A Sector-Based Graphical Password Scheme with Resistance to Login-Recording Attacks

Wei-Chi KU†(a), Member, Yu-Chang YEH1, Bo-Ren CHENG1, and Chia-Ju CHANG†, Nonmembers

SUMMARY Since most password schemes are vulnerable to login-recording attacks, graphical password schemes that are resistant to such attacks have been proposed. However, none of existing graphical password schemes with resistance to login-recording attacks can provide both sufficient security and good usability. Hence, we design and implement a simple sector-based graphical password scheme, RiS, with dynamically adjustable resistance to login-recording attacks. RiS is a pure graphical password scheme by using the shape of the sector. In RiS, the user can dynamically choose the login mode with suitable resistance to login-recording attacks depending on the login environment. Hence, the user can efficiently complete the login process in an environment under low threat of login-recording attacks and securely complete the login process in an environment under high threat of login-recording attacks. Finally, we show that RiS can achieve both sufficient security and good usability.

key words: accidental login, graphical password, login-recording attack, shoulder-surfing attack

1. Introduction

Textual password authentication is regarded as one of the most widely used user authentication mechanisms. However, weak textual passwords are susceptible to the dictionary attack and strong textual passwords are hard to remember. Nowadays, a physical keyboard is not a necessity for modern hand held devices, e.g., smart phones, PDAs, and tablet computers. In addition, it is difficult for the user to input his textual password, containing many characters, by using the on-screen keyboard on a small-sized hand held device. Since psychological studies [15] support the notion that people recall pictures with higher probability than texts, graphical password schemes have been proposed as alternatives to textual password schemes. Existing graphical password schemes can be categorized into three types:

- Recognition-based graphical password schemes: the user is presented with a set of images and the user has to pass the authentication by recognizing and identifying the images the user selected during the registration stage.

- Pure recall-based graphical password schemes: the user is asked to reproduce something that the user created or selected during the registration stage.

- Cued recall-based graphical password schemes: the user is presented with some hints about the password and the user has to pass the authentication by reproducing something that the user created or selected during the registration stage.

Biddle et al. [2] and [3] gave a comprehensive overview of most existing well-known graphical password schemes, covering usability and security aspects and Renaud [19] recommended guidelines for designing and implementing graphical password schemes with high efficacy and efficiency.

However, most conventional textual and graphical password schemes are vulnerable to login-recording attacks, which involve the following attacks for obtaining the user’s password: (1) the shoulder-surfing attack: watching over the user’s shoulder during the user’s login session; (2) the hidden-camera attack: recording the user’s login session with a hidden-camera; (3) the spyware attack: using keylogging software or Trojan software to record the user’s login session; and (4) the wiretapping attack: using sniffing tools to intercept the information transmitted between the user and the system during the user’s login session. In 2002, Sobrado and Birget [20] proposed three graphical password schemes with resistance to login-recording attacks, the Triangle scheme, the Movable Frame scheme, and the Intersection scheme. After that, various graphical password schemes with different degrees of resistance to login-recording attacks have been proposed and surveyed, e.g., [6], [7], [10], [13], [14], [16], [18], [21], [23], [26], [28], and [30].

However, none of existing graphical password schemes with resistance to login-recording attacks can provide both sufficient security and good usability. On the other hand, as existing graphical password schemes with resistance to login-recording attacks do not provide the user with the capability of dynamically choosing level of resistance to login-recording attacks depending on the user’s login environment, the user has to complete the login process inconveniently and inefficiently even under no threat of login-recording attacks, e.g., the user logs into a system by using a secure computer at home via a secure connection. In this paper, we will propose a simple sector-based graphical password scheme, RiS (Rotating into Sector), with dynamically adjustable resistance to login-recording attacks based on the login environment. By using RiS, the user can dynamically choose the login mode with suitable resistance to
login-recording attacks depending on the login environment. Thus, the user can efficiently complete the login process in an environment under low threat of login-recording attacks and securely complete the login process in an environment under high threat of login-recording attacks. Finally, we will show that RiS can achieve both sufficient security and good usability. The rest of this paper is organized as follows. In Sect. 2, we will review the related works. In Sect. 3, we will describe the proposed scheme, RiS. Next, we will theoretically and experimentally analyze the security and usability of RiS in Sect. 4. Finally, discussion and conclusion are made in Sect. 5.

