한국정보전자통신기술학회논문지(jkiiect)'20-2, Vol.13 No.1
논문 20-13-01-17 http://dx.doi.org/10.17661/jkiiect.2020.13.1.17

Security Analysis of Partially Hidden Password Systems Resistant to Shoulder Surfing Attacks

Jin-Taek Seong*

Abstract As more users use mobile devices, shoulder surfing attacks have emerged as an important issue in security. According to research report, in fact, the result showed that about 30% of smartphone users are hit by shoulder surfing attacks. To this end, in this paper, we consider a shoulder surfing attack and propose a partially hidden password system to resistant to its attack. In order to help readers understand, we describe the proposed password system in more detail using one simple example. The core idea behind the proposed system is to place the user's password randomly in the specified grid instead of entering a password directly. As a result, even if an attacker makes a shoulder surfing attack to observe the password, the user can hide the preset password and defend against the attack. We also show how the security of the password system proposed in this paper is improved. In addition, even if there are consecutive shoulder surfing attacks, the security of the proposed password system is robust.

Key Words : Hidden Password System, Random Guessing Attack, Security, Shoulder Surfing Attack

1. Introduction

Conventional smartphone unlocking principles rely on user presets such as personal identification numbers (PINs), passwords or graphical pattern locks. So far, these are practical and widely used [1], [2]. Despite the increased availability of biometric options such as fingerprint and face recognition, conventional approaches are used as alternative authentication ways when biometric tools fail. However attackers do not use special equipment or techniques, so that shoulder surfing attacks are particularly deadly and irreversible for the conventional password systems. As a result, much effort has been made to protect existing password systems to defend against these malicious attacks [3]-[5].

There have been some defensive efforts lately, but there was no fundamental way to combat shoulder surfing attacks [2], [7]. In [2], the authors surveyed on an online, and showed that about 30% of the participants were concerned which someone can see those while mobile devices unlock and steal their authentication processes. In practice, participants were aware of that shoulder surfing occurs one out of five times. In case of that shoulder surfing may takes place in private spaces, the possible attackers are likely malicious insiders. Another way to defend against the most shoulder surfing is to tilt or rotate their screens so that the devices are not visible to the attackers. Another research showed that the use of this defense was carried out in a subtle way when the observer

This paper was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (NRF- 2017R1C1B5075823).
*Department of Convergence Software, Mokpo National University (jtseong@mokpo.ac.kr)
Received January 09, 2020 Revised January 16, 2020 Accepted January 20, 2020

recognized [7].

In addition, several variations of shoulder surfing resistance for conventional authentication methods have been proposed in [4], [8]. Most alternatives require major changes to the latest PIN input entry or the addition of new communications. Recent promising ways do not require any changes to the PIN input entry but utilize a pressure-sensitive capacitive touchscreen [3], [5]. In this case, users put more high pressure on a subset of PIN keypads as their passwords. The result of this experiment showed that the invisible pressure subpart prevents shoulder surfing [5].

Shoulder surfing was a well-known attack on password authentication, but it was limited to defending it in the conventional way. If an attacker is observing this while the user is entering a password using a mobile device in a public place, the attacker can be aware of the password. An attacker can also intercept the password by observing it or by remembering the individual's authentication process. Current approaches to preventing shoulder surfing generally reduce the system's usability and convenience. In addition, users are often required to use security tokens. And the conventional approaches not only provide direct feedbacks, but also interact with systems that require additional steps to ensure that the observers are not sure of the passwords the users entered to steal their passwords.

