Contemporary Engineering Sciences, Vol. 10, 2017, no. 5, 203 - 210
HIKARI Ltd, www.m-hikari.com
https://doi.org/10.12988/ces.2017.612194

An Enhanced Simple PIN Input Technique Resisting Shoulder Surfing and Smudge Attacks

Il-Soo Jeon and Myung-Sik Kim[*]

School of Electronic Engineering, Kumoh National Institute of Technology
61 Daehak-ro, Gumi-si, Gyeongbuk-do 39177, South Korea
[*]Corresponding author

Abstract

PIN (personal identification number) is widely used as the method of user authentication. PINs composed of four digit passwords are usually used to authenticate users such as in automatic teller machines (ATMs) or mobile phones. The authentication method using PIN is also widely used to unlock the digital door-locks. However, the authentication method using PIN is vulnerable to shoulder-surfing and smudge attacks. To overcome those attacks, some authentication methods are proposed by using non-visual channels such as sound or vibration. Recently, Jeon and Yoon [1] proposed a very simple PIN input technique (SPIT) by using sound cue. The user interface of SPIT is simple enough to be used for children, the weak and elderly, and even the visually impaired person. However, the success rate of PIN input is relatively low especially for visually impaired persons. Therefore, this paper proposes an improved authentication method of SPIT to reduce the PIN input errors. The proposed method uses four different object groups, and each object group contains ten distinct items.

Keywords: PIN, Authentication, Shoulder Surfing Attack, Smudge Attack, Sound Cue, Visually Impaired Person

1 Introduction

Biometric authentication systems using iris or fingerprints are gradually increasing for secure and strong authentication of entities these days. However, personal identification number (PIN) has been used for a long time and is still widely used as the method of user authentication. To authenticate users, passwords of four-digit-number are usually used in ATMs and credit cards. Since the authentication method of PIN input is so simple and convenient, it will be still used in future. However, the authentication method is vulnerable to the shoulder-surfing attacks, recording attacks, and smudge attacks.

The shoulder-surfing attack is performed by observing the PIN input process 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 hidden camera installed. The smudge attack is performed by observing the smudge caused by the finger marks on the touchscreen or digital door locks’ keypad. 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. [1]

To overcome the weaknesses of the authentication method using PIN input, various PIN input techniques [1-15] are proposed. Some researches [7-12] use non-visual channel like sound or vibration, and they seem to be a good solutions. Recently, Jeon and Yoon [1] proposed a very simple PIN input technique (SPIT) by using sound cue. However, in SPIT, the rate of PIN input error is relatively high especially for visually impaired persons. This paper proposes an improved authentication method of SPIT that reduces the error rate of PIN input. The user interface of the proposed scheme is so simple that it is especially useful for visually impaired persons.

The rest of this paper is organized as follows. In the following section, we briefly describe The Phone Lock and SPIT system as related research. Then in section 3, we present the proposed scheme in this paper. In section 4, we discuss the security analysis and performance evaluation of the proposed scheme. Finally in section 5, the conclusion is given.

2 Related Research

As related researches, we briefly describe two authentication methods that can resist the shoulder-surfing attacks, the recording attacks, and the smudge attacks.

The Phone Lock [8] is one of the feasible PIN input techniques. This system uses sound cues and requires users to put on an earphone. As the PIN input screens of The Phone Lock are shown in Fig. 1, The Phone Lock displays ten identical targets on the touchscreen. Each target is mapped to a random sound cue from 0 to 9. Although each target corresponds to a sound cue arbitrarily, the numbers mapped to the targets must be in sequential order according to the predetermined direction. When a target is touched, and the sound cue matches the number of PIN digit, the user drags the target to the center circle and takes his/her finger off of the screen to complete entering one digit of PIN. If the sound cue does not match the digit of PIN that is to be entered, the user have to move to another target and seek for the right one. Before each digit of PIN is entered, the sound cue that is mapped to each target has to be randomized.

