セカンダリチャネルを用いた覗き見耐性を持つ認証方式

荒谷, 光 / ARATANI, Akira

(出版者 / Publisher)
法政大学大学院理工学・工学研究科
(雑誌名 / Journal or Publication Title)
法政大学大学院紀要. 理工学・工学研究科編
(巻 / Volume)
56
(開始ページ / Start Page)
1
(終了ページ / End Page)
3
(発行年 / Year)
2015-03-24
(URL)
https://doi.org/10.15002/00011225

セカンダリチャネルを用いた 覗き見耐性を持つ認証方式

AUTHENTICATION METHOD AGAINST SHOULDER-SURFING ATTACKS USING SECONDARY CHANNEL

荒谷光
Akira ARATANI
指導教員　金井敦

法政大学大学院理工学研究科応用情報工学専攻修士課程

We propose an authentication method against shoulder-surfing attacks using two kinds of channel, which are a primary channel on which there is a possibility of shoulder-surfing attacks and a secondary channel on which there is information only recognized by the user. Security and usability of the proposed method is evaluated.

***Key Words**: Shoulder-surfing Attacks, Authentication Method, PIN, Smart Phone*

I. INTRODUCTION

Smartphones and tablet devices, such as android and iPhone devices, have been rapidly spreading. However, an attacker can easily observe the authentication process (shoulder-surfing attacks) since the input device has a large touch panel. Therefore, the possibility to break authentication has been increasing. The generally used personal identification number (PIN)-entry method has vulnerability over shoulder-surfing attacks because input characters are easily observed. In this paper, an authentication method against shoulder-surfing attacks is proposed and security of the proposed method is evaluated. Furthermore, usability is experimentally evaluated using the prototype of the proposed method.

II. RELATED WORK

Authentication can be divided into two categories. One is PIN-entry methods, for example, Android pattern lock method. It has the advantage of quick PIN input. However pin code can be guessed from smudges on the touch screen [1] and the password space of this method contains only 389,112 possible patterns (≈ Safety of 6-digit PIN or less). There are also other methods of this kind for example Binary PIN [2], Color PIN [3], Phone Lock [4] and LIN [5], et al. These other methods do not balance usability and security. The other is biometric authentication using human's biometric characteristics, for example, a fingerprint sensor. This type of authentication is an effective defense against shoulder-surfing attacks, but has other security issues such as a fake fingerprinting [6], Keystroke authentication [7] and rhythm authentication [8].

III. AUTHENTICATION METHOD

A. Concept

Desktop and notebook computers are mainly used in safe places such as the home or office. On the other hand, there is a risk of shoulder-surfing attacks on mobile terminals such as smart phones, because they are often used in crowded places such as trains or road in town. Furthermore, it is necessary to repeatedly and frequently unlock such devices to check e-mail or telephone. Therefore, it is necessary to consider usability as well as shoulder-surfing

TABLE I
REQUIREMENTS OF PROPOSED METHOD

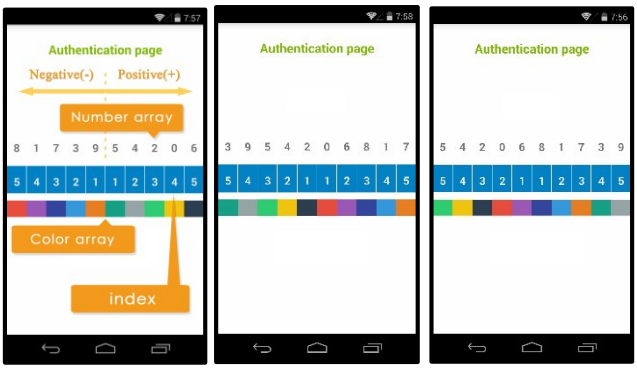
1	Prevent shoulder-surfing attacks
2	More secure than PIN-entry method
3	High usability

attacks. Table I lists the requirements of the proposed method for solving these problems.

The proposed method uses two kinds of channel, which are indicators recognized by other people such as visual information and indicators only recognized by the user such as auditory information using earphones or vibrations to satisfy the requirements. We call the former a main channel and the latter a secondary channel.

