Secure and Usable PIN-Entry Method with Shoulder-Surfing Resistance

Mun-Kyu Lee and Hyeonjin Nam

School of Computer and Information Engineering,
Inha University, Incheon 402-751, Korea
mklee@inha.ac.kr, jin0639@hanmail.net

Abstract. We propose a new PIN-entry method which prevents shoulder surfing attacks effectively. The proposed method uses a random mapping between the PIN digits and alphabets given as challenges to the users. The user's task is to recognize this mapping and to enter the mapped alphabet sequence instead of directly entering the PIN digits. The intuitive nature and easy interface of the proposed scheme enables the users to learn it easily, and the experimental results in the pilot test show that the new method guarantees fast and reliable authentication. To be precise, the average authentication time was 5.8 to 6.8 seconds, and the average error rate was 3.3 to 6.7%.

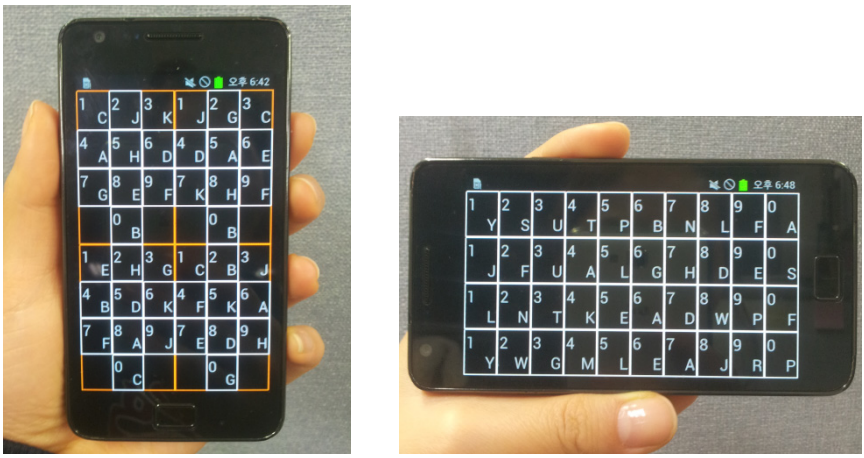
Keywords: user authentication, personal identification number, shoulder surfing attack.

1 Introduction

The personal identification number (PIN) is a well-known user authentication method used in many devices such as a smartphone, ATM, and an electronic doorlock. However, the regular PIN-entry method is quite vulnerable to the shoulder surfing attack (SSA) because its layout is fixed and the user always inputs the same information based on the PIN. To solve this problem, there have been various proposals for countermeasures involving random challenges and user's appropriate responses calculated from the secret PIN digits [1-7]. Those countermeasures require users either to perform complicated mental tasks or to use secondary channels to recognize audio and tactile information. Obviously, those proposals increase the authentication time and raise the rate of erroneous input, significantly degrading the usability of PIN-entry scheme.

We propose a new PIN-entry method without any secondary channel. We performed a pilot test with various settings. According to the experimental results, the authentication time is only twice the regular PIN-entry method and significantly faster than those of the existing SSA-resistant methods. In addition, the error rate is much lower than those of the existing methods.

C. Stephanidis (Ed.): Posters, Part II, HCII 2013, CCIS 374, pp. 745–748, 2013.



(a) portrait mode (4 regular PIN pads) (b) landscape mode (4 rows of linear pads)

Fig. 1. The challenge stage where random mappings between PIN digits and characters are given

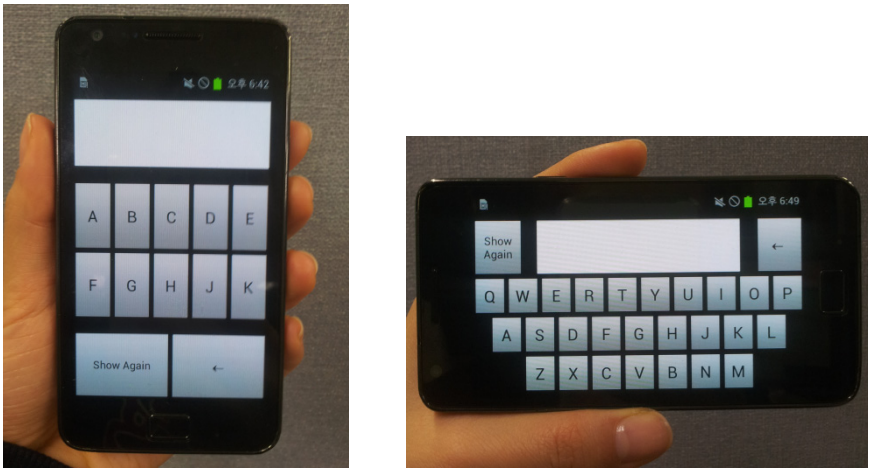
2 Proposed PIN-Entry Method

The proposed method is composed of two stages; the challenge stage and the response stage. In the first stage, the user is given a challenge screen which provides a random mapping between the user's PIN digits and alphabet characters. In the example of Fig. 1(a), the user may find 4 regular PIN pads where each digit is associated with a character. Each of the 4 PIN pads are for each PIN digit. To be precise, the top left PIN pad is for the first PIN digit and the top right for the second. The bottom left PIN pad is for the third PIN digit and the bottom right for the final PIN digit. The required task of the user in this stage is to recognize this mapping and memorize the characters associated with his/her PIN digits. For example, let us assume that the PIN is 3146. Then, the matching character sequence is KJBA. For security reasons, this association between PIN digits and characters should be randomized for each authentication session.