2. Related Works

In 1996, Blonder [5] initially proposed a graphical password scheme, in which a password is a sequence of clicks at points in a predetermined image. In 1999, Jermyn et al. [11] proposed a graphical password scheme, the DAS scheme, in which a password is a picture drawn on a two-dimensional grid. The coordinates of the touched grids are recorded in temporal order of the drawing. The user is authenticated while the same cells are crossed with same order. In 2005, Wiedenbeck et al. [25] proposed an improved version of Blonder’s graphical password scheme, the PassPoints scheme, in which the user can use any image provided by the system or chosen by the user. The only requirement is that the image be intricate and rich enough so that many possible click points are available. Unlike Blonder’s graphical password scheme, the PassPoints scheme does not need artificial predefined click regions with well-marked boundaries. In 2006, Birget et al. [4] generalized Blonder’s graphical password scheme to arbitrary images and solved a robustness problem in their generalized scheme. In 2010, Oorschot et al. [17] introduced and evaluated various methods for purely automated attacks against PassPoints-style graphical password schemes.

However, none of the above described graphical password schemes can resist login-recording attacks. In 2002, Sobrado and Birget [20] developed three graphical password schemes with resistance to login-recording attacks, the Triangle scheme, the Movable Frame scheme, and the Intersection scheme. In the Triangle scheme, the system randomly scatters a set of $N$ icons on the screen and there is a subset of $K$ pass-icons previously chosen and memorized by the user. In the login phase, the system first randomly chooses a patch that covers half the screen and randomly places the $K$ pass-icons in that patch and the other $N-K$ icons are randomly placed on the screen. To log into the system, the user must correctly pass the predetermined number of challenges. In each challenge, the user must find three of the pass-icons and click inside the invisible triangle created by those three pass-icons. In the Movable Frame scheme, the user must locate three out of his pass-objects and moves a frame and the icons within it until the pass-icons on the frame lines up with the other two pass-icons. In the login phase of the Movable Frame scheme, one randomly chosen pass-icon is randomly placed on the frame and two other randomly chosen pass-icons are randomly placed within the frame. The user must locate these displayed pass-icons, and then move the frame clockwise or counterclockwise until the pass-icon on the frame lines up with the other two pass-icons within the frame. However, the Movable Frame scheme has some disadvantages as follows: (1) the appearance probability of the pass-icon on the frame is higher than the other two pass-icons within the frame; and (2) the pass-icons are difficult to line up once the pass-icons are scattered far away from each other. In 2006, Hartanto et al. [9] pointed out that the Movable Frame scheme has high failure rate due to that the pass-icons are hard to line up for the user. The Intersection scheme uses the intersection of the invisible lines formed by four displayed pass-icons out of $K$ previously chosen pass-icons. The user must click near the intersection of the two invisible lines inside the convex quadrilateral formed by those four pass-icons. However, the Intersection scheme has similar problems as those in the Triangle scheme and the Movable Frame scheme. In 2005, Sobrado and Birget [21] proposed the Convex-Hull Click scheme, which is a more detailed version of the Triangle scheme. To avoid the high probability of accidental login of central area, it employs the out-of-shadow placements to ensure that all locations on the screen have roughly similar probabilities of being in the convex hull formed by the pass-icons. However, Hoanca and Mock [10] pointed out that the Convex-Hull Click scheme has a corner effect that may reduce the security. In 2006, Wiedenbeck et al. [26] reported on the design and evaluation of the Convex-Hull Click scheme and pointed out that the login time of the Convex-Hull Click scheme is too long. Asghar et al. [1], in 2013, further showed that the Convex-Hull Click scheme is vulnerable to two probabilistic attacks, in which the user’s pass-icons may be revealed by using login-recording attacks. In 2013, Wu et al. [27] also proposed a graphical password scheme with resistance to login-recording attacks, SSP, using the convex-hull graphical algorithm. In SSP, dynamic moving color balls are employed to enhance its resistance to login-recording attacks.

