Poster: Input Password Only with Arrow Keys

Nami Hidaka
Kanagawa Institute of Technology
Shimo-ogino 1030, Atsugi-shi
Kanagawa, Japan

Saki Naguchi
Kanagawa Institute of Technology
Shimo-ogino 1030, Atsugi-shi
Kanagawa, Japan

Manabu Okamoto
Kanagawa Institute of Technology
Shimo-ogino 1030, Atsugi-shi
Kanagawa, Japan
manabu@nw.kanagawa-it.ac.jp

1. INTRODUCTION

A password is a basic technique to authenticate the user. Almost all web services require the user to input an ID/Password. But password authentication has some problems.

Keyloggers are one problem. A keylogger is a hardware device or a software program that records all activity of a PC user, including the keyboard keys the user presses. A malicious attacker may use keyloggers on public computers to steal passwords or credit card information. Keylogger software [1] is freely available on the Internet.

In addition, a surveillance camera or peeping by a secret camera is a threat for passwords. By recording the scene of someone inputting a password and then analyzing the video, an attacker can guess the password.

In this paper we propose a new method to input a password. To use this method, only arrow keys are used. The four arrow keys, which are smaller than the ten-key pad, are on every PC, including notebook PCs. This technique works against both keylogger and peeping activities.

2. RELATED WORK

To make passwords more secure, various techniques have been proposed. A one-time password is the most popular method. The one-time password is a password that is valid for only one login. Usually, a hardware token generator is used. In this method, a problem is that we always have to possess the token. If we lose it, we cannot use it. In addition, distributing hardware tokens for all users is costly.

Many techniques that work against peeping or keylogger have also been proposed [2]. Especially, SECUREMATRIX [3] is very attractive. SECUREMATRIX is matrix authentication that combines patterns and images to form a one-time password. A token generator is not used.

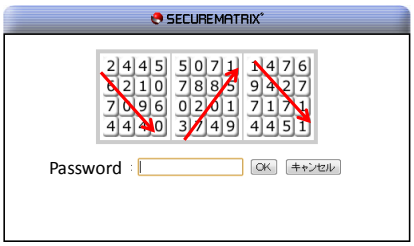

Figure 1. SECUREMATRIX.

The user needs only to remember a pattern that is mentally superimposed on a matrix table. Whenever authentication is requested, the server randomly generates a unique matrix table and shows it on the browser of the user. The user enters the numbers within his chosen superimposed pattern in sequence. The password entered by the user is a different one-time password every time. For example, in Figure 1, the user enters 229032811471 as the password according to the user-chosen pattern, which is denoted by the red arrow in this case.

SECUREMATRIX can fight against a keylogger as a one-time password but is weak against video recording. By analyzing video, an attacker may be able to learn the pattern on the matrix.

3. PROPOSED METHOD

In this section, we propose a new password system that uses only key arrows. This method can work against both keylogger and peeping.

We assume that a user inputs a password for some service. We assume that the password consists of English letters and numbers and the English letters are all capitals and other signs are not usable as a password. The length of the password is unlimited.

Whenever authentication is requested, the server generates a random matrix table and shows it to a user. This matrix table consists of A-Z and 0, 1-9 with a 6x6 size. A server adds a mark to some random cell of the matrix. Figure 2 shows a matrix and a red circle mark. The sequences of characters and the position of the red circle are different every time.

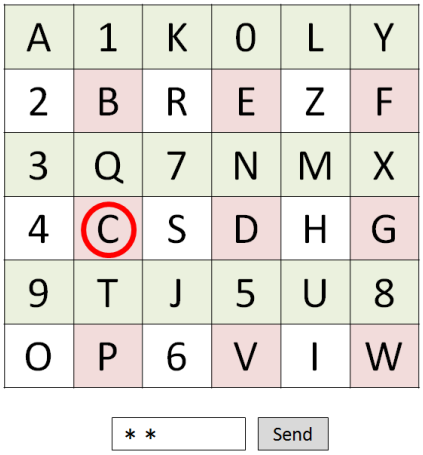

Figure 2. Proposed method.

If the initial word of a password is "A", then one inputs left-up-up-up-enter with arrow keys ← ↑ ↑ ↑ + Enter. Of course, one can input also up-left-up-up-Enter. Figure 3 shows an image of this action, although the red circle DOES NOT actually move.

