Analysis and Evaluation of the ColorLogin Graphical Password Scheme

Haichang Gao, Xiyang Liu, Ruyi Dai, Sidong Wang, and Xiuling Chang
Software Engineering Institute, Xidian University 710071, P.R.China
{hchgao, xyliu}@xidian.edu.cn

Abstract

It is believed that graphical passwords are more memorable than traditional textual passwords, but usually seen as complex and time-consuming for users. Furthermore, most of the existing graphical password schemes are vulnerable to spyware and shoulder surfing. ColorLogin uses color, a method not previously considered, to decrease login time. Multiple colors are used to confuse the peepers, while not burdening the legitimate users. Meanwhile, the scheme is resistant to shoulder surfing and intersection attack to a certain extent. This paper analyzes and evaluates the ColorLogin scheme using some experiments.

1. Introduction

Alphanumeric passwords are no doubt the most commonly used method by far for user authentication. However, alphanumeric passwords have several well-known limitations: Passwords have low entropy in practice (making them susceptible to dictionary attacks [1]), are often difficult to remember, and are vulnerable to shoulder surfing or observation by nearby third party [2].

Graphical password is a promising solution to this problem [4]. Psychologists have shown that in both recognition and recall tasks, images are more memorable than words or sentences [3]. Various graphical password schemes have been demonstrated as feasible alternatives to alphanumeric-based or biometric-based authentications. In the paper [9], a novel password scheme ColorLogin is proposed as a promising recognition-based graphical password scheme. For the first time, the image background color is used as a safety factor in ColorLogin. The main contributions of ColorLogin include providing an appealing authentication method, with resistance to shoulder surfing and intersection attack.

This paper analyzes and evaluates the ColorLogin scheme using some theoretical analysis and actual experiments.

2. The ColorLogin scheme

In ColorLogin, the system challenges a user who wants to be authenticated. The challenge is conducted in R rounds and each round provides random icons displayed on the screen. An example of a challenge round is shown in Figure 1; in which red is the focused color while blue and green are inducing ones. A pass-icon is chosen correctly when the user clicks on the row which contains the pass-icon. The icons in that row are all replaced by a substituted Lock icon to resist shoulder-surfing. A round is considered to be a successful one when all the h hiding pass-icons are correctly chosen. In order to reduce users' memory burden, it is not necessary for users to choose in a particular order.

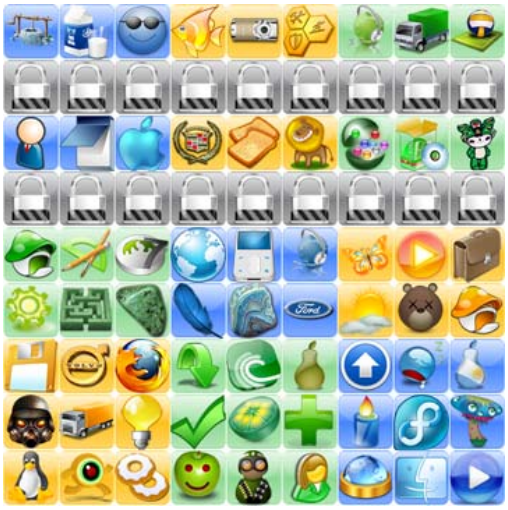

Figure 1: A completed authentication round. It contains two pass-icons in two lines. When the user clicks on a line, the icons in that line are replaced by the substituted icon.

3. Analysis of the proposed scheme

3.1. Resistance to shoulder surfing

It is well-known that, like alphanumeric passwords, most graphical password schemes are vulnerable to

shoulder surfing attacks [8]. Shoulder surfing usually refers to someone watching over a user's shoulder when the user logs into a system and analyzing the stolen information to retrieve the password. Shoulder surfing attacks do not happen often, but the consequences can be severe. It can occur in offices and public places without user awareness [11].

Some proposed password schemes have proved to be shoulder surfing resistant. But they are actually alphanumeric-based, for instance the scheme proposed in paper [7], which requires users to remember and input text characters, or not a good user experience, such as CHC proposed in [11], which may cause difficulties for users in clicking icons. ColorLogin provides a shoulder surfing resistant scheme which can overcome the drawbacks noted above.

In ColorLogin, there are different icons on the screen in each login round. Neither the icons nor the pass-icons displayed are fixed. When the user finds one pass-icon, he only needs to click on the line where the pass-icon lies, rather than the pass-icon itself. The clicked icon is either a pass-icon or only a casual icon and it may not be the same as the previous authentication, which makes it hard for the attackers to crack the password by analyzing the stolen information. What is more, after the action of the mouse, the icons in the clicked line would be replaced by substituted icons. Although such replacement is no use in resisting shoulder surfing when the process is recorded by video tape, it is very helpful to resist shoulder watchers, where the peepers cannot remember the icons in a short time.

