LETTER

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

Wei-Chi KU[†a)], *Member*, Bo-Ren CHENG[†], Yu-Chang YEH[†], *and* Chia-Ju CHANG[†], *Nonmembers*

SUMMARY Recently, Ku et al. proposed a sector-based graphical password scheme, RiS, with dynamically adjustable resistance to login-recording attacks. However, since most users are more familiar with textual passwords than graphical passwords, we propose a secure and efficient textual-graphical password scheme, T-RiS, which is a variant of RiS. The T-RiS 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. T-RiS can be used in environments where the users are more familiar with passwords based on texts than passwords based on icons/images and the number of login sessions the adversary can record is usually less than five.

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

1. Introduction

Since common password schemes are vulnerable to login-recording attacks, which involve the shoulder-surfing attack, the hidden-camera attack, the spyware attack, and/or the wiretapping attack, graphical password schemes that are resistant to such attacks have been proposed, e.g., [1], [3]–[5], [7]–[9]. However, these schemes do not provide the user with the capability of dynamically choosing the level of resistance to login-recording attacks. That is, the user of these schemes faces inconvenience and inefficiency in completing the login process, even without the threat of login-recording attacks. Thus, Ku et al. [2], in 2015, proposed a simple and efficient sector-based graphical password scheme, RiS (Rotating into Sector), with dynamically adjustable resistance to login-recording attacks based on the login environment. 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. However, in practice, most users are more familiar with textual passwords than graphical passwords. In addition, if the user has to access many systems using various graphical password schemes, which may employ entirely different icons/images, it may be difficult for him to memorize all these passwords. Herein, we propose a textual-graphical password scheme with dynamically adjustable resistance to login-recording attacks, T-RiS (Rotating into Sector based on Texts), which is a variant of RiS. Next, we will theoretically and experimentally analyze the security and usability of T-RiS. As in RiS, the user of T-RiS 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.

2. The Proposed Scheme – T-RiS

In this section, we will describe a textual-graphical password scheme with dynamically adjustable resistance to login-recording attacks, T-RiS, which is a variant of RiS [2]. The T-RiS user can dynamically choose the login mode with suitable resistance to login-recording attacks depending on the login environment. Unlike RiS, T-RiS uses alphanumeric characters instead of icons. The alphabet contains 62 alphanumeric characters, including 26 upper case letters, 26 lower case letters, and 10 decimal digits. Notation L represents the number of characters of the user's textual password, i.e., the password length. T-RiS involves two phases, the registration phase and the login phase, which can be described below.

2.1 Registration Phase

Initially, a secure channel is established between the system and the user by using TLS [6]. The user has to set his textual password of length L ($6 \leq L \leq 15$) characters. The system should advise the user to register in an environment free of spyware, hidden camera, and shoulder-surfing attack. The system stores the user's textual password 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.

2.2 Login Phase

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

Manuscript received April 1, 2015.
Manuscript revised October 23, 2015.
Manuscript publicized November 19, 2015.

[†]The authors are with the Department of Computer Science, National Taichung University of Education, Taichung City, Taiwan 403, R.O.C.
a) E-mail: wcku@mail.ntcu.edu.tw

DOI: 10.1587/transinf.2015EDL8080

the screen to switch to the LR0 login mode.

The LR1 login mode

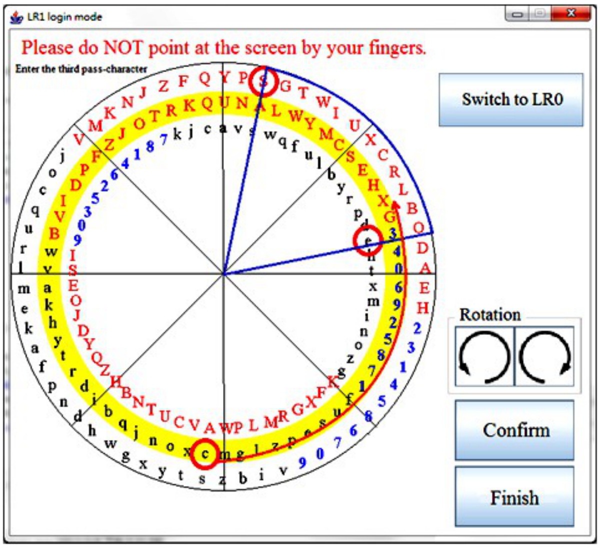
Step 1: The user requests to log into the system. A secure channel is established between the system and the user by using TLS [6]. The system displays three concentric rings, including the external ring, the middle ring, and the internal ring, and each ring is evenly divided into 62 slots aligned with the slots of another two rings. Each of these three rings is composed of three consecutive segments of slots containing characters, including the segments of the slots containing 26 randomly arranged upper case letters, the slots containing 26 randomly arranged lower case letters, and the slots containing 10 randomly arranged decimal digits. The characters on the external ring and the internal ring are fixed, and the characters 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.