In this paper we propose a partially hidden password system to defend from a shoulder surfing attack. And we discuss its security and usability by obtaining two resistances, i.e., random guessing and shoulder surfing. A detail introduction to our proposed password system is provided in Section 3. The key idea behind the proposed password system is to place the user's password randomly in the specified password grid instead of entering a password. We can unlock the password system by placing one digit of the correct password in each column of the specified grid. As a result, even if an attacker makes a shoulder surfing attack to steal a password, the user can hide the preset password and defend against the attack. The reason for increase of the security in our proposed system is that it displays user's password by including decoy digits like noise on the screen. The contribution of this paper is more sophisticated security analysis than the paper [6]. In this paper, we obtain a more accurate probability of guessing a password when there are consecutive shoulder surfing attacks.

This paper is organized as follows. First, we provide a variety of authentication and introduce related works for defenses against shoulder surfing attacks in Section 2. And then, in Section 3, we introduce our proposed partially hidden password system and describe a detail principle for the use of the password system. In Section 4, we present its security with respect to two resistances from random guessing and shoulder surfing attacks. Finally, we summarize and conclude our contributions in Section 5.

2. Related Work

2.1 Authentication

As an approach for user authentication in a mobile device, a text-based password method, a graphical-based password, a combination of both, and a way using a user's fingerprint or face have been studied. In this section, we will

look into the research except for biometric information that requires additional equipment.

2.1.1 Text-based Password

Text-based password authentication is a method of entering a password using numbers or a combination of numbers and letters. Among the text-based authentication methods, a PIN is a user authentication approach that is used for various aims, such as a bank account, a credit card password, or a smartphone unlock number. The conventional password system inputting simple 4-digit numbers is known to be vulnerable to surfing or shooting attacks because authentication is always performed using the same input method, and a lot of studies have been conducted to supplement it.

The binary system consists of binary 10 digits using 1 or 0 in the same order as a normal PIN password, with five backgrounds painted in white and the rest in black [9]. For each authentication, the numbers in black and white are randomly determined. The user does not press the number that needs to be entered at the current step, but instead enters the background color of the number by selecting the black or white button below. To enter a single PIN number, four color selection steps are required. To enter a commonly used four-digit PIN number, 16 black or white buttons must be repeated.

The LIN system performs authentication by randomly placing familiar symbols under 10 digits and matching PIN numbers to the symbols [10]. That is, the user first remembers the symbol under the first digit of the PIN number as the session key and presses the confirmation button. In steps 2 to 4, the second to fourth digits of the PIN are entered according to this session key. When entering, press the Left or Right button appropriately to move the session key to match the PIN number of the step and press OK to enter.

ColorPIN defines a new PIN so that each digit of the PIN consists of an ordered pair of numbers from 1 to 9 and one of black, red and white [11]. For example, if the PIN is equal to 1 (black), 2 (red), 3 (white) and 4 (black), the user is given a randomly selected three letters below the first one of his first PIN number. We check the 'Q' painted in black, our first PIN, and enter it on the keypad. The letters on the PIN pad are designed so that 9 different letters appear below the three number pads.

2.1.2 Graphical-based Password

A graphical password system is a technique for users to create and authenticate passwords using images or graphics provided by its system [12]. Graphical-based password schemes have been developed rapidly to overcome the shortcomings of text-based authentication and to replace text-based passwords. Passfaces proposed in [13] is a way of entering passwords using the image of a person's face rather than numbers or letters. In this way, a human face for user authentication is stored in a database and a password is set using four human faces from among the stored human face images.

And in [14], the Draw-A-Secret system allows the user to draw patterns on divided screens. The order of the passing sections is stored when the pattern is drawn, and the user performs authentication by remembering and reproducing the pattern drawn when creating the password and the order in which section to draw the pattern [14].

2.1.3 Combination of Graphical and Text-based Password

A hybrid system using a combination of graphical-based and text-based passwords is proposed called as Scalable Shoulder-surfing Resistant Textual Graphical Password Authentication System (S3PAS) in [15]. In this system, the user finds the original path-characters shown in the login screen and clicks inside the invisible triangle called pass-triangles. In this S3PAS, each user has two passwords: the original password and the session password. The user selects the original password when the account is created and the user enters a different session password during every login process. Therefore, the original password of the user can be prevented from being exposed.

