Contemporary Engineering Sciences, Vol. 8, 2015, no. 17, 747-755
HIKARI Ltd, www.m-hikari.com
http://dx.doi.org/10.12988/ces.2015.56164

A Simple PIN Input Technique Resisting Shoulder Surfing and Smudge Attacks

Il-Soo Jeon

School of Electronic Engineering, Kumoh National Institute of Technology
77 Sanho-Ro, Yangho-Dong, Gumi, Kyungsangpuk-Do 730-701, South Korea

Eun-Jun Yoon*

Department of Cyber Security, Kyungil University
33 Buho-Ri, Hayang-Ub, Kyungsan-Si, Kyungsangpuk-Do 712-701, South Korea
*Corresponding author

Abstract

The authentication method which uses Personal Identification Number (PIN) is widely used in these days. The user authentication through the input of password is a well-known authentication method such as in Automatic Teller Machines (ATMs), mobile phones, smartcards, and digital door locks. However, the authentication method is vulnerable to shoulder-surfing attacks and smudge attacks. Therefore, this paper proposes a new simple PIN input technique (SPIT) resisting the attacks by using the non-visual sound channel which does not sacrifice the probability of random guessing attacks. Since the user interface of the proposed SPIT is very simple and the input method of PIN is so easy, SPIT can be used as the authentication method such as in ATMS, mobile phones, and digital door locks. Especially the user interface of SPIT is simple enough to be used for children, the weak and the elderly, and visually impaired persons.

Keywords: PIN, Authentication, Shoulder Surfing Attack, Smudge Attack, Sound Cue

1 Introduction

It is widely used personal identification number (PIN) input as the method of

user authentication. Four digit numbers are usually used to authenticate users in ATMs and credit cards, and in case of smartphones and digital door locks, similar way is applied to authenticate the devices. Since the authentication method is convenient to the users, it will be still used in the future. However, since the authentication method is vulnerable to the shoulder-surfing attacks and smudge attacks, it can get tremendous losses to the users in the aspect of money or privacy.

The shoulder-surfing attack is performed by observing the PIN input processing over the user's shoulder to obtain the PIN of the user. Another attack of this type is recording attack which is performed by replaying the moving image that is recorded around the user using the attacker's smartphone. Even if the attacker does not exist around the user, the attack is possible by the installing of a hidden camera. The smudge attack is performed by observing smudge caused by the finger marks on the touchscreen or digital door locks' keypad of those devices. The numbers composing PIN can be guessed easily by the combination of the numbers that have much smudge on the buttons. There is another PIN acquisition attack using key-logger program which is secretly installed in the user's terminal by the attacker. The attacker can acquire the user's PIN by capturing all the key inputs.

To countermeasure shoulder-surfing attacks, recording attacks, and smudge attacks, various PIN input techniques [1-10] are proposed. This paper proposes a new simple PIN input technique (SPIT) that resists effectively those attacks. The proposed SPIT uses the non-visual sound channel to resist the attacks. However, it does not sacrifice the probability of random guessing attacks. SPIT has very simple user interface, good security, and very convenient usage compared to the existing research results that uses non-visual sound or tactile cues to authenticate users via PIN entry.

The rest of this paper is organized as follows. In the following section, we describe The Phone Lock system which is a representative research using the sound channel as related research. Then in section 3, we present a new simple PIN input technique, SPIT using the sound channel. In section 4, we discuss the security analysis and performance evaluation of SPIT. Finally in section 5, the conclusion is given.

2 Related Research

In the PIN authentication methods, since they are not secure from the shoulder-surfing attacks, the recording attacks, and the smudge attacks, recently some PIN input techniques[1-7] have been proposed using non-visual channel such as sound channel or vibration channel to resist those attacks. We introduce a PIN input method, The Phone Lock [7], proposed by Bianchi et al. as the related research of ours. The method of Bianchi et al. is estimated one of the outstanding methods which use sound cues or tactile cues [11]. The Phone Lock can use both sound cues and tactile cues. However, we introduce only the sound based technique that has better performance than tactile based one.

Fig. 1 shows the PIN input pictures in The Phone Lock. As we can see at Fig. 1, The Phone Lock displays 10 same shaped targets on the touchscreen. Each target is mapped to a random sound cue between 0 and 9. Even though each target is mapped to a sound cue randomly, the numbers mapped to the targets have to be sequential order according to the predetermined direction. For example, if the sound of 5 was heard to the user when the target was touched like in the left side picture of Fig.1, the sound cues of both sides of the target will be 4 and 6. If a target is touched and the sound cue of the target does not match to the digit of PIN which is to be entered, the user have to move to another target by moving one or more than one target until seeking the target matched to the digit of PIN being entered. If the sound cue matches to the digit of PIN is to be entered, the user drags the target to the center circle and takes his/her finger off from the touchscreen and then finishes one digit input of PIN. Whenever each digit of PIN is inputted, the sound cue of each target has to be randomized. Whenever randomized, the sound cues mapped to the targets always keep to be sequential order according to the predetermined direction. The Phone Lock system requires users to put on an earphone not to be heard the sound cues to the persons around them.

