ComEX

IEICE Communications Express, Vol.4, No.3, 95–98

Proposal of a puzzle authentication method with shoulder-surfing attack resistance and high-usability

Yoshihiro Kita[1], **Kentaro Aburada**[2], **Mirang Park**[1], **and Naonobu Okazaki**[3a)]

[1] *Kanagawa Institute of Technology,*
1030 Shimo-Ogino, Atsugi, Kanagawa 243–0292, Japan

[2] *Oita National College of Technology,*
1666 Oaza-Maki, Oita, Oita 870–0152, Japan

[3] *University of Miyazaki,*
1–1 Gakuen-Kibanadai-Nishi, Miyazaki, Miyazaki 889–2192, Japan

a) *oka@cs.miyazaki-u.ac.jp*

Abstract: Most existing authentication methods have a common problem, referred to as shoulder-surfing, in which authentication information is covertly obtained by peeking over the shoulder of a user as he/she completes the authentication sequence. In this paper, we propose a puzzle authentication method that is very simple and sufficiently secure, even when the authentication sequence is being leaked. We also implemented the proposed method on a mobile terminal and is evaluated through experiments and questionnaire surveys.

Keywords: mobile security, sholder-surfing, puzzle, android OS

Classification: Multimedia Systems for Communications

References

[1] Z. K. Wazir, Y. A. Mohammed, and X. Yang, "A graphical password based system for small mobile devices," *Int. J. Comput. Sci. Issues*, vol. 8, issue 5, no. 2, pp. 145–154, 2011.

[2] T. Takada, "fakePointer: an authentication scheme for a better security against a peeping attack by a video camera," Proc. of the 2nd International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies (UBICOMM2008), 2008. DOI:10.1109/UBICOMM.2008.76

[3] N. H. Zakaria, D. Griffiths, S. Brostoff, and J. Yan, "Shoulder surfing defense for recall-based graphical passwords," Proc. of the 7th Symposium On Usable Privacy and Security (SOUPS) 2011, no. 6, pp. 1–12, 2011. DOI:10.1145/2078827.2078835

[4] A. D. Luca, M. Harbach, E. V. Zezschwitz, M. E. Maurer, B. Slawik, H. Hussmann, and M. Smith, "Now you see me, no you don't — protecting smartphone authentication from shoulder surfers," Proc. of the SIGCHI Conference on Human Factors in Computing Systems, pp. 2937–2946, 2014. DOI:10.1145/2556288.2557097

[5] Y. Kita, F. Sugai, M. Park, and N. Okazaki, "Proposal and its evaluation of a

DOI: 10.1587/comex.4.95
Received February 4, 2015
Accepted February 25, 2015
Published March 26, 2015

shoulder-surfing attack resistant authentication method: secret tap with double shift," *Int. J. Cyber-Security Digital Forensics (IJCSDF)*, vol. 2, no. 1, pp. 48–55, 2014.

1 Introduction

Due to increased computing capabilities, modern mobile terminals hold massive amounts of private and potentially sensitive user data. This is very convenient for the users but becomes problematic should they ever lose their phone or if it gets stolen. Many users are aware of this problem and thus, want to protect access to their devices.

Mobile terminals are equipped with their own display lock system that uses personal authentication methods such as passwords, personal identification numbers (PINs) and Android Password Pattern in order to prevent data theft. However, most existing authentication methods are not resistant to shoulder-surfing. Shoulder-surfing is the process in which authentication information is covertly and deliberately obtained by a person peeking over-the-shoulder of a user as he/she completes the authentication sequence.

Existing authentication methods [1, 2, 3, 4, 5] with shoulder-surfing attack resistance are indeed more secure against peeking, but they are hard to use by complex operations and much information that must be remembered. Therefore, they are not used by most users of the mobile terminals.

In this paper, we present a puzzle authentication method that we designed to overcome shoulder-surfing attack and reinforce usability. We aim to gain the usability and the operatively that users can fun likes puzzle games.

2 Puzzle authentication method

We propose a puzzle authentication method having shoulder-surfing attack resistance and high-usability. We define the following puzzle authentication scheme. This scheme uses the challenge-response protocol. The mobile terminal prepares N-by-M array that it includes random numbers from 0 to $N \times M$ (not duplicate) as challenge, and assigns to each user pass-numbers and pass-locations as common keys. Pass-numbers consist N numbers from 0 to $N \times M$. Pass-locations are the element numbers of array, and consist N numbers from 0 to $N \times M$.

During authentication, the mobile terminal shows the array to user. The user can swap the adjacent each element in array freely. If the element numbers that elements include pass-number, are the same numbers as pass-locations, authentication is success, otherwise authentication is failure.

Fig. 1 shows the example of panels operation. This example uses the $N \times M = 4 \times 4 = 16$ panels: 0 to 9, and 6 colors. The 6 color panels assign the number from 10 to 15. These panels are placed randomly in the display area. The user registers the four authentication panels and the four locations.

