Poster: Input Password Only with Four Keys, Three Times

Akane Ito
Kanagawa Institute of Technology, Japan

Yui Ohtaka
Kanagawa Institute of Technology, Japan

Yoshie Yamada
Kanagawa Institute of Technology, Japan

Manabu Okamoto
Kanagawa Institute of Technology, Japan

1. INTRODUCTION

A Password-based authentication is a basic technique used for user authentication [1]. However, phishing, shoulder surfing [2], or keyloggers pose a threat to security. We proposed a new password inputting method at SOUPS'13 [3]. In this method, the user uses only the four arrow keys and the Enter key to input passwords and this method helps secure the password against keyloggers and shoulder surfing. However, a wrong password can be easily input by this method. And the number of times a key is pressed increases. In this paper, we propose a new improved method to input a password. In this method, only four keys and Enter key are used, errors when inputting the password are few, and when a certain letter is input, a key is pressed thrice.

2. RELATED WORK

In the proposed method [3], whenever authentication is requested, the server generates a 6 × 6 random matrix table that consists of A–Z, 0, and 1–9. The server adds a red circle mark to a random cell of the matrix. The sequences of characters and the position of the red circle vary each time. When the initial letter of the password is "A" and the red circle is on "C" as shown in Figure 1, we need to input left-up-up-up-enter with the arrow keys ←↑↑↑+ Enter. Of course, we can also input up-left-up-up-Enter. However, the red circle does not move.

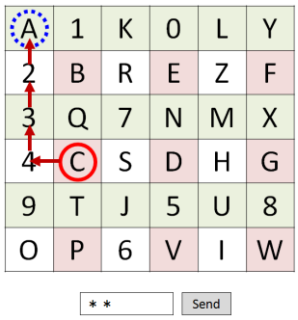

Figure 1. Method presented at SOUPS'13.

Note that this method has some issues, for example, the success rate for this method is low. The user test rate of success in inputting a correct password is less than 60% as demonstrated at SOUPS'13. The user incorrectly pressed the arrow key twice. In addition, the number of times the key is pressed widely ranges from 0 to 10. When the target word is far from the red circle, we are more likely to input a wrong password.

3. PROPOSED METHOD

In this section, we describe our proposed system. This system of inputting a password is robust against keyloggers and shoulder surfing. We can minimize the number of input mistakes. Further, note that a key needs to be pressed three times to input a single letter of the password..

We assume that a user inputs a password for some service. There is not size limit on the length of the password. When authentication is requested, the server generates an 8 × 8 random matrix table, which consists of the characters a-z, A-Z, 0, and 1-9 as shown in Figure 2. The sequence of characters varies each time.

Automatically, the matrix table is divided into four sections, and each section moves diagonally and creates space between the other sections. A user can recognize the four sections as shown in Figure 3. In fact, section 1, 2, 3, and 4 are not displayed. The user presses from numbers 1–4 to select the section in which the letter of his/her password to be input is present. When the user wants to input "p," he/she presses "2."

Further, each section is subdivided into four smaller subsections, and each subsection moves diagonally and creates space between the other subsections. Therefore, there are 16 sections as shown in Figure 4. The user presses the number of the section in which a letter of his/her password to be input is present. When the user wants to input "p," he/she presses "3." Finally, each of these 16 sections is further divided into four sections, and now, the total number of sections is 64, as shown in Figure 5. The user presses the number to select a particular section in which the letter of his/her password is present. When the user wants to input "p," he/she presses "3," as shown in Figure 5.

In this example, when the user inputs "p," which is the first letter of his/her password, he/she presses 2-3-3.

For inputting the next letter of the password, the server generates another 8 × 8 random matrix table. The sequences of characters of the new matrix are different from those of the last one. As shown in Figure 6, the user is required to press 4-1-2 in order to input "a."

When the user finishes inputting all letters included in a password and is not required to input any more letters, he/she presses only the Enter key to finish the authentication.

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

Figure 2. Base matrix.