In 2008, the GrIDSure Enterprise [8] proposed a graphical password scheme with resistance to login-recording attacks, GrIDSure. However, the resistance of GrIDSure to login-recording attacks is weak. In 2009, Gao et al. [7] proposed a graphical password scheme with resistance to login-recording attacks, ColorLogin, in which the background color is a usable factor for reducing the login time. However, the resistance of ColorLogin to login-recording attacks is also weak. Later, Gao et al. [6] also proposed a graphical password scheme with resistance to login-recording attacks based on CAPTCHA (CompletelyAutomated Public Turing tests to tell Computers and Humans Apart), in which there is a CAPTCHA under each icon on the login screen. The user has to find his pass-icons and input the CAPTCHAs with the right characters under his pass-icons to log into the system. However, the usability of this scheme is unsatisfactory because the user has to memorize both the pass-icons and the corresponding digits of each pass-icon. In 2009, Yamamoto
et al. [28] proposed a graphical password scheme with resistance to login-recording attacks, TI-IBA, in which icons are presented not only spatially but also temporally. TI-IBA is less constrained by the screen size and easier for users to find their pass-icons. However, the resistance of TI-IBA to login-recording attacks is unsatisfactory. In 2011, Zakaria et al. [29] proposed three graphical password schemes with resistance to login-recording attacks, which use decoy strokes, disappearing strokes, and line snaking, respectively. However, Zakaria et al.’s schemes cannot achieve good balance between usability and security. In the same year, Kim et al. [12] proposed a graphical password scheme with resistance to login-recording attacks, in which the user has to shift his pass-icons on four quadrants of the screen. Unfortunately, the resistance of Kita et al.’s scheme to login-recording attacks is unsatisfactory. In 2013, Kita et al. [13] proposed a graphical password scheme with resistance to login-recording attacks, in which icons are presented not only spatially but also temporally. TI-IBA is less constrained by the screen size and easier for users to find their pass-icons. However, Zakaria et al.’s schemes cannot achieve good balance between usability and security. In the same year, Kim et al. [12] proposed a graphical password scheme with resistance to login-recording attacks, in which the user has to shift his pass-icons on four quadrants of the screen. Unfortunately, the resistance of Kita et al.’s scheme to login-recording attacks is unsatisfactory.

3. The Proposed Graphical Password Scheme – RiS

We will propose a simple sector-based graphical password scheme, RiS (Rotating into Sector), with dynamically adjustable resistance to login-recording attacks depending on the login environments. The user can efficiently complete the login process in an environment under low threat of login-recording attacks and securely complete the login process in an environment under high threat of login-recording attacks. Additionally, we will theoretically and experimentally analyze the security and usability of RiS.

The notations used in RiS can be described as follows. The positive integer \( N \) denotes the size of icons pool, i.e., the total number of icons, the positive integer \( k \) denotes the number of pass-icons, and the positive integer \( n \), which should be a multiple of 3, is the number of all displayed icons in a challenge. The value of \( \frac{n}{k} \) should be equal to the value of \( \frac{3}{k} \) so that pass-icons would appear as frequently on the screen as non-pass-icons. RiS involves two phases, the registration phase and the login phase, which can be described below.