Even if the peeper fortunately clicks on the correct lines and is authenticated, he does not have the real pass-icons and can not change the legitimate user's password. There is little chance for him to be authenticated next time. This is also helpful to protect user privilege.

3.2. Resistance to intersection attack

Intersection attack mentioned in Déjà Vu means that if all the password images are part of the challenge sets, and decoy icons are changed in each round, intruders can use the intersection of two challenge sets to reveal the password images [5]. It is the most common problem in most existing graphical password schemes using multiple images choice as pass objects, such as Passfaces[6], Déjà Vu [5] and Convex Hull Click [8]. ColorLogin considers the probability of each icon's appearance to resist intersection attack completely.

The login screen is divided into $C \times C$ background color squares. To authenticate the user, each screen presents H icons, which are randomly chosen from a database consisting of L icons. We call $\frac{H}{L}$ display probability. If the display probability of a pass-icon is higher than a decoy icon, pass-icons will appear more often than decoy icons in several rounds. It is much easier for intruders to guess the user's choices from the icons which appear more. Conversely, intruders can guess the user's choices by excluding the icons which appear more. Therefore, in order to resist intersection attack, display probabilities of pass-icons and decoy icons must be equal.

In ColorLogin, the requirement that display probabilities are equal is satisfied. There are h pass-icons shown on each screen which are randomly chosen from the predefined k pass-icons ($h<k$), while for the same color there are $9 \times C$ decoy icons shown which are randomly chosen from the N_C icons ($9 \times C < N_C$). Thus, as a pass-icon, the probability of being shown on each screen is $\frac{h}{k}$, while as a decoy icon, the probability of shown on each screen is $\frac{9 \times C}{N_C}$. If the probabilities of pass-icons and decoy icons shown on each screen are equal, intruders can not guess pass-icons by comparison of appearance frequency of icons. Therefore, $\frac{9 \times C}{N_C} = \frac{h}{k}$ are set in ColorLogin, making the probabilities of pass-icons and decoy icons shown on each screen equal and this prevents intersection attack.

Accordingly, different N_C are set according to the security level in the realization of ColorLogin. For example, the probability of the pass-icon in Low-level (C=3, k=3, h=2, N_3=40) is 2/3, while the probability of the decoy icon is about 27/40≈2/3; The probability of the pass-icon in Middle-level (C=4, k=4, h=3, N_4=72) is 2/4 = 0.5, while the probability of the decoy icon is 36/72 = 0.5; The probability of the pass-icon in High-level (C=5, k=5, h=4, N_5=112) is 2/5=0.4, while the probability of the decoy icon is 45/112 ≈0.4. The probabilities of pass-icons and decoy icons shown on each screen are almost equal. In other words, when C=5, if the intruder gains 100 screens or more, he will find that the same icon appears about 40 times, whether it is a pass-icon or a decoy icon. The intruder can not find pass-icons by appearance frequency no matter how frequently he tries because of the equal probabilities of icons in our theory. As a result of the equal probabilities, it is difficult to crack the pass-icons by statistics or probability analysis of the displayed icons.

The mean number of intersection icons of two challenge sets as equation (2):

$$p_i = \frac{C_{Nc}^{9\times C} \cdot (C_{9\times C}^{i} \cdot C_{Nc-9\times C}^{9\times C-i})}{(C_{Nc}^{9\times C})^2} = \frac{C_{9\times C}^{i} \cdot C_{Nc-9\times C}^{9\times C-i}}{C_{Nc}^{9\times C}} \quad (1)$$

$$m_c = \begin{cases} C \cdot \sum_{i=14}^{9\times C} (i \cdot p_i), & C = 3 \\ C \cdot \sum_{i=1}^{9\times C} (i \cdot p_i), & C = 4, or 5 \end{cases} \quad (2)$$

Here i is the number of overlapping icons from two screens for each color icon, and $9\times C$ expresses the number of each color shown on a screen. For a single color, there are as many as $\left(C_{N_C}^{9\times C}\right)^2$ choices of icons shown on each of two screens. Suppose there are i icons displayed on both screens, the number of all possible combination choice is $C_{N_C}^{9\times C} \cdot C_{9\times C}^{i} \cdot C_{N_C-9\times C}^{9\times C-i}$. Thus, the probability of i overlapping icons over all possible combinations forms Equation (1). When C=3, there must be at least 14 duplicated icons for one color, so computing the weighted average value from i=14 to $9\times C$, the mean number gained is Equation (2). It can be calculated that $m_3 = 54$, when $C \geq 4$, computing the weighted average value from i=0 to $9\times C$, the mean number of repeated icons for a single color is Equations (2). $m_4 = 72$ (C=4) and $m_5 = 90$ (C=5).

