Journal of information and communication convergence engineering
http://jicce.org

J. Inf. Commun. Converg. Eng. 15(2): 91-96, Jun. 2017 **Regular paper**

Hidden Indicator Based PIN-Entry Method Using Audio Signals

Hwajeong Seo[1] and Howon Kim[2*], *Member, KIICE*

[1]Department of IT Convergence Engineering, Hansung University, Seoul 02876, Korea
[2]Department of Computer Engineering, Pusan National University, Busan 46241, Korea

Abstract

PIN-entry interfaces have high risks to leak secret values if the malicious attackers perform shoulder-surfing attacks with advanced monitoring and observation devices. To make the PIN-entry secure, many studies have considered invisible radio channels as a secure medium to deliver private information. However, the methods are also vulnerable if the malicious adversaries find a hint of secret values from user's naïve gestures. In this paper, we revisit the state-of-art radio channel based bimodal PIN-entry method and analyze the information leakage from the previous method by exploiting the sight tracking attacks. The proposed sight tracking attack technique significantly reduces the original password complexities by 93.8% after post-processing. To keep the security level strong, we introduce the advanced bimodal PIN-entry technique. The new technique delivers the secret indicator information through a secure radio channel and the smartphone screen only displays the multiple indicator options without corresponding numbers. Afterwards, the users select the target value by following the circular layout. The method completely hides the password and is secure against the advanced shoulder-surfing attacks.

Index Terms: Personal identification number, Random guessing attack, Shoulder surfing attack, User authentication

I. INTRODUCTION

Traditional PIN-entry interfaces have high risks to leak secret values if the malicious attackers perform shoulder-surfing attacks with advanced monitoring and observation devices. Since the shoulder-surfing attacks usually capture the visual information on the screen or the user's gestures, many studies have considered invisible radio channels as a secure medium to deliver private information. The recent radio channel based PIN-entry technique suggested by Lee et al. [1] is a method that can deliver the minimum indicator information through a radio channel and then the users match the indicator to the corresponding target number on the screen.

This approach has accomplished the high usability together with security against shoulder-surfing attacks. However, the method can be cracked by adversaries who can observe the user's touch screen and user's sight information. In this paper, we demonstrate the new hacking techniques by Lee et al. that can track the user's sight together with a touch screen. The method can reduce the list of possible passwords by extracting the potential password from collected information. To resolve the vulnerabilities, we introduce a secure hidden-indicator based PIN-entry technique. The method hides all secret values, but the users can efficiently enter their passwords.

Received 15 April 2017, **Revised** 12 May 2017, **Accepted** 19 June 2017
***Corresponding Author** Howon Kim (E-mail: howonkim@pusan.ac.kr, Tel: +82-51-510-1010)
Department of Computer Engineering, Pusan National University, 2, Busandaehak-ro 63beon-gil, Geumjeong-gu, Busan 46241, Korea.

Open Access **http://doi.org/10.6109/jicce.2017.15.2.91** print ISSN: 2234-8255 online ISSN: 2234-8883

II. RELATED WORK

A. PIN-Entry Method

The service providers need to check the validity of the user's identity before providing private and confidential services. The well-known authentication medium is Personal Identification Number (PIN), which indicates the user's authenticity in a virtual world. Therefore, the information should be transferred from users to service servers through secure PIN-entry methods. If the PIN information is delivered from the user's devices to service servers in an encrypted format, the adversaries cannot extract confidential information from the network's packets. However, if adversaries observe the input patterns by performing shoulder-surfing attacks, the user's confidential information can be easily extracted from the observed information. To prevent shoulder-surfing attacks, the PIN-entry methods need to provide high security against shoulder-surfing attacks.