2.2 Shoulder Surfing Attack Resistance

Some ways to be resistant shoulder surfing attacks have been proposed for knowledge-based authentication systems. In [2], the authors widely classified them into four categories: 1) indirect input schemes, 2) additional layer of implicit biometric schemes, 3) input obfuscation schemes, and 4) nonobservable channel schemes. We review a brief overview and canonical examples for each scheme.

Indirect input schemes display problems on one interface and require a response to another interface in [4], [16]. The requirements of additional interfaces or devices are inherent limitations of these systems.

Considering the device user's touch input behavior during authentication, the authors proposed a system that provides an additional layer of defense. However, previous studies have demonstrated that shoulder surfing attacks can mimic touch input gestures.

An input obfuscation scheme converts secret input interface to prevent shoulder surfing [7], [17]-[20]. However, most proposed systems are complex and less convenient to use [2]. For example, in [8] SwiPIN converts the interface by displaying PIN numbers in a red and yellow layout. It also displays the PIN entry field as a field of the same color. The user enters a number in the input field using a swipe or tap gesture that corresponds to the layout color of the PIN number. After each number input, the layout is randomized again. In [21], the authors demonstrated that the increased complexity of SwiPIN can be broken through computer-based simulations after 6-11 observations by human observers.

Systems for setting up unobservable channels include an approach using pressure dimensions [3], [5], [22] and tactile feedback [23]. The former approach takes advantage of the observation that smartphone touch screens can distinguish different pressure levels. In [5], the authors proposed a scheme for adding explicit pressure to a subset of the digits entered by the user. Introducing a binary state for pressure increases the password space of 4-digit PINs. The authors performed two experiments to show that their scheme was resilient to shoulder surfing attacks.

3. Partially Hidden Password System

In this section, we propose a new partially hidden password system that is robust to shoulder surfing attacks. First, we define the proposed model. And a simple example is used to help clearly clarify our password system. For the terminology described in this paper, see in [6].

3.1. Description of Proposed Model

The key idea behind a partially hidden password system to be resistant to shoulder surfing attacks is to place the dummy digits on the screen as shown in Figure 1. The user is required to place its password on the given $W \times H$ grid instead of entering the password in order to be authenticated. The user can rotate or slide the digit array to see a different choice of characters. This way allows attackers to not observe a user's password. In this section, we define an authentication model for our partially hidden password system as shown in Figure1.

Now we introduce the proposed password system. Let $\Omega(N, W, H)$ be a partially hidden password system with an $W \times H$ grid as a user screen to input a user's password. And let N be the number of available digits in a grid in our password system. Let W be the number of columns in an $W \times H$ grid, i.e., it is the length of the user's password. And, let H be the number of rows in an $W \times H$ grid that is used for a selection of candidate digits.

The steps for setting and unlocking a password is as follows. First, to set a password, we randomly generate permuted sequences equivalent to the number of columns in the grid in any order. We set arbitrary one password of size W.

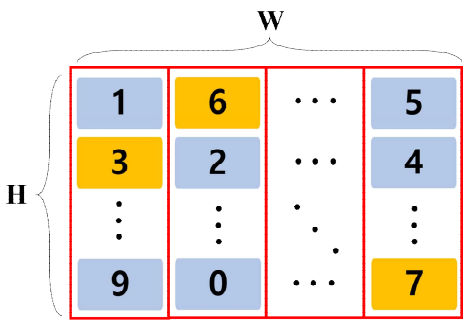

Fig. 1. The proposed partially hidden system with H rows and W columns on digit of user's password is located on each column to be authenticated, respectively.