Thus, when C=3, for a whole screen with all three colors, there will be 54 duplicated icons on the average. When C=4 and 5, the mean number of intersection of two challenge sets is 72 and 90 respectively. It is also an impossible task for intruders who want to guess the pass-ions by intersection analysis of two screens.

3.3. The probability of successful intruder login

It is well known that an intruder can possibly log into the system by random clicks on an image in a graphical password scheme. Consider an interface consisting of a rectangle grid of size $n\times n$, the probability P of an intruder's successful login each time is computed with three variables: n, h and R, shown as equation (3).

$$p = \frac{1}{\left(C_n^h\right)^R} \quad (3)$$

For each round, picking h from n rows yields as many as C_n^h choices. When there are R rounds, the total choices are $\left(C_n^h\right)^R$. For example, for n=15, h=2 and R=3, we obtain $\frac{1}{\left(C_{15}^2\right)^3} = \frac{1}{1157625}$. When the three variables have correct values, a brute-force intruder attack will have an extremely small chance of success. Table 1 gives the probability of a successful intruder login when using ColorLogin. For a better understanding, representative graphical password scheme, Passfaces [6], is chosen to evaluate the probability of successful intruder login. By comparison, it can be easily concluded that ColorLogin is harder for an intruder to crack. Users can select the corresponding security level according to their need.

Table 1. The probability of a successful intruder login using ColorLogin and Passfaces.

	Passface	**Grid size of ColorLogin**		
		9×9	**12×12**	**15×15**
R = 1	1/9	1/36	1/66	1/105
R = 2	1/81	1/1296	1/4356	1/11025
R = 3	1/729	1/46656	1/287496	1/1157625

3.4. Password space

Most of the proposed recognition-based graphical password schemes calculate password space by different methods, based on different mechanisms. The password space of Déjà Vu and CHC schemes is the number of possible passwords C_M^D (choose any D pictures among M. M being the total number of pictures, and D the number of password pictures). The password space of Passface and Picture Password is C_M^D (D is the number of rounds of authentication, M is the total number of pictures at each round) [10].

In ColorLogin, the password space S can be determined by equation (4).

$$S = C \times \binom{N_c}{k} \quad (4)$$

Expression $\binom{N_c}{k}$ denotes the combination number of choosing any k icons among N_C icons of the same color. Then, for all C colors, the password space S can be obtained. The password space varies with C N_C and k. According to the value of C N_C and k given in this paper, the password space of ColorLogin can be obtained as shown in Table 2. The system can also extend the password space by increasing both the number of colors and the number of pass-icons.

When C=5, the password space is approximately $5\times\binom{112}{5}\approx 6.7e+8$, which is smaller than text-based passwords with a length of 5 ($94^5\approx$7.3e + 9). However, it is more difficult to carry out a brute force attack against graphical passwords than text-based passwords [10]. So as a graphical password scheme, the password space of ColorLogin is sufficient. As mentioned in [10], most recognition-based graphical passwords tend to have a small password space. Picture Passwords are used for mobile devices, thus the total number of pictures is small due to the size limit of mobile devices and the password space must be limited. Déjà Vu and CHC pointed out that the password space can enlarge by increasing the number of total icons and pass-icons, but it is not realistic for users.

Table 2. The password space of ColorLogin.

C, k, N_C	**3, 3, 40**	**4, 4, 72**	**5, 5, 112**
space	3e+5	4e+7	6e+9

4. Experiments and results

The proposed ColorLogin is implemented in C++. The tool can be used as a password login scheme replacing that of Windows XP's. ColorLogin provides different interfaces with grid of size n×n (9×9, 12×12, 15×15) varying with different security levels. The password space can be made very large by increasing the grid density, the authentication rounds, and the icon number of the database. The practical limitation is that the interface size is finite and if the icons are too small, users cannot easily identify them.

A number of experiments were conducted, aimed at showing the usability, security and memorability of ColorLogin. For the study, we targeted a population of experienced computer users. The participants were 30 university members who were unfamiliar with ColorLogin, including 4 teachers and 26 college students. 17 were female and 13 were male. The majority of the students were studying for their Master's degrees. The average age of the participants was 26 years old.