In [1], the author introduced the regular PIN-entry method with audio signals. The PIN-entry is a set of ordered decimal digits and only the starting point is randomized. The authenticator is randomly selected and vocalized in an incremental order. When the target number is vocalized, the users can select the number by pressing the confirmation button. This can be optimized by adding the skip buttons. The formal form of the decimal digit based PIN-entry technique is the Phone Lock method. In the Phone Lock method, an empty dial with ten sectors are displayed [2]. The user scrolls the dial in a clockwise or counter clockwise direction and the numbers are vocalized in incremental or decremental orders. When the user finds the target number, the user selects it by dragging and dropping the corresponding sector to the center of the Phone Lock, which confirms the current inputs. In [1], the author presented the audio channel based PIN-entry method. The method only transmits the minimal required data, which represents the indicator. On the screen, the indicators and corresponding numbers are only displayed. By placing the target number below the indicator, the users can enter the target PIN. The method shows that the PIN-entry timing is shorter than traditional audio-based methods while its error rate is kept as low as that of previous methods.

However, we found that the method can be vulnerable to advanced shoulder surfing attacks if adversaries can observe the user's sight and touch screen in high precision by using advanced observation devices such as small camera or Google Glass. In the following section, we introduce the attack models on the PIN-entry methods.

B. Threat Model

To get the authenticated services, the users need to enter the valid passwords into the target systems. However, traditional password input methods are not secure against sophisticated shoulder-surfing attacks with advanced monitoring/wearable devices, which can lead to information disclosure and security holes. These threat models are largely categorized in vision, haptic, and acoustic channels. The vision based eavesdropping directly captures the password entry by using a hidden small camera or a close look around the users. In Black Hat USA 2014, the authors demonstrated that adversaries can infer the password entry position from a long distance with the Google Glass while the attacker cannot see any text or pop-ups from the video of the victim tapping on the touch screen [3]. This captures the user's finger movements and angle information, which indicated the possible passwords. As the wearable devices are getting pervasive and common platforms, sophisticated recording attacks can be easily performed. The second threat is haptic based eavesdropping. This includes a physical key logger to infer the touched position. The physical key logger installed below the touch screen can capture the exact touched position. Afterwards, malicious attackers can perform a matching process between the touched position and corresponding numbers/letters. The last model is acoustics-based eavesdropping such as key-press sound or tones. Depending on the touched position and power of key-strokes, different patterns of tones and sound can be observed. These unique sounds indicate the specific password entered by the users. However, the attacks are conducted in a very controlled place since the tones cannot be captured properly in noisy environments. Lastly, the user's behavior becomes one source of an attack scenario. The wearable device equips the various sensors and these sensors can monitor the user's acceleration information. This information can be abused by malicious users to extract private information. In WISA'15, the hacking methods for the door lock system with a smart watch were introduced [4]. The author showed that the accelerator information includes the user's activities and gestures. This information can be used to infer the proper input password through PIN-entry devices.

III. ATTACK ON ARRANGEMENT PAD

The radio channel based arrangement PAD suggested by Lee et al. [1] ensures strong security against shoulder-surfing attacks with reasonable usability. This approach is flawless against the shoulder-surfing attacks under traditional computer settings. However, as the wearable devices with high precision cameras such as Google Glass

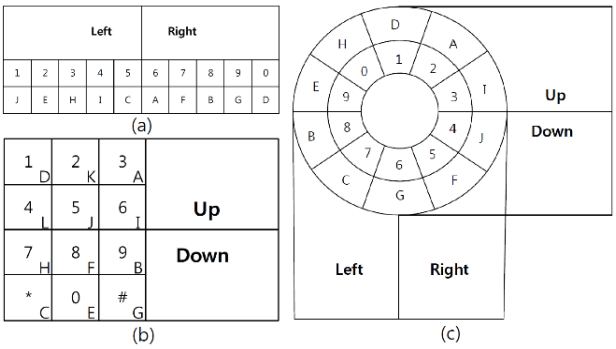

Fig. 1. Design of arrangement PAD: (a) LinA, (b) RegA, (c) DialA.

and smartwatches became available, some of the traditional secure measures have encountered new vulnerabilities since the devices are able to record the user's gestures or activities in high precision and the data can be exploited for malicious attacks.

