ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol4, Issue 6, June 2017

6*6 Radom Color Grid Authentication (2 Step)

[1] Sudershan M, [2] Veena Potdar, [3] Madhu B
[1] Dept. of CSE Dr. AIT Bangalore, India
[2][3] Assoc. Prof, Dept. of CSE, Dr. AIT, Bangalore, India

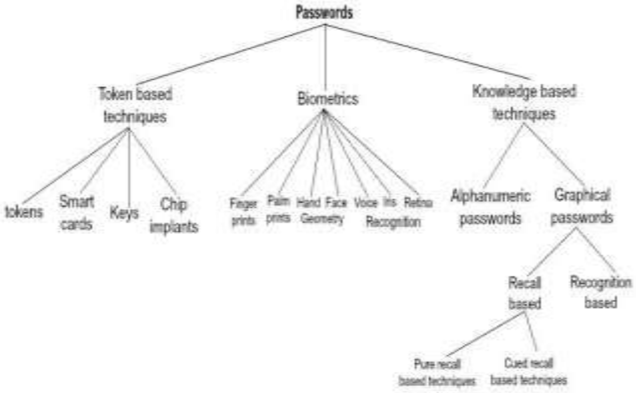
Abstract— **Security in the computer is largely supported by passwords for authentication process. Use of alphanumeric passwords is the most common Authentication method. This conventional authentication method has been shown to have significant drawbacks. To overcome the vulnerabilities of traditional methods, numerous graphical password authentication systems have been proposed. These graphical passwords are usually seen as complex and time consuming. Furthermore, the existing graphical passwords are susceptible to spyware and shoulder surfing attacks. In this paper we propose this novel graphical password scheme to abolish well known security threats like brute force attacks, dictionary attacks, phishing attacks and spyware attacks.**

Keywords: **Recall based graphical passwords, computer security, authentication, attack patterns..**

I. INTRODUCTION

Authentication is a process by which system verifies the identity of a user. Authentication is the main step of any security system. Text passwords remain the most common method for several reasons. This method is susceptible to various predominant attacks like phishing, spyware attacks etc. To address the problem with conventional models alternative authentication models such as biometrics were used. A very high level of security can be achieved with the help of biometrics. But this authentication system involves a lot of expense. In the recent times there has been a great deal of hype for the graphical passwords. A graphical password is an authentication system that works by having the user select images shown in a GUI. That is why graphical passwords are also called as Graphical user authentication systems. Besides, graphical passwords offer better security than traditional text based passwords. It is difficult for the intruder to break graphical passwords using conventional attack methods like brute force attack, dictionary attack etc. The idea of graphical passwords was initially developed by Greg Blonder in the year 1996. Though Graphical passwords are much easier to remember, they provide high level of security. Graphical passwords are classified into two types i.e. recognition based graphical passwords and recall based graphical passwords. Recognition-based systems, also known as cognometric systems or search metric systems. Recall bases systems are further classified into 2 types i.e. a pure recall based graphical passwords and cued recall based graphical passwords.

In Recognition based schemes, user will be shown a set of images. In the authentication step user selects a couple of images which were chosen at the registration phase. In Recall based schemes, user is supposed to reproduce something which he/she created or selected during the registration phase. In Pure recall based schemes the user has to reproduce the password without any help from the system. Draw-A-Secret technique, grid selection and Passdoodle are some of the examples of this method. In recall based schemes the user will have some assistance from the system to reproduce their passwords. User has to click on some points at the registration phase to set them as his password and has to click on the same points during the authentication. Passpoints scheme, cued click points scheme are the examples of this method.

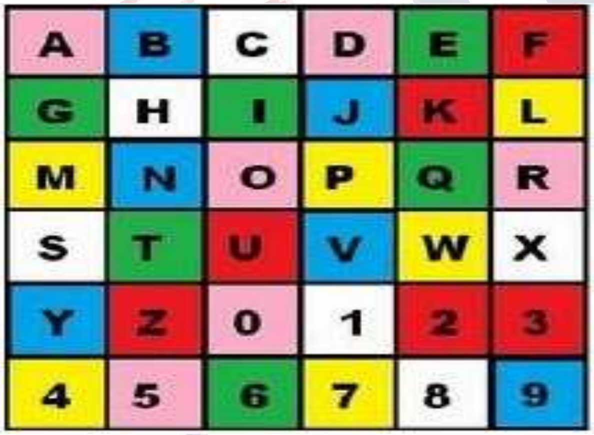


The existing graphical passwords are seen as complex and time consuming for the users. An Authentication system should force the user to select strong password while not affecting the memorability. We applied this approach to propose a novel two step authentication graphical password scheme.

II. PROPOSED SYSTEM

Considering the drawbacks of the existing graphical password systems, we have proposed a robust graphical password scheme, which is highly adaptable for traditional desktop systems, smart phones and other web applications. Our proposed system consists of 2 phases. The first phase is the user registration phase and the second phase is the authentication phase. Phase 1: In this phase (registration phase) user enters his desired username and an alphanumeric password. Then the user will be shown a 6*6 grid in which the user have to assume an imaginary pattern line across the randomly colored squares and enter the character in the squares through which his assumed pattern line passes. This is the security code.

