Touch Logger Resistant Mobile Authentication Scheme Using Multimodal Sensors

Hyunyi Yi, Yuxue Piao, and Jeong Hyun Yi*

Department of Computer Science and Engineering
Soongsil University, Seoul, Korea
{hyunyiyi,qianbin127,jhyi}@ssu.ac.kr

Abstract. The PIN that is widely used for various services in mobile devices is highly vulnerable to attacks such as shoulder surfing. Various schemes have been proposed to solve this vulnerability of the PIN. However, despite the enhanced security of existing schemes, usability such as authentication time and error rate has decreased. In this paper, we propose a new scheme called PassWindow that allows enter a PIN securely through a window moving on the virtual keypad. PassWindow provides improved usability in the mobile devices and prevents shoulder-surfing attacks at the same time. We also propose an input method using multimodal sensors. This method strengthens the security against recording attacks and touch logger attacks.

Keywords: usable security, password-based authentication, shoulder-surfing attack, touch logger attack.

1 Introduction

Mobile devices store not only private information, such as pictures and contacts, but also store important information that allows the user to use various services conveniently such as e-mail and financial transactions. Therefore, the access to critical information and services are restricted through the password-based authentication. However, the user authentication for mobile devices is frequently performed in public places. As a result, there is a risk of password exposure by attacker observing the authentication interface over the user's shoulder [1].

Typical password authentication schemes well known to users are PIN(Personal Identification Numbers) and alphanumeric password. The PIN, which uses four digits numeric (0 to 9) as a password, is commonly used in financial services because it is easy to remember and input. However, there are only 10,000 available password combinations. Thus, the security against brute force attack is low. The alphanumeric password, which uses 6 to 12 digits including numbers and letters, is secure than the PIN against brute force attack. However, the alphanumeric password increases the burden on the user's memorization capabilities by requiring the user to set a strong password with restrictions such as text length, composition, etc. As a result, users tend

* Corresponding author.

H.-Y. Jeong et al. (eds.), *Advances in Computer Science and Its Applications*,
Lecture Notes in Electrical Engineering 279,
DOI: 10.1007/978-3-642-41674-3_4,

to write down their passwords or apply the same password in several systems [2, 3], which reduces the security of the alphanumeric password. Therefore, the existing schemes [4-7] do not satisfy the requirements of security and usability at the same time. In this paper, we propose a user authentication scheme that allows for the secure input of PIN. The proposed scheme makes the user to enter different values each time through a window that moves freely in the virtual keypad, thereby preventing shoulder-surfing attacks. Also, an additional method to input the password is proposed that using the sensors in mobile devices to defend against touch logger attacks.

The rest of the paper consists of the following sections. In section 2, we review related studies. Section 3 introduces the proposed scheme in detail and section 4 analyzes the security of proposed scheme. Section 5 presents the experimental results. Finally, Section 6 presents the conclusion.

2 Related Works

2.1 Shoulder-Surfing Attacks in Mobile Devices

Shoulder-surfing attacks are attacks that extort personal information deliberately by observing the user's behavior [8]. A shoulder-surfing attack can be categorized into two types depending on the attacker's capabilities: cognitive shoulder surfing and recording-based shoulder surfing [9].

2.2 Touch Logger Attacks in Mobile Devices

A touch logger is a type of spyware that applies the keylogger to the touch interface. The touch logger, by logging touch location, can determine which characters are selected on the virtual keypad, and can be utilized as a means to capturing a state of screen when a touch event generates. The touch logger attacks that have been studied to date can be categorized into two types depending on the method for detecting the touch location. Cai and Chen proposed a new key logging scheme, TouchLogger [10], that utilizes the motion sensors in mobile devices. This scheme measures the variability of the values of motion data depending on the screen location that is being touched. This information is then used to extract the input. Damopoulos et al. proposed a touch logger that can record all of the touch events that occur on the screen [11]. This scheme makes it possible to collect the touch events in the background by hooking the touch event API of iPhone.

3 Proposed Scheme

We propose a new PIN-based authentication scheme that considers the security issues that arise when authentication in mobile devices and the usability of small touch screens on these devices. This scheme is called "PassWindow [12]." PassWindow blocks direct exposure of password by enabling the input of the password through a grid-configured window, thereby preventing shoulder-surfing attacks. Users can move

the window freely over the virtual keypad using a simple touch event. This provides an additional input method that using the sensors in mobile devices. As a result, it strengthens security against recording and touch logger attacks.