To ensure the high security under wearable computing environments, we need to revisit the previously secure PIN-entry techniques and re-evaluate the security under these new conditions. In this section, we revisit the radio channel based arrangement PAD and introduce the new vulnerability under new computing environments. The arrangement PAD displays the layout consisting of ten numbers and their corresponding mixed indicators. This layout does not reveal the secret correlation information between the target numbers and indicators in the visual channel do not have information about the selected indicator. Since the indicator information is transferred through a secure radio channel, the indicator information is always kept in a secret value. If the users receive the indicator information, the users try to match the indicator to the corresponding target numbers by controlling the buttons. The layout on the screen does not include any secret values and only the legitimate users can recognize the secret values.

However, the method can be broken if the adversaries can observe the user's gestures and touch screen in high precision. Through the touch screen, the current layout and adjustment activities can be observed. This information does not include any secret values since the adversaries cannot recognize the secret input values. To find the secret input values, the adversaries need to know the secret indicators. This secret indicators can be extracted if the adversaries observe the user's gestures, which include the secret indicator information. The procedures for arranging the PAD largely consists of three steps to enter the secret values. First the secure radio channel delivers the secret indicator information to the users. Second, the legitimate users adjust the PAD and place the indicator under the corresponding target number. Finally, the users press the enter button to add the selected number to the input list. This whole process is flawless, but at the end of second step, the users need to place the indicator under the target number and check whether the secret indicator is placed correctly under the target number. At that moment, the adversaries can capture the secret indicator position on the touch screen by observing the user's sight and status of the touch screen.

For the general attack model, we first reduce the possible password list. Instead of the exact password input, we infer the password group which includes all possible adjacent passwords. Fig. 1 shows the partitioning of arrangement PAD for Linear Arrangement (LinA), Regular Arrangement (RegA), and Dial Arrangement (DialA). The LinA displays the layout in a horizontal way and we divide the layout into two parts, including left and right. The RegA displays the layout in a rectangular form and we divide the layout vertically into two parts, including up and down. The DialA displays the layout in a circular form, and we divide the layout into four parts, including up, down, left, and right.

The detailed attack procedures are described in Table 1. In each key-entry, the user's touch gestures and sight movements are recorded and observed. When the user presses the confirm button, the indicator position is estimated with the user's sight and pad layout on the touch screen. We choose the password group that is indicated by the user's sight. To demonstrate the attack model, we tested the LinA layout on a Galaxy Note5 smartphone. The height and weight of the touch-screen are 153.2 mm and 76.1 mm, respectively [5]. The experimental layout is divided into left and right sections and each part includes five different elements.

Table 1. Attack on arrangement PAD

input: Touch gesture, sight movement **output**: Estimated password group

while User adjusts the PIN-entry PAD **do**
  if User presses the confirm button **then**
  Analyze the user's sight before pressing the button
  Determine the password group (user watched)
  return Estimated password group

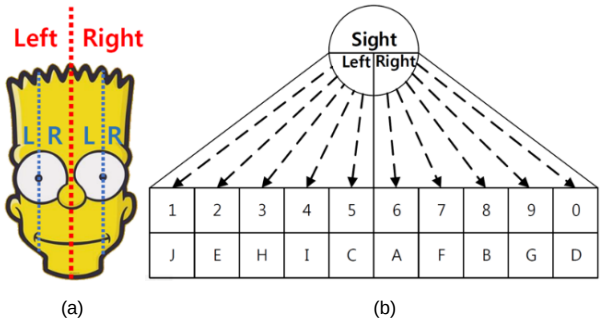

Fig. 2. (a) User's sight and gesture separations, (b) model of sight tracing for arranged PAD.