3.1 RiS’s Registration Phase

Initially, a secure channel is established between the system and the user by using SSL/TLS [22] and [24]. The system displays all \( N \), say 400, icons to the user in random order by using several icons pages. The user selects \( k \), say 8, icons as his pass-icons, i.e., graphical password, among these \( N \) icons. The system will advise the user to register in an environment free of spyware, hidden camera, and shoulder-surfing attack. The system stores the identifiers of the user’s pass-icons in the user’s entry in the password table, which should be encrypted by the system key. Additionally, the user has to register an e-mail address for unlocking his account once his account has been locked out, which will be described later.

3.2 RiS’s Login Phase

The login screen contains three concentric rings, including the external ring, the middle ring, and the internal ring from the outer to the inner, and each ring is evenly divided into \( \frac{3}{n} \) slots, which are aligned with the slots of another two rings, as in Fig. 1. The user can dynamically choose the login mode with strong resistance to login-recording attacks, the LR1 login mode, or the normal login mode, the LR0 login mode, depending on the login environment. The LR1 login mode is the default mode, and the user can click the “Switch to LR0” button on the screen to switch to the LR0 login mode. In each challenge of the LR1 login mode, 3 randomly chosen decoy-icons are randomly and uniformly placed on the slots of the external ring, the middle ring, and the internal ring so that there are exactly one pass-icon and \( \frac{n-3}{3} \) decoy-icons on each ring. The icons on the external ring and the internal ring are fixed, and the icons on the middle ring can be rotated clockwise or counterclockwise from slots to slots on the middle ring by scrolling the mouse wheel or clicking the “Rotation” buttons. The user has to identify the pass-icons and then rotate the middle ring clockwise or counterclockwise from slots to slots to respond the challenge. To log into the system in the LR1 login mode, the user has to pass \( r \) challenges. In the LR0 login mode, 3 randomly chosen pass-icons and \( n - 3 \) randomly chosen decoy-icons are randomly and uniformly placed on the slots of the external ring, the middle ring, and the internal ring so that each ring exactly contains one pass-icon and \( \frac{n-3}{3} \) decoy-icons. To log into the system in the LR0 login mode, the user has to click the three displayed pass-icons correctly.
fault login mode, and the LR0 login mode of RiS can be described respectively as follows:

**RiS’s LR1 login mode**

1. **Step 1:** The user requests to log into the system. A secure channel is established between the system and the user by using SSL/TLS [22] and [24]. The number of finished challenges, denoted by \( i \), is initialized to 0.

2. **Step 2:** The system randomly chooses 3 pass-icons among the \( k \) pass-icons and \( n-3 \) decoy-icons among the \( N-k \) non-pass-icons, randomly places one chosen pass-icon on the middle ring and the other two chosen pass-icons on the external ring and the internal ring, respectively, and then places the chosen decoy-icons randomly and uniformly on these three rings.

3. **Step 3:** If the center of the three rings and the two pass-icons on the external ring and the internal ring are on a line, the user must scroll the mouse wheel or click the “Rotation” buttons to rotate the icons on the middle ring until the pass-icon on the middle ring gets on the line passing through the center and the two pass-icons on the external ring and the internal ring. Otherwise, the user has to identify his pass-icons on the three rings, and then scroll the mouse wheel or click the “Rotation” buttons to rotate the middle ring until the pass-icon on it falls into the sector region formed by the center and the other two pass-icons. Next, the user must click the “Confirm” button to respond this challenge. Let \( i = i + 1 \).

4. **Step 4:** If \( i < r \), then the system jumps to Step 2. Otherwise, the user is authenticated by the system.

The LR1 login mode of RiS can be illustrated by an example as shown in Fig. 2, in which the three randomly chosen pass-icons are marked with red color for illustration and the user has to rotate the middle ring until the pass-icon on it falls into the sector region formed by the center and the other two pass-icons.

**RiS’s LR0 login mode**

1. **Step 1:** The user requests to log into the system and then clicks the “Switch to LR0” button on the login screen. A secure channel is established between the system and the user by using SSL/TLS [22] and [24].

