication scheme which eases the user to remember the password and restricts the attacker from SSA. This paper is organized as follows. Section II discusses related work, proposed algorithm is presented in section III. Experiments and Simulations are given in section IV. Conclusions in section V.

- *P Aditya Kiran is currently pursuing bachelor's degree program in Computer Science engineering in RVR&JC College of Eng., Guntur, Andhra Pradesh India, PH-+919848254173. E-mail: aditya.pentyala@gmail.com*
- *Dr.A.Srikrishna, Professor, Dept of Information Technology, R.V.R. & J.C. College of Engineering, Guntur, Andhra Pradesh, India, PH-+919441577577, Email: atlurisrikrishna@gmail.com*

2 Related Works

2.1 Convex hull click scheme

The Convex Hull Click Scheme (CHC) is a graphical password scheme that resists shoulder-surfing attack. These attacks may be done by observation, video recording, or electronic capture [5]. This system uses a large set consisting of several hundreds of icons, and the set of icons could be any kind of small icons or even user provided ones. The icons are displayed using the image without text. To select a password the user chooses several icons from the set to be his or her pass-icons as shown in Figure 1. The number of pass-icons is determined by the administrator. The user has to remember the icons that he or she has chosen.

Figure 1. Five pass-icons (from right to left: Netscape, Mozilla, Internet Explorer, Quark Express, and Adobe Photoshop).

At login time a large number of icons from the set of icons is randomly arranged in the Login interface as shown in Figure 2. These icons include mostly non-pass-icons along with a few pass-icons.

When the login begins, the user must visually identify three or more of his or her selected icons known as pass-icons. The user's next step is to mentally create the convex hull formed by those pass-icons. A convex hull is the area encompassed by the edges joining three or more points. In Convex Hull Click scheme the convex hull is visualized by assuming the pass-icons as the points, and lines as edges visualized in the user's mind. Figure 2 shows a convex hull formed by five pass-icons.

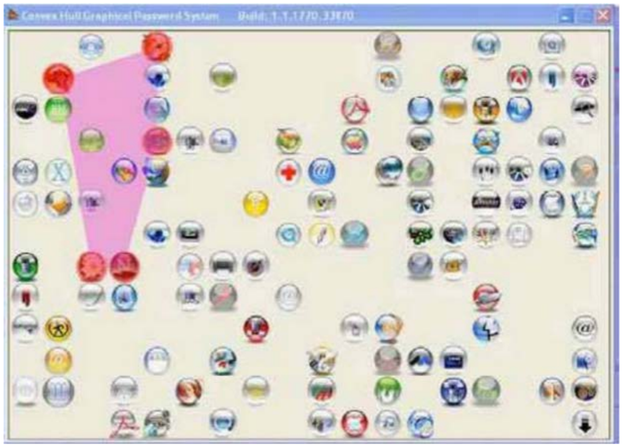


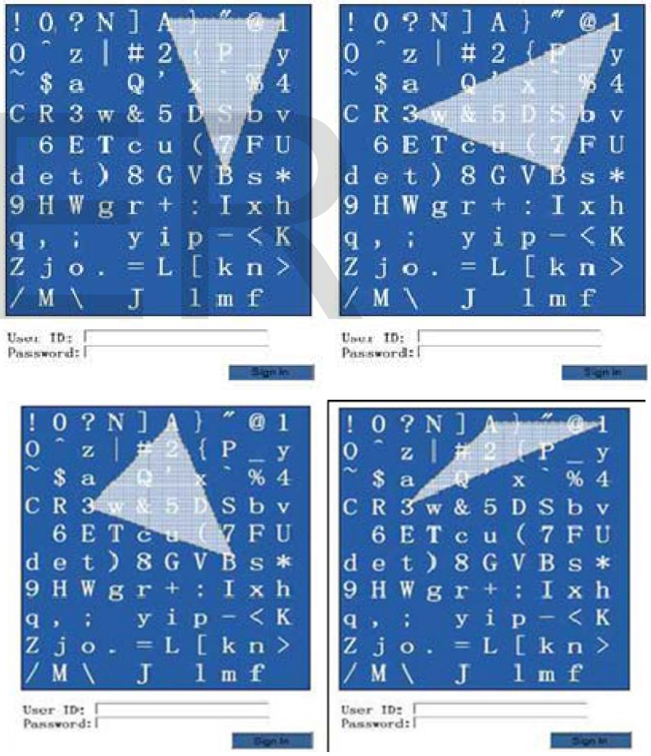
Figure 2. Example of a convex hull with 5 pass-icons.

