ISSN: 2321-7782 (Online)
Volume 2, Issue 10, October 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Authentication Scheme for Shoulder surfing using Graphical and Pair Based scheme

Doke Ashvini Ankush[1]
B.E.Comp.
Department of Computer Engineering,
Jaihind College of Engineering, Kuran,
Pune, India

Wagh Dhanashree B[2]
B.E.Comp.
Department of Computer Engineering,
Jaihind College of Engineering, Kuran,
Pune, India

Shaikh Saddam Husain[3]
B.E.Comp.
Department of Computer Engineering,
Jaihind College of Engineering, Kuran,
Pune, India

Abstract: ***Today's all over Word Textual passwords are the most commonly used for authentication. But textual passwords are vulnerable to eves dropping, dictionary attacks, social engineering and shoulder surfing Graphical passwords are introduced as alternative techniques to textual passwords .In this paper we are use two different method for Authentication .Their Schemes are Graphical Authentication scheme and another is Pair Based AuthenticationScheme. These Schemes are avoid the dictionary attacks and shoulder surfing. The Graphical password authentication and pair based authentication scheme are more secure than textual password. In this paper, we will propose an improved text-based shoulder surfing resistant graphical password scheme by using colors. The operation of the proposed scheme is simple and easy to learn for users familiar with textual passwords.The user can easily and efficiently to login the system without using any physical keyboard or on-screen keyboard.***

Keywords:Authentication,Shoulder Surfing, Dictionaryattacks, GraphicalScheme, Pair Based scheme, session password.

I. INTRODUCTION

The Shoulder surfing attacks can be performing by password shown over a shoulder at the time of user entering password. Sobrado and Birget[1] proposed three shoulder surfing resistant graphical password schemes. Since then, many graphical password schemes with different degrees of resistance to shoulder surfing have been proposed, e.g., [2][3][4][5][6][7][8][9], and each has its pros and cons.The most common method used for authentication is textual password. The vulnerabilities of this method like eves dropping, dictionary attack, social engineering and shoulder surfing are well known. Random and lengthy passwords canmake the system secure. But the main problem is the difficulty of remembering those passwords. Studies have shown that users tend to pick short password or passwords that are easy to remember. Unfortunately, these passwords can be easily guessed or cracked. The alternative techniques are graphical passwords and Pair based. But these two techniques have their own disadvantages. Biometrics, such as finger prints, iris scan or facial recognition have been introduced but not yet widely adopted. The major drawback of this approach is that such systems can be expensive and the identification process can be slow. There are many graphical password schemes that are proposed in the last decade. But most of them suffer from shoulder surfing which is becoming quite a big problem. There are graphical password schemes that have been proposed which are resistant to shoulder-surfing but they have their own drawbacks like usability issues or taking more time for user to login or having tolerance levels. In this paper, we use two authentication schemes namely Pair-based authentication scheme and Graphical authentication scheme.

II. DEFINITION

A] Dictionary attack:

These are attacks directed towards textual passwords. Here in this attacker, hacker uses the set of dictionary words and authenticate by trying one word after one. The Dictionary attacks fails towards our authentication systems because session passwords are used for every login.

B] Shoulder Surfing:

Shoulder surfing is attack can be attacker showing password over a shoulder. This attack most commonly found in textual password.

III. PROPOSED SYSTEM

In this paper we will avoid shoulder surfing and dictionary attacks using two schemes.

1] Graphical Authentication scheme.

2] Pair based Authentication Scheme.

a) Even Method

b) Odd Method

1] Graphical Authentication scheme.

In this method we will make GUI circle and circle is dividing in 8 equal parts, each part is called as sector. Circle consist of 8 sector having 8 arc, each arc have different colour assign and user colour can be select at the time of registration.

Fig.1 Graphical Authentication Scheme

In this method we will describe a simple and efficient shoulder surfing resistant graphical password scheme based on texts and colours. The alphabet used in the propose scheme contains 64 characters, including 26 upper case letters, 26 lower case letters, 10 decimal digits, and symbols "." and "/". This method can be perform in 3 phases, the registration phase and the login Phase, verification phase which can be described as in the following.

A. Registration phase

The user has to set his textual password K of length L ($8 \leq L \leq 15$) characters, and choose one colour as his pass-colour from 8 colours assigned by the system. The remaining 7 colours not chosen by the user are his decoy-colours. And, the user has to register an e-mail address for re-enabling his disabled account. The registration phase should proceed in an environment free of shoulder surfing. In addition, a secure channel should be established between the system and the user during the registration

phase by using SSL/TLS [16][17] or any other secure transmission mechanism. 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.

