Personal Identification with Any Shift: Authentication method for smartwatches having shoulder-surfing resistance

Makoto Nagatomo¹, Kazuki Watanabe¹, Kentaro Aburada², Naonobu Okazaki², and Mirang Park¹a)

1 Kanagawa Institute of Technology,
1030 Shimo-Ogino, Atsugi, Kanagawa 243–0292, Japan
2 University of Miyazaki,
1–1 Gakuen-Kibanadai-Nishi, Miyazaki 889–2192, Japan
a) mirang@nw.kanagawa-it.ac.jp

Abstract: Recently, mobile terminals having small touchscreen such as smartwatches are increasing. PIN or pattern lock are used for personal authentication for smartwatches, but it is possible to leak authentication information by peeking the screen because the information is displayed directly. Therefore, in this paper, we propose Personal Identification with Any Shift (PIAS), which user taps different icon from registered icon on 3 × 3 icons. In addition, we implemented PIAS and evaluated it by confirming the usability and shoulder-surfing resistance. As a result, authentication time and success rate was 13.8 s and 89.4%, and the rate of successful shoulder-surfing attack was 0.0%.

Keywords: authentication, shoulder-surfing attack, smartwatch

Classification: Multimedia Systems for Communications

References

[1] Smartwatch Market Expected to Grow 41% in 2018, https://www.futuresource-consulting.com/press-release/consumer-electronics-press/smartwatch-market-expected-to-grow-41-in-2018/, accessed 13 May 2019.
[2] K. A. Siek, Y. Rogers, and K. H. Connelly, “Fat finger worries: How older and younger users physically interact with PDAs,” Proc. of the 2005 IFIP TC13 International Conference on Human-Computer Interaction, pp. 267–280, 2005. DOI:10.1007/11555261_24
[3] M. Tanaka and I. Hiroyuki, “Proposal of improved background pattern slide authentication against shoulder surfing in consideration of convenience,” J. Inf. Process. Soc. Japan, vol. 58, no. 9, pp. 1513–1522, 2017 (in Japanese).
[4] Y. Kita, N. Okazaki, and H. Nishimura, “Implementation and evaluation of shoulder-surfing attack resistant users,” IEICE Trans. Inf. & Syst., vol. J97-D, no. 12, pp. 1770–1784, 2014 (in Japanese).
[5] The Galaxy S8 and Pixel Should Copy LG’s Knock Code, https://www.forbes.com/sites/bensin/2017/03/02/the-galaxy-s8-and-pixel-should-copy-lg’s-knock-code/, accessed 13 May 2019.

[6] I. Oakley, J. H. Huh, J. Cho, G. Cho, R. Islam, and H. Kim, The personal identification chord: A four button authentication system for smartwatches,” ASIACCS’2018, 2018. DOI:10.1145/3196494.3196555

[7] S. G. Hart and L. E. Staveland, “Development of NASA-TLX (task load index): Result of empirical and theoretical research,” Adv. Psychol., vol. 52, no. 3, pp. 139–183, 1988. DOI:10.1016/S0166-4115(08)62386-9

1 Introduction

Recently, mobile terminals having small touchscreen such as smartwatches has been increasing. The shipments of smartwatches are predicted to rise to 66 million by 2022 [1]. Currently, many people use PIN code and pattern lock as personal authentication method for smartwatches. These authentication methods have two problems, shoulder-surfing attacks by peeking on the screen, and fat finger problem [2] which causes the decrease of the usability by difficulty of touching screen.

Tanaka et al. [3] proposed the method that the user inputs authentication characters by moving background color of the matrix having a–z and 0–9 characters on each cell. This method has shoulder-surfing resistance if the authentication color does not leak but it is possible to leak authentication information by several peeking the movement of background colors. STDS [4] is performed by user’s tapping illustration icons different from registered icon on 4 × 4 icons by shift rule in order to strengthen shoulder-surfing resistance. Shift rule separates four groups of 2 × 2 icons, then the user touches icon processed by the registered two shift numbers between groups and in a group. However, the fat finger problem arises if above two methods apply for smartwatches because these are for smartphones, which have larger screen than smartwatches.

In Knock Code [5], the user touches four square regions on the screen of the smartphone. The user can touch correctly when applying for smartwatches because of the large regions. As an authentication method for smartwatches, PIC [6] also has four regions (buttons) on the screen. The user taps buttons using single-tap or dual-tap in authentication phase. Above two methods solve fat finger problem. However, shoulder surfer can obtain authentication information by peeking the screen because tapped regions equals authentication information directly.

Therefore, in this paper, we propose Personal Identification with Any Shift (PIAS) that improves STDS [4] for smartwatches. In our proposed method, the user taps alternative icons to registered icons on 3 × 3 icons by using shift rule in authentication phase. In addition, we implement PIAS and perform experiments to confirm its usability and shoulder-surfing resistance.

2 Personal Identification with Any Shift

We propose Personal Identification with Any Shift (PIAS), an authentication method for smartwatches with shoulder-surfing resistance. As for input interface
in authentication phase, it seems to be easy for users to tap an icon on $3 \times 3$ icons on the smartwatch’s screen, so we set input interface as a $3 \times 3$ icons. In addition, we use simple 0–9, A–Z icons and a shift rule as authentication information. In authentication phase, the user selects the icon proceeded from registered icon by shift number along registered shift rule. The user can decide arbitrary shift number in every first of authentication phase, using first registered icon in order to strengthen resistance against several shoulder-surfing attacks.

Here, we propose three shift rules in Fig. 1 as red arrow (back to the start of arrow when reaching the end of arrow). These three shift rule are as follows.