2.2 S3PAS

S3PAS is designed to be used in client/server environments as password authentication systems [10]. Note that, the S3PAS system generates the login image locally and transmits the image specification (e.g., the coordinates of every character or icon in the image) instead of the entire image pixel-by-pixel from clients to servers, which greatly reduces communication overheads and authentication time. To show the login process, let us consider an instance.

Without loss of generality, this proposed system assumes that the user's original password k is "A1B3". Since the length of the password is 4-digits, based on the basic click-rule, user has to click four times in the right sequence to be authenticated. The four combinations of password in order are "A1B", "1B3", "B3A" and "3A1". The login procedure consists of the following four steps and is also shown in Figure 3.

1. User finds his pass-characters "A", "1" and "B", then clicks inside the pass-triangle or input a session pass character inside A1B (e.g., "P").
2. User finds his pass-characters "1", "B" and "3", then clicks inside the pass-triangle or input a session pass character inside 1B3 (e.g., "D").
3. User finds his pass-characters "B", "3" and "A", then clicks inside the pass-triangle or input a session pass character inside B3A (e.g., "5").
4. User finds his pass-characters "3", "A" and "1", then clicks inside the pass-triangle or input a session pass character inside 3A1 (e.g., "2").



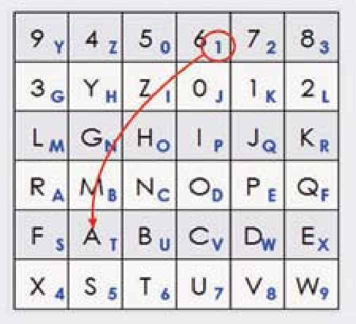
```
! 0 ? N ] A } " @ 1
0 ˆ z | # 2 { P _ y
~ $ a   Q ' x ` % 4
C R 3 w & 5 D S b v
  6 E T c u ( 7 F U
d e t ) 8 G V B s *
9 H W g r + : I x h
q , ;   y i p - < K
Z j o . = L [ k n >
/ M \   J   l m f
```

Figure 3. S3PAS: input password method

However, S3PAS is vulnerable to intersection attack [11].

2.3 SecurePass

KISA (Korea Internet Security Agency) presented SecurePass in 2010 [4]. This mechanism resists Key Logging and Shoulder Surfing attack and is vulnerable to keyboard input method intended to replace the technology and password input method using graphic and mouse.



9 Y	4 Z	5 0	6 1	7 2	8 3
3 G	Y H	Z I	0 J	1 K	2 L
L M	G N	H O	I P	J Q	K R
R A	M B	N C	O D	P E	Q F
F S	A T	B U	C V	D W	E X
X 4	S 5	T 6	U 7	V 8	W 9

Figure 4. SecurePass input method proposed by KISA

As shown in Figure 4, SecurePass is password input map using the graphic. Password input map is randomly mapping a black color number and blue color number. Proceed in the following order:

If user password is blue color '1', '3', '4', 'A' and certification authority specified number is black color 'A'.

Step1. Server sends to user a password input map and certification authority specified number.

Step2. Mapping map pop-up window for authentication appears.

Step3. Users click blue color '1' drag to black color 'A' (certification authority specified number).

Step4. Map relocation characters for the next authentication process.

Step5. Proceed in the same way.

However, this mechanism is one cycle (entered on password) need to a graphic map of the relocation. This is due to increase of the operation process can lead to the degradation of operation speed and memory space required an increase.

3 Secure Authentication Algorithm using Textual Passwords

The authentication pattern is first registered in the user registration phase and verified in the authentication phase. The overall authentication is given by means of a Flow chart.

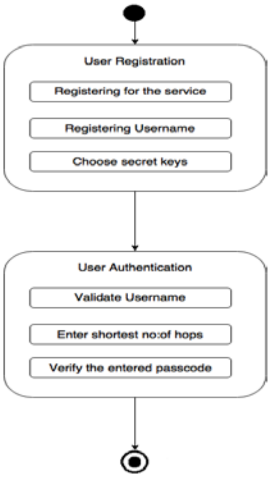


Figure 5.Flow chart for the proposed algorithm

3.1 User Registration

This is done at the time of users registering for the services. The user enters or chooses a 4-digit number as a password I.e. he chooses the password as a sequence of two two-digit numbers which are known to be as keys k1 and k2.These k1 and k2 are stored in the database of the organization/company and are retrieved at the time of validation. The users should not disclose the secret keys to anyone so as to maintain strict privacy.

% Registering for the service %

1. Select type of service
2. Enter details of the user for the service
3. Submit the request to the server
4. System validates the details
5. Go to register username

% Registering the username %

1. Enter the person details
2. Enter the username for creating account
3. System checks for the account
4. Go to choose secret keys

% Choose the secret keys %

1. Enter the secret keys of the user
2. Store the secret keys in the database

3.2 User Authentication

In this phase the users are authenticated with the help of the keys k1 and k2 stored in the database at the time of registration.