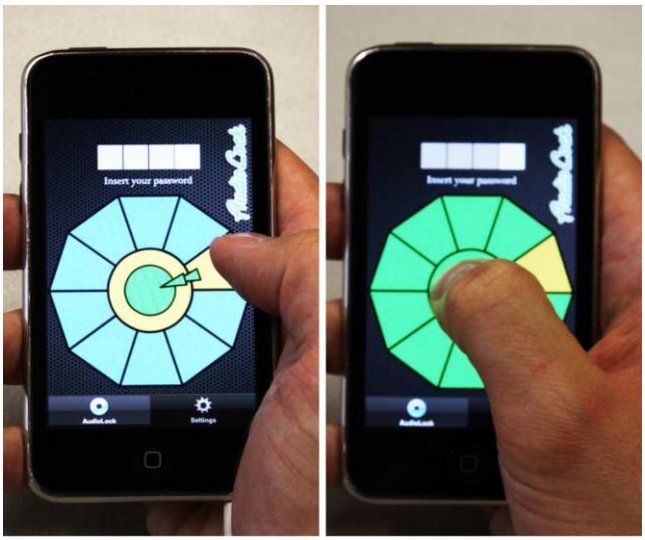

Fig. 1 PIN Input of the Phone Lock [7]

Even if an attacker does observation attacks such as shoulder-surfing attacks or recording attacks for The Phone Lock system, he/she cannot succeed because he/she cannot hear the sound cues heard to the users through the earphone and each target is mapped to a sound cue randomly every digit input of PIN. In addition, since The Phone Lock system does not leave a particular pattern of smudge, the system is safe from the smudge attacks. Therefore, The Phone Lock system is considered as a practical PIN input technique that can resist the shoulder-surfing attacks, recording attacks, and smudge attacks.

3 Proposed Simple PIN Input Technique(SPIT)

In this section, we propose a new simple PIN input Technique, SPIT which can resist the shoulder-surfing attacks, recording attacks, and smudge attacks by using non-visual sound cues like in The Phone Lock. Unlikely The Phone Lock, the proposed SPIT uses not 10 targets but only 1 target to receive each digit of PIN. To receive each digit of PIN, SPIT system prepares a list which is composed of randomized distinct 10 numbers between 0 and 9. If a user touches the target, the system tells the user a sound cue corresponding to the first item's number of the list through user's earphone. If the sound cue is different from the digit of PIN to be inputted, the user repeats touching the target. Whenever the user touches the target again, the system tells the sound cue corresponding to the next item's number of the list through the user's earphone. While these processing, if the user hear the sound cue of the digit to be inputted, then he/she keeps touching the screen and slides his/her finger and finishes one digit input of PIN. Whenever a new digit is inputted, the system uses a new list that is randomized with the distinct 10 numbers again.

Fig. 2 shows an example of user interface of the proposed method that uses 4 digit numbers as PIN. The left side picture of Fig. 2 is initial screen of SPIT to input the first digit of PIN. The right side of Fig. 2 represents the screen state to input the second digit after completing the first digit input. In Fig. 2, four rectangles located at the upper side of the pictures represent each digit composing PIN respectively. The empty circle in a rectangle represents the digit that is to be entered, and the filled circle represents the digits that have been already entered. The big rectangles located in the middle side of the pictures are the target which receives PIN input. There are three buttons positioning bottom side of the pictures. The OK button is used to execute an authentication after completing the PIN input, and the BACK button is used to delete one digit just before entered digit, and the CANCLE button is used to delete all the entered digits and to exit the authentication process.

The three buttons can be eliminated by the replacing of the directed finger's sliding of users. Assume the direction of finger's sliding is from the left to the right on the target to input one digit of PIN. The BACK button can be replaced by the finger's sliding from the right to the left on the target, and the CANCEL button can be replaced by the finger's sliding from the right to the left on the target. The OK button does not need to be replaced by any finger's sliding if automatic authentication process is initiated after the completion of PIN input. If the three buttons is eliminated, the user interface of SPIT will be very simple and the target can be widen.