PassWindow uses a PIN and an additional secret value as the password. In this section, the proposed scheme using an image as the additional value will be explained. The corresponding image is called a "pass-icon" and is used by the user to identify the location where the PIN is entered. The user selects the number N digits and the pass-icon during the password setup step. The authentication system randomly selects decoy icons, which are then stored along with the pass-icon. The secret value that should be memorized with the PIN can influence the ease of memorization. Therefore, it should be up to the users to determine which kind of elements are easier for them to memorize as secret values among the elements of image, text, color, etc.

The user identifies the location that matches with the PIN using the image that is displayed on the $x \times y$ sized grid at the time of user authentication. This grid, which is called the "pass-window," consists of the pass-icon and other decoy icons. Each cell in the pass-window is an image location and is represented as (i, j). The user recalls the pass-icon within the pass-window and memorizes the location. The location of pass-icon within the pass-window is different whenever authenticated. After the pass-location is confirmed, then the virtual keypad consisted as numbers and the pass-window with its images disappeared, show up in the center. The user moves the pass-window, which is floating over the virtual keypad, so that the pass-icon moves over each digit of the PIN on the pass-location for authentication. Fig. 1 shows the PassWindow authentication process.

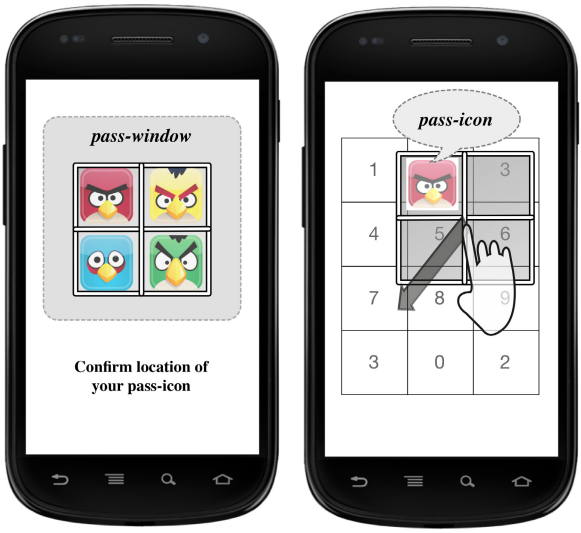

Fig. 1. PassWindow Authentication Process

The process of authentication is explained by assuming that the user selects 1234 as the PIN and by taking Fig. 1 as an example. First, the user, after confirming that the pass-icon is located at $(1,1)$ in the 2×2 pass-window, memorizes this as the pass-location. After this, we let the virtual keypad numbers "1," "2," "3," and "4" overlap in the proper order with the pass-location and then make a selection. The pass-window is an important element that has a direct influence on both the security and usability of the proposed scheme. Therefore, some methods are provided below for pass-window composition and operation. There are two methods for operating the pass-window: the Touch Enter and the Hidden Enter method. These control methods are specialized for mobile devices, are convenient, and improve security against interface attacks. Fig. 2 shows the operation method for the pass-window.

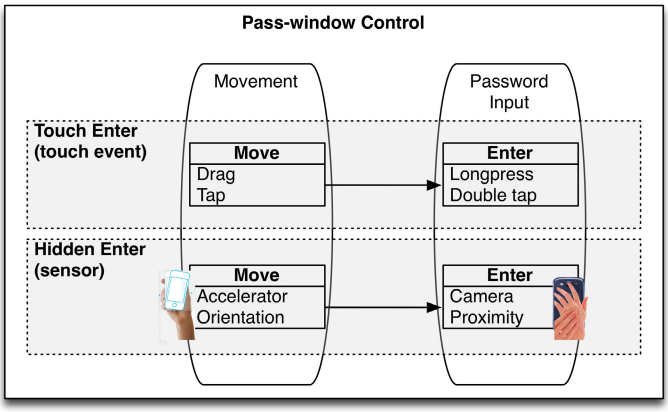

Fig. 2. Methods of Pass-window Control

Pass-Window with Touch Enter. This method utilizes the touch event in mobile devices. For example, after matching the number on the pass-location by moving the pass-window using a drag event, the input of password can be performed by touching the screen. As the user touches the screen directly, it may be possible for an attacker to identify the numbers that are being entered through the pass-window, but it is still not easy to acquire the PIN because the pass-icon is not known.