The following steps have to be observed to unlock the password. Each digit of the password we set is placed on arbitrary position of each column in the defined grid. If $W=1$, we can only unlock this password if we set it on one row. This case is the same as setting and unlocking passwords with numbers in the past. However, this method can be decrypted as soon as the password is compromised by a malicious attacker. Considering $W \geq 2$, we can safely protect the password system even if there is a shoulder surfing attack. In other words, even if all the digits on the screen are observed, the set password is hidden on the screen to be resistant to shoulder surfing attacks. This is the reason for increasing the security of the proposed password system.

3.2. One Example

Next, a more detailed example of the proposed password system is shown in Figure 2. The proposed password system has $W=3$ and $H=3$. Assume that the password is (3 6 7). Three digits in each column of the grid are randomly generated sequences without duplicates. To unlock password (3 6 7), the first digit 3 should be located anywhere in the three rows of the first column. The second digit 6 should be placed in the second column. In the same way, the third digit 7 must be placed in an arbitrary row in the last column. If any of (3 6 7) three digits are not in each corresponding column of the given $W \times H$ space, the password cannot be solved easily.

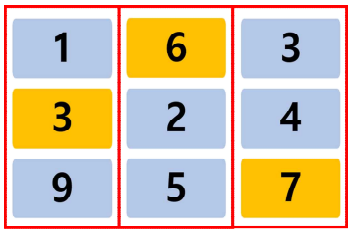

Fig. 2. An example of the proposed partially hidden password system with $H=3$ and $W=3$ where the password is (3 6 7) three digits.

We describe the relationship between the number of rows H and shoulder surfing resistance. Suppose an attacker observes a user entering a password. If the number of rows in the given password grid is 1, i.e., $H=1$, the attacker sees a single password sequence on the screen so that a single shoulder surfing attack can break a user's password. On the other hand, if $H \geq 2$, it is slightly difficult to know the exact password even if the attacker has a shoulder surfing attack. In the case of $H=2$ and $W=5$, there are 32(=25) possible passwords. Setting a larger H makes it more difficult for an attacker to guess a user's password. For example, an attacker knows the entire authentication process, but only knows that the user's password is one of 243 sequences for the proposed password system with $H=3$ and $W=5$.

4. Theoretical Analysis of Security

In this section, we define the two matrices such as Random Guessing Attack Resistance (RGAR) and Shoulder Surfing Attack Resistance (SSAR) for a model $\Omega(N,W,H)$ to be resistant to shoulder surfing attacks. This section refers to the security analysis presented in [6]. In this section, we improve the SSAR because the paper [6] does not accurately analyze the security of SSAR. We analyze its security with respect to random guessing and should surfing attacks. And then, we show that our proposed model is superior and more secure compared to other approaches

4.1 Security for Random Guessing Attack

A random guessing attack is an attack where an attacker randomly guesses and enters a password through guessing. For example, suppose that the choice of the user's password is random, the larger the available password space, the higher the safety. The password space is defined by the number of combinations for feasible passwords. The number of combinations that a user or an attacker can enter can be defined as the safety of the random guessing attack. The security of random guessing attacks and the security of peeping attacks are inversely related. In other words, if the password by using input method is designed to be more secure against the peeping attack, the success rate of the guessing attack is higher. As a solution to this, a method of increasing the size of the password space or using an unobservable channel when an attacker inputs a password is proposed.

For $\Omega(N,W,H)$ with an $W \times H$ grid as defined in Section 3.1, let RGAR be defined as the probability that random guessing attacks break the proposed partially hidden password. Now we consider and compute a RGAR. First, we define the probability that the ith password letter is on ith column is H/N, where $i \in \{1,2,\cdots,W\}$. The reason is that for each column, H elements are selected from N digits that in the total number of letters in a grid. Since each column is independent with each other, the probability that random attacks

break $\Omega(N, W, H)$ becomes $(H/N)^W$. Therefore, RGAR for the defined system $\Omega(N, W, H)$ is obtained as follows [6],

