International Journal of Research in Advent Technology (IJRAT) Special Issue
E-ISSN: 2321-9637
Sharadchandra Pawar college of Engineering, Dumbarwadi, Pune 410504,
Organizes
National Conference "MOMENTUM-17", 14th & 15th February 2017
Available online at www.ijrat.org

Secure Graphical Password Authentication System

Asst. Prof. Rahul R. Rathod[1]
Computer Department, SGOI College Of Engineering, Belhe, SPPU Pune[1]
Email: rathod.r.rahul@gmail.com

Abstract- Conventional password schemes like as textual password scheme, graphical scheme are commonly used for authentication. But also these schemes are vulnerable to dictionary attack, brute force attack, shoulder surfing attack, accidental login. These existing schemes are not secure and efficient enough and have high failure rate. Hence the secure graphical password auther Asst. Prof. Rahul R. Rathod[1] The secure graphical password authentication system is amend by using colors. So it has become safer. User can motile login to the system. Unauthorized user cannot get the password easily. Hence this scheme supply protection against the shoulder surfing

Index Terms- Dictionary attack, brute force attack, shoulder surfing attack, accidental login, textual password scheme, graphical scheme, vulnerable.

1. INTRODUCTION

The shoulder surfing attack is an attack that can be performed by the adversary to obtain the user's password by watching over the user's shoulder as he/she enters his/her password. As conventional password plan are vulnerable to shoulder surfing, Birget[1] as well as Sobrado proposed three shoulder surfing resistant graphical password schemes. Since then, many graphical password plans with different degrees of resistance to shoulder surfing have been proposed, and each has its pros and cons. Seeing that unique that most of the users are better known with textual password for user than pure graphical passwords, Zhao et al. [10]

Proposed a secure graphical password authentication system, S3APS. In S3PAS, the user has to mix his textual the login screen on password to get the session password. However, the login process of Zhao et al.'s plan is tedious and hard. And then, several secure graphical password authentication systems have been proposed, unfortunately, none of existing secure graphical password authentication systems is both efficient and secure enough. In this system, we will propose an improved secure graphical password authentication systems by using colors. The operation of the proposed scheme is easy and simple to learn for users familiar with textual passwords. The user can easily and efficiently login to the system without using any on-screen keyboard or physical keyboard. The rest of this paper is arranged as follows. In Sec. II, we will review literature survey works. In Sec. III, we will describe the proposed system. Next, we will analyze the security and system architecture of the proposed scheme in Sec. IV. Finally, we concluded in Sec. V

2. LITURATURE SURVEY

In 2002, Birget as well as Sobrado proposed three shoulder surfing resistant graphical password schemes, the Movable Intersection scheme, the Frame scheme, and the Triangle scheme. However, both the Movable Frame scheme and the Intersection scheme have high failure rate. In the Triangle scheme, the user has to memorize and to choose several pass-icons as his/her password. In every time whenever login the user has to find three pass-icons among a set of randomly chosen icons displayed on the login screen, and then click inside the invisible triangle created by those three pass-icons. In 2006, Wiedenbeck et al. proposed the Convex Hull Click 1Scheme as an improved version of the Triangle scheme with superior usability as well as security. To login the system, the user has to correctly respond several challenges. In each challenge, the user has to find any three pass-icons displayed on the login screen, and then click inside the invisible convex hull formed by all the displayed pass-icons. However, the login time of Convex-Hull Click scheme may be too long and more tedious. In 2009, Gao et al proposed a secure graphical password authentication scheme, Color Login, in which the background color is a usable factor for reducing the login time. However, the password space is too small and probability of accidental login of Color Login is too high. As most users are familiar with textual passwords as well the conventional textual password authentication schemes have no shoulder surfing resistance, Zhao et al. in 2007,

proposed a secure graphical password authentication system, S3PAS, in which the user has to find his textual password and also then follow a special rule to mix his textual password to get a session password to login the system. However, the login process of Zhao et al.'s scheme is tedious and complex. In 2011, Sreelatha et al. also proposed a secure graphical password authentication system by using colors. Clearly, as the user has to additionally memorize the order of several colors, the memory burden of the user is high. In 2012, Rao et al. proposed a secure graphical password authentication system, PPC. To login the system, the user has to mix his/her textual password to produce several pass-pairs, and then follow four predefined rules to get his/her session password on the login screen. However, the login process of PPC is too complicated and tedious.