The alphabets given as challenges may be selected from either the whole alphabet set (26-character mode) or the set of only 10 characters, A, B, C, D, E, F, G, H, J, and K (10-character mode). We do not consider the character 'I', because it may confuse the user with the digit, '1.' The example in Fig. 1(a) shows the 10-character mode.

We also may use a completely different layout such as Fig. 1(b). In this layout, the digits are not arranged as those of a PIN pad, but they are arranged in a row. To provide a complete mapping for a 4-digit PIN, the challenge screen is composed of 4 rows. In this example, if the user's PIN is 3146, the matching sequence will be UJKE. We name the layouts in Fig. 1(a) and Fig. 1(b) as a portrait mode and a landscape mode, respectively. In total, there are 4 combinations of modes (portrait vs. landscape as well as 26 vs. 10) which can be pre-configured according to the user's preference.

When the user touches any region in the screen in the first stage, the second stage begins. In this stage, the user inputs the 4 characters through a keypad (Fig.2).



(a) 10-character mode (b) 26-character mode

Fig. 2. The response stage: One of (a) and (b) is performed according to the alphabet set given as the challenge in the previous stage

3 Performance Analysis

We performed a pilot test with various settings. According to the experimental results given in Table 1, the authentication time is 5.8 to 6.8 seconds, which is significantly faster than those of the existing SSA-resistant methods. The error rate is 3.3 to 6.7%, which is much smaller than those of the existing methods. What is more encouraging is that the data in Table 1 were measured from participants who were not sufficiently trained for the new method. We may expect that the time and error rate should be improved if the users become accustomed to the new method.

According to Table 1, the first and second stages seem to consume almost the same amount of time. Therefore, we cannot point out a specific bottleneck in our method which could have been a target for optimization. However, the data in Table 1 shows us non-negligible correlation between the performance and the configuration modes. Therefore, in our future research, we will find the optimal combination though extensive experiments involving a wide range of users. In addition, other factors that may affect the performance should be analyzed precisely. These factors include the font of digits and characters which decides the recognition speed of the user, and the size and arrangements of touch buttons which decide the amount of movement of fingers.

Regarding the security against shoulder surfing, the proposed method is significantly more secure than the regular PIN pad, because an ordinary human attacker cannot completely memorize the instant mapping shown in the challenge stage which lasts for only about 3 seconds. However, it would be desirable that this claim should

be verified by experiments involving real human attackers, especially educated ones, which will be included in our future research. We also remark that the proposed method does not prevent recording attacks.

Table 1. Performance Comparison (Authentication Time and Error Rate)

Method		Stage 1 (sec)	Stage 2 (sec)	Total time (sec)	Error rate (%)
Existing	Regular	-	-	approx. 3	approx. 0
	Binary [1]	-	-	23.2	9.0
	Undercover [2]	-	-	32-45	> 31.5
	VibraPass [3]	-	-	8.2	> 14.8
	Haptic Wheel [4]	-	-	23.0	16.4
	ColorPIN [5]	-	-	13.3-13.9	N.A.
	Phone Lock [6]*	-	-	12.2	4.8(+6.9)
	SpinLock [7]*	-	-	10.8-16.9	3.3(+64.0)
Proposed**	L/26	3.8	3.0	6.8	6.7
	L/10	3.2	3.2	6.4	3.3
	P/26	3.6	3.1	6.7	3.3
	P/10	2.9	2.9	5.8	6.7

* Among the audio and tactile versions, we only consider the audio versions, which are more practical ones. ** L vs. P: landscape vs. portrait modes, 26 vs. 10: 26 vs. 10-character modes.

Acknowledgments. This research was supported by the MSIP, Korea, under the ITRC support program (NIPA-2013-H0301-13-1003) supervised by the NIPA and the IT R&D program of MOTIE/KEIT (10039180).

References

1. Roth, V., Richter, K., Freidinger, R.: A PIN-entry method resilient against shoulder surfing. In: Proceedings of the 11th ACM Conference on Computer and Communications Security, pp. 236–245 (October 2004)
2. Sasamoto, H., Christin, N., Hayshi, E.: Undercover: Authentication Usable in Front of Prying Eyes. In: CHI 2008, pp. 183–192 (April 2008)
3. Luca, A.D., Zezschwitz, E.V., Hußmann, H.: VibraPass-Secure Authentication Based on Shared Lies. In: CHI 2009, pp. 913–916 (April 2009)
4. Bianchi, A., Oakley, I., Lee, J.K., Kwon, D.S.: The Haptic Wheel: Design & Evalua-tion of a Tactile Password System. In: CHI 2010, pp. 3625–3630 (April 2010)
5. Luca, A.D., Hertzschuch, K., Hussmann, H.: ColorPIN – securing PIN entry through indirect input. In: CHI 2010, pp. 1103–1106 (April 2010)
6. Bianchi, A., Oakley, I., Kostakos, V., Kwon, D.S.: The Phone Lock: Audio and Haptic Shoulder-Surfing Resistant PIN Entry Methods for Mobile Devices. In: TEI 2011, pp. 197–200 (January 2011)
7. Bianchi, A., Oakley, I., Kwon, D.S.: Spinlock: A single-cue haptic and au-dio pin input technique for authentication. In: Cooper, E.W., Kryssanov, V.V., Ogawa, H., Brewster, S. (eds.) HAID 2011. LNCS, vol. 6851, pp. 81–90. Springer, Heidelberg (2011)