$$RGAR(\Omega(N, W, H)) = \left(\frac{H}{N}\right)^W \quad (1)$$

4.2 Security for Shoulder Surfing Attack

Shoulder surfing attack cannot be successful even if the user enters the same digits obtained through observing because they cannot distinguish between tapping a number or color even if a user presses a button. In the case of the general PIN system, when an attacker observes the authentication process, the probability of successful authentication through the observation is 1. In other words, assuming that the user's password is (1 2 3 4), since the information obtained by the attacker requires the same digits to be input every time, the probability of successful attack is 1 through the obtained information. In the case of the proposed partially hidden password system, since the information obtained through peeping contains H possible events of information for each digit, even if four digits of information are obtained, the probability of success using the information for the next authentication is $1/243$ for $H=3$ and $W=5$.

Now we aim to find the resistance for shoulder surfing attacks. To this end, we assume that K times are tried consecutively by an attacker to observe the hidden password. And then, the attacker randomly chooses a possible password that meets the requirement for K times of shoulder surfing. In other words, the one digit of the preset password for each column in a $W \times H$ grid should be shown in every shoulder surfing. As the observation to the attacker increases, the preset password is highly expected. Suppose that for $\Omega(N, W, H)$ with an $W \times H$ grid, let SSAR be defined as the probability that shoulder surfing attacks break the proposed partially hidden password. And a password in an $W \times H$ grid is revealed by shoulder surfing attacks.

To find SSAR, in [6], the authors consider the following idea. Each column of the password grid is independent with each other. For each column at K shoulder surfing attacks, there is the average number of possible passwords. That is, it is a combination of one exact digit and the average number of non-password letters. Assume there is a password in a $W \times H$ grid. For each column, one digit is correct and the $H-1$ other digits are randomly chosen from letters for K times. Therefore, in [6] using the average number of possible passwords in each column, the authors obtain SSAR as follows,

$$SSAR(\Omega(N, W, H), K) = \left(\frac{1}{1+(H-1)\left(\frac{H-1}{N-1}\right)^{K-1}}\right)^W \quad (2)$$

Since Eq. (2) is not concrete, we need to obtain a more precise and accurate the SSAR . As defined in [6], we also find out the probability of guessing the password when there are K shoulder surfing attacks. First consider a simple model where $M=1$. That is, the password is designed by only one digit in our scheme. In the case of one shoulder surfing attack, we can guess the password with a probability of $1/H$. What if there are two consecutive shoulder surfing attacks? Since there are two attacks, the correct password will be appeared twice. The same number may appear twice in different $H-1$ positions. Otherwise, you may see different numbers in two attacks.

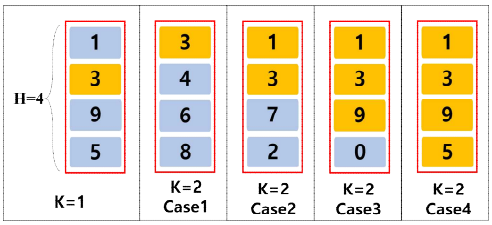

Fig. 3. Cases of the password system with $H=4$ and $W=1$ having 2 times shoulder surfing attacks

Figure 3 shows a simple example when $H=4$. In the first shoulder surfing attack, SSAR is $1/4$ because one of {1, 3, 9, 5} is the correct password. In the case of a second shoulder surfing attack, four different cases can be seen as shown in Figure 3. Case1 is the case where only the correct password 3 appears twice in a row. In this case the correct password is exactly 3. In the case of Case2, we can say that the password is 1 or 3 because {1, 3} is shown in duplicate. And in Cases 3 and 4 we have $1/3$ and $1/4$ chances of guessing a password.