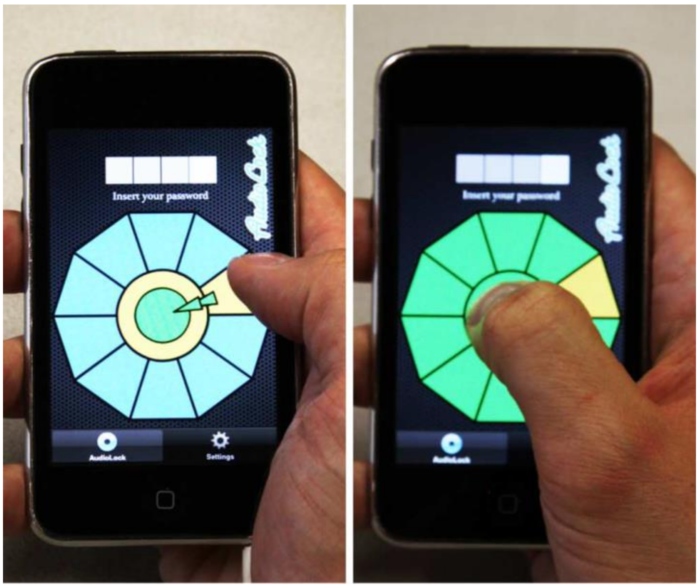

Fig. 1. PIN Input of The Phone Lock

Recently, Jeon and Yoon [1] introduced a simple PIN input technique, SPIT, using sound cues just like The Phone Lock. Unlike The Phone Lock, SPIT only uses one target as shown in Fig. 2 to receive each digit of PIN. SPIT system develops a list that are randomly composed of ten numbers from 0 to 9. When the user touches the target on the screen to enter each digit of PIN, the system speaks the sound cue that corresponds to the first item’s number on the list to the user through the earphone. If the sound cue that is heard does not match to the digit to be entered, the user repeats touching the target, and the system moves on to the next item’s number of the list and speaks each corresponding sound cue to the user. During this process, when the user hears the sound cue that matches the digit of PIN to be entered, the user keeps his/her finger on the screen and slides to the side to complete the input of one digit of PIN. Whenever one digit of PIN is entered, the system develops a new list that is randomized with ten numbers from 0 to 9.

Fig. 2 shows an example of user interface of SPIT that uses four digit numbers as PIN. Four rectangles located at the upper side of the pictures represent each digit of PIN respectively, and the big rectangles located in the middle of the pictures is the target that receives PIN input. The left picture of Fig. 2 is the initial screen of SPIT to input the first digit of PIN, and the right picture represents the screen state where the second digit is to be entered after completing the first digit input. 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. There are three buttons located on the bottom side of the pictures. The OK button executes an authentication after completing the PIN input, the BACK button deletes one digit that was entered just before, and the CANCLE button deletes all entered digits and exits the authentication process. Those buttons can be replaced by directed finger sliding of users.

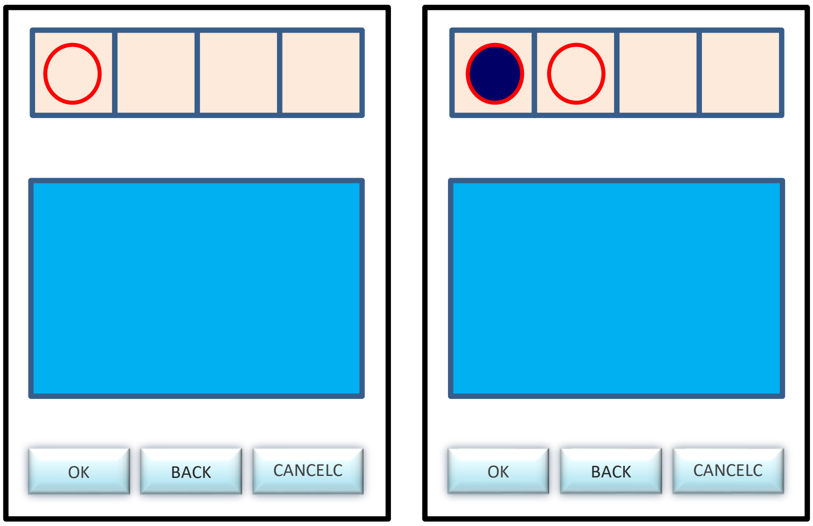

Fig. 2. User Interface of SPIT

Unlike The Phone Lock, the proposed SPIT has very simple interface and is especially convenient for visually impaired persons.