Step 2: The user has to identify the first character of his textual password (the first pass-character) on the external ring and the second character of his textual password (the second pass-character) on the internal ring. The index of the pass-character to be entered, denoted by i, is initialized to 3.

Step 3: If the center of the three rings, the first pass-character on the external ring, and the second pass-character on the internal ring are on a line, the user has to rotate the characters on the middle ring until the i-th pass-character on the middle ring gets on the line passing through the center and the first pass-character on the external ring and the second pass-character on the internal ring. Otherwise, the user has to rotate the characters on the middle ring until the i-th pass-character on the middle ring falls into the sector region formed by the first pass-character, the second pass-character, and the center. Next, the user has to click the "Confirm" button to respond this challenge. Let $i = i + 1$.

Step 4: If $i < L+1$, the characters in each of the three segments of the middle ring are randomly rearranged in the same segment, and then jumps to Step 3. Otherwise, the user has to click the "Finish" button. If all the responses to the $L-2$ challenges are correct, the user is authenticated by the system.

The LR1 login mode of T-RiS can be illustrated by a scenario shown in Fig. 1, in which the three pass-characters are marked with red colors for illustration only. The user has to rotate the middle ring until the third pass-character on the middle ring falls into the sector region, which is marked with blue color for illustration only, formed by the first pass-character on the external ring, the second pass-character on the internal ring, and the center. On the login screen, the user's pointer is disallowed to enter into the characters area, and the user will be warned of not pinpointing his pass-characters by fingers on the screen so that the adversary cannot easily capture the user's pass-characters by directly watching or recording the login screen.



LR1 login mode

Please do NOT point at the screen by your fingers.

Enter the third pass-character

Fig. 1 A scenario of the LR1 login mode of T-RiS.

The LR0 login mode

Step 1: The user requests to log into the system in the LR1 login mode 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 TLS [6].

Step 2: The user directly enters his textual password. If the entered textual password is correct, the user is authenticated by the system.

Note that three consecutive failed login attempts 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.

3. Analysis of T-RiS

Next, we will theoretically and experimentally analyze the security and usability of T-RiS.

3.1 Security Analysis of T-RiS

We assume that the probability distribution of the length of the password L is uniform between 6 and 15, i.e., the probability of each valid value of L is $\frac{1}{10}$.

3.1.1 Password Space

For the LR1 login mode and the LR0 login mode:

$$\sum_{L=6}^{15} 62^L \approx 7.81 \times 10^{26}.$$

3.1.2 Resistance to Accidental Login

For the LR1 login mode: Assume that the probability distribution of L is uniform between 6 and 15. Since the locations of the characters on the external ring and the internal ring will not be changed in one login session, the locations of the first pass-character and the second pass-character are fixed in one login session. The success probability of accidental login, denoted by P_{al}^{LR1}, is

$$P_{al}^{LR1} = \frac{1}{10}\sum_{L=6}^{15} \frac{2 \times (\frac{2}{62})^{L-2} + 2 \times \sum_{i=2}^{31} (\frac{i}{62})^{L-2}}{62}$$
$$\approx 2.37 \times 10^{-3}.$$

where $2 \times (\frac{2}{62})^{L-2}$ in the numerator denotes the probability that the center of the three rings, the first pass-character on the external ring, and the second pass-character on the internal ring are on a line and the last $L-2$ pass-characters on the middle ring are rotated on this line, sequentially.