3. PROPOSED SYSTEM

We will describe a simple and efficient secure graphical password authentication system based on colors and texts. The alphabet used in the propose scheme contains 64 characters, including 26 lower case letters, 26 upper case letters, and symbols "." and "/",10 decimal digits . The proposed scheme involves two phases, the login phase and the registration phase, which can be described as in the following.

3.1 REGISTRATION PHASE

The user has to set his/her textual password K of length is L(8≤L≤15) characters, and then choose one color as his pass color from 8 colors assigned by the system. The remaining 7 colors not selecting by the user are his bait colors. And, the user has to note an e-mail address for re-enabling his/her disabled account. The registration stage should proceed in an environment free of shoulder surfing. In addition, a secure channel should be created between the system and any other secure transmission mechanism or the user during the registration phase by using SSL/TLS [16][17]. the system accumulation the user's textual password in the user's entry in the password scheme, which should be decoded by the system key.

3.2 LOGIN PHASE

The user requests to login the system, and the system displays a circle designed of 8 equally sized sectors. The colors of the arcs of the 8 sectors are separated, and each area is identified by the color of its arc, e.g. the red area is the area of red arc. Initially, 64 characters are placed randomly and averagely among these sectors. All the displayed characters can be simultaneously rotated into either the adjacent sector counterclockwise by clicking the "counter clockwise" button once or, the adjacent sector clockwise by clicking the "clockwise" button once and the rotation operations can also be performed by the scrolling the mouse wheel. The login screen of the proposed scheme,To login the system, the user has to finish the following steps:

Step 1: *The user requests to login the system.*

Step 2: *The system displays a circle designed of 8 equally sized sectors, and places 64 characters among the 8 sectors randomly and averagely so that each sector contains 8 characters. The64 characters are in three typefaces in that the26 lower case letters ,the26 upper case letters are in bold typeface and the 10 decimal digits are in italic typefaceand the two symbols "." and "/" are in regular typeface. In addition, the button for rotating counterclockwise, the button for rotating clockwise, the "Confirm" button, and the "Login" button are also displayed on the login screen. All the displayed characters can be simultaneously rotated into either the adjacent sector counterclockwise by clicking the "counterclockwise" button once,or the adjacent sector clockwise by clicking the "clockwise" button once and the rotation operations can also be performed by scrolling the mouse wheel .*

Step 3: *The user has to rotate the sector containing the i-th pass-character of his/her password K, denoted by Ki, into his pass-color sector, and then clicks for the "Confirm" button. Let i = i + 1.*

Step 4: *If i < L, the system randomly permutes all the64 displayed characters, and then GOTOs Step 3. Otherwise, the user has to click the "Login" button to absolute the login process.*

4. ADVANTAGES

The operation of the proposed plan is simple and easy to learn for users well known with textual passwords. The user can easily and efficiently login to the system without using any on-screen keyboard or physical keyboard. Secure graphical password authentication system.

