Implementation and User Testing of Personal Authentication Having Shoulder Surfing Resistance with Mouse Operations

Makoto Nagatomo\(^1\), Yoshihiro Kita\(^2\), Kentaro Aburada\(^3\), Naonobu Okazaki\(^3\), and Mirang Park\(^1\)\(^a)\)

\(^1\) Kanagawa Institute of Technology
1030 Shimo-Ohino, Atsugi, Kanagawa 243-0292, Japan

\(^2\) Tokyo University of Technology
1404-1 Katakura, Hachioji, Tokyo 192-0982, Japan

\(^3\) University of Miyazaki
1-1 Gakuen-Kibanadai-Nishi, Miyazaki, Miyazaki 889-2192, Japan

\(^a\) mirang@nw.kanagawa-it.ac.jp

Abstract: Typically, typing character strings on a keyboard is used for personal authentication for PC login and unlocking. Although some graphical and biometric-based methods have been developed, most of them have weak authentication strength, weak shoulder surfing resistance, or other drawbacks. In this paper, we propose a personal authentication method that employs mouse operations, although the mouse itself does not need to be moved. Thus, the user can hide the mouse during authentication, so the method has shoulder surfing resistance and can be used in public places. We performed user testing to validate the proposed method.

Keywords: personal authentication, mouse operation, shoulder surfing resistance

Classification: Multimedia system for communications

References

[1] CSE: SECUREMATRIX, http://cse-america.com/index.htm, accessed Sept. 20, 2017.

[2] Vijay Rajanna, Seth Polsley, Paul Taele, Tracy Hammond, “A Gaze Gesture-Based User Authentication System to counter Shoulder-Surfing Attacks,” Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems, pp. 1978-1986, 2017. DOI: 10.1145/3027063.3053070

[3] M. Karim, H. Heikal, and Md. Hasanuzzaman, “User Authentication from Mouse Movement Data Using Multiple Classifiers,” Proceedings of the 9th International Conference on Machine Learning and Computing, pp. 122-127, 2017. DOI: 10.1145/3055635.3056620
[4] Yoshihiro Kita, Naonobu Okazaki, Hiromitsu Nishimura, Hideyuki Torii, Takeshi Okamoto, and Mirang Park, “Implementation and Evaluation of Shoulder-Surfing Attack Resistant Users,” The IEICE Transactions on Information and Systems (Japanese Edition), vol. J97-D, no. 12, pp1770-1784, 2014 (in Japanese).

1 Introduction

Currently, many people use character-based passwords entered by keyboard for personal authentication in public places, such as a classroom of office to unlock a PC or sign into a service on the user’s own PC or a public PC. This method in these situations risks leakage of passwords by shoulder surfing.

SECUREMATRIX[1] provides a graphical password as positions on three or four matrices. The memory burden is less than it is for a character string. An attacker, however, can identify the password by shoulder surfing attack by watching the keyboard and the monitor.

In the gaze-following method[2], a user performs authentication by following a moving icon on the monitor using their eyes. This method has shoulder surfing resistance, but the user must use a camera.

In the method presented in [3], the user registers extracted features of the user’s mouse movements on a desk. The user can use this method in many public places since most PCs have a mouse. However, the attacker can imitate mouse movements by shoulder surfing.

The Secret Tap with Double Shift (STDS) method[4] requires the user to register icons as a password on the screen of a smartphone. The user authenticates the icons by selecting the icons. This method has shoulder surfing resistance, but the genuine icons can be revealed by recording attack twice.

As described above, no easy-to-use method has shoulder surfing resistance for a PC in public places. In this paper, we propose a method that uses mouse clicks and mouse wheel rotations. This method has shoulder surfing resistance because the user does not need visual feedback and can operate the mouse under a desk.

2 Mouse authentication method

2.1 Overview

Here we define the personal authentication method. The input interface is a common mouse with right and left click, upward and downward wheel rotation, and wheel click. The output interface is an $N \times N$ matrix.

**Use case:** A user unlocks a PC or signs into a service on a PC in a public place while hiding the mouse such as under the desk. For example, a user signs into an e-mail service on their own laptop in a café.

**Strength:** When the user registers $m$ positions (including the registration order) on an $N \times N$ matrix, the probability that an attacker succeeds in a random attack on this method (accidental authentication probability) is $1/N^{2m}$. We are aiming for an accidental authentication probability of less than 1/10,000.
**Registration phase:** Registration is performed as follows.
1. The screen displays an $N \times N$ matrix with an initial position randomly selected.
2. The user registers a position on the matrix using mouse operations. The current position is marked by a red circle, and the positions moves left by left click, right by right click, up by upward wheel rotation, and down by downward rotation. The user registers the current position with a wheel click.
3. The user registers $m$ positions by repeating (1) and (2). The registered order is part of the authentication information.

**Authentication phase:** Authentication is performed as follows.
1. The screen displays an $N \times N$ matrix with a randomly selected initial position.
2. The user specifies the first registered position with mouse operations. The mouse operations and its effects are the same as (2) in the registration phase. The user hides the mouse such as under the desk, and only the initial position is displayed, not the current positions, to strengthen shoulder surfing resistance.
3. The user specifies $m$ registered positions in their registered order using the same mouse operations used during registration.