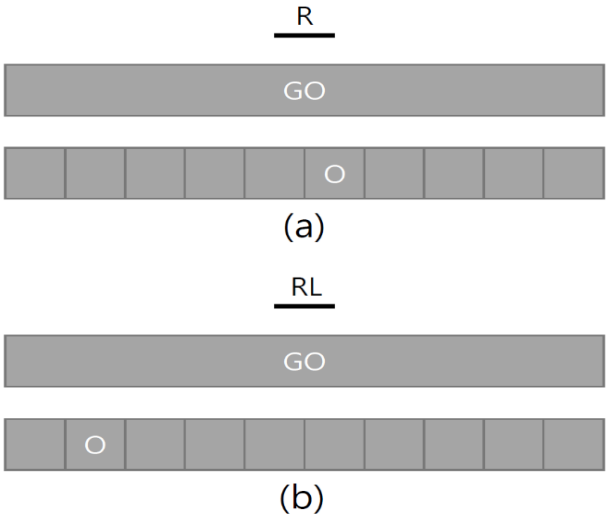

Fig. 3. Experiment of eye tracking attack: (a) right direction, (b) left direction.

The specific gesture and sight are easily classified by setting the simple boundaries. The detailed descriptions are available in Fig. 2.

First, the user's facial gestures are separated into left and right directions by setting red dotted lines to the middle line. Second, the user's sight is separated into left and right directions by setting blue dotted lines to the middle line. During the experiments, two different views, including the user's face and screen, are recorded with smart-phones, and this was analyzed by the authors. Afterwards, the real indicator position and predicted position are compared to evaluate the accuracy.

The detailed experiment procedures are drawn in Fig. 3. First the user presses the GO button to start the experiment session.

Then, a symbol (O) randomly appears on one button and the user watches the button for a while. At that moment, the user's sight is observed to determine the direction and whether the user looks at the right or left screens. This attack scenario reduces the possible PIN number cases from 10 to 5 when the observation is correct since we divided the password layout into left and right sections. Each section also only includes 5 different options every time. We tested this attack scenario 10 times for 10 candidates. The observation results showed high success rates (89%) to determine the user's possible password section. For 4-digit PIN cases, a total of 10,000 (10^4) cases of password combinations are available. However, after performing the proposed attack on the PIN-entry method, the possible cases can be reduced to roughly 625 (5^4) cases, which is about a 93.8% complexity reduction. Furthermore, the possible cases can be reduced again if multiple attacks are performed, if the password is '1', and if the adversary observes two times the input entry. Every time, the users look at the groups that included (1, 3, 5, 7, 9) and (1, 2, 3, 6, 9). The common elements in both groups are only (1, 3, 9) so we can reduce the cases from 5 to 3. With these multiple trials, the possible cases are reduced and accuracy is improved. The proposed attack method can be performed for other arranged PAD techniques, including RegA and DialA by grouping the layout as described in Fig. 1.

Table 2. Hidden-Indicator PAD

input: Touch screen, random channel **output**: Password

Password is initialized
while EXIT is not entered **do**
Indicator is randomly generated
Indicator is vocalized
if Target button is entered **then**
Target number is updated to password
else if CLEAR is entered **then**
Last input in password is removed
return Password

IV. HIDDEN-INDICATOR PAD

In the previous section, we demonstrated that the close observations on the user's sight and touchscreen can reveal the secret indicator information handled in the arranged PAD. The sight tracking attack model finds the pre-knowledges that the arranged PAD has hidden relations between the indicator and corresponding number. For this reason, we should hide the relation information completely to protect the proposed attack model. To resolve this issue, we present the new PIN-entry techniques called Hidden-Indicator PAD. The proposed PIN-entry method delivers the indicator information through the radio channel but the corresponding numbers are not displayed on the screen. Instead, the corresponding numbers are reconstructed with hidden indicator information and layout. The details of the proposed Hidden-Indicator PAD are described in Table 2.

The requirements for the proposed method are touch screen and radio channel, which are identical settings with previous radio based PIN-entry techniques. Firstly, the password is initialized to get the new password inputs. Then, the current indicator is randomly selected from random numbers by using random number generator. The selected random indicator is delivered through a radio channel. This information is only accessible when the users have valid equipment to receive the indicator information without any leakage. With the indicator information, the users map the target numbers over the given indicator interfaces, where the indicator represents the '0' value, and when the other numbers are mapped to values in a circular form. If the user

finds the target number from the layout, the user presses the button to update the password. When the user wants to remove the last input from the password, the user presses the ‘CLEAR’ button. This process is iterated several times until the password is fully filled. Finally, the user finishes the session by pressing the ‘EXIT’ button.