When unlock the display lock system, the user taps and slide the any panel, place the four authentication panels on the four registered locations.

DOI: 10.1587/comex.4.95
Received February 4, 2015
Accepted February 25, 2015
Published March 26, 2015

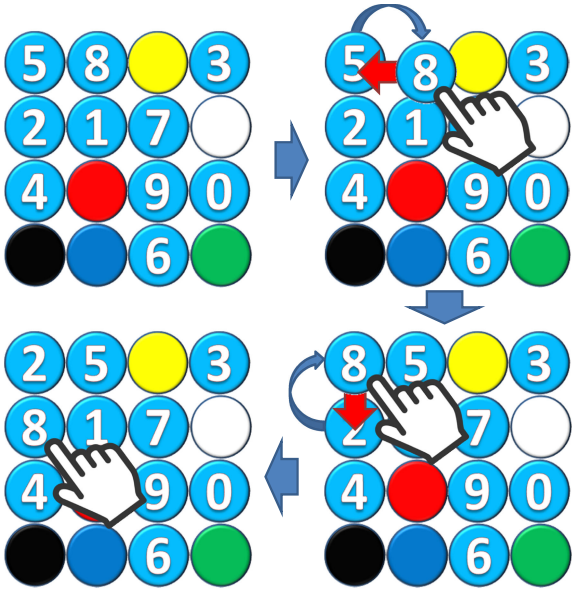

Fig. 1. Example of panels operation

Fig. 2. Movie for the operation of puzzle authentication method

Example of panels operation in Fig. 1, the user tap the panel '8', and slide to the panel '5'. The panel '8' is swapped the place for the panel '5'. And, the user tap the panel '8', and slide to the panel '2'. The panel '8' is swapped the place for the panel '2'.

Fig. 2 shows the movie for the operation of puzzle authentication method. The user taps and drags the panels in the registration of locations and panels(icons), and the operations for authentication as the movie.

3 Evaluation and discussion

The puzzle authentication method was then examined in order to confirm this usability, and to evaluate this resistance to be observed convertly from others. The subjects were fifteen students at Kanagawa Institute of Technology. This experiment was conducted as follows:

1. We confirmed the students knew how to use each authentication method, i.e., PINs, Android Password Pattern, and puzzle authentication method.

DOI: 10.1587/comex.4.95
Received February 4, 2015
Accepted February 25, 2015
Published March 26, 2015

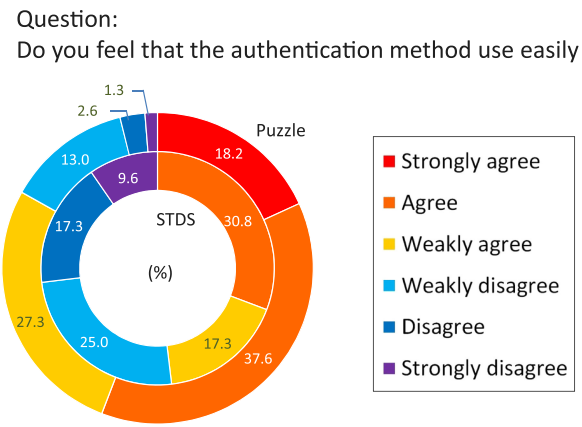

Fig. 3. Rates of user's answers about usability

2. One student was then chosen at random to act as the user.
3. The user sets the authentication information and performed the authentication operation in the presence of the other students.
4. The other students attempted to detect the authentication information by observing the authentication operation.

In the case of PINs and Android Password Pattern, all of student was able to detect the registered panels and locations. In the case of puzzle authentication method, none of student was able to detect the registered panels and locations. Thus, puzzle authentication method has resistant to be observed covertly from others better than PINs and Android Password Pattern.

Next, we compared the usability of puzzle authentication method with STDS method [5] by means of a questionnaire containing a question to 77 users: "Do you feel that the authentication method use easily?" For each method, the question was evaluated using the six ranks: strongly agree, agree, weakly agree, weakly disagree, disagree, and strongly disagree.

Fig. 3 shows the rate of 77 user's answer about the question. Puzzle authentication method has many agree users than STDS method about usability. Thus, puzzle authentication method has high-usability more than STDS method.

4 Conclusion

In this paper, we proposed a puzzle authentication method having shoulder-surfing attack resistance and reinforced usability. In order to enhance resistance to shoulder-surfing attack, the proposed method uses two authentication information: pass-numbers and pass-locations. We then implemented the puzzle authentication method and evaluated it experimentally. The results of our experiments indicate the proposed method has a sufficient level of resistance to shoulder-surfing attacks.

DOI: 10.1587/comex.4.95
Received February 4, 2015
Accepted February 25, 2015
Published March 26, 2015