%Validate the user %

1. Enter username
2. System validates the username by checking in the database
3. System randomly generates two-dimensional vector table
4. System retrieves the secret keys of the user and shortest no: of hops is calculated between key k1 and key k2 using dijsktras shortest path algorithm [7] [12].

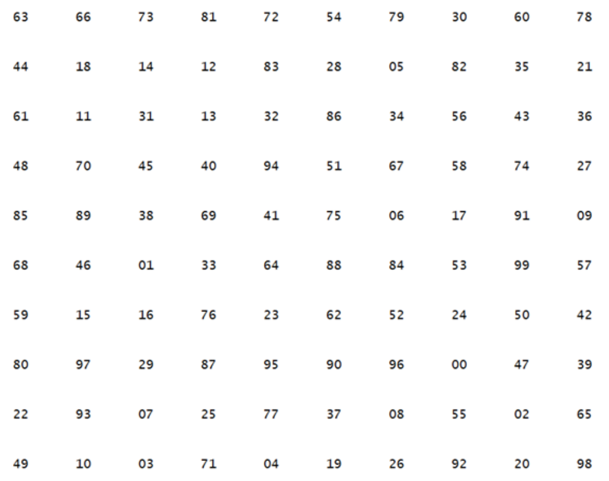
% Validate the shortest distance %

1. System request for shortest no: of hops between the two keys
2. System checks for the shortest no: of hops given by the user and that is generated by the system.
3. If validation is successful then user is allowed to start the transaction, else user is requested for the validation of user.

When the user shows his Identity (Either by inserting a card or by means of any username) a screen is displayed as

ISSN 2229-5518

follows.



63	66	73	81	72	54	79	30	60	78
44	18	14	12	83	28	05	82	35	21
61	11	31	13	32	86	34	56	43	36
48	70	45	40	94	51	67	58	74	27
85	89	38	69	41	75	06	17	91	09
68	46	01	33	64	88	84	53	99	57
59	15	16	76	23	62	52	24	50	42
80	97	29	87	95	90	96	00	47	39
22	93	07	25	77	37	08	55	02	65
49	10	03	71	04	19	26	92	20	98

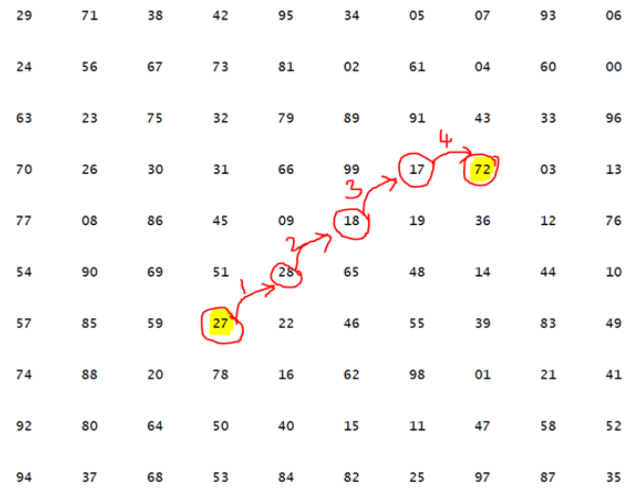
Figure 6. An instance of two dimensional vector table

The user has to identify both his keys in the vector table shown in Figure 6 and has to find the shortest distance between his two keys. The distance is calculated by counting the number of hops between the two keys. The shortest distance is the path with the minimum number of hops between the two keys. The vector table is generated randomly. So this makes the process highly resistant to shoulder surfing. The shoulder surfing attacker cannot identify the keys as the user is entering only the shortest distance between the keys.

The mechanism is as follows:

Consider the case in which the user has chosen 2772 as his password. This means 27 and 72 are his keys. So a random vector table is generated as shown and the shortest distance is identified.

The path from 27-28-18-17-72 is the shortest path and its number of hops required are 4 as shown Figure 7. Hence the user has to enter 4 as a password rather than entering the password that can be easily captured in a high definition video recording device.



29	71	38	42	95	34	05	07	93	06
24	56	67	73	81	02	61	04	60	00
63	23	75	32	79	89	91	43	33	96
70	26	30	31	66	99	17	72	03	13
77	08	86	45	09	18	19	36	12	76
54	90	69	51	28	65	48	14	44	10
57	85	59	27	22	46	55	39	83	49
74	88	20	78	16	62	98	01	21	41
92	80	64	50	40	15	11	47	58	52
94	37	68	53	84	82	25	97	87	35

Figure 7. An instance showing the shortest number of hops

4 Experiment and Simulation Analysis

4.1 Size of password space

There are 100 numbers in total (from 0 to 99) that can be printed in the table. There exists a 100! (=9.332622e+157) Unique tables which are quite a large number. So, the probability of repeating the same vector table is very small. So, the attacker couldn't get through it.