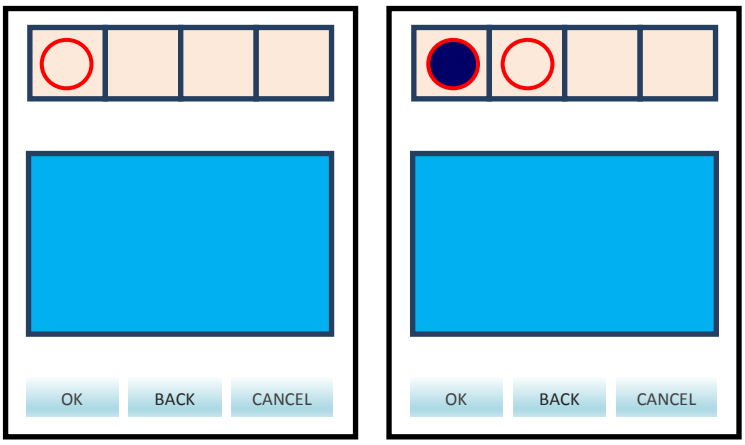

Fig. 2 PIN Input Interface of SPIT

The user interface of SPIT can be implemented as in Fig. 2 in case of ATMs and smartphones. In case of digital door locks, SPIT can be implemented by two buttons instead of existing 10 buttons. One button is used for target button, and the other button is used for the finger's sliding when the sound cue is matched to the digit to be entered.

Unlikely The Phone Lock, the proposed SPIT has very simple user interface and easy to use in various devices. Therefore, it can be applied to implement the interface of PIN input that is aimed at for children, the weak and the elderly, and especially visually impaired persons.

4 Security Analysis and Performance Evaluation

4.1 Security Analysis

In this section, we analyzed the security and privacy of the proposed DRAPLT protocol. The basic structure of the proposed protocol is similar to that of RAPLT except that it contains distance bounding protocol property. Therefore, DRAPLT can resist the various attacks which can be prevented in RAPLT, and additionally resist the relay attacks.

- **Shoulder-Surfing Attack**

Since the users hear the sound cues through an earphone, any attackers cannot hear the sound cues and cannot guess a part or the whole of the PIN through shoulder-surfing over the users. Therefore SPIT is secure enough from the shoulder-surfing attacks.

- **Recording Attack**

Even if an attacker records the whole process of PIN input using smartphones or cameras, he/she cannot know the PIN because there is no sound cues in the record-

ed moving image. So the attacker can get no information for PIN guessing. Therefore, SPIT can resist the recording attacks.

- **Smudge Attack**

Since SPIT uses only one target for PIN input, it is impossible to guess using the smudge caused by fingers. Therefore, SPIT is safe from the smudge attacks.

- **Random Guessing Attack**

The success probability of random guessing attack for a PIN composed of 4 digits is 1/10000. Even though attackers observe the PIN input process over the user's shoulder or they use hidden cameras to record the PIN input processing, the success probability of guessing for the PIN under SPIT environment is also 1/10000. Since the touching count of the target does not have any relation with the value of each digit, the guessing probability of each digit is 1/10, and the guessing probability of all digits is 1/10000. Therefore, SPIT does not need to sacrifice the probability of random guessing.

4.2 Performance Evaluation

Lee [12] proposed four criteria for the design of PIN input system: security, usability, compatibility, and cost-effectiveness. In this paper, we propose an additional one criteria, simplicity, for more detailed evaluation. The specific explanation of the five criteria is as followings.

- Security: The system has resistance for the various attacks such as shoulder-surfing attacks, recording attacks, smudge attacks, and random guessing attacks.
- Usability: The usage of PIN input method is intuitive and easy, so operation time for an authentication should be short and error rate of authentication should be low.
- Compatibility: The system does not change the definition of currently used PIN but only change the PIN input interface. However, if it is used limited applications such as smartphones or digital door locks, it is possible to redefine the definition of PIN.
- Cost-effectiveness: It is recommended not to use additional expensive equipment such as extra eye-gaze [13,14], BCI (Brain-computer Interface) [15] but to use the interface of the attached systems or terminal devices.
- Simplicity: The user interface should be designed simple enough to be easily used for the visually impaired persons, children, and the weak and the elderly.

In Table 1, we evaluated the performance of The Phone Lock and SPIT using the five criteria described above. The evaluation is a little subjective but it is considered objective for relative evaluation of the two methods in each criteria. As we can see from the table 1, both methods have high performance for security, compatibility, and cost-effectiveness. However, proposed SPIT has better perform-

ance than The Phone Lock for usability and simplicity. Therefore, SPIT can be applied to a practical PIN input technique such as ATMs, smartphones, and digital door locks, etc.