2. **Step 2:** The system randomly chooses three pass-icons among the \( k \) pass-icons and \( n-3 \) decoy-icons among the \( N-k \) non-pass-icons, randomly places each of the chosen pass-icon on each of the rings, respectively, and then places the chosen decoy-icons randomly and uniformly on these three rings.

3. **Step 3:** The user has to identify his pass-icons on the three rings, and then click his three displayed pass-icons in any order. If all the three displayed pass-icons are clicked and none of the decoy-icons is clicked, the user is authenticated by the system.

The LR0 login mode of RiS can be illustrated by an example as shown in Fig. 3, in which the three randomly chosen pass-icons are marked with red color for illustration only.

In both the LR1 login mode and the LR0 login mode of RiS, \( \frac{3}{k} \) should equal \( \frac{n}{N} \) so that pass-icons would appear as frequently on the screen as non-pass-icons. In addition,
three consecutive failed login attempts, no matter in which login mode, will lock out the account, and then the system will send an e-mail containing the account-unlocking link, which can only be used once to unlock the locked account, to the user’s registered e-mail address.

4. Analysis of RiS

4.1 Security Analysis of RiS

4.1.1 RiS’s Password Space

For the LR1 login mode and the LR0 login mode: The total number of all possible combinations of icons that the user can select is $C_N^k$. For example, if $N = 400$ and $k = 8$, the password space is $C_{400}^8 = 1.5 \times 10^{16}$, which is greater than the password space $95^8 \approx 6.6 \times 10^{15}$ of the 8-characters textual password with 95 printable characters.

4.1.2 RiS’s Resistance to Accidental Login

For the LR1 login mode: Since the icons are uniformly placed on the three rings, there are $\frac{n}{3}$ icons on each ring. The success probability of accidental login, denoted by $P_{al}$, is

$$P_{al} = \left( \frac{n^2 \times \left(2 + 2 \times \sum_{i=2}^{\frac{n}{3}} i\right)}{(\frac{n}{3})^3} \right)^r$$

where $r$ denotes the number of challenges, the denominator $\left(\frac{n}{3}\right)^3$ within the braces denotes the number of combinations of three icons picked from three rings, respectively, on the screen, and the numerator $\frac{n^2 \times \left(2 + 2 \times \sum_{i=2}^{\frac{n}{3}} i\right)}{(4n^2)}$ within the braces denotes the number of combinations of three icons satisfying the required condition in each login challenge. For example, if $n = 150$ and $r = 5$, the success probability of accidental login is $P_{al} \approx 1.20 \times 10^{-3}$.

Figure 4 shows the success probabilities of accidental login ($P_{al}$) for $r = 5$ and different values of $n$ in the LR1 login mode. To verify our theoretical analysis result for RiS’s resistance to accidental login, we also perform the following accidental login simulation on RiS. First, the simulator randomly chooses 8 icons from icons pool as pass-icons. In each accidental login attack, the simulator will complete 5 challenges/responses, in which the simulator randomly rotates the middle ring and then clicks the “Confirm” button. For each value of $n$, 3,000,000 accidental login attempts are made. In our simulation, the ratio of the number of the icons in a challenge ($n$) to the number of the icons of the icons pool ($N$) is $\frac{3}{8}$. Figure 5 shows the results of our accidental login simulation for RiS, in which the success rate of accidental login simulation is extremely close to our theoretical analysis result for RiS’s resistance to accidental login, i.e., the results of our theoretical analysis and simulation are quite consistent.

For the LR0 login mode: Since the adversary must find the pass-icon on each of the three rings, the success probability of accidental login, denoted by $P_{al}$, is

$$P_{al} = \frac{C_3^3}{\left(\frac{n}{3}\right)^3} = \left(\frac{3}{n}\right)^3$$

Figure 6 shows the success probabilities of accidental login ($P_{al}$) for different values of $n$ in the LR0 login mode. Additionally, no matter in the LR1 login mode or the LR0 login mode, three consecutive failed login attempts will lock out the account so that only the legitimate user can unlock his
locked account. Such a mechanism can significantly improve the resistance of RiS to accidental login.