B. *User Interface (Input Sequence)*

In this method, the combination of number and color (called "key") is used as a main channel. The "key" means the password as PIN-entry method. And an index, which is displayed in the center of the screen [Figure 1-(a)] is used to indicate the position to align the key. There are two kind of directions as an index value: positive (right direction) and negative (left direction). The user distinguishes positive or negative from vibration. If the direction is positive, there are only the number of short vibration. If the direction is negative, the number of short vibration follows one long vibration. The user positions the key of number and color to the designated index. These key arrays loop left and right from the user flicking them like a wheel. In this paper, "n" and "c" represents the number of kind of number and color key, respectively (here the number of kind of number key is same as the number of kind of color key). "i" represents the digits of indices value and "m" represents the number of the pare of number and color. So, "m" means digits of the password as PIN-entry method. When the user starts the authentication, first the value of an index is informed to the user through vibration of the terminal as a secondary channel. Second, the user positions the number of the key at the designated index. Third, the user also positions the color of the key in the same way. Forth, the user repeats the above sequence "m" times.



(a) (b) (c)

Fig. 1. User interfaces of proposed method

TABLE II

NUMBER OF CASES A PIN-ENTRY METHOD AND PROPOSED METHOD

	Observed	Not observe
PIN-entry method	1	n^m
Proposed method	$(ic)^m$ $\begin{cases} i \le n \\ c \le n \end{cases}$	$(i^2nc)^m$

For example, when the key is {7: orange, 4: yellow} (so m=2). Here we assume i=n=c=10. The user positions 7 on the number array and orange on the color array to "+3" on index when the device notifies the user the value of index by three times of short vibration [Figure 1-(b)]. Next, the user positions 4 and yellow to "-2" when the device notifies the user the value of index by one long vibration and two times of short vibration, then the user taps the screen [Figure 1-(c)]. It is possible to enter the key easily because this interface is very simple.

IV. EVALUATION

A. *Security Analysis*

The security of the PIN-entry and the proposed method with or without shoulder-surfing attacks are analyzed. Table II lists the number of attempted attacks in these methods. In this case, we do not consider if n and c are less than the width of the index because the number of attempted attacks does not increase even if the digit of the index increases. Figure 2 depicts the security of these methods by taking into account the binary logarithm when m=2, 3, 4 of the proposed method and n=10 and m=4 of the PIN-entry method. The proposed

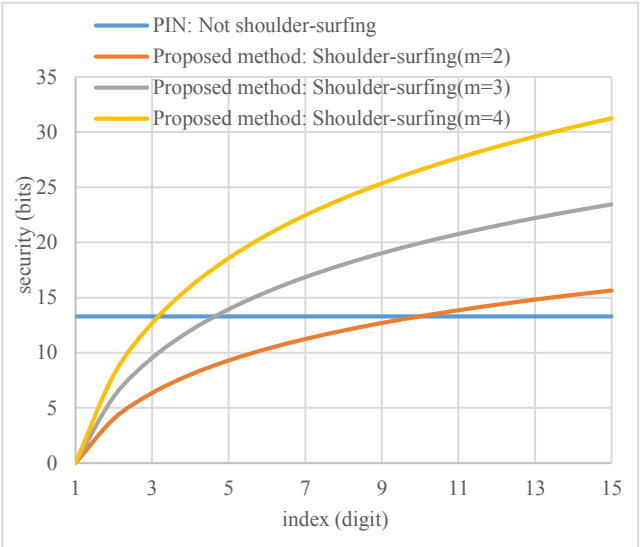


Fig. 2. Security of proposed method (m=2, 3, 4) and PIN-entry method (n=10, m=4)