Table 1. Comparisons of Performance

Technique / Comparison factor	The Phone Lock[7]	SPIT
Security	high	high
Usability	middle	high/middle
Compatibility	high	high
Cost-effectiveness	high	high
Simplicity	middle	high

5 Conclusions

In this paper, we proposed a new simple PIN input technique, SPIT that can resists shoulder-surfing attacks, recording attacks, and smudge attacks. The proposed SPIT uses non-visual sound cues and does not sacrifice the probability of random guessing attacks. Furthermore, SPIT has very simple user interface and easy enough to input PIN. Therefore, the proposed SPIT can be usefully applied as PIN input method for easily vulnerable devices (ATMs, smartphones, and digital door locks) from shoulder-surfing attacks, recording attacks, and smudge attacks. Since the user interface of SPIT has 1 target not 10 targets, and the input of each PIN digit is simply done by touching the target, it can be used for children, the weak and the elderly, and visually impaired persons.

Acknowledgements. This paper was supported by Research Fund, Kumoh National Institute of Technology.

References

[1] H. Sasamoto, N. Christin and E. Hyashi, Undercover: Authentication usable in front of prying eyes, *Proc. CHI*, (2008), 183 - 192. http://dx.doi.org/10.1145/1357054.1357085

[2] A. D. Luca, E. von Zezschwitz, and H. HuBmann, Vibrapass: Secure authentication based on shared lies, *Proc. CHI*, (2009), 913 - 916. http://dx.doi.org/10.1145/1518701.1518840

[3] T. Perković, M. Čagalj and N. Rakić, SSSL: Shoulder surfing safe login, *Pro. Int. Conf. Softw., Telecommun. Comput. Netw.*, (2009), 270 - 275.

[4] A. Bianchi, I. Oakley, J.K. Lee and D.S. Kwon, The haptic wheel: Design & evaluation of a tactile password system, *Proc. CHI*, (2010), 3625 - 3630. http://dx.doi.org/10.1145/1753846.1754029

[5] A. Bianchi, I. Oakley and D. S. Kwon, The secure haptic keypad: A tactile password system, *Proc. CHI*, (2010), 1089 - 1092. http://dx.doi.org/10.1145/1753326.1753488

[6] A. Bianchi, I. Oakley and D. S. Kwon, Spinlock: A single-cue haptic and audio PIN input technique for authentication, HAID, *Lecture Notes in Computer Science*, **6851** (2011), 81 - 90. http://dx.doi.org/10.1007/978-3-642-22950-3_9

[7] A. Bianchi, I. Oakley, V. Kostakos and D. S. Kwon, The phone lock: Audio and haptic shoulder-surfing resistant PIN entry methods for mobile devices, *Proc. TEI*, (2011), 197 – 200. http://dx.doi.org/10.1145/1935701.1935740

[8] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze and J. M. Smith, Smudge attacks on smartphone touchscreens, *Proc. 4th USENIX Conf. Offensive Technol. WOOT*, **7** (2010), 1 - 10.

[9] E. von Zezschwitz, A. Koslow, A.D. Luca and H. Hussmann, Making graphic-based authentication secure against smudge attacks, *Proc. IUI*, (2013), 277 - 286. http://dx.doi.org/10.1145/2449396.2449432

[10] T. Kwon and S. Na, TinyLock: Affordable defense against smudge attacks on smartphone pattern lock systems, *Computers & Security*, **42** (2014), 137 - 150. http://dx.doi.org/10.1016/j.cose.2013.12.001

[11] M. K. Lee, Security notions and advanced method for human shoulder-surfing resistant PIN-entry, *IEEE Transactions on Information Forensics and Security*, **9** (2014), 695 - 708. http://dx.doi.org/10.1109/tifs.2014.2307671

[12] M. K. Lee, A user interface for secure personal identification number input, *Journal the Korea Institute of Information Security and Cryptology*, **24** (2014), 27 - 35.

[13] M. Kumar, T. Garfinkel, D. Boneh and T. Winograd, Reducing shoulder-surfing by using gaze-based password entry, *Proc. SOUPS*, (2007), 13 - 19. http://dx.doi.org/10.1145/1280680.1280683

[14] A. Forget, S. Chiasson and R. Biddle, Shoulder-surfing resistance with eye-gaze entry in cued-recall graphical passwords, Proc. CHI, (2010), 1107 - 1110. http://dx.doi.org/10.1145/1753326.1753491

[15] J. Thorpe, P. van Oorschot and A. Somayaji, Pass-thoughts: Authentication with our minds, *Proc. NSPW*, (2005), 45 - 56. http://dx.doi.org/10.1145/1146269.1146282

Received: June 19, 2015; Published: July 27, 2015