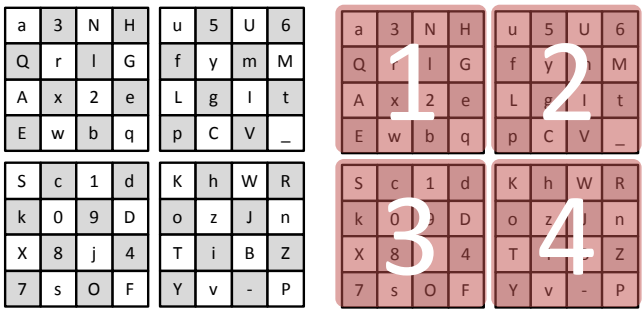

Figure 3. Four sections.

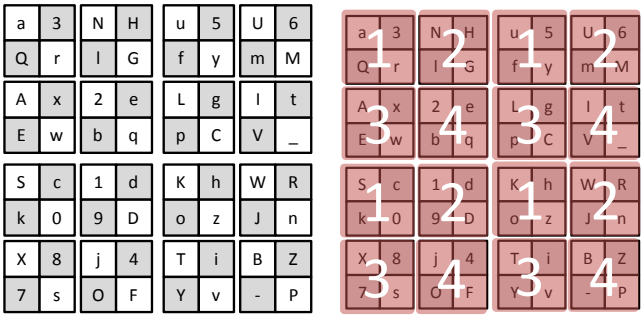

Figure 4. Sixteen sections.

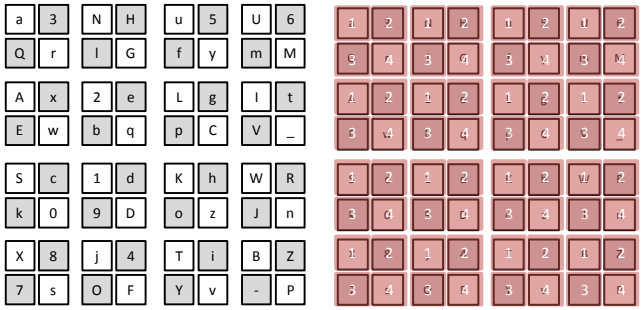

Figure 5. Sixty-four sections.

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

Figure 6. Another base matrix.

When it is required to input "s," 4-2-1 is pressed.

4. ADVANTAGES

4.1 Usability

In the proposed authentication scheme, we require only four keys to input a password, and they have to be pressed three times to input one letter. In addition, by inputting eight words, the success rate for correctly inputting the password is over 90% based on the results of our test. Ten students participated in the test and used this system for a week. The users understood the procedure easily and quickly.

However, we require more time to input a password by using this method when compared with directly inputting the password. Almost all users require time to determine the letters of his/her password in the matrix. It is necessary to evaluate this method by conducting more tests.

4.2 Efficiency and Security

This method is robust against keyloggers. A keylogger saves only the operations of the number keys, which is insufficient for an attacker to guess the password. For example, key operations such as 2-2-3 or 1-1-4 do not mean anything. Further, shoulder surfing is not a threat because we use only four keys, and we can also easily shade the keys with our hand. The attacker cannot obtain the password by only capturing the display because a hint on the letter recently inputted by the user is not displayed.

The strengths of all passwords are almost the same as that of a typical password; however, the input method varies. We can use a password that includes English alphabets and numbers, and we also can use a long password. In particular, 64 letters can be used in this method, which is more than those used in the last proposed method where 36 letters could be used.

The user presses a key three times while inputting one letter of the password. The attacker can guess the length of the password; however, he/she cannot guess the password itself owing to the number of keys pressed.

5. CONCLUSION

In this paper, we proposed a method to input a password. The user operates only the four keys and the Enter key and is required to press a key three times in order to input one letter of the password. In addition, the user can freely use a typical password that is available with 64 characters. Our method is suitable for existing systems, and it works against both keyloggers and shoulder surfing. In our future work, we will conduct more user tests to evaluate the usability of the proposed system.

6. REFERENCES

[1] Matsumoto, T. and Imai, H.. 1991.Human Identification through Insecure Channel. Eurocrypt'91.

[2] Wiedenbeck, S., Waters, J., Sobrado, L., and Birget, J.C.. 2006. Design and evaluation of a shoulder-surfing resistant graphical password scheme.In Proceedings of the Working Conference on Advanced Visual Interfaces, pp. 177-184.

[3] Nami, H., Saki, N. and Manabu, O..2013. Input Password Only with Arrow Keys.SOUPS 2013.