**Benefits:** The mouse operations in this method are intuitive. Some people cannot operate a keyboard intuitively while hiding it. In addition, the proposed method is a challenge and response authentication system, in which the screen position and position order are hidden. Therefore, users can use this method in public places safely.

### 2.2 Implementation

We implemented the proposed method using a $5 \times 5$ matrix ($N=5$), which struck a balance between the usability and authentication strength. A position count of $m \geq 3$ meets $1/5^2 m \leq 1/10,000$, so we decided to make the “password” three or more positions long.

Fig. 1 shows an animation of the proposed method. It is natural to fix the initial position on the matrix, but the shoulder surfing resistance is weak against hearing the mouse sounds sometimes. Therefore, although it seems that the usability is lower than when the initial position is fixed, we decided that the initial position is determined randomly. The registered position is revealed when an initial position is near it in the authentication phase, so the user must register a position after moving at least three times.

We developed two variations in which the user (1) selects positions directly by combinations of mouse clicks and mouse movements, or (2) selects by combinations of colors and numbers on the matrix. A user can select a variation according to their taste.

### 3 Evaluation

We conducted two experiments on the usability and shoulder surfing resistance of the implemented method. The subjects used a desktop PC and a common mouse with mouse clicks and wheel rotations (Logitech wireless mouse M186). This mouse emits the sound of clicks and rotations clearly. In the user testing and shoulder surfing experiment reported here, we did not use the two variations, but
we plan to conduct experiments of these in the future.

3.1 Usability test
We conducted the usability test as follows:

1. We explained to the subject how to use the method.
2. The subject completed a tutorial to become familiar with the mouse operations.
3. The subject registered three positions.
4. The subject performed three authentications successfully.
5. The subject answered a questionnaire on comprehension, ease of use, ease of familiarization, safety for shoulder surfing, and user needs. These items were rated from 1 to 5 (very bad to very good).

Fig. 2 shows the result of the usability tests. The subjects were 20 Kanagawa Institute of Technology students. The average time to complete the third successful authentication was 15.5 s [see Fig. 2(a)], and the average authentication success rate was 63.1%. It took time for users to get used to this authentication method, and the success rate was not enough due to the invisibility of the current positions. Fig. 2(b) shows the result of the responses to the usability testing questionnaire. All five averages are over 3, so usability of this method is confirmed.

3.2 Shoulder surfing resistance test
In the second experiment, shoulder surfers were positioned 1 m behind the user so that the surfer could see the monitor and hear the mouse sounds. We eliminated ambient noise so that the surfer could hear the mouse sound clearly. The procedure of the shoulder surfing resistance experiment was as follows:

1. We formed teams consisting of five or six people.
2. We choose a user from each team, and the user registered three positions in the method. Shoulder surfers were the other people in each team, and not allowed
to see the monitor during the registration.

3. The user performed ten authentication successes while hiding the mouse under the desk. Shoulder surfers observed the authentication and tried to detect the registered positions; they were allowed to take notes.

4. We repeated steps 2-4 until everyone on the team was a user once.

The subjects were 16 Kanagawa Institute of Technology students. We performed this experiment using one team with six people and two teams with five people each. The result shows that the detection rates for one, two and three positions were 22.8%, 8.6%, and 1.4%, respectively. Only once were all three of a user’s registered positions detected (by one person). For the other 15 subjects, only one or two registered positions were detected. Under real conditions in public places, ambient sound would interfere with the shoulder surfing, so the results indicate that this method has shoulder surfing resistance.

### 3.3 Comparison with other methods

We compared the proposed method with related methods[1,2,4], as shown in Table I. The proposed method has fewer password combinations than SECUREMATRIX[1] and the gaze-following method[2], but it has shoulder surfing resistance and needs no special device. The STDS method on a smartphone[4] has shoulder surfing resistance and does not require special devices,
but the proposed method has more password combinations than does STDS.

4 Conclusion
We proposed a personal authentication method with shoulder surfing resistance using mouse operations. In the proposed method, a user can hide the mouse and thereby achieve shoulder surfing resistance. We implemented the proposed method and evaluated it for usability and shoulder surfing resistance. The results show that the proposed method has good usability, shoulder surfing resistance. However, the sounds made by the mouse during operation is a possible source of password detection. A measure to protect against this will be developed in the future. Moreover, although we assumed that a user always hides a mouse such as under a desk in authentication phase, we will develop the method that have shoulder surfing resistance without hiding a mouse.

Acknowledgments
This work was supported by JSPS KAKENHI Grant Numbers JP17H01736, JP17K00139.

| Table I. Comparison with related methods |
|-----------------------------------------|
| Existing method                         |
| SECURE MATRIX [1]                      |
| Gaze-following method [2]              |
| STDS [4]                                |
| Proposed method                        |
| Combinations (in case of 3 digits of passwords) | 32\(^3\) = 32,768 |
|                                         | (in case of three matrices) |
|                                         | 36\(^3\) = 46,656 |
|                                         | (including dummy icons) |
|                                         | 16\(^3\) = 4,096 |
|                                         | 25\(^3\) = 15,625 |
| Shoulder surfing resistance             | -                     |
|                                         | x                     |
|                                         | x                     |
|                                         | x                     |
| Secret information                      |
| Positions                               |
| Icons                                   |
| Icons and shifts                        |
| Positions                               |
| Special devices                         |
| none                                    |
| camera                                  |
| none                                    |
| none                                    |