AUTHENTICATION SCHEME FOR SESSION PASSWORDS USING COLOR AND IMAGE

[1]P. Saranya,, [2]S. Sharavanan, [3]R.Vijai and [4]RM. Balajee

[1]PG Scholar/ Department of CSE,

[2]Professor & Head / Department of CSE,

[3, 4] AP / Department of CSE,

Annapoorana Engineering College, Salem.

Email: rajeswariselvaraj89@gmail.com

Submitted: May 27, 2017 ***Accepted: June 15, 2017*** ***Published: Sep 1, 2017***

Abstract- ***Graphical passwords are believed to be more secure than traditional textual passwords, but the authentications are usually complex and boring for users. Furthermore, most of the existing graphical password schemes are vulnerable to spyware and shoulder surfing. A novel graphical password scheme ColorLogin is proposed in this paper. ColorLogin is implemented in an interesting game way to weaken the boring feelings of the authentication. ColorLogin uses background color, a method not previously considered, to decrease login time greatly. 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. Experiments illustrate the effectiveness of ColorLogin.***

Index terms*:* Graphical Passwords, Shoulder-Surfing, Intersection Attack

.

I. INTRODUCTION

Lack of security has become a major concern, given the prevalence of attackers, hackers, crackers, scammers and spammers. A key area in security research and practice is authentication, the determination of whether a user should be allowed to access a given system or resource. Adequate authentication is the first line of defense for protecting resources. Existing authentication processes are usually accomplished by user ID and password, with the authentication schemes alphanumeric-based, biometric-based or increasingly graphical-based.

Alphanumeric passwords are no doubt the most commonly used method by far for user authentication, but the "password problem" [1] arises because such passwords are expected to comply with two conflicting requirements, namely: (1) Passwords should be easy to remember, and the user authentication protocol should be executable quickly and easily. (2) Passwords should be secure, i.e. they should be random-looking and should be hard to guess; they should be changed frequently, and should be different for multi-accounts; they should not be written down or stored in plain text. Meeting these conditions is almost impossible for humans, with the result that the use of alphanumeric passwords has several well-known limitations: Passwords have low entropy in practice (making them susceptible to dictionary attacks [8]), are often difficult to remember, and are vulnerable to shoulder surfing or observation by nearby third party [2].

Biometric systems rely upon unique features unchanged in the lifetime of a human, such as fingerprints, retina pattern, iris, voice print and face pattern, and are used as an alternative to alphanumeric passwords, but not yet widely adopted. The major drawback of using biometrics as an authentication technique is that such systems may be expensive for additional devices to obtain and handle the physical characters of users, and the identification process may cost a significant amount of time. If the biometric identification feature is physically altered through an accident or operation, the authentication becomes invalid [11]. However, biometric-based passwords are believed to provide the highest level of security.

Researchers have developed several authentication methods based on graphical passwords, originally proposed by Blonder in 1996 [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 this paper, ColorLogin is demonstrated and assessed as a

promising recognition-based graphical password scheme, in which, for the first time, the image background color is used as a safety factor. The main contributions of ColorLogin include providing an appealing authentication method, with resistance to shoulder surfing.

The major disadvantage in most of the existing graphical password schemes is that the mouse-click. ColorLogin does depend on mouse clicks, however it is effective in overcoming this weakness. It is possible in ColorLogin that users can click on deceptive icons instead of pass-icons (used as password). Such action makes ColorLogin resistant to shoulder surfing.

II. RELATED WORKS

Graphical password schemes based on choosing multiple images as pass objects usually require users to recognize the pre-selected pictures and repeat the correct select actions. As the first choice of multiple images as pass objects scheme, based on Hash Visualization technique [9], Déjà Vu authenticates a user through his ability to recognize previously registered images [5]. As a result of the random generation of candidate pictures, it is not convincing to conclude that passwords are easier to remember and recall than text-based passwords. Real User employs facial photographs in its graphical password system Passfaces [6], a technique using human faces as passwords, developed because people usually recognize faces better than ordinary pictures. However, given the limited candidate faces on the screen, the security of Passfaces is vulnerable to trial attacks. Convex Hull Click is developed to overcome the problem of passwords that are vulnerable to shoulder surfing in a public environment. It motivates the users to log in quickly and accurately [7]. The suggested number of icons to ensure a large password space makes the screen crowded for users to find out the right click region. It was also be found that, the Convex Hull occasionally forms too narrow a space for users to click on. Another shoulder surfing resistant graphical password scheme is obtained by adding a light graphic layer to traditional textual -based password scheme. The scheme has proved to be effective against shoulder surfing attacks, and yet as it is alphanumeric-based, it contains the inevitable drawbacks of alphanumeric passwords.