3 Proposed Enhanced PIN Input Technique, ESPIT

SPIT is a useful authentication method to resist the shoulder-surfing attacks, recording attacks, and smudge attacks, and its interface is good to be used especially for visually impaired persons. However, while it is easy to enter the first digit of PIN, entering the rest of the digits can be confusing. Since the user has to touch the screen multiple times to enter one digit of the PIN, this can cause confusion to the user whether he/she is entering the second digit, third digit, or forth digit. This phenomenon is harsh to visually impaired persons, for they have difficulties to see the upper-side rectangles in Fig.2 that represents the status of which digit was entered and is being entered. Consequently, we can say that the probability of input error can be high in SPIT.

Therefore, we propose an Enhanced Simple PIN Input Technique (ESPIT) which improves the weakness of SPIT discussed above. The main idea of ESPIT that we propose is to keep one of the four digits as a number and change the rest three digits into each object from different object groups. For example, the user can choose one of the ten different color items instead of the second number digit of PIN, and choose a fruit from the ten fruit items instead of the third number, and instead of the forth number of PIN, the user can choose one of the ten items of body parts. The list of ten items of color, fruits, and body parts are shown in Table 1.

Table 1. Items of Each Object

Number	Color	Fruit	Body Part
0	White	Apple	Head
1	Black	Orange	Eye
2	Gray	Banana	Nose
3	Red	Grape	Mouth
4	Green	Peach	Ear
5	Blue	Pear	Neck
6	Yellow	Strawberry	Hand
7	Brown	Tomato	Foot
8	Purple	Mango	Arm
9	Pink	Melon	Leg

In ESPIT, the user can choose one item from each object group that is suggested from Table 1 and registers as his/her PIN. For entering one digit of PIN, the system develops the randomized list for the items of each object. Whenever the user touches the target on the screen, the system speaks one item to the user through earphone according to the order of the list that was developed. When the user hears the sound cue that matches the item that he/she registered, the user slides his/her finger on the screen to complete input of one digit of PIN.

The order of digits of PIN mattered in SPIT, but the order between each object group does not matter in ESPIT, because all the objects are different from each other, and the user will intuitively know which item belongs to which object group. Therefore, the proposed ESPIT can be used as an effective PIN input technique that can easily overcome the weakness of SPIT. This property also can contribute to easy extension of additional digits composing the PIN. For example, we can add ten sports items as an object group to make five-digit-PIN. However, in current PIN input techniques, it is not easy to add additional digit, because as the number of digits increases, it gets harder to memorize the PIN.

4 Security Analysis and Performance Evaluation

Just like SPIT, ESPIT uses sound channel, and therefore it is a PIN input technique that can resist to shoulder-surfing attacks, recording attacks, and smudge attacks. Since the number of target touched have no relation with the item of each object group in ESPIT, the guessing probability of one object group is 1/10, and the guessing probability of all four object groups is 1/10000. Therefore, ESPIT has the same random guessing probability of PIN input techniques using four digit numbers. Moreover, unlike other techniques, ESPIT can extend additional digits easily for there is no burden of memorizing extended PIN, and this property can only increase the resistance to random guessing attack.

Lee [16] proposed four criteria for the design of PIN input system: security, usability, compatibility, and cost-effectiveness. Jeon and Yoon [1] proposed an additional criterion, simplicity, for more detailed evaluation. In Table 2, we evaluated the performance of The Phone Lock, SPIT, and ESPIT using the five criteria described above. Even though the evaluation can be subjective, it can be used for relative evaluation of those three methods in each criteria. As we can see from table 2, ESPIT is overall outstanding compared to other methods. Lower input error rate in ESPIT compared to SPIT is reflected in Usability criterion in table 2.

As a result, the proposed ESPIT can be applied to a practical PIN input technique such as ATMs, smartphones, digital door locks, and etc. This is not only a strongly secured PIN input technique but also a useful PIN input technique for children, the weak and elderly, and especially visually impaired persons.