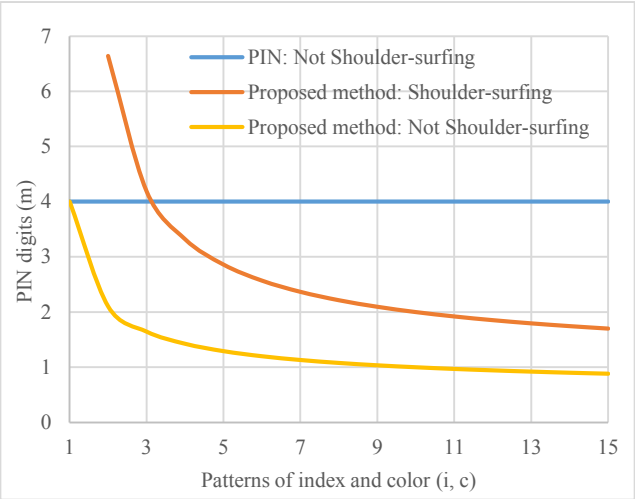


Fig. 3. Pattern of combination of m, i, c, n with same safety of PIN-entry method

TABLE III
PIN ENTRY TIME WITH PROPOSED METHOD

		Entry time (second)		
i, c, n	m	Average	Fastest	Slowest
10	2	14.2	9.7	19.6
5	3	14.4	11.2	20.9
3	4	12.8	10.2	14.8

method is more secure than the PIN-entry method when m=4 and i≥3, m=3 and i≥5 or m=2 and i≥10, as shown in Table II and Figure 2. Figure 3 shows the combination patterns of m, i, c, n with the same security of the PIN-entry method when n=10 and m=4.In the proposed method, security is higher than the PIN-entry method in any combination without shoulder-surfing attacks.

B. Usability Evaluation

The usability of the proposed method is evaluated by using our prototype software implemented on the Android 4.4 platform. 12 Students participated in the experiment as subjects. We measured the entry time after three trials [Table III]. The subjects learn the number and color combinations and practice three times. Table III shows that the proposed method can be used practically for any combination. The proposed method takes more time to input than the PIN-entry method, however it is still practical.

V. CONCLUSION

We proposed a new authentication method using two kinds of channel, then analyzed our authentication method against shoulder-surfing attacks using a secondary channel. We confirmed that the proposed method is safer than the PIN-entry method. Furthermore, the proposed method is experimentally evaluated. The result shows the proposed method is practical from the viewpoint of usability. For future study, we will investigate an optimal interface suitable for a parameter set corresponding to the security level.

VI. ACKNOWLEDGEMENTS

I would like to show my greatest appreciation to Prof. Kanai whose comments and suggestions were of inestimable value for my study. I also owe a very important debt to members of Kanai laboratory whose meticulous comments were an enormous help to me.

REFERENCES

[1] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith, "Smudge attacks on smartphone touch screens," in *Proc. 4th USENIX Conf. Offensive Technol. WOOT*, 2010, article 1–7, pp. 1–10.

[2] V. Roth, K. Richter, and R. Freidinger, "A PIN-entry method resilient against shoulder surfing," in Proc. ACM CCS (Computer and Communications Security), 2004, pp. 236–245.

[3] A. D. Luca, K. Hertzschuch, and H. Hussmann, "ColorPIN: Securing PIN entry through indirect input," in *Proc. CHI*, 2010, pp. 1103–1106.

[4] 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," in *Proc. TEI*, 2011, pp. 197–200.

[5] M.-K. Lee, "Security Notions and Advanced Method for Human Shoulder-Surfing Resistant PIN-Entry," in Proc. IEEE Trans. Inf. Forensics Security, vol. 9, no. 4, pp. 695–708, APRIL 2014.

[6] (2013). *iPhone 5S Fingerprint Sensor Hacked by Germany's Chaos Computer Club* [Online]. Available: http://www.theguardian.com/technology/2013/sep/22/apple-iphone-fingerprint-scanner-hacked

[7] K. Yamada, A. Noguchi, K. Notomi and K. Saito, "Keystroke Authentication like the Gamepad Style for Smartphone – Evaluation of Flick Input Mode –," in Proc. National Convention of IPSJ 2013(1), pp. 565-567, 2013-03-06

[8] R. Ichimura, A. Noguchi, K. Notomi, K. Saito, "A rhythm Authentication Method for Smartphone using Self-Organizing Maps – Rhythm Feature Extraction by Melody of Music – ," in Proc. National Convention of IPSJ 2013(1), pp. 567-569, 2013-03-06