The above-mentioned graphical password schemes have not provided a satisfactory answer for usability and security, the two of major design and implementation issues of graphical passwords. ColorLogin is basically a recognition-based graphical password scheme, choosing multiple

images as password icons or pass-icons. It is designed as a Windows XP login authentication scheme which can be used in logging into the system or unlocking the screen.

III. DESIGN OF COLORLOGIN

In ColorLogin, there are four security levels called low, medium, high and self-define respectively. There are six parameters, *R*, *C*, *k*, N_C , *h* and *n* wherein *R*, *C*, *k* and *n* are determined by the level.

1) *R* is the number of rounds for authentication, ranging from 1 to 3 respectively to define low, medium and high security levels.
2) *C* is the number of colors used, ranging from 3 to 5.
3) *k* is the number of pass-icons.
4) N_C is the number of total icons per color in the database for different value of *C*. N_3 =40, N_4 =72 and N_5 =112. The reason of selecting different will be illuminated in section 4.3.
5) *h* is the number of pass-icons shown on each screen, and *h*=2 is used in this paper.
6) *n* is the number of rows or columns, and *n*=9, 12 or 15.

Figure 1. A group of chosen-color icons are displayed for the user to set as his pass-icons. Here, the user chooses three red icons as his password. (All icons used in ColorLogin are obtained from http://www.chinaz. com freeware and processed for study only.)

In registration phase, shown in Figure 1, the user operations can be divided into three steps:

1) Choose a security level needed.
2) Choose one color from the *C* colors randomly provided by system.
3) Choose *k* images from the sets of the chosen color as pass-icons (i.e. password).

The generation process of each round in the authentication phase can be described below:

1) Randomly generate the *i*th round screen, where the icon groups are distributed by a sliding color sequence. In each group, icons randomly chosen from

the database form a single color icon square, but are not permanent. On the whole screen, there would be *C* such color squares, filling in the coarse grid. And each icon on the screen is different.

2) When the icons are distributed, *h* of the *k* pass-icons must be displayed randomly in *h* different lines. For example, in Figure 2 (a), there are two of the three pass-icons lying in two different lines in the authentication round.
3) Wait for the user to click on the pass-icon lines and replace all icons on the line with substituted icons.
4) Gather the input information to authenticate the user.

(a). The displayed screen.

(b). A completed round.

Figure 2. A completed authentication round is shown here (R = 1, C = 3, n = 9, h = 2). 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.

In each login, 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 2; 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, shown in Figure 2. In order to reduce users' memory burden, it is not necessary for users to choose in a particular order.

The login screen is divided into $C \times C$ background color squares. Once a user chooses his color, both colors and their positions shown on each screen for the same user are fixed. The icons of each color are randomly chosen from the database and are all different. The *h* pass-icons randomly chosen are displayed on different rows. Considering security and usability, we set $h=2$. If $h=1$, the probability of an intruder's successful login will be greater. And if $h \geq 3$, the time period for finding pass-icons will be longer for legal users.

IV. ANALYSIS OF THE PROPOSED SCHEME

4.1 Contribution of Background Color

When users log into the schemes which choose multiple images as pass- icons, most time is spent in locating the pass-icons from large number of icons which are randomly placed. Color is one of the most important features of images. But it has never before been considered in previous multiple image choice schemes. The background color of images is first proposed and used in ColorLogin.

In ColorLogin, the icons on the screen are distinguished clearly by different colors. When users are asked to recognize the pass-icons in the authentication, they only need to pay attention to the icons of the predefined color rather than all the icons displayed. As shown in Figure 2, users only need to search for the pass-icons from 27 red icons, while 81 are presented. Thus, introduction of colors can cut workload 2/3 relative to similar schemes without background colors. This is just an

instance at the lowest level. In higher levels, more colors are introduced with a decreased workload. At most, 5 colors can be used In ColorLogin and 4/5 of the workload is reduced. It is easy to conclude that the login time can be reduced greatly. In addition, if the authentication procedure is too tedious, it may create memorization difficulties and annoy users. The use of background colors can make the user interface friendly, which helps users escape from the irritation of large numbers of confusing icons. Experiments in section 5 demonstrate these results.

4.2 Resistance to Shoulder Surfing

Some proposed password schemes have proved to be shoulder surfing resistant. But they are actually alphanumeric-based, which requires users to remember and input text characters, or not a good user experience, such as CHC proposed in [10], 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. 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.

4.3 Password Space

System security largely depends on having sufficiently large password space, the main defense against a brute force search.

Alphanumeric based passwords have a password space of 94^n , where n is the password length, 94 is the number of printable characters excluding SPACE. One major problem faced by graphical passwords is ensuring that the password space is comparable to that of alphanumeric passwords.