Table 2. Comparisons of Performance

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

5 Conclusion

In this paper, we proposed an Enhanced Simple PIN Input Technique, ESPIT. Just like SPIT, ESPIT not only can resist shoulder-surfing attacks, recording attacks, and smudge attacks, but also has very simple user interface and is easy enough to input PIN. Moreover, ESPIT has lower error rate of PIN input than that of SPIT, and it is also more flexible in expanding number of digit composing PIN. Therefore, the proposed ESPIT can be practically used as PIN input method for ATMs, smartphones, digital door-locks, and etc. Especially, since the PIN of ESPIT is easy to memorize and use, it is a very helpful PIN input method to children, elders, and visually impaired persons.

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

References

[1] I.-S. Jeon, E.-J. Yoon, A Simple PIN Input Technique Resisting Shoulder Surfing and Smudge Attacks, *Contemporary Engineering Sciences*, **8** (2015), 747 - 755. https://doi.org/10.12988/ces.2015.56164

[2] H. Sasamoto, N. Christin and E. Hyashi, Undercover: Authentication usable in front of prying eyes, *Proceeding of the Twenty-Sixth Annual CHI Conference on Human Factors in Computing Systems - CHI '08*, (2008), 183 - 192.

https://doi.org/10.1145/1357054.1357085

[3] A. D. Luca, E. von Zezschwitz, and H. HuBmann, Vibrapass: Secure authentication based on shared lies, *Proceeding of the 27th International Conference on Human Factors in Computing Systems - CHI '09*, (2009), 913 - 916. https://doi.org/10.1145/1518701.1518840

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

[5] A. Bianchi, I. Oakley, J.K. Lee and D.S. Kwon, The haptic wheel: Design & evaluation of a tactile password system, *Proceedings of the 28th of the International Conference Extended Abstracts on Human Factors in Computing Systems - CHI EA '10*, (2010), 3625 - 3630. https://doi.org/10.1145/1753846.1754029

[6] A. Bianchi, I. Oakley and D. S. Kwon, The secure haptic keypad: A tactile password system, *Proceeding of the 28th International Conference on Human Factors in Computing Systems - CHI '10*, (2010), 1089 - 1092. https://doi.org/10.1145/1753326.1753488

[7] A. Bianchi, I. Oakley and D. S. Kwon, Spinlock: A single-cue haptic and audio PIN input technique for authentication, Chapter in *Haptic and Audio Interaction Design*, Vol. 6851, 2011, 81 - 90. https://doi.org/10.1007/978-3-642-22950-3_9

[8] 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, *Proceedings of the Fifth International Conference on Tangible, Embedded, and Embodied Interaction - TEI '11*, (2011), 197 - 200. https://doi.org/10.1145/1935701.1935740

[9] 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*, Vol. 7, (2010), 1 - 10.

[10] E. von Zezschwitz, A. Koslow, A.D. Luca and H. Hussmann, Making graphic-based authentication secure against smudge attacks, *Proceedings of the 2013 International Conference on Intelligent user Interfaces - IUI '13*, (2013), 277 - 286. https://doi.org/10.1145/2449396.2449432

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

[12] 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. https://doi.org/10.1109/tifs.2014.2307671

[13] M. Kumar, T. Garfinkel, D. Boneh and T. Winograd, Reducing shoulder-surfing by using gaze-based password entry, *Proceedings of the 3rd Symposium on Usable Privacy and Security - SOUPS '07*, (2007), 13 - 19. https://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, *Proceeding of the 28th International Conference on Human Factors in Computing Systems - CHI '10*, (2010), 1107 - 1110. https://doi.org/10.1145/1753326.1753491

[15] J. Thorpe, P. van Oorschot and A. Somayaji, Pass-thoughts: Authentication with our minds, *Proceedings of the 2005 Workshop on New Security Paradigms - NSPW '05*, (2005), 45 - 56. https://doi.org/10.1145/1146269.1146282

[16] 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.

Received: January 6, 2017; Published: January 25, 2017