If there are K shoulder surfing attacks, only the number of K consecutive digits should be considered except the correct password. In other words, if a digit has never been found in K observations, this digit is not a password. Therefore we can specifically express it as

$$\sum_{S=1}^{H}\Pr(Correct|X_S)\Pr(X_S) \tag{3}$$

where $\Pr(Correct|X_S)$ is the conditional probability that the correct password is guessed when all of the S candidate passwords are observed by K shoulder surfing attacks. And $\Pr(X_S)$ is the probability that all of the S candidate passwords are observed in K times attacks. The probability $\Pr(X_S)$ is

$$\Pr(Correct|X_S)=\frac{1}{S} \tag{4}$$

Our next step is to find the probability $\Pr(X_S)$. We express this probability as follows,

$$\Pr(X_S)=\begin{cases}1-\sum_{S=2}^{H}\Pr(X_S), & \text{if } S=1\\ \binom{H-1}{S-1}\prod_{k=1}^{K-1}\left(\frac{H-k}{N-k}\right), & \text{if } S\geq 2\end{cases} \tag{5}$$

where one out of H digits is correct, so that the remaining $H-1$ digits observed in the first attack means that all of the $S-1$ digits are observed K times in K consecutive attacks.

For a password system having W digits, SSAR is expressed as follows by integrating Eq. (4) and (5),

$$SSAR=\left(\sum_{S=1}^{H}\Pr(Correct|X_S)\Pr(X_S)\right)^{W} \tag{6}$$

5. Conclusion

In this paper, we proposed a partially hidden password system resistant to a shoulder surfing attack. In more detail, we introduced the proposed password system by using one simple example. The key idea behind the proposed password system is to place the user's password randomly in the specified password space instead of entering a password directly. This system has the advantage that the password can be hidden by the attacker when there are shoulder surfing attacks. And we proved security and usefulness through two aspects: random guessing attack resistance and shoulder surfing attack resistance.

REFERENCES

[1] M. Harbach, A. De Luca, and S. Egelman, "The Anatomy of Smartphone Unlocking: A Field Study of Android Lock Screens," *Proceedings of the 2016 CHI conference on Human Factors in Computing Systems*, pp. 4806-4817, 2016.

[2] M. Harbach, E. V. Zezschwitz, A. Fichtner, A. De Luca, and M. Smith, "It's a hard lock life: A field study of smartphone (un)locking behavior and risk perception," *Proceedings of 10th Symposium on*

Usable Privacy and Security, Menlo Park, CA, Jul. 2014.

[3] A. S. Arif, A. Mazalek, and W. Stuerzlinger, "The use of pseudo pressure in authenticating smartphone users," *Proceedings in 11th International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, London, UK, Dec. 2014.

[4] A. De Luca, M. Harbach, E. V. Zezschwitz, M. Maurer, B. Ewald Slawik, H. Hussmann, and M. Smith, "Now you see me, now you don't: protecting smartphone authentication from shoulder surfers," *Proceedings in 32nd Annual ACM Conference on Human Factors in Computing Systems*, Toronto, CA, Apr. 2014.

[5] K. Krombholz, T. Hupperich, and T. Holz, "Use the Force: Evaluating Force-Sensitive Authentication for Mobile Devices," *Proceedings in 12th Symposium on Usable Privacy and Security*, Denver, CO, Jun. 2016.

[6] J.-W. Kim, S.-H. Kim, S.-Y. Park, and H.-G. Cho, "Hangul Password System for Preventing Shoulder-Surfing," *The Journal of the Korea Contents Association*, vol. 11, no. 4, pp. 33-41, Apr. 2011.

[7] M. Eiband, M. Khamis, E. V. Zezschwitz, H. Hussmann, and F. Alt, "Understanding shoulder surfing in the wild: Stories from users and observers," *Proceedings in 35th Annual ACM Conference on Human Factors in Computing Systems*, Denver CO. May 2017.

[8] E. V. Zezschwitz, A. De Luca, B. Brunkow, and H. Hussmann, "SwiPIN: Fast and secure pin-entry on smartphones," *Proceedings in 33rd Annual ACM Conference on Human Factors in Computing Systems*, Seoul, Korea, Apr. 2015.