5. SYSTEM ARCHITECTURE

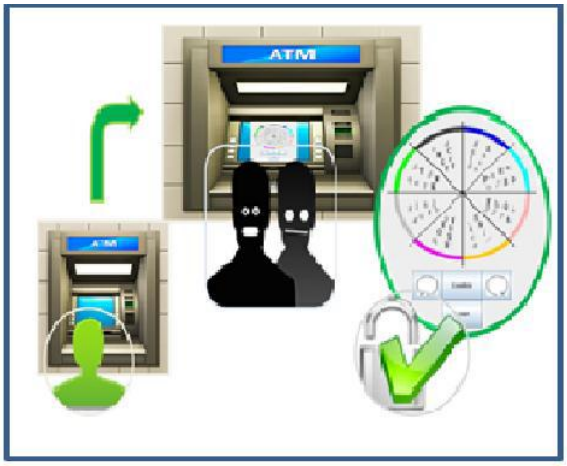

Fig. 1. System architecture

6. FIGURES, TABLES AND PHOTOGRAPHS

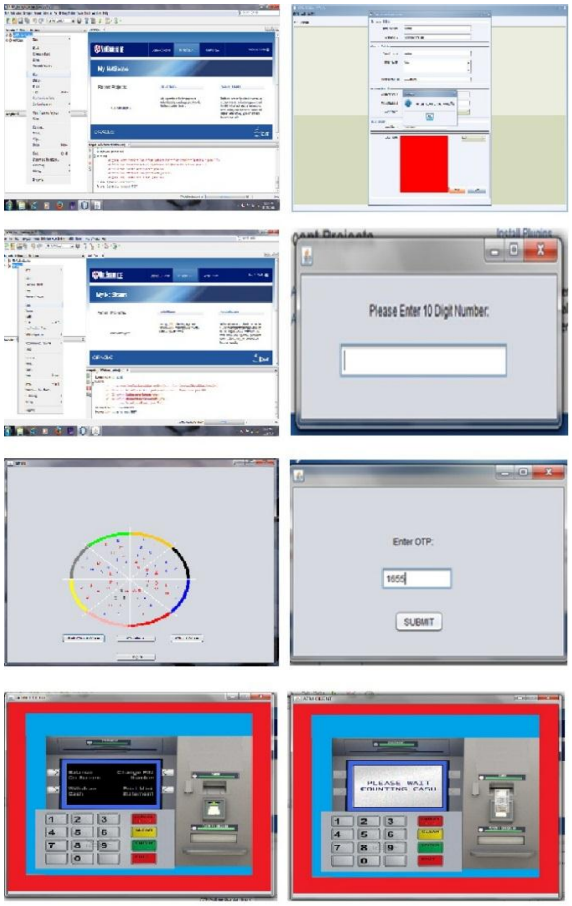

Fig. 1. GUI of System

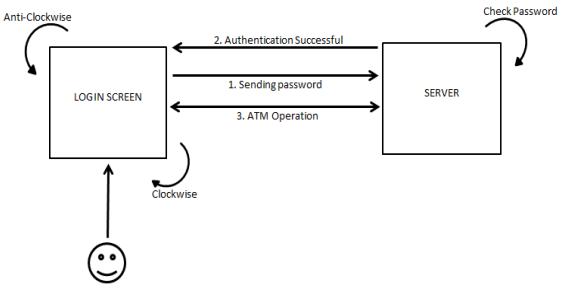

Fig. 1. Block Diagram

7. CONCLUSION

We have proposed at secure graphical password authentication system, in which the user can easily and efficiently complete the login process without worrying about shoulder surfing attacks. The operation of the proposed scheme is simple and easy to learn for users well known with textual passwords. The user can efficiently and easily to login the system without using any on-screen keyboard or physical keyboard. Finally, we have analyzed the resistances of the proposed scheme to shoulder surfing and accidental login.

8. REFERNCES

[1] S. M. Metev and V. P. Veiko, Laser Assisted Microtechnology, 2nd ed., R. M. Osgood, Jr., Ed. Berlin, Germany: Springer-Verlag, 1998.
[2] J. Breckling, Ed., The Analysis of Directional Time Series: Applications to Wind Speed and Direction, ser. Lecture Notes in Statistics. Berlin, Germany: Springer, 1989, vol. 61.
[3] 3 S. Zhang, C. Zhu, J. K. O. Sin, and P. K. T. Mok, "A novel ultrathin elevated channel low-temperature poly-Si TFT," IEEE Electron Device Lett., vol. 20, pp. 569–571, Nov. 1999.
[4] 4 M. Wegmuller, J. P. von der Weid, P. Oberson, and N. Gisin, "High resolution fiber distributed measurements with coherent OFDR," in Proc. ECOC'00, 2000, paper 11.3.4, p. 109.
[5] 5 R. E. Sorace, V. S. Reinhardt, and S. A. Vaughn, "High-speed digital-to-RF converter," U.S. Patent 5 668 842, Sept. 16, 1997.
[6] 6 (2002) The IEEE website. [Online]. Available: http://www.ieee.org/
[7] 7 M. Shell. (2002) IEEEtran homepage on CTAN. [Online]. Available: http://www.ctan.org/tex-archive/macros/latex/contrib/supported/IEEEtran/
[8] 8 FLEXChip Signal Processor (MC68175/D), Motorola, 1996.
[9] 9 "PDCA12-70 data sheet," Opto Speed SA, Mezzovico, Switzerland.
[10] 10 A. Karnik, "Performance of TCP congestion control with rate feedback: TCP/ABR and rate adaptive TCP/IP," M. Eng. thesis, Indian Institute of Science, Bangalore, India, Jan. 1999.
[11] 11 J. Padhye, V. Firoiu, and D. Towsley, "A stochastic model of TCP Reno congestion avoidance and control," Univ. of Massachusetts, Amherst, MA, CMPSCI Tech. Rep. 99-02, 1999.
[12] 12 Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification, IEEE Std. 802.11, 1997.