In ColorLogin, the password space S can be determined by equation (1).

$$N \quad c \qquad (1)$$

$S \square C \square$

k

N

Expressio ^{c} denotes the combination number of

n choosing

k

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 1. 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

approximatel112 $\approx 6.7e \square 8$, which is smalle1

y 5□ than text-

5

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. So as a graphical password scheme, the password space of ColorLogin is sufficient. As mentioned in [8], 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 1. 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

V. USABILITY EXPERIMENTS

The proposed ColorLogin is implemented in C++. The tool can be used as a password login scheme replacing that of Windows XP's. Before the experiments, the experimenter explained the purpose of the system and how it worked, using the tutorial materials.In the first session, thirty participants repeatedly attempted to authenticate themselves until ten successful logins were achieved. The mean times to log into ColorLogin are shown in Figure 3,

which indicates that there is a slight downward trend in the time taken for the user to be authenticated.

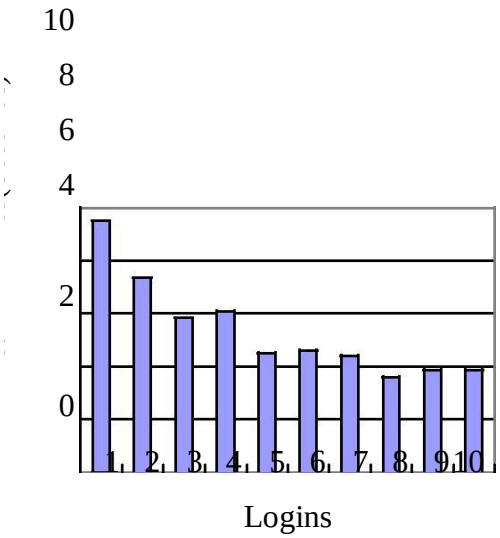

Figure 3. Mean times of 30 participants for 10 correct logins in ColorLogin with a 9×9 grid screen，R=1.

The results in Table 2 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 2. Mean times (seconds) of 30 participants for 5 correct logins.

	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 [10]. 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.

VI. CONCLUSIONS AND FURTHER WORKS

ColorLogin is a graphical passwords method to develop more effective, user friendly and secure . In this project, 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. It aims to motivate the user with a fun, friendly interface designed to improve user experience and provide acceptable login time. Color Login is a promising technique which can be developed by further studies. Future work should consider higher security mechanisms, and reducing time

consumption. 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. Meanwhile, the color-blind users will be taken into accounted. In the near future, ColorLogin is expected be further tested in actual projects.

REFERENCES

[1] Aizat Azmi, Ahmad Amsyar Azman, Sallehuddin Ibrahim, and Mohd Amri Md Yunus, "Techniques In Advancing The Capabilities Of Various Nitrate Detection Methods: A Review", International Journal on Smart Sensing and Intelligent Systems., VOL. 10, NO. 2, June 2017, pp. 223-261.

[2] Tsugunosuke Sakai, Haruya Tamaki, Yosuke Ota, Ryohei Egusa, Shigenori Inagaki, Fusako Kusunoki, Masanori Sugimoto, Hiroshi Mizoguchi, "Eda-Based Estimation Of Visual Attention By Observation Of Eye Blink Frequency", International Journal on Smart Sensing and Intelligent Systems., VOL. 10, NO. 2, June 2017, pp. 296-307.

[3] Ismail Ben Abdallah, Yassine Bouteraa, and Chokri Rekik , "Design And Development Of 3d Printed Myoelctric Robotic Exoskeleton For Hand Rehabilitation", International Journal on Smart Sensing and Intelligent Systems., VOL. 10, NO. 2, June 2017, pp. 341-366.

[4] S. H. Teay, C. Batunlu and A. Albarbar, "Smart Sensing System For Enhanceing The Reliability Of Power Electronic Devices Used In Wind Turbines", International Journal on Smart Sensing and Intelligent Systems., VOL. 10, NO. 2, June 2017, pp. 407- 424

[5] SCihan Gercek, Djilali Kourtiche, Mustapha Nadi, Isabelle Magne, Pierre Schmitt, Martine Souques and Patrice Roth, "An In Vitro Cost-Effective Test Bench For Active Cardiac Implants, Reproducing Human Exposure To Electric Fields 50/60 Hz", International Journal on Smart Sensing and Intelligent Systems., VOL. 10, NO. 1, March 2017, pp. 1- 17

[6] P. Visconti, P. Primiceri, R. de Fazio and A. Lay Ekuakille, "A Solar-Powered White Led-Based Uv-Vis Spectrophotometric System Managed By Pc For Air Pollution Detection In Faraway And Unfriendly Locations", International Journal on Smart Sensing and Intelligent Systems., VOL. 10, NO. 1, March 2017, pp. 18- 49

