Secure smartphone user authentication using rear audio equipment[1]

Mun-Kyu Lee [2]

Inha University, Incheon 402-751, KOREA

Abstract

User authentication is a procedure to verify the authenticity of a claimed user who tries to access a system. The most frequently used authentication mechanism, i.e., knowledge-based authentication such as a password or a PIN (Personal Identification Number), has several security issues such as the possibility of shoulder surfing attacks. In this paper, we propose two user authentication methods using the rear audio equipment of smartphone which are resistant to shoulder surfing attacks. The first one is to use the rear speaker as an indicator for true or false. For this, we may use any legacy input interface such as a regular PIN pad. However, we input additional information using the rear speaker to notify the smartphone if the digit currently touched is a real one or false one. The second proposed method is to use the rear speaker as a direct input device. That is, the user does not receive any visual information from the front display panel, but all tasks are done only using the rear speaker.

Keyword : User Authentication, Audio Equipment, Shoulder Surfing Attack

---

[1] This paper is an extended version of the paper presented at JKCCS 2012 [1].

[2] Mun-Kyu Lee
mklee@inha.ac.kr
Address: Department of Computer Science and Information Engineering,
Inha University, 100 Inha-Ro, Nam-Gu, Incheon 402-751, KOREA
Tel. +82-32-860-7456

1. Introduction

User authentication is a procedure to verify the authenticity of a claimed user who tries to access a system. In general, user authentication methods are classified into three categories; password or PIN (Personal Identification Number)-based schemes based on human memory, biometric schemes using the feature or behavior of a user, and hardware token-based schemes. Although the first class is being used in most systems, it has several security issues such as the possibility of shoulder surfing attacks where an attacker looks over the user's input over the user's shoulder. Although there have been many proposals in the literature to resolve this issue [2-5], none of them achieve both usability and security. In this paper, we propose two new user authentication methods using the rear audio equipment of a smartphone such as a rear speaker.

2. Proposed Method

(a) The rear speaker is open. (b) The rear speaker is closed.

Fig. 1. Using a rear speaker as an input medium.

We propose two new user authentication methods using the rear audio equipment of a smartphone such as a rear speaker. As Fig. 1 shows, almost all commercially available smartphones have a speaker on their back, although the specific position of this speaker is different between devices. To use the speaker as an input mechanism, the smartphone may continuously generate a high frequency audio signal which is hardly audible by a human user and monitor if this signal is heard by its microphone. If the user closes the rear speaker, the smartphone will not hear its own audio signal and recognize that

the user has closed the rear speaker. This task may be easily done by slightly moving only a finger. Because the attacker is usually located behind the user, i.e., the opposite side of the speaker, s/he cannot see the movement of the user's finger on the rear panel of the smartphone. Consequently, we may use the speaker as a secure channel.

2.1 Using the rear speaker as a binary channel

Our first method is to use the rear speaker as a binary input mechanism, i.e., an indicator for true or false. For this, we may use any legacy input interface such as a regular PIN pad. But we input additional information using the rear speaker to notify the smartphone if the digit currently touched is a real one or false one. For example, if we close the rear speaker with one finger while touching the digit displayed in the front display panel, this implies that the digit is a false one. Therefore, the smartphone will ignore this digit. If we open the rear speaker while touching a digit, this digit is a true one that the smartphone should recognize. Because the attacker is on the opposite side of the speacker, s/he cannot distinguish between the true and false inputs. An example input sequence may be as follows:

2 (open), 7 (closed), 4 (closed), 1 (closed), 0 (open), 6 (closed), 8 (open), 6 (open), 1 (closed).

Then, what the user has input is 2086, although what the attacker sees is 274106861.

2.2 Using the rear speaker as a direct input channel

The second user authentication method is to use the rear speaker as a direct input device. That is, the user does not receive any visual information from the front display panel, but all tasks are done only using the rear speaker. In this case, the pattern by which the user opens and closes the speaker is the password of this user. For example, the order of closing and opening tasks and the duration of each status may constitute a password. Because it is actually hard to numerically remember these patterns and durations, it would be a good solution to remember the password as a kind of rhythm. The obvious merit of the second method is that it may be used in a dark room or even in a pocket without any visual information. An example PIN would be as follows:

Closed (0.2s), open (0.6s), closed (0.2s), open (0.1s), closed (0.4s), open (0.1s), closed (end).

3. Discussion

In this section, we examine the security and usability of the two proposed method. First, regarding the binary method, we should remark that it is not completely secure from a shoulder surfing attack. For example, in the example of section 2.1, the attacker observes a sequence 274106861. If s/he knows that the PIN is composed of four numerical digits as typical PINs are, s/he may mount a guessing

attack by randomly choosing four digits among the nine observed digits. Thus, the success probability is 1/126. Although this probability is significantly lower than that of a regular PIN pad, i.e., ≈ 1, it is much greater than that of a random guessing attack without any information about the PIN, i.e., 1/10000. In addition, the task of opening and closing the speaker may be a cognitive burden for a user, which may degrade usability.

On the other hand, the second method changes the PIN space, which implies that the form of a PIN and the set of possible PINs are different from those of a standard 4-digit PINs. Then, a compatibility issue may be raised. In addition, because a user should remember a new form of PIN, a memorability issue may also be a concern.

In order to analyze the usability and practical security of the proposed methods and to solve the potential issues, we should implement the methods and perform an extensive user study. We leave this as a future research topic.

Reference

[1] M.-K. Lee, "User authentication with rear audio equipment of mobile device," In Proc. of Japan-Korea Joint Workshop on Complex Communication Sciences (JKCCS 2012), 2012.

[2] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter and A. D. Rubin, "The design and analysis of graphical passwords," In Proc. of the 8th USENIX Security Symposium, pp. 1-14, 1999.

[3] V. Roth, K. Richter, R. Freidinger, "PIN-Entry Method Resilient Against Shoulder Surfing," ACM CCS'04, pp. 236-245, 2004.

[4] H. Sasamoto, N. Christin and E. Hayshi, "Undercover: Authentication Usable in Front of Prying Eyes," CHI 2008, pp. 183-192, 2008

[5] 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," TEI 2011, pp. 197-200, 2011.