To improve the usability, we introduce two techniques. The first technique is a multiple-indicator based approach. The basic version only informs the starting indicator and the users need to map the nine numbers based on the obtained single indicator. The number is estimated by offsets and the maximum offset is 5 by considering both the clockwise and counter clockwise directions. This technique can be improved, as we set multiple indicators to estimate the numbers with short offsets. Taking an example of two indicators, the first indicator presents the number '0' and the second indicator presents the number '5'. This model shortens the maximum offsets from 5 to 3 compared to the original model. The second technique is the optimal input layout. If we design the input layout on a traditional keyboard, the users cannot find the proper numbers on the buttons by counting the offsets. We chose the circular form of input-entry and the users can easily explore the target numbers by following the circular path.

V. EVALUATION

A. Usability

To evaluate the usability, we implemented the proposed PIN-entry method on an android smartphone. The vocalization is available through the radio data obtained from Ivona [6]. Each radio data vocalized the two English letters within 1 second. Among the several options, we chose the female British English option for pronunciation, which showed the clearest and most accurate pronunciation among the options. The radio data were operated by using android libraries, including android.media.AudioManager and android.media.MediaPlayer. For the randomization of indicator, we used the random Java library (java.util. Random). The detailed experiment settings are described in Fig. 4. In the initial stage, 10 indicator letters are placed on the screen. If the users press the (‘TEST #4’) button, a random 4-digit (8074) appears on the screen. After the users receive the indicator information through a radio channel, they can enter the secret values. Finally, the users press the ‘ENTER’ button to enter the secret values. Afterwards, the performance based on accuracy and timing is displayed. The process is performed 10 times and the average values are used for comparison results. The Phone Lock method needs to check the base number, and then the users can explore the target numbers through the pad. The arranged PAD method needs to check the indicator information and then place the indicator below the target number. For this reason, the techniques require two or three inputs per letter on average. On the other hand, the proposed hidden-indicator method only requires a single click to select each target number. As we can see in Table 3, the proposed method shows the highest performance.

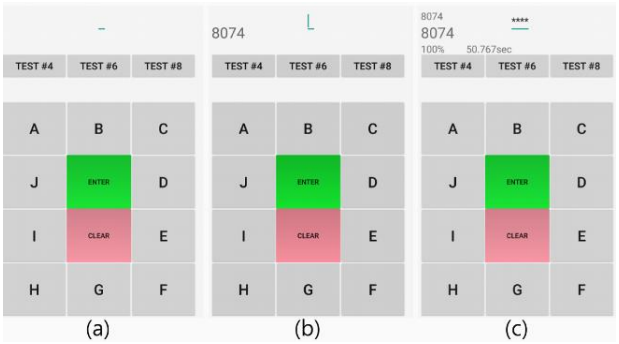

Fig. 4. Experiment of hidden indicator PAD: (a) initial idle screen, (b) initial test screen, and (c) test result screen.

Table 3. Comparison of usability and security

Method	Transmitted audio data	Time (s)	P_{GA}	P_{RA}	P_{CA}
IOC [7]	None	23.2	$\frac{1}{10^4}$	1	$\frac{1}{10^4}$
IOC_A [7]	Color	N/A	$\frac{1}{10^4}$	$\frac{1}{10^4}$	$\frac{1}{10^4}$
$mTimelock_A$ [1, 8]	Beep	16.4	$\frac{1}{10^4}$	$\ll \frac{1}{10^4}$	$\frac{1}{10^4}$
Phone Lock [2]	Number	13.9	$\frac{1}{10^4}$	$\frac{1}{10^4}$	$\frac{1}{10^4}$
LinA [1]	Indicator	12.8	$\frac{1}{10^4}$	$\frac{1}{5^4} \ll$	$\frac{1}{10^4}$
Proposed	Indicator	9.1	$\frac{1}{10^4}$	$\frac{1}{10^4}$	$\frac{1}{10^4}$