[7] Samarendra Nath Sur, Rabindranath Bera and Bansibadan Maji, "Feedback Equalizer For Vehicular Channel", International Journal on Smart Sensing and Intelligent Systems., VOL. 10, NO. 1, March 2017, pp. 50- 68

[8] Yen-Hong A. Chen, Kai-Jan Lin and Yu-Chu M. Li, "Assessment To Effectiveness Of The New Early Streamer Emission Lightning Protection System", International Journal on Smart Sensing and Intelligent Systems., VOL. 10, NO. 1, March 2017, pp. 108- 123

[9] Iman Heidarpour Shahrezaei, Morteza Kazerooni and Mohsen Fallah, "A Total Quality Assessment Solution For Synthetic Aperture Radar Nlfm Waveform Generation And Evaluation In A Complex Random Media", International Journal on Smart Sensing and Intelligent Systems., VOL. 10, NO. 1, March 2017, pp. 174- 198

[10] P. Visconti ,R.Ferri, M.Pucciarelli and E.Venere, "Development And Characterization Of A Solar-Based Energy Harvesting And Power Management System For A Wsn Node Applied To Optimized Goods Transport And Storage", International Journal on Smart Sensing and Intelligent Systems., VOL. 9, NO. 4, December 2016 , pp. 1637- 1667

[11] YoumeiSong,Jianbo Li, Chenglong Li, Fushu Wang, "Social Popularity Based Routing In Delay Tolerant Networks", International Journal on Smart Sensing and Intelligent Systems., VOL. 9, NO. 4, December 2016 , pp. 1687- 1709

[12] Seifeddine Ben Warrad and OlfaBoubaker, "Full Order Unknown Inputs Observer For Multiple Time-Delay Systems", International Journal on Smart Sensing and Intelligent Systems., VOL. 9, NO. 4, December 2016 , pp. 1750- 1775

[13] Rajesh, M., and J. M. Gnanasekar. "Path observation-based physical routing protocol for wireless ad hoc networks." International Journal of Wireless and Mobile Computing 11.3 (2016): 244-257.

[14]. Rajesh, M., and J. M. Gnanasekar. "Congestion control in heterogeneous wireless ad hoc network using FRCC." Australian Journal of Basic and Applied Sciences 9.7 (2015): 698-702.

[15]. Rajesh, M., and J. M. Gnanasekar. "GCCover Heterogeneous Wireless Ad hoc Networks." Journal of Chemical and Pharmaceutical Sciences (2015): 195-200.

[16]. Rajesh, M., and J. M. Gnanasekar. "CONGESTION CONTROL USING AODV PROTOCOL SCHEME FOR WIRELESS AD-HOC NETWORK." Advances in Computer Science and Engineering 16.1/2 (2016): 19.

[17]. Rajesh, M., and J. M. Gnanasekar. "An optimized congestion control and error management system for OCCEM." International Journal of Advanced Research in IT and Engineering 4.4 (2015): 1-10.

[18]. Rajesh, M., and J. M. Gnanasekar. "Constructing Well-Organized Wireless Sensor Networks with Low-Level Identification." World Engineering & Applied Sciences Journal 7.1 (2016).

[19] L. Jamal, M. Shamsujjoha, and H. M. Hasan Babu, "Design of optimal reversible carry look-ahead adder with optimal garbage and quantum cost," International Journal of Engineering and Technology, vol. 2, pp. 44–50, 2012.

[20] S. N. Mahammad and K. Veezhinathan, "Constructing online testable circuits using reversible logic," IEEE Transactions on Instrumentation and Measurement, vol. 59, pp. 101–109, 2010.

[21] W. N. N. Hung, X. Song, G. Yang, J. Yang, and M. A. Perkowski, "Optimal synthesis of multiple output boolean functions using a set of quantum gates by symbolic reachability analysis," IEEE Trans. on CAD of Integrated Circuits and Systems, vol. 25, no. 9, pp. 1652–1663, 2006.

[22] F. Sharmin, M. M. A. Polash, M. Shamsujjoha, L. Jamal, and H. M. Hasan Babu, "Design of a compact reversible random access memory," in 4th IEEE International Conference on Computer Science and Information Technology, vol. 10, june 2011, pp. 103–107.

[23] Dr. AntoBennet, M, Sankar Babu G, Suresh R, Mohammed Sulaiman S, Sheriff M, Janakiraman G ,Natarajan S, "Design & Testing of Tcam Faults Using T_H Algorithm", Middle-East Journal of Scientific Research 23(08): 1921-1929, August 2015 .

[24] Dr. AntoBennet, M "Power Optimization Techniques for sequential elements using pulse triggered flipflops", International Journal of Computer & Modern Technology , Issue 01 ,Volume01 ,pp 29-40, June 2015.