4.1.3 RiS’s Resistance to Login-Recording Attacks

For the LR1 login mode: The average ratio of the sector region satisfying the required condition to the entire region in each challenge, denoted by \( P_{rc} \), is

\[
P_{rc} = \frac{\binom{C_3^k}{C_3^k} \times \left(\frac{2}{3}\right)^2 + 2 \times \left(\frac{1}{3}\right)^2 \times \left(\sum_{i=2}^{n} \binom{C_3^i}{C_3^i}\right)}{\binom{C_3^n}{C_3^n}}
\]

If the adversary has recorded \( T \) login sessions, he can eliminate some combinations of the icons in guessing the pass-icons. Assume that the appearance probability of each icon on the login screen is the same. The success probability of login-recording attacks, denoted by \( P_{lr} \), is

\[
P_{lr} = \frac{C_3^k}{C_3^k + (C_3^n - C_3^k) \times (1 - E)^T x r}
\]

where

\[
E = \frac{[C_3^n - P_{rc} \times \binom{C_3^i}{C_3^i}] \times (1 - C_3^i/C_3^k)}{C_3^n}
\]

\( E \) denotes the ratio of the combination of icons that can be eliminated by using the recorded login information. In the numerator of the formula for \( E \), \( C_3^i \) denotes the number of combinations of three icons in each recorded challenge/response, \( P_{rc} \times \binom{C_3^i}{C_3^i} \) denotes the number of combinations of three icons satisfying the required condition in each recorded challenge/response, and \( C_3^n - P_{rc} \times \binom{C_3^i}{C_3^i} \) denotes the number of combinations of icons that can be eliminated by using each recorded challenge/response. As the appearance probability of each icon in the recorded challenge/response is the same, the number of combinations of icons that can be eliminated is

\[
[C_3^n - P_{rc} \times \binom{C_3^i}{C_3^i}] \times (1 - C_3^i/C_3^k)
\]

The numerator of the formula for \( P_{lr} \), \( C_3^k \), denotes the number of combinations of three pass-icons that are picked from the user’s \( k \) pass-icons for each login challenge/response. And, the denominator of the formula for \( P_{lr} \),

\[
C_3^k + (C_3^n - C_3^k) \times (1 - E)^T x r
\]

denotes the total number of the combinations of all the three icons minus the number of the combinations of the three icons unsatisfying the required condition in any of the \( T \) recorded login sessions. Figure 7 shows the success probabilities of login-recording attacks in the LR1 login mode of RiS for \( r = 5 \) and different values of \( N \). Figure 8 shows the success probabilities of login-recording attacks in the LR1 login mode of RiS for \( N = 600 \) and different values of \( r \). To verify our theoretical analysis result for the resistance of the LR1 login mode of RiS to login-recording attacks, we also perform the different values of \( N \), 30 simulated user data, including IDs and graphical passwords, are pre-generated randomly by the simulator, and 15 records of successful logins are generated for each simulated user. Next, the simulator performs actual login-recording attacks. As expected, none of the simulated login-recording attacks is successful by capturing only 15 login records.

For the LR0 login mode: The LR0 login mode can only provide weak resistance to login-recording attacks as wiretapping can be withstood by the secure channel established between the system and the user.