Pass-Window with Hidden Enter. This method operates the pass-window using the embedded sensors in mobile devices [13]. As the user moves the mobile device, the sensors detect the movement and use the information from this movement to move the pass-window. The entry of the password can be performed by covering the rear camera lens with a finger. Operating the pass-window via sensors helps to prevent touch logger attacks because it does not generate touch events, and entering the password through the rear camera sensor enables the users to hide the password input, thereby improving the security against shoulder-surfing and recording attacks.

4 Security Analysis

In this section, the security of the PassWindow is analyzed in relation to shoulder-surfing attacks and touch logger attacks.

4.1 Resistance to Shoulder-Surfing Attacks

Table 1 shows a comparison of the resistance of existing authentication schemes and the proposed scheme to shoulder-surfing attacks where N denotes the length of the password and L does the number of cells in the pass-window.

Table 1. Resistance to Shoulder-surfing Attacks

	Resistant to cognitive shoulder-surfing attack	One-time recording attack probability
Passfaces [4]	NO	1
DAS [5]	NO	1
PIN-Entry [6]	YES	1
ColorPIN [7]	YES	$1/3^N$
PassWindow	YES	$1/L$

Authentication schemes where the original password is input, such as DAS and Passfaces, are vulnerable to cognitive shoulder-surfing attacks. On the other hand, PIN-Entry and ColorPIN perform the authentication using varied response values and thereby prevent direct exposure of the password. Further, the PassWindow allows the indirect entry of the password through the pass-window. Therefore, an attacker who attempts a shoulder-surfing attack must memorize each of the $\mathrm{L} \times \mathrm{N}$ characters that are entered through the pass-window in order to obtain the password. With regards to recording attacks, the security of the PassWindow is influenced by the size and composition of the pass-window and the input methods. The number of response values that an attacker can acquire with a one-time recording attack is equal to the number of the pass-window cells. Because each one of the cell values, respectively, becomes the actual password, the one-time recording attack success probability is $1/\mathrm{L}$. The probability of acquiring the password with a one-time recording attack when ColorPIN is used is $1/3^{\mathrm{N}}$, which is more secure than PassWindow. As the pass-icon is not known to the attacker, it is not easy to find out the PIN from a single observation. However, if the authentication process is recorded several times for analyses, the PIN can be deduced. Nevertheless, the security of PassWindow can be improved against recording attacks through the use of the Hidden Enter. The attacker may identify the pass-window movement location throughout the authentication process recording, but it is not easy to detect the actions that cover the camera lens on the rear side of the device. This makes it possible to hide the selections of the response values as the pass-window is moving, thereby preventing the attacker from acquiring the input response values.

4.2 Resistance to Touch Logger Attacks

Table 2 shows a comparison of the probabilities of success of the proposed and existing schemes for touch logger attacks.

Table 2. Resistance to Touch Logger Attacks

	Motion sensor value-based attack probability	Touch event-based attack probability
Passfaces [4]	1	1
DAS [5]	1	1
PIN-Entry [6]	1	1
ColorPIN [7]	$1/3^N$	$1/3^N$
PassWindow (Touch Enter)	$1/L$	$1/L$
PassWindow (Hidden Enter)	$1/L$	N/A

As the authentication for Passfaces, DAS, PIN-Entry, and ColorPIN schemes is performed by touching the screen, it is possible to detect the generation of the touch event and to obtain the entire authentication screen and touch locations as well. Therefore, the probabilities of success for touch logger attacks on the existing schemes are equal to those for recording attacks. The security of PassWindow against touch loggers attack varies depending on the operation method that is used for the pass-window. When Touch Enter is used, the resistances to touch logger attacks and to recording attacks are equal to the resistance of the existing schemes. The Hidden Enter, on the other hand, allows the authentication to be performed using acceleration sensors and the camera lens. However, as this does not generate touch events, touch loggers cannot acquire any useful information.

5 Experimental Results

This section compares and analyzes the usability of existing authentication schemes and the proposed scheme using two experiments. One experiment is based on a user interface evaluation tool and the other experiment is based on a real user experiment. Table 3 shows a comparison of the experimental results for two experiments.

Table 3. Experimental Results

	CogTool Authentication time [s]	User Test Authentication time [s]	User Test Error rate [%]
Passfaces [4]	8.65	14.55	14.00
DAS [5]	11.23	9.87	12.00
PIN-Entry (Immediate) [6]	20.05	19.55	28.00
PIN-Entry (Delayed) [6]	16.99	26.60	34.00
ColorPIN [7]	19.58	20.10	16.00
PassWindow	18.12	17.86	4.00

5.1 CogTool Test

We describe experiments that predict the authentication times for existing authentication schemes and the proposed scheme using CogTool [14].