The squares of 6*6 grids shown to the user contain 26 alphabets and 0-9 numerals. The squares of the grids are randomly colored using 6 different colors (Red, Blue, Green, Yellow, White and Pink). For each login attempt the colors squares of the grid are randomized, but the letters and numbers are places in an order for the convenience of the user. As the user enters the first letters of the colors there is no chance of phishing and shoulder surfing. Even if the intruder knows the color of the square through phishing or some spyware, he can't identify the exact password and security code since there will 6 same colored grids containing different characters. To increase the security levels the user is supposed to choose passwords which are at least 6 characters long.



A	B	C	D	E	F
G	H	I	J	K	L
M	N	O	P	Q	R
S	T	U	V	W	X
Y	Z	0	1	2	3
4	5	6	7	8	9

Resilience of Proposed System

1. Dictionary Attacks: Graphical passwords are less vulnerable to dictionary attacks. In our proposed system, as the user enters only the starting letters of the colors, it will be impractical to carry out dictionary attacks against this graphical password method.
2. Guessing Attacks: Guessing attack is another eminent strategy used by the intruders. Even if the attacker tries to guess the password, the security code used in our proposed system makes our system resilient against guessing attacks since user has a chance to select an imaginary pattern of his own choice. Even if the attacker tries on guessing the colors it would be of no use since the colors of the squares get changed for every login attempt. Hence the probability of guessing attacks is very low.
3. Spyware attacks: Excluding a few exception, key loggers and screen loggers cannot be used to attack against this method. By using a key logger if the attacker knows the colors of the squares in which the password characters lie, it would be of no use to him since there will be another 5 characters lying in the same color. The colors of the squares of the grid will be randomized for the next attempt he tries.
Hence our proposed system is resistant to spyware attacks.

4. Shoulder surfing: Unlike recognition based graphical passwords, recall based graphical passwords are more resistant to shoulder surfing. In the proposed system, even if the peeper observes the color of the square in which the password character lies, he cannot identify the exact password character since the user enters the first letter of the color of the square (not the actual character).Thus proposed system is resilient to shoulder surfing attacks.
5. Social Engineering: compared to ordinary alphanumeric passwords, it is inconvenient for a user to give his graphical password to another person. Hence graphical passwords are less susceptible to social engineering attacks.
6. Phishing Attacks: Phishing attacks are easily done in web applications. A phishing website can easily copy the login page from a legitimate site, including the area for entering the graphical password. In the proposed system when the users enters their username and the starting letters of the colors of the squares in the phishing site this entire information is sent to the attacker. Even if the attacker knows the colors of the grids he cannot identify the exact code since there will be 5 other characters residing in the same colored grid.

III. CONCLUSION

Access authentication is crucial for computer security. As the graphical passwords are attack resistant, there is a growing interest for them. Presently numerous authentication techniques and models are available. But, each of them have their own pros and cons. In this paper we have proposed a graphical password scheme that is more resilient to dictionary attacks, shoulder surfing, spyware and phishing attacks. This 2 step random colored grid graphical password authentication scheme shows promise as a usable and memorable authentication mechanism. Overall, the existing graphical password schemes are still immature. Much more research and user studies are needed for graphical password mechanisms to achieve higher level of maturity and usefulness.

IV. ACKNOWLEDGMENT

We are thankful to our colleagues and friends who provided expertise and suggestions that greatly assisted the research work.

REFERENCES

[1] G. Blonder. Graphical passwords. United States Patent 559961, 1996.

[2] K. Gilhooly, "Biometrics: Getting Back to Business," in Computerworld, May 09, 2005.

[3] A. Jain, L. Hong, and S. Pankanti, "Biometric identification," Communications of the ACM, vol. 33, pp. 168-176, 2000.

[4] Real User Corporation (2007) PassfacesTM, http//:www.realuser.com.

[5] Brostoff S. and Sasse M.A. In People and Computers XIV
– Usability or Else: Proceedings of HCI. Sunderland, U.K, 2000.

[6] Sobrado L. and Birget J. (2007) http://rutgersscholar.rutgers.edu/volume04/sobrbirg/sobrbirg.htm.

[7] S. Chiasson, P. van Oorschot, and R. Biddle, "Graphical password authentication using Cued Click Points," in European Symposium On Research In Computer Security (ESORICS), LNCS 4734, September 2007, pp. 359–374.

[8] A. Forget, S. Chiasson, and R. Biddle, "Shoulder-surfing resistance with eye-gaze entry in click-based graphical passwords." in ACM SIGCHI Conference on Human Factors in Computing Systems: Note (CHI), 2010.
[9] A. Adams and M. A. Sasse, "Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures," Communications of the ACM, vol. 42, pp. 41-46, 1999.

[10] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A.D. Rubin, "The Design and Analysis of Graphical Passwords," in Proceedings of the 8th USENIX Security Symposium, 1999.

[11] A. De Angeli, L. Coventry, G. Johnson, and K. Renaud, "Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems," International Journal of Human-Computer Studies, vol. 63, no. 1-2, pp.
128–152, 2005.

[12] K. Renaud, "Guidelines for designing graphical authentication mechanism interfaces," International Journal of Information and Computer Security, vol. 3, no. 1, pp. 60–85, June 2009.

[13] K. Renaud, "Evaluating authentication mechanisms," in Security and Usability: Designing Secure Systems That People Can Use, L. Cranor and S. Garfinkel, Eds. O'Reilly Media,
2005, ch. 6, pp. 103–128.

[14] C. Herley, P. van Oorschot, and A. Patrick, "Passwords: If Were So Smart, Why Are We Still Using Them?" in Financial Cryptography and Data Security, LNCS 5628, Springer, 2009