B. Login phase

The user requests to login the system, and the system displays a circle composed of 8 equally sized sectors. The colours of the arcs of the 8 sectors are different, and each sector is identified by the colour of its arc, e.g., the red sector is the sector of red arc. Initially, 64 characters are placed averagely and randomly among these sectors. All the displayed characters can be simultaneously rotated into either the adjacent sector clockwise by clicking the "clockwise" button once or the adjacent sector counter clockwise by clicking the "counter clockwise" button once, and the rotation operations can also be performed by scrolling the mouse wheel. The login screen of the proposed scheme can be illustrated by an example shown in Fig. 1. 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 composed of 8 equally sized sectors, and places 64 characters among the 8 sectors averagely and randomly so that each sector contains 8 characters. The 64 characters are in three typefaces in that the 26 upper case letters are in bold typeface, the 26 lower case letters and the two symbols "." and "/" are in regular typeface, and the 10 decimal digits are in italic typeface. In addition, the button for rotating clockwise, the button for rotating counter 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 clockwise by clicking the "clockwise" button once or the adjacent sector counter clockwise by clicking the "counter clockwise" button once, and the rotation operations can also be performed by scrolling the mouse wheel. Let i = 1. The rotation operation can be illustrated by an example shown in Fig. 1.

Step 3:

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

Step 4:

If i < L, the system randomly permutes all the 64 displayed characters, and then GOTOs Step 3. Otherwise, the user has to click the "Login" button to complete the login process.

C. Verification phase

In this phase after successfully registration of new user then user can login phase to entering password and password is correct or not perform by verification scheme.

2] Pair Based Scheme:

At the time of registration user can submits password. Minimum length of the password is 8 and it can be called as secret pass. The secret pass should be containing either even or odd number of characters. Session passwords are generated based on this secret pass. During the login phase, when the user enters his username an interface consisting of a grid is displayed. The grid is of size 6 x 6 and it consists of alphabets and numbers. These are randomly placed on the grid and the interface changes every time. He first letter in the pair is used to select the row and the second letter is used to select the column. The intersection of that letter click on that letter is part of the session password. This is repeated for all pairs of secret pass. Below Figure shows the pair based scheme in that 6 X 6 grid. Suppose the user password is ANIL then in login time 6 X 6 grid

display on the screen select first row having A and select colour having N and where they intersect click on L. The password entered by the user is verified by the server to authenticate the user. If the password is correct, the user is allowed to enter into the system. The grid size can be increased to include special characters in the Password.

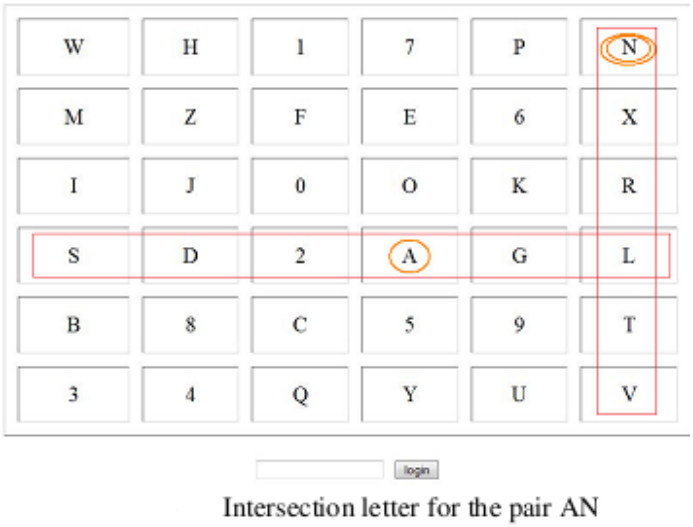

Fig 2.Pair Based Scheme

IV. ALGORITHM USED

1. *Bresenham's Algorithm:*

Bresenham's algorithm is used the Graphical scheme in this scheme circle dividing in 8 equal partsis called sector .Each sector 8 letter consist of random Combination of number, symbol, upper character, lower character. By using Bresenham's algorithm we will put the letter in appropriate line. This algorithm is used for graphical representation.

In The Algorithm, Consider a line with initial point (x1, y1) and terminal point (x2, y2) in device space. If _x = x2 −x1and _y = y2 − y1, we define the driving axis (DA) to be the x-axis if |_x| _ |_y|, and the y-axisif |_y| > |_x|. The DA is used as the "axis of control" for the algorithm and is the axis of maximum movement. Within the main loop of the algorithm, the coordinate corresponding to the DA is incremented by one unit. The coordinate corresponding to the other axis usually denoted the passive axis or PA) is onlyincremented as needed.