Before the experiments, the experimenter explained the purpose of the system and how it worked, using the tutorial materials. The participants were told to remember the color which they chose and mentally locate the h pass-icons in the window. The participants were specifically told not to click on the pass-icons, but on other icons on the same line. The experimenter explained to the users that feedback on accuracy would be given only at the end of the whole password input, not between each of the R challenges. All the participants were asked to test ColorLogin after training.

4.1. Usability

In the first session, thirty participants repeatedly attempted to authenticate themselves until ten successful logins were achieved with a 9×9 grid screen and R=1. The mean times to log into ColorLogin are shown in Figure 2, which indicates that there is a slight downward trend in the time taken for the user to be authenticated.

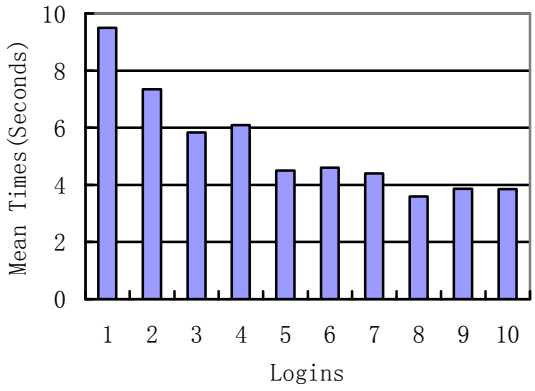

Figure 2: Mean times of 30 participants for 10 correct logins in ColorLogin with a 9×9 grid screen, R=1.

The results in Table 3 are encouraging. With proper grid density and authentication challenge rounds, ColorLogin demonstrated good performance. Though it took a longer time to log into ColorLogin than in text-based schemes, approximately 85% participants thought that the time of login was acceptable according to the post-test questionnaire. The reason may be that an appealing login process can shorten the perception of time taken.

Table 3. Mean times (seconds) of 30 participants for 5 correct logins in ColorLogin.

	Grid size of ColorLogin		
	9×9	**12×12**	**15×15**
R = 1	3.4	5.2	5.5
R = 2	8.2	9.6	11.2
R = 3	11.3	13.6	15.2

The mean time of Convex Hull Click Scheme (CHC) for one round is 10.97 seconds and for five rounds is 71.66 seconds [11]. The mean time of Déjà Vu for one round is 32 seconds [5]. Compared to these similar schemes ColorLogin takes less time for users to be authenticated.

Figure 3: The interface of the scheme without background color.

To demonstrate the effect of the background color, a further experiment was conducted. Here, the same 30 participants were required to login ten times to a similar scheme without background color, as shown in Figure 3. Compared with ColorLogin, the mean times (grid size 9×9) of the 30 participants are clearly longer, as shown in Figure 4. In other words, the use of background color is effective in reducing login time.

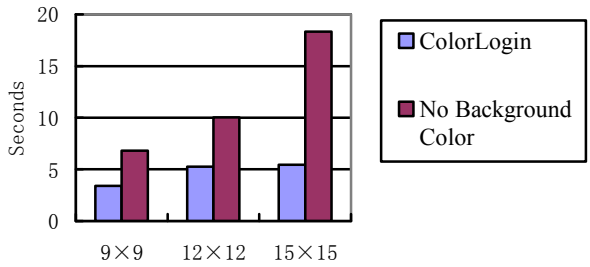

Figure 4: Mean times (seconds) of 30 participants for 10 correct logins in ColorLogin and the similar scheme without background color respectively, R=1.

At the end of this session, all participants answered a simple questionnaire. According to questionnaire results, ColorLogin is appealing to three-quarters of the interviewees and the login time is rated as highly acceptable or acceptable. As we had expected, ColorLogin was rated easy to master by more than 85% of the participants. Additionally, the results indicate that ColorLogin provides a user-friendly interface by using the background color. 50% of the participants preferred to choose ColorLogin as a login system. Ten of them thought it was interesting to find a pass-icon from a number of icons, similar to playing a game. Five of them thought it was easy to remember the pass-icons, or highly resistant to shoulder surfing. Two of the 50% of participants who chose text-based password login offered the reason that pass-icons were easily forgotten, and the remainder provided other reasons such as they had been used to the text-based password. It is encouraging that 50% of the participants preferred using ColorLogin.

The experiments and survey demonstrate that ColorLogin provides usability, is appealing and easily mastered. Even though there are still some aspects to improve, ColorLogin's advantages make it competitive as a graphic password scheme.

4.2. Resistance to shoulder surfing

In the first stage, 30 participants were asked to act as peepers to steal their counterpart's account and password. They attempted 3 times to use the stolen information to log into ColorLogin. Experiment results showed that none of the total 30 peepers were able to successfully authenticate the login. This demonstrates that ColorLogin is highly resistant to shoulder surfing.