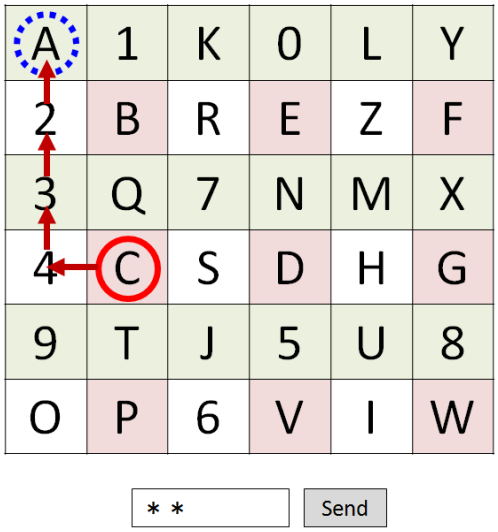

Figure 3. Image of action. "A" is left-up-up-up-up from "C".

After a user inputs one word, the server randomly generates another matrix table and shows it to the user. If the user inputs all of the password, he pushes the Send button. Note that the matrix and the position of the red circle are different every time, as shown in Figure 4.

We use the Enter key as the end of inputting arrows. The password box shows the number of passwords that a user has ever inputted with an asterisk (*).

If a position that a user attempts with arrow keys is out of bounds, the server shows an error and the user needs to repeat the input again.

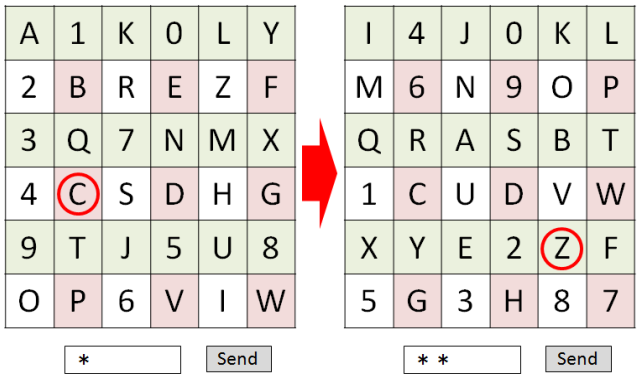

Figure 4. Image of action sequence.

4. SECURITY ANALYSIS

In this section, we describe the advantages of our method.

4.1 Usability

In this scheme, we need more time to input a password than is input directly. By inputting 6-12 words, the password takes approximately 30 seconds, according to our test of 10 students using this system in one week. The users understood the procedure quickly. The user action is simple and easy for everyone, including children.

4.2 Efficiency and Security

This method can fight against a keylogger. Keylogger saves only operations of the arrow keys, and the attacker cannot guess a password by the obtained information, such as up-up-left-left. Peeping is also not threat in this method, because the attacker cannot know a password by only the display capture. The display shows only the matrix and the starting point as a red circle. The four arrow keys are smaller than those on the ten-key pad, and we can also shade them by our hand. So, a video camera cannot capture the movement of the arrow key. Especially, the video of a user inputting a password by using the number keys on a notebook PC can be easily analyzed, because a notebook PC may not have a ten-key pad. But all PCs, including notebook PCs and tablets, have arrow keys.

The strength of the password is almost the same as that of a typical password; only the method of inputting the password is different. We can use a password including English letters and numbers and use a long password, too.

To evaluate this method is future work. We assume that we can shade key operation by our hand and it can be not recorded with video. Actually the range of the key operation is very small in this method and it is difficult for attackers to analyze the video and get a password. But we need to consider whether you can suppose a password by supposing the number of times that the key was pushed.

5. CONCLUSION

In this paper we propose an easy method to input a password. The user operates only the four arrow keys and the Enter key. The user does not need to have any hardware token and does not need to remember the pattern of the matrix. Additionally, the user can use a typical password, not a one-time password. This system, which is suitable for existing systems, works against both keylogger and peeping.

6. REFERENCES

[1] Free Keylogger, http://download.cnet.com/Free-Keylogger/3000-2162_4-10419683.html.

[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. AVI'06, pp. 177-184, 2006.

[3] SECUREMATRIX, http://www.csessi.com/.