A Proposal of Shoulder-surfing Attack Countermeasure Method with Improved Usability

Yoshihiro Kita
Faculty of Information Systems,
University of Nagasaki,
1-1-1 Manabino, Nagayo, Nishisonogi , Nagasaki 851-2195, Japan

Shingo Nakamura
Faculty of Information Systems,
University of Nagasaki,
1-1-1 Manabino, Nagayo, Nishisonogi , Nagasaki 851-2195, Japan

E-mail: kita@sun.ac.jp

Abstract

Shoulder-surfing attacks are one of the most familiar password exploitation attacks. It is vulnerable to be attacked while unlocking a smartphone screen. The smartphone users need to take countermeasures against that attack. The fingerprint-based screen unlock system has become the norm, but it is not safe, as there has been increased in the user's fingerprint theft. The existing methods to prevent the shoulder-surfing attacks are effective against such attacks, but many of them are complicated to operate, and difficult to use. In this paper, we propose the prevent method for surfing attacks that it is easy to use. The tool's user operates the lower buttons, moves characters to on the trump's marks in specified advance. The user can input as likely as the password. On the other hand, the attacker does not understand the input characters only shown these buttons has been pushed.

Keywords: shoulder-surfing attack, unlocking a smartphone screen, security and usability.

1. Introduction

Recently, mobile devices had the screen lock using the authentication methods, e.g., PINs and patterns, for the prevention of unlawful using by others. These authentication methods are vulnerable to attack by peeking (shoulder-surfing attack).

These numbers/patterns as the passwords are leaked to others who peek mobile device's screen. The authentication methods [1][2][3][4] have the resistance to shoulder-surfing attack. However, these methods have complicated user interface.

In this paper, we propose the shoulder-surfing attack countermeasure method that is improved usability. In this method, numbers, characters, symbols, and colors are arranged on each of the two layers in reference the background pattern slide authentication [3], and the user selects the combination in which they overlap to be authenticated the user. We confirm the usability of our proposal method, an experiment was performed in which several combination patterns were prepared, and the subjects were asked to choose the one with the best usability.

Fig.1. A sample of the secret tap with double shift (STDS) method [2]

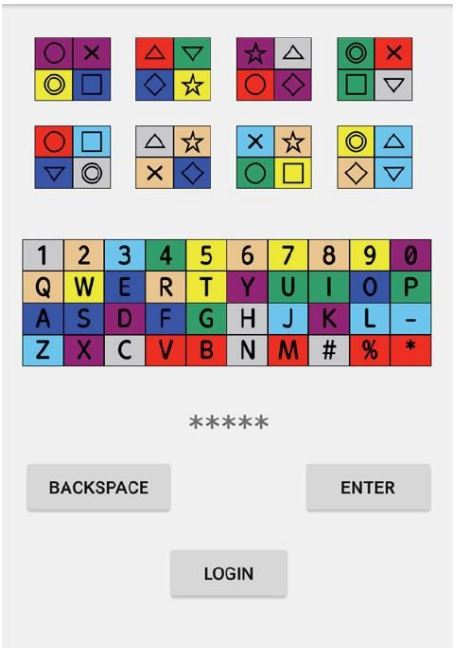

Fig.2. A sample of the background pattern slide authentication [3]

2. Related Works

2.1. *Secret Tap with Double Shift (STDS)*

The secret tap with double shift (STDS) method [2] is an unlock system for smart phone's display as shown as Fig.1. This method places 16 randomly selected icons in the display area, which is a 4×4 square. The user selects the authentication icon from the 16 icons and taps the selected icon. The user repeats this operation for a predetermined number of registry icons. If all selected icons are correct authentication icons, the authentication is successful, and the smart phone's display is unlocked.

The user needs to memorize the 4 icons and shifts as PIN and needs to calculate the place of tap icons from these. These are a heavy burden for the user. These operations have to be made simpler to reduce the burden of the user.

2.2. *Background Pattern Slide Authentication*

The background pattern slide authentication [3] is an unlock system for smart phone's display as shown as Fig.2. First, the user selects a square from upper grids. Next, changes a target character's color to same color as selected square, and enter the target characters as PIN.