For the LR0 login mode: The success probability of accidental login, denoted by P_{al}^{LR0}, is

$$P_{al}^{LR0} = \frac{1}{10}\sum_{L=6}^{15}(\frac{1}{62})^L \approx 1.79 \times 10^{-12}.$$

In addition, as three consecutive failed login attempts will lock out the account, accidental login cannot easily occur.

3.1.3 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

$$P_{rc} = \frac{62 \times [2 + 2 + 2 \times (\sum_{i=2}^{31} i)]}{62^3} \approx 0.2585.$$

Suppose that the adversary has recorded T login sessions. It should be noted that the locations of the characters, including the first pass-character, on the external ring and the locations of the characters, including the second pass-character, on the internal ring are fixed in one login session. Since the first two pass-characters will be referred in entering the remaining $L-2$ pass-characters, the average number of the combinations satisfying the required conditions in each challenge/response of the T recorded login sessions for the first two pass-characters is $(1+P_{rc}^{T\times(L-2)-1}\times(62^2-1))$. Thus, the success probability of cracking the first pass-character and the second pass-character by login-recording attacks, denoted by $P_{lr[1,2]}$, is

$$P_{lr[1,2]} = \frac{1}{1 + (P_{rc}^{T\times(L-2)-1} \times (62^2 - 1))}$$

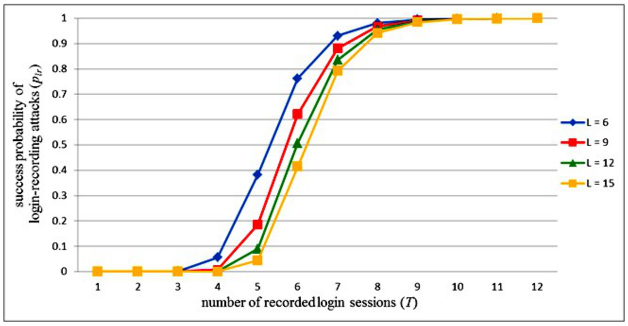


Fig. 2 The success probabilities of login-recording attacks P_{lr} in the LR1 login mode of T-RiS.

On the other hand, the average number of the combinations on the middle ring satisfying all the required conditions in each challenge/response of the T recorded login sessions for each of the last $L-2$ pass-characters is $(1+P_{rc}^{T-1}\times(62-1))$. It should be noted that none of the last $L-2$ pass-characters will be referred in entering another one of the last $L-2$ pass-characters. Thus, the success probability of cracking the characters from the third character to the L-th character of the user's password by login-recording attacks is

$$P_{lr[3,L]} = \left(\frac{1}{1 + P_{rc}^{T-1} \times (62-1)}\right)^{L-2}$$

Therefore, the success probability of login-recording attacks, denoted by P_{lr}, is

$$P_{lr} = P_{lr[1,2]} \times P_{lr[3,L]}.$$

Figure 2 shows the success probabilities of login-recording attacks with different values of L in the LR1 login mode.

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.

3.1.4 Resistance to On-Line Guessing Attacks

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-unlocking link to the user's registered e-mail address. As only the legitimate user can unlock his locked account, on-line guessing attacks cannot be performed efficiently.

3.2 Usability Analysis of T-RiS

Compared with RiS, the operation of T-RiS is simpler and easier to learn. Additionally, each ring is composed of three consecutive sectors of alphanumeric characters, including

Table 1 The login time and success rate of our T-RiS experiment.

Login Mode	LR1		LR0	
	average login time (seconds)	success rate	average login time (seconds)	success rate
Average	24.27	99.09%	3.37	100.00%
Std. Dev.	9.05	0.04	1.55	0

*The average password length of the participants is 10 characters.

Table 2 Comparison of RiS and T-RiS.