B. Security

The security levels are evaluated in three different aspects. The first test is the probability of a successful guessing attack (P_{GA}). This attack tests the probability of guessing the correct PIN or correct responses The second test is the probability of a successful recording attack against the PIN-entry method (P_{RA}). The attacker challenges the PIN-entry by using the information obtained from recorded sessions against the identical PIN. The last test is the probability of a successful challenge-only attack against the PIN-entry method (P_{CA}). The attacker can pass the PIN-entry test by using the information from previous challenges for the identical PIN. All probabilities are evaluated under the

random choice of the attacker. In terms of P_{GA}, the proposed method can be any password given from a list of possible password so it is impossible to guess. For P_{RA}, the proposed method does not reveal any information through recorded information since the visual channel does not leak any secret values. However, the previous LinA method has vulnerability as we explored before. The attack reduces the complexity of the LinA technique significantly. For P_{CA}, the proposed method changes the input layout at every session, which hides the secret value completely.

VI. CONCLUSION

In this paper, we explored the secure PIN-entry method for user authentication. First, we pointed out that the previous radio channel based PIN-entry method can be broken if the adversaries can record the user's touch screen and sight with a high-end camera or Google Glass devices. This is the first trial to combine both information to extract the secret values from radio channel based PIN-entry methods. Second, to resolve the security hole in the arranged PAD technique, we suggest the hidden indicator based PIN-entry method. The proposed method only displays the indicator without corresponding numbers. This technique introduces security against advanced shoulder-surfing attacks. Furthermore, the users can select the target password directly without exploring the all cases, which improves the performance.

ACKNOWLEDGMENTS

This research was supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIP) (No. 2012-0-00265, R0101-17-0129, Development of high performance IoT device and Open Platform with Intelligent Software). This research of Hwajeong Seo was financially supported by Hansung University.

REFERENCES

[1] M. K. Lee, H. Nam, and D. K. Kim, "Secure bimodal pin-entry method using audio signals," *Computers & Security*, vol. 56, pp. 140-150, 2016.

[2] 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 *Proceedings of the 5th International Conference on Tangible, Embedded, and Embodied Interaction*, Funchal, Portugal, pp. 197-200, 2011.

[3] Q. Yue, Z. Ling, B. Liu, X. Fu, and W. Zhao, "Blind recognition of touched keys: attack and countermeasures," 2014 [Internet], Available: https://arxiv.org/abs/1403.4829.

[4] H. Seo, Z. Liu, G. Seo, T. Park, J. Choi, and H. Kim, "Open sesame! Hacking the password," in *Information Security Applications, Lecture Notes in Computer Science*, vol. 9503, pp. 215-226, 2015.

[5] Specification of the Samsung Galaxy Note5, 2016 [Internet], Available: http://www.gsmarena.com/samsung_galaxy_note5-7431.php.

[6] V. Roth, K. Richter, and R. Freidinger, "A pin-entry method resilient against shoulder surfing," in *Proceedings of the 11th ACM Conference on Computer and Communications Security*, Washington, DC, pp. 236-245, 2004.

[7] A. Bianchi, I. Oakley, and D. S. Kwon, "Counting clicks and beeps: Exploring numerosity based haptic and audio pin entry," *Interacting with Computers*, vol. 24, no. 5, pp. 409-422, 2012.

[8] Ivona Text-to-Speech, 2016 [Internet], Available: https://www.ivona.com.

Hwajeong Seo
received the B.S.E.E. degree in 2010, and the M.S. degree in 2012 and the Ph.D. degree in 2016 in Pusan National University. He is currently an assistant professor in Hansung University.

Howon Kim
received the B.S.E.E. degree from Kyungpook National University, Daegu, Korea, in 1993, and the M.S. and Ph.D. degrees in electronic and electrical engineering from the Pohang University of Science and Technology, Pohang, Korea, in 1995 and 1999, respectively. From 2003 to 2004, he studied with the COSY Group, Ruhr University Bochum, Germany. He was a Senior Member of the Technical Staff with the Electronics and Telecommunications Research Institute, Daejeon, Korea. He is currently an Associate Professor in Pusan National University.