In this method, the target character is not directly touched during PIN enter, multiple target characters on the same background color, are listed as PIN candidates. The attacker cannot be identified PIN uniquely.

However, this method is less usability due to the small size of each grid and complicated coloring. The user needs nervous operation to use this method.

2.3. *CCC (Circle Chameleon Cursor)*

CCC (Circle Chameleon Cursor) [4] is the unlock system using background pattern and phone's vibration. This method is based on fakePointer [1], consists of 3 parts; PIN indicator, the number input dial, and PIN enter button. The numbers are placed on the number input dial.

First, PIN indicator rotates on the number input dial, when PIN indicator comes to a specified position, the smartphone vibrates. The user feels this vibration and recognizes the position as a cursor for PIN enter. Next, the user operates the number input dial, adjust the number as PIN to this position, and tap the PIN enter button.

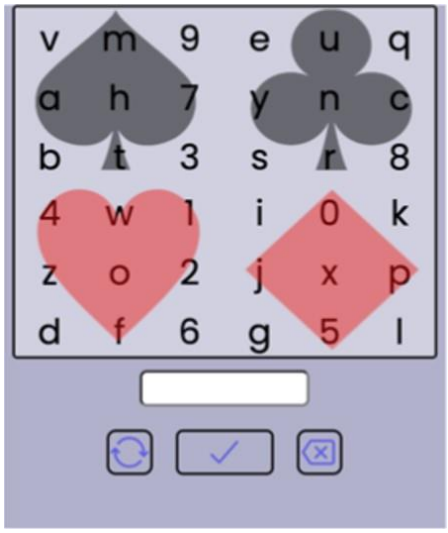

Fig.3. The background pattern (1) of our proposal method

Fig.4. The background pattern (2) of our proposal method

This method takes time to unlock the smartphone because the user must detect the position for PIN enter by the smartphone's vibration.

3. Our proposal method for improving usability

In this paper, we propose the shoulder-surfing attack countermeasure method that is improved usability. We consider the following to keep the security for against shoulder-surfing attack.

- PIN is formed by choosing 4 characters from 36 characters that includes numbers and English alphabets.
- The 36 characters are displayed randomity.
- When enter a PIN, multiple characters are candidates for the PIN, so that a character is not uniquely defined it.
- When enter a PIN, the user not directly touch the character as the PIN.

The other hand, we consider the following to improve usability.

- The minimize as much information as possible for the user must be to memorize.
- The user's operation and display are simpler as possible.

We propose 3 patterns that satisfy these conditions as shown as Fig.3, Fig.4, and Fig.5.

Fig.3 shows pattern (1) which uses trump's marks at background pattern. This is divided into 4 areas according to the mark, and each area contains 9 characters. The user moves and enter the mark for each PIN so that each mark of area containing a PIN, is all same. In other words, the smartphone is unlocked if all entered marks are same, i.e., 4 marks are entered for 4-digits PIN. The marks are moved clockwise by tapped lower-left button. A mark of the area containing a PIN is entered by tapped lower-center button. If the user is necessary to cancel an entered mark, taps the lower-right button.

Fig.4 shows pattern (2) which colored black and red at background pattern. This is divided into 2 areas, and each area contains 18 characters. The operation and algorithm are the same as pattern (1). The user enter each color of the area containing a PIN. If all entered colors are same, the smartphone is unlocked. Each color is replaced by tapped lower-left button.

Fig.5 shows patten (3) which uses trump's marks at background patten as same as patten (1). This is divided into 9 areas according to the mark, and each area contains 4 characters. Each mark is rotated clockwise around the center mark by tapped lower-left button. The center mark is displayed a mark "Spade", but the center area is always

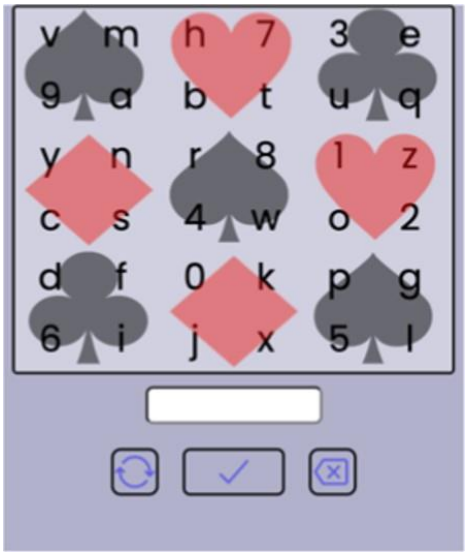

Fig.5. The background pattern (3) of our proposal method

entered, it means “Wildcard”. (Currently using a different mark that is not a trump’s mark.)