4.2 Success probability of password guessing attacks

The user is given a total of 3 chances to validate his/her pass keys. The maximum possible password is 9 and minimum is 0. So the chances that the attacker could guess are 3/10 which is a small value and is based only upon pure guessing strategies which may be true or may not be.

To check the compatibility of the system with the current world, 200 novice users have been taken into consideration. A user selects a 4-digit number at the time of registration. It was observed that all the users could comfortably go through the process by overcoming the shortcomings in the textual and graphical passwords.

Our system requires the memorization of only four digit number by the user. This is advantageous when compared to graphical passwords. One might feel that graphical passwords are easy to be remembered and reproduced efficiently, but since people are accustomed to traditional passwords i.e., textual passwords, users feel advantageous and comfort in this system.

Shoulder surfing attacks – Shoulder surfing is done at a distance using binoculars or other vision-enhancing devices. The algorithm has resistance against Shoulder Surfing Attacks. The user enters the shortest path and the attacker is not able to identify the secret keys. When the user interface is called again the table is generated randomly which gives the new shortest path.

5 Conclusion

Weak passwords are threat to the authentication system. This paper suggests an efficient authentication algorithm that produces strong passwords that resist SS attacks. It is observed that the algorithm is simple and more user friendly than other textual and graphical passwords. The strength of the system is that the user need not memorize the large textual passwords and could only remember four digits that are hidden from the attackers by giving a single digit which could reduce the success probability of the attack. Each user is given only three chances to strengthen the algorithm. The algorithm can be made more resistant by increasing the table size.

References

[1] Arash Habibi Lashkari, Samaneh Farmand, Dr. Rosli Saleh, Dr. Omar Bin Zakaria, "A wide-range survey on Recall-Based Graphical User Authentications algorithms based on ISO and Attack Patterns", International Journal of Computer Science and Information Security, Vol. 6, No. 3, 2009

[2] Tzong-Sun Wu, Ming-Lun Lee, Han-Yu Lin, Chao-Yuan Wang, "Shoulder-surfing-proof graphical password authentication scheme" International Journal of Information Security June 2014, Volume 13, Issue 3, pp 245-254

[3] Xiaoyuan Suo; Ying Zhu; Owen, G.S., "Graphical passwords: a survey," Computer Security Applications Conference, 21st Annual , vol., no., pp.10 pp.,472, 5-9 Dec. 2005

[4] KISA(Korea Internet Security Agency), "SecurePass", "http://news.donga.com/3/all/20100415/27578455/1", 2010.4

[5] S. Wiedenbeck, J. Waters, L. Sobrado and J. Birget, “Design and evaluation of a shoulder-surfing resistant graphical password scheme”, Proceedings of the Advanced Visual Interfaces, pp. 177-184, May 2006.

[6] Farnaz Towhidi and Maslin Masrom, “A survey on Recognition-Based Graphical User Authentication Algorithm”, International Journal of Computer Science and Information Security, vol.6,no.2, 2009

[7] Dijkstra E W. A node on two problem in connexion with graphs. Numerische Mathemartik. vol. 1, 1959, pp.269-271.

[8] Beum Su Park; Choudhury, A.J.; Tae Yong Kim; Hoon Jae Lee, "A study on password input method using authentication pattern and puzzle," Computer Sciences and Convergence Information Technology (ICCIT), 2011 6th International Conference on , vol., no., pp.698-701, Nov. 29 2011-Dec. 1 2011

[9] D. Sharek, C. Swofford and M. Wogalter, "Failure to Recognize Fake Internet Popup Warning Messages," proceedings of the human factors and ergonomics society 52nd annual meeting, 557-560, 2008

[10] H. Zhao and X. Li, “S3PAS: A scalable shoulder-surfing resistant textual graphical password authentication scheme,” Proceedings of the 21st IEEE International Conference on Advanced Information Networking and Applications Workshops, vol. 2, Pp. 467-472, May 2007.

[11] DongOh Shin, Jeonil Kang, DaeHun Nyang, KyungHee Lee, “On the Security of S3PAS against Intersection Attack”, KIISC Journal, vol 21, no 1, pp.77~pp84, 2011.2

[12] James B. Orlin, Kamesh Madduri, K. Subramani, and M. Williamson. 2010. “A faster algorithm for the single source shortest path problem with few distinct positive lengths. J. of Discrete Algorithms” 8, 2 (June 2010), 189-198.