[9] V. Roth, K. Richter, and R. Freidinger, "A PIN-entry method resilient against shoulder surfing," *Proceedings of ACM Conference Computer and Communications Security*, pp. 236-245, 2004.

[10] M. K. Lee, "Security notions and advanced method for human shoulder-surfing resistant PIN-entry," *IEEE Transactions on Information Forensics and Security,* vol. 9, no. 4, pp.695-708, Apr. 2014.

[11] A. D. Luca, K. Hertzshuch, and H. Hussmann, "ColorPin-securing PIN Entry through indirect input," *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 1103-1106, 2010.

[12] G. E. Blonder, "Graphical passwords", United States Patent 5559961, 1996.

[13] P. Dunphy, J. Nicholson and P. Olivier, "Securing passfaces for description," *Proceedings of the 4th symposium on Usable privacy and security*, pp. 24-35, Jul. 2008.

[14] I. Jermyn, A. Mayer, F. Monrose, K. Reiter, and A. D. Rubin, "The design and analysis of graphical passwords," *Proceedings of the 8th conference on USENIX Security Symposium*, Aug. 1999.

[15] H. Zhao and X. Li, "S3PAS: A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme," *Proceedings of 21st International Conference on Advanced Information Networking and Applications Workshops*, May. 2007.

[16] A. De Luca, E. V. Zezschwitz, N. D. H. Nguyen, M. Maurer, E. Rubegni, M. P. Scipioni, and M. Langheinrich, "Back-of-device authentication on smartphones," *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems,* May 2013.

[17] J. Gugenheimer, A. De Luca, H. Hess, S. Karg, D. Wolf, and E. Rukzio, "Colorsnakes: Using colored decoys to secure authentication in sensitive contexts," *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services*, Aug. 2015.

[18] A. Maiti, K. Crager, M. Jadliwala, J. He, K. Kwiat, and C. Kamhoua, "RandomPad: Usability of randomized mobile keypads for defeating inference attacks," *Proceedings of the IEEE Euro S&P Workshop on Innovations in Mobile Privacy & Security*, Jan. 2017

[19] Q. Yan, J. Han, Y. Li, J. Zhou, and R. H Deng, "Designing leakage-resilient password entry on touchscreen mobile devices," *Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security*, pp. 37-48, May 2013.

[20] N. H. Zakaria, D. Griffiths, S. Brostoff, and J.

Yan, "Shoulder surfing defence for recall-based graphical passwords," *Proceedings of the Seventh Symposium on Usable Privacy and Security*, Jul. 2011.

[21] O. Wiese and V. Roth, "See you next time: a model for modern shoulder surfers," *Proceedings of the 18th International Conference on Human-Computer Interaction with Mobile Devices and Services*, Sep. 2016.

[22] B. Malek, M. Orozco, and A. El Saddik, "Novel shoulder-surfing resistant haptic-based graphical password," *International Journal of Information Security*, vol. 13, no. 3, pp. 245-254, Jun. 2014.

[23] A. Bianchi, I. Oakley, V. Kostakos, and D. S. Kwon, "The phone lock: audio and hapticshoulder-surfing resistant PIN entry methods for mobile devices," *Proceedings of the fifth international conference on Tangible, embedded, and embodied interaction*, Jan. 2011.

Author Biography

Jin-Taek Seong **[Member]**

- Aug. 2014: Dep. Information & Communication Eng., GIST (Ph.D.)
- Mar. 2008 ~ Dec. 2010: LG Elec., Junior Researcher
- Sep. 2014 ~ Sep. 2016: DGMIF, Researcher
- Sep. 2016 ~ Mar. 2017: DAPA, Program Manager
- Mar. 2018 ~ Current: Dep. Convergence Software, Mokpo National University, Assistant Professor

〈Research Interests〉 Information Theory, Machine Learning, Communication Theory