4.1.4 RiS’s Resistance to On-Line Guessing Attacks

No matter in the LR1 login mode or the LR0 login mode, the adversary may attempt to guess a possible password to pass the verification of the server in the on-line manner. However, if the adversary makes three consecutive failed login attempts at any time, this account will be locked out and the system will send an e-mail containing the account-locking link to the user’s registered e-mail address. That is, only the legitimate user can unlock his locked account. Thus, on-line guessing attacks cannot be performed efficiently.
4.2 Usability Analysis of RiS

The user of RiS can dynamically choose the login mode with suitable resistance to login-recording attacks depending on the login environment. That is, the user can efficiently complete the login process in an environment under low threat of login-recording attacks and securely complete the login process in an environment under high threat of login-recording attacks. To log into the system, the user only has to rotate the middle ring until the pass-icon on the middle ring falls into the sector region formed by the other two pass-icons and the center. Even if the pass-icons are scattered far away from each other, the user still can finish the login session easily and efficiently. In addition, since there is exactly one pass-icon on each ring, the user can ignore the remaining icons on that ring to save the search time. To evaluate the usability of RiS, an experiment is conducted as follows. The participants of our experiment are 22 college students majored in computer science. All the participants are unfamiliar with graphical password schemes. The participant can freely choose his password and sufficiently practice to familiarize with the operations of RiS. Each participant is given 5 chances to log into the system by using the LR0 login mode and the LR1 login mode with 3 challenges, respectively. Table 1 shows the results of our usability experiment for RiS.

Note that the login success rate of our experiment for RiS is very close to 100%. Actually, the major usability problem of existing secure graphical password schemes with resistance to login-recording attacks is that the average login time is long. Next, we compare RiS with three well-known graphical password schemes with resistance to login-recording attacks, the Convex-Hull Click scheme [21], the Movable Frame scheme [20], and Kim et al.’s scheme [12] with respect to the average login time and the login success rate. We assume that the LR0 login mode and the LR1 login mode of RiS are chosen by the user with equal probability. Thus, the average login time of our experiment for RiS is

\[
\frac{27.90+10.16}{2} = 19.03 \text{ seconds.}
\]

Table 2 shows that RiS is superior to the Convex-Hull Click scheme, the Movable Frame scheme, and Kim et al.’s scheme with respect to the average login time and the login success rate. Within Table 2, the average login time of the Convex-Hull Click scheme with 3 challenges, the Movable Frame scheme, and Kim et al.’s scheme is adopted from [26], [9], and [12], respectively.

5. Discussion and Conclusion

In this paper, we have proposed a sector-based graphical password scheme, RiS, which provides the user with the capability of dynamically choosing level of the resistance to login-recording attacks depending on the user’s login environment without increasing memory burden by using the same password. In RiS, the user can efficiently complete the login process in an environment under low threat of login-recording attacks and securely complete the login process in an environment under high threat of login-recording attacks. We have shown that RiS can achieve both sufficient security and good usability. In particular, we have justified the theoretical analysis results of the resistances of RiS to accidental login and login-recording attacks by using practical simulations and quantified some major features of the usability of RiS by conducting user studies.

Acknowledgements

This work was supported in part by the Ministry of Science and Technology, Taiwan, under Grant MOST-102-2221-E-142-003.

References

[1] H.J. Asghar, S. Li, J. Pieprzyk, and H. Wang, “Cryptanalysis of the convex hull click human identification protocol,” International Journal of Information Security, vol.12, pp.83–96, April 2013.
[2] R. Biddle, S. Chiasson, and P.C. Van Oorschot, “Graphical passwords: learning from the first twelve years,” Technical Report TR-11-01, School of Computer Science, Carleton University, 2011.
[3] R. Biddle, S. Chiasson, and P.C. Van Oorschot, “Graphical passwords: learning from the first twelve years,” ACM Computing Surveys, vol.44, no.4, article 19, 2012.
[4] J.C. Birget, D. Hong, and N. Memon, “Graphical passwords based on robust discretization,” IEEE Trans. Information Forensics and Security, vol.1, no.3, pp.395–399, 2006.
[5] G.E. Blonder, “Graphical passwords,” Lucent Technologies Inc, Murray Hill, NJ (US), US Patent No. 5559961, 1996.
[6] H. Gao, X. Liu, S. Wang, and R. Dai, “A new graphical scheme against spyware by using CAPTCHA,” Proc. 2009 Symposium Usable Privacy and Security, 2009.