- Spiral shift (see Fig. 1a)
  This shift proceeds at a right angle when reaching the corners on matrix.
- S-shaped shift (see Fig. 1b)
  This shift proceeds in the opposite direction after going down one line when the shift reaches the corners on matrix.
- Lightning shift (see Fig. 1c)
  This shift proceeds from the left edge end after going down one line when reaching the corners on matrix.

In addition to above three shift rules, the user can choose not to use shift rule (non-shift).

On the digit of registered icons, we decide the digit of icons as 6 or more so that probability of the accidental successful authentication (hereinafter called “accidental authentication probability”) is under $1/10,000$ as well as four-digit PIN code. When the digit of registered icons is $n$, PIAS has $(n-1)$-digit authentication information because first registered icon is used only to decide shift number (0–8) in authentication phase. Hence, accidental authentication probability is $1/9^{(n-1)}$. Hence, the number 6 or more as digit of registered icons is obtained from following equation.

$$1/9^{n-1} \leq 1/10,000 \rightarrow n \geq 6$$  \hspace{1cm} (1)

Registration and authentication procedures are as follows:

**Registration phase:**
1. $4 \times 9$ icons (0–9 and A–Z icons) are displayed.
2. The user taps 6 icons as registration icons.
3. The user selects a shift rule out of 3 rules and non-shift rule.
4. Confirmation screen of registered icons and shift rule is displayed.

**Authentication phase:**
1. $3 \times 3$ icons are displayed. First registered icon includes in these icons.
2. The user selects shift number (0–8) by tapping icon proceeded from registered icon by arbitrary number along registered shift rule.
(3) 3 × 3 icons including registered icon are displayed again. The user selects alternative icon proceeded from registered icon by the shift number along registered shift rule.

(4) Repeat step (3) according to the number of registration digit.

3 Implementation

We implemented the application of PIAS using Java language on AndroidStudio, then deployed on Sony SmartWatch 3, whose screen size is 1.6 inch.

The implemented registration and authentication phase is shown in Fig. 2 when registered icons are \((0, 1, 2, 3, 4, 5)\) and registered shift rule is spiral shift. In registration phase, registration icons outside the screen appear when the user slides the screen down. Registration completes when the user taps REG. button on the confirmation screen. In authentication phase, the user taps alternative icons to registered icons on each screen in order. The application finishes when authentication succeeds, and redoes authentication again from the first authentication step when the authentication fails.

4 Experiments

We perform two experiments to confirm the usability and shoulder-surfing resistance of PIAS. In this paper, we confirm shoulder-surfing resistance of PIAS just by eyes, and will conduct it by video recording in the future. Subjects wear the SmartWatch 3 on the arm opposite to dominant hand, and sit on a chair during the experiments.

4.1 Usability

We confirm the usability of PIAS when using shift rule or not using it. Subjects are 17 Kanagawa Institute of Technology students. Measurement items are authentication success rate, authentication time, and touch success rate that the number of touched correct pass icons over total number of touched icons. Touch success rate is measured in order to confirm whether the fat finger problem is solved.

The experimental procedure is as follows:

(1) We explain about PIAS to the subject.

(2) The subject uses PIAS until getting used to it.
The subject registers 6 icons and a shift rule, then performs authentication 5 times regardless of success or failure.

The subject answers a questionnaire. As a result, average authentication time was 5.3 s and 13.8 s when not using shift rule and using shift rule. In addition, authentication success rate was 98.8% and 89.4%, and touch success rate was 99.8% and 96.2% each. We found that PIAS solved fat finger problem since touch success rate was high.

About questionnaire, subjects answer 6 items (understanding, easy to use, hurry, effort, accomplishment, frustration) based on NASA-TLX [7]. The 6 items are valued from 0 to 100 points by subjects, and mental workload is high when these items are high. Fig. 3a shows the average value of each item. We found that PIAS was easy to understand, but the items of effort and frustration were high when using shift rule because the subject must count shift number during authentication. However, taking into account of continuous use in real life, we expect that above two items decrease close to values without shift rule because the user gets used to counting shift number.

4.2 Shoulder-surfing resistance

We perform shoulder-surfing resistance check testing by comparing PIAS using shift rule with pattern lock deployed on SmartWatch 3 by default. Subjects are 12 Kanagawa Institute of Technology students. The experimental procedure is as follows:
(1) We organize a pair of 2 subjects, and decide a parent from the pair.

(2) The parent registers authentication information (patternlock: pattern on 3 × 3 dots, PIAS: 6 icons and a shift rule).

(3) The parent (user) performs 10 successful authentications. The other subject (shoulder surfer) predicts authentication information by peeking the screen. Here, the shoulder surfer can take note during the authentication.

(4) We switch the parent, and repeat step (2) and (3).

Fig. 3b shows leaked rate of authentication information in pattern lock. The authentication information leaked until 6th attack, in particular, the information leaked at rate of 58.3% at the first attack. The percentage of leaked authentication information on PIAS in 10 attacks is shown in Fig. 3c. No authentication information leaked at the rate of 75% (0-digit leaked). In addition, The maximum leaked information was 2-digit regardless of 10 attacks. Therefore, we found that PIAS has higher shoulder-surfing resistance than that of pattern lock.

5 Conclusion

In this paper, we proposed PIAS, a personal authentication method having shoulder-surfing resistance for smartwatches, which uses 3 × 3 icons as input interface and shift rule. In addition, we evaluated its usability and shoulder-surfing resistance. The authentication time and success rate of PIAS were 13.8 s and 89.4%, and touch success rate was 96.2%. Therefore, we found that PIAS solved fat finger problem. As a result of shoulder-surfing resistance, all authentication information did not leak regardless of 10 attacks. This indicates that PIAS has high shoulder-surfing resistance.

As future work, we will evaluate recording attack and perform continuous experiment assuming real life use.

Acknowledgments

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