4. Evaluation of usability

We conducted the trial experiment to confirm the usability of these patten. The subjects are the 10 students belong to University of Nagasaki.

First, each subject register PIN using their devices. Next, they try to unlock each pattern of our proposal method at 10 times. Finally, they scored each pattern on 4 points scale as usability score as follows.

- Excellent (score 4)
- Good (score 3)
- Fair (score 2)
- Poor (score 1)

Table.1 shows the results of experiment for usability of our method. Pattern (2) had the shortest unlock time and highest usability score of all patterns, although there was 1 mistouch.

The subject’s most common opinion was:
“Pattern (2) is easy to operate, view, and understand.”
Therefore, pattern (2) is the highest usability of patterns.

However, we consider that pattern (2) is not secure against the accidental unlocking. Table.2 shows the probability of accidental unlocking of each patten. Pattern (1) and (3) have a probability of less than 1%, while Pattern (2) has a high probability as 6.25%. In usually, safety and usability are trade-off, so high usability means less safety. Too high level of usability can be dangerous. If the probability of accidental unlocking is kept less than 1%, pattern (1) is suitable high usability method for against shoulder-surfing attack.

5. Conclusion

Table.1. The results of experiment for usability

Patterns	Unlock average time (sec)	Times of mistouch (total)	Usability score (average)
Pattern (1)	16.75	0	3.0
Pattern (2)	11.81	1	3.5
Pattern (3)	15.62	0	2.1

Table.2. The probability of accidental unlocking of each pattern

Patterns	The probability of accidental unlocking
Pattern (1)	(9/36) ^ 4 = 0.39%
Pattern (2)	(18/36) ^ 4 = 6.25%
Pattern (3)	(8/36) ^ 4 = 0.24%

In this paper, we proposed the shoulder-surfing attack countermeasure method that is improved usability. The proposal methods were defined 3 patterns by the different of background patten.

The experiment results shows that pattern (2) is the highest usability method of all patterns, but we led to conclusion that pattern (1) is suitable high usability method for against shoulder-surfing attack by safety factors.

Our future works are as follows,

- Conducting additional experiments to confirm the accidental unlocking by subjects
- Conducting additional experiments to confirm our proposal methods resistance to shoulder-surfing attack.
- Discuss the other safety considerations for smartphone's unlocking

References

[1] T. Takada, "fakePointer: An Authentication Scheme for a Better Security Against a Peeping Attack by a Video Camera", Proceedings of the 2nd International Conference on Mobile Ubiquitous Computing, Systems, Service and Technologies (UBICOMM2008), 2008.

[2] Y. Kita, F. Sugai, M. Park, and N. Okazaki, "Proposal and its Evaluation of a Shoulder-Surfing Attack Resistant Authentication Method: Secret Tap with Double Shift", International Journal of Cyber-Security and Digital Forensics (IJCSDF), Vol.2, No.1, pp.48-55, 2014.

[3] M. Tanaka and H. Inaba, "Proposal of Improved Background Pattern Slide Authentication against Shoulder Surfing in Consideration of Convenience", Journal of Information Processing Society of Japan, Vol.58, No.9, pp.1513-1522, 2017 (in Japanese).

[4] M. Ishiduka and T. Takada, "CCC: Repeated Observation Attack Resilient PIN Authentication System Using Vibration", Journal of Information Processing Society of Japan, Vol.56, No.9, pp.1877-1888, 2015 (in Japanese).

Authors Introduction

Dr. Yoshihiro Kita

He received his Doctor's degree from the Department of Engineering, University of Miyazaki, Japan in 2011. He belongs to University of Nagasaki, Japan. His research area is biometrics, mobile security, and software testing.

Mr. Shingo Nakamura

He belongs to the Faculty of Information Systems, University of Nagasaki, in Japan. He researchs the security and usability when unlock a smart phone's display. He interested in mobile security.