Scheme	Login Mode	Password Space	Success Probability of Accidental login	Login-Recording Attacks Resistance	Average Login Time (seconds)	Memory Burden
RiS	LR1	1.5×10^{16}	1.2×10^{-3}	30 login sessions	27.9	8-icon password
	LR0		8×10^{-6}	0 login session	10.16	
T-RiS	LR1	7.81×10^{26}	2.37×10^{-3}	4 login sessions	24.27	(6~15)-character password
	LR0		1.79×10^{-12}	0 login session	3.37	

*The parameters setting of RiS: $N = 400$, $k = 8$, $n = 150$, and $r = 5$.

the sector of upper case letters, the sector of lower case letters, and the sector of decimal digits. Thus, the user can find his pass-character in a specific sector rather than in the whole ring. In addition, since there is exactly one pass-character on each ring, once the user finds the pass-character on a ring, he can ignore the remaining characters on it. To evaluate the usability of T-RiS, an experiment was conducted. The participants of our experiment are 22 college students majored in computer science. The participant can freely choose his password. Before the experiment, the participants were given two weeks to fully familiarize with T-RiS. In our T-RiS experiment, each participant was given 5 chances to log into the system by using the LR0 login mode and the LR1 login mode, respectively. Table 1 shows the results of our usability experiment for the LR0 login mode and the LR1 login mode of T-RiS.

Note that if the LR0 login mode and the LR1 login mode are chosen by the user with equal probability, the average login time for T-RiS is $\frac{24.27+3.37}{2} = 13.82$ seconds.

4. Comparison of T-RiS and RiS

In Table 2, we compare T-RiS with RiS [2] with respect to the password space, the success probability of accidental login, the login-recording attacks resistance, the average login time, and the memory burden. Although the resistance of T-RiS to login-recording attacks is weaker than the one of RiS, T-RiS is superior to RiS with respect to the password space and the average login time. However, the memory burdens of RiS and T-RiS cannot be easily compared because a textual password may be either meaningful or meaningless, either simple or complicated, either random or nonrandom, either regular or irregular, and either user-chosen or system-assigned and a graphical password may be either abstract or not, either easily identifiable or difficultly identifiable, either impressive or not, and either user-chosen or system-assigned. Such an issue deserves further research.

It should be noted that the order effect on the average login times of RiS and T-RiS was eliminated because the participants of our experiment were given two weeks to fully familiarize with T-RiS and RiS before conducting the experiment.

5. Conclusions

We have proposed a textual-graphical password scheme, T-RiS, which provides the user with the capability of dynamically choosing the level of the resistance to login-recording attacks depending on the user's login environment. The T-RiS 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. T-RiS can be used in environments where the users are more familiar with passwords based on texts than passwords based on icons/images and the number of login sessions the adversary can record is usually less than five.

Acknowledgments

This work was supported in part by the Ministry of Science and Technology, Taiwan, under Grant MOST-103-2221-E-142-007.

References

[1] H. Gao, X. Liu, S. Wang, H. Liu, and R. Dai, "Design and analysis of a graphical password scheme," Proc. 4th International Conf. Innovative Computing, Information and Control, pp.675–678, 2009.

[2] W.-C. Ku, Y.-C. Yeh, B.-R. Cheng, and C.-J. Chang, "A sector-based graphical password scheme with resistance to login-recording attacks," IEICE Trans. Inf. & Syst., vol.E98-D, no.4, pp.894–901, 2015.

[3] A.H. Lashkari, O.B. Zakaria, S. Farmand, and R. Saleh, "Shoulder surfing attack in graphical password authentication," International Journal of Computer Science and Information Security, vol.6, no.2, pp.145–154, 2009.

[4] L. Sobrado and J.C. Birget, "Graphical passwords," The Rutgers Scholar, vol.4, 2002.

[5] L. Sobrado and J.C. Birget, "Shoulder-surfing resistant graphical passwords," Draft, 2005.

[6] The Transport Layer Security (TLS) Protocol Version 1.2, RFC 5246, 2008.

[7] S. Wiedenbeck, J. Waters, L. Sobrado, and J.-C. Birget, "Design and evaluation of a shoulder-surfing resistant graphical password scheme," Proc. 2006 Advanced Visual Interfaces, 2006.

[8] T.-S. Wu, M.-L. Lee, H.-Y. Lin, and C.-Y. Wang, "Shoulder surfing-proof graphical password authentication scheme," International Journal of Information Security, vol.13, no.3, pp.245–254, 2013.

[9] T. Yamamoto, Y. Kojima, and M. Nishigaki, "A shoulder-surfing-resistant image-based authentication system with temporal indirect image selection," Proc. 2009 Security and Management, pp.188–194, 2009.