The authentication time predicted by CogTool for PassWindow is measured at 18.12 s, which is longer than those for the simpler Passfaces and DAS authentication methods. In the meanwhile, it is expected that the authentication for PassWindow will be faster than the authentications for the PIN-Entry and ColorPIN schemes that require complicated password input processes.

5.2 User Test

For the user experiments, the existing and proposed schemes were implemented using an Android-based application program. The implementation used Eclipse Helios, Android SDK 2.3, and JAVA 1.6.0. Five units of the Samsung Smartphone SHW-M250S (1.2 GHz) were used as test equipment. The tests were performed by a total of ten persons. The testers requested to set up password and repeated the authentication process 5 times. Table 3 summarizes the average authentication times and error rates that were calculated using the authentication logs.

The test results show that PassWindow has more improved authentication time than the existing schemes that have similar or higher security do. The results also demonstrate its superiority for the ease of password memorization with relatively lower error rates than the schemes with speedier authentication speeds.

6 Conclusion

In this paper, we proposed a new PIN authentication scheme that prevents shoulder-surfing attacks. The proposed scheme uses a secret value in addition to the PIN. The authentication method works by matching the PIN with the particular location of the window on which the virtual keypad moves freely. A particular location of the window varies each time based on the secret values, thereby preventing the exposure of the real PIN. The Hidden Enter that utilizes multimodal sensors was also proposed. This input method blocks the generation of touch events and is hard to catch a timing of the password input.

The security analysis results showed that the proposed scheme prevents shoulder-surfing attacks. Further, the input method that uses sensors showed that it strengthens the security against recording and touch logger attacks. From the analysis of the usability test results, it was observed that the proposed scheme enabled speedier authentication than existing schemes that are secure against shoulder-surfing and recording attacks. Furthermore, an ease of password memorization through significantly reduced error rates was demonstrated.

Acknowledgment. This research was supported by the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2013R1A1A2013041).

References

1. Schaub, F., Deyhle, R., Weber, M.: Password Entry Usability and Shoulder Surfing Susceptibility on Different Smartphone Platforms. In: 11th International Conference on Mobile and Ubiquitous Multimedia, pp. 1–10 (2012)
2. Sasse, M.A., Brostoff, S., Weirich, D.: Transforming the 'weakest link'— a Human/Computer Interaction Approach to Usable and Effective Security. BT Technology Journal 19(3), 122–131 (2001)
3. Payne, B.D., Edwards, W.K.: A Brief Introduction to Usable Security. IEEE Internet Computing 12(3), 13–21 (2008)
4. Passfaces, http://www.realuser.com
5. Park, S.B.: A Method for Preventing Input Information from Exposing to Observers. 10-2004-0039209, Korea (2004)
6. Roth, V., Richter, K., Freidinger, R.: A PIN-entry Method Resilient against Shoulder Surfing. In: 11th ACM Conference on Computer and Communications Security, pp. 236–245 (2004)
7. Luca, A.D., Hertzschuch, K., Hussmann, H.: ColorPIN: Securing PIN Entry through Indirect Input. In: 28th International Conference on Human Factors in Computing Systems, pp. 1103–1106 (2010)
8. Tari, F., Ozok, A.A., Holden, S.H.: A Comparison of Perceived and Real Shoulder-surfing Risks between Alphanumeric and Graphical Passwords. In: 2nd Symposium on Usable Privacy and Security, pp. 56–66 (2006)
9. Shi, P., Zhu, B., Youssef, A.: A PIN Entry Scheme Resistant to Recording-based Shoulder-surfing. In: 3th International Conference on Emerging Security Information, Systems and Technologies, pp. 237–241 (2009)
10. Cai, L., Chen, H.: TouchLogger: Inferring Keystrokes on Touch Screen from Smartphone Motion. In: 6th USENIX Workshop on Hot Topics in Security, p. 9 (2011)
11. Damopoulos, D., Kambourakis, G., Gritzalis, S.: From Keyloggers to Touchloggers: Take the Rough with the Smooth. Computers & Security 32, 102–114 (2013)
12. Yi, J.H., Ma, G., Yi, H., Kim, S.: Method and Apparatus for Authenticating Password of User Device. 10-1175042, Korea (2012)
13. Yi, J.H., Yi, H., Piao, Y., Kim, T.: Method and Apparatus for Authenticating Password using Sensing Information. 10-2012-0103897, Korea (2012)
14. CogTool, http://cogtool.hcii.cs.cmu.edu/