4.3. Memorability

All of the 30 participants carried out a memorability experiment one week later, in session 2. The results were categorized for the following characteristics: matched pass-icons at the first chance, matched pass-icons in three login chances, color errors and icon errors. Results showed that 93.3% of participants could be successfully authenticated on one login attempt and 100% successfully when given three login chances. None of them forgot the predefined color. One month later, all of the participants were asked to retry, and all of them logged in successfully within three attempts. It is predictable that users would be used to ColorLogin and remember their color and pass-icons clearly after a short time's use.

5. Conclusions and further works

ColorLogin is a graphical passwords method to develop more effective, user friendly and secure . In this paper, image background color is introduced for the first time as a means of reducing the legal user's login time, considered to be crucial to the usability of a password scheme. In doing so it aims to motivate the user with a fun, friendly interface designed to improve user experience and provide acceptable login time.

ColorLogin is resistant to shoulder surfing and spyware because of the random display of icons, the selection of the row which pass-icons lies in and the concealment of the clicked row. The password space can be made very large, and therefore more secure, by increasing the number of icons, the number of pass-icons, and the number of authentication rounds, or all of these factors. The only practical limits are the size of

the window and the ability of users to locate their pass-icons among a large number of icons. In ColorLogin, the correct number of the pass-icons shown at each round and total icons per color in the database are set for different numbers of color, targeting total resistance to intersection attack.

The user study presented demonstrates that the use of background color provides higher security while remaining user-friendly, while at the same time increasing defenses against shoulder surfing. It is also concluded that ColorLogin is easy to learn and the login time is acceptable. Memorability was demonstrated to be high.

Generally speaking, ColorLogin is a promising technique which can be developed by further studies. Future work should consider higher security mechanisms, reducing time consumption and the encryption of the icons. Individual user personality has an effect on choice of color and icons, and some icons are frequently chosen as pass-icons, creating so-called hotspots, a problem that also needs addressing. Further research into these factors is continuing. Meanwhile, the color-blind users will be taken into accounted. In the near future, ColorLogin is expected be further tested in actual projects.

6. Acknowledgments

The authors would like to thank the reviewers for their careful reading of this paper and for their helpful and constructive comments. This work was supported in part by the Natural Science Basic Research Plan in Shaanxi Province of China under grant No. SJ08F25, the Foundation of China under grant No. 9140A15050206DZ01 and the Pre-Research project of China under grant No. 51315050105.

Reference

[1] Klein, D., Foiling the Cracker: A Survey of, and Improvements to, Password Security. *In Proceedings of the USENIX Security Workshop*, 1990, 5-14.

[2] Roth, V., Richter, K., and Freidinger, R., A PIN-Entry Method Resilient Against Shoulder Surfing. *In Conference on Computer and Communications Security*, 2004, 236-245.

[3] Paivio, A., Rogers, T.B., and Smythe, P.C., Why are pictures easier to recall then words? *Psychonomic Science*, 1976, 11(4), 137-138.

[4] Blonder G. E., Graphical passwords. *In Lucent Technologies*, Inc., Murray Hill, NJ, U. S. Patent 5559961, Ed. United States, 1996.

[5] Dhamija R. and Perrig A., Déjà Vu: A User Study Using Images for Authentication. *In Proceedings of 9th USENIX Security Symposium*, 2000.

[6] Passfaces. http://www.realuser.com, site accessed on Jan, 2009.

[7] Man S., Hong D., and Mathews M., A shoulder surfing resistant graphical password scheme. *In Proceedings of International conference on security and management*. Las Vegas, NV, 2003.

[8] Sobrado L. and Birget J.C., Graphical passwords, http://rutgersscholar.rutgers.edu/volume04/sobrbirg/ sobrbirg.htm. The Rutgers Scholar, *An Electronic Bulletin for Undergraduate Research*, vol. 4, 2002.

[9] Haichang Gao, Xiyang Liu, Sidong Wang, Honggang Liu, and Ruyi Dai, Design and Analysis of a Graphical Password Scheme, *in Fourth International Conference on Innovative Computing, Information and Control (ICICIC)*, Kaohsiung, Taiwan, Dec 7-9, 2009.

[10] Suo X., Zhu Y., Owen G.S., Graphical passwords: A survey. ACSAC'05, *21st Annual Computer Security Applications Conference*, 2005, pp.463-472

[11] Wiedenbeck S., Waters J., and Sobrado L. et al., Design and evaluation of a shoulder surfing resistant graphical password scheme. *In Proceedings of the working conference on Advanced visual interfaces*, Venezia, Italy, 2006.