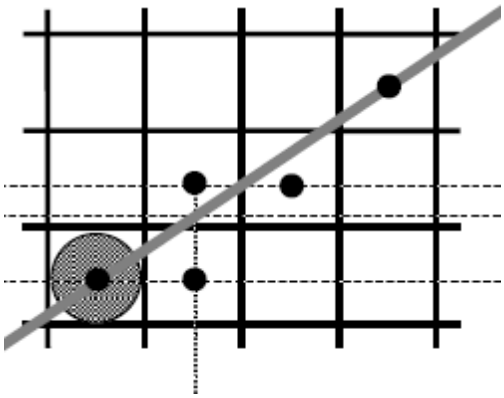

Fig. 3 Bresenhm's algorithm

2. *Random Algorithm*

The algorithm is usually simple and easy to implement, the algorithm is fast with very high probability, and it produces optimum output with very high probability. In this algorithm we put the randomly letter in the circle and 6 X 6 grid. Suppose in one bucket having different color bolls, close eyes and take randomly boll and put on the table, similarly random algorithm is

used. There is a finite probability of getting incorrect answer. However, the probability of getting a wrong answer can bemade arbitrarily small by the repeated employment of randomness. Analysis of running time or probability of getting a correct answer is usually difficult. Getting truly random numbers is impossible. One needs to depend on pseudo random numbers. So, the result highly depends on the quality of the random numbers. Employing randomness leads to improved simplicity and improved efficiency in solving the problem. It assumes the availability of a perfect source of independent and unbiased random bits. Access to truly unbiased and independent sequence of random Bits is expensive. So, it should be considered as an expensive resource like time and space. Thus, one should aim to minimize the use of randomness to the extent possible. Assumes efficient reliability of any rational bias. However, this assumption introduces error and increases the work and the required number of random bits. There are ways to reduce the randomness from several algorithms while maintaining the efficiency nearly the same.

V. ADVANTAGES

A. Easy to register:

In this system new user can easily register and use this system, new user can register such as fill information such as username, birthdate address, city, mobile number ,password, first name, last name etc. also more filed are fill at the time registration.

B. More secure:

Passwords should be easy to remember, and the user authentication protocol should be executable quickly, easily by humans and it should more secure than other methods.

C. Easy to use:

This system is very easy to use because new user can register and use this method.

D. Very difficult to hack

Very little research has been done to study the difficulty of cracking graphical passwords. Because graphical passwords are not widely used in practice, there is no report on real cases of breaking graphical passwords. Passwords should be secure, i.e., they should look random and should be hard to guess, they should be changed frequently the password, also we avoid many dictionary attack and this methods are difficult to hack.

VI. APPLICATION

1. Instead of pattern lock in Mobile, we can use this system as is more secure.
2. In Military purpose we can also use this method to secure confidential data.
3. Companies can store secret Business and all important data with maximum security.
4. To avoid shoulder surfing in ATM and to provide privacy to your personal account.

VII. CONCLUSION

We have concludedthat to avoiding shoulder surfing and dictionary attacks by using this two scheme. We have proposed a simple text-based shoulder surfing resistant graphical password, 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 familiar with textual passwords. The user can easily and efficiently to login the system without using any physical keyboard or on-screen keyboard. Finally, we have analyzed the resistances of the proposed scheme to shoulder surfing and accidental login.

References

1. Sobrado and J. C. Birget, "Graphical passwords," The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4, 2002.
2. L. Sobrado and J.C. Birget, "Shoulder-surfing resistant graphical passwords," Draft, 2005.(http://clam.rutgers.edu/~birget/grPssw/srgp.pdf).
3. "A Simple Text Based shoulder surfing Resistent Graphical Password scheme" IEEE 2nd International Symposium on Next-Generation Electronics (ISNE),2013.
4. H. Zhao and X. Li, "S3PAS: A Scalable Shoulder-Surfing Resistant Textual-Graphical PasswordAuthentication Scheme," in 21st International Conference on Advanced Information Networking andApplications Workshops (AINAW 07), vol. 2. Canada, 2007, pp. 467-472.
5. S. Man, D. Hong, and M. Mathews, "A shoulder surfing resistant graphical password scheme," inProceedings of International conference on security and management. Las Vegas, NV, 2003.
6. X. Suo, Y. Zhu and G. Owen, "Graphical Passwords: A Survey". In Proc. ACSAC'05.
7. H. Zhao and X. Li, "S3PAS: A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme," in 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW 07), vol. 2. Canada, 2007, pp. 467-472.
8. HaichangGao, ZhongjieRen, Xiuling Chang, Xiyang Liu UweAickelin, "A New Graphical Password Scheme Resistant to Shoulder-Surfing.

AUTHOR(S) PROFILE

Miss.Ashvini Doke currently pursuing her B.E degree in Computer Engineering from Jaihind College of Engineering, Kuran (Savitribai Phule University, Pune). Also received the Diploma in Computer Engineering from Government Polytechnic ,Awasari (MSBTE) in 2011

Miss. Wagh Dhanashree currently pursuing her B.E degree in Computer Engineering from Jaihind College of Engineering, Kuran (Savitribai Phule University). Also received the Diploma in Computer Technology from Jaihind Polytechnic, kuran (MSBTE) in 2011

Mr. Shaikh Saddam Husain currently pursuing his B.E degree in Computer Engineering from Jaihind College of Engineering, Kuran (Savitribai Phule University,Pune). Also received the Diploma in Computer Technology from Vamanrao Ithape Polytechnic,Sangamner (MSBTE) in 2011

