A Survey on Shoulder Surfing Resistant Text Based Graphical Password Schemes

Mokal P. H.[1], Devikar R. N.[2]

[1]M. Tech Scholar, Information Technology Department, AVCOE Sangamner, Pune University, India

[2]Assistant Professor, PhD Scholar, Information Technology Department, AVCOE Sangamner, Pune University, India

Abstract: ***For security authentication is important factor in any computer system. Authentication is the process of determining whether someone or something is in fact, who or what it is declared to be. In computer system authentication is done through use of password. The alphanumerical username and password is well known and commonly used authentication approach. As this approach is easiest one and provides security to some extent but it has some significant drawbacks such as if user selects short password which is easier to remember then it can be easily guessed or hacked by hackers and on the other side if user selects too long and difficult password then it is difficult for user to remember it for long time. To overcome the drawbacks of traditional authentication approach researcher have been developed new authentication approach as possible alternative to alphanumeric or text based approach. This new proposed approach uses images, pictures as a password known as graphical password approach. The researcher have been designed Graphical passwords in such a way that passwords are easier for people to use, to create and so that more usable and secure. As graphical password provides security to certain degree but it is vulnerable to shoulder surfing attack. When user enters their password in public place then it can be capture by attacker by direct observation or by recording the user's authentication session. This attach is known as Shoulder surfing attack. In this paper we will conduct comprehensive survey of existing shoulder surfing attacks in text based graphical password approach by studying five papers on shoulder surfing resistant graphical passwords and explains the problems and their possible solutions.***

Keywords: Authentication approaches, Text based password, Graphical password, Shoulder surfing resistant, Key logger

1. Introduction

Authentication is the important factor in information and computer security. Authentication is supported by passwords so that it is significant part of authentication process. In the current state, there are various authentication schemes have been developed by the researchers. The traditional and most commonly used authentication scheme is Text based authentication scheme which is also known as alphanumeric authentication scheme. In alphanumeric authentication scheme, user has to submit username and text password. This may result in vulnerabilities such as password is difficult to remember in case of long and difficult password otherwise passwords are easily guessed or hacked by attacker in case of short and easy password. Textual password is vulnerable to guessing, dictionary attack, key-loggers, and social engineering, shoulder surfing, hidden-camera and spyware attacks.

According to an article presented in Computerworld in May 2005, the security team at any large company tested and ran a network password cracker and surprisingly within 30 seconds and also they manage to crack approximately 80% of the passwords. To overcome the drawbacks of alphanumeric password, techniques graphical password have been developed by the researchers. There are two well known and commonly used graphical password techniques viz. recognition based and recall based. In recognition based technique, the user has to select the certain series of images from the images shown by the program and then the user has to identify and recognize that images in order which are selected before. In recognition based technique, decision is binary i.e. either the user recognizes image or not. In recall-based technique, it is required that the user has to repeat or reproduce a secret that the user created before. Both the techniques have memory advantage over text based approach. The prime advantage of graphical passwords over text based passwords is the improved memorability. Graphical password has large password space as compared to alphanumeric password. For example, for text based passwords of length 8 over a 64 character alphabet, so that the number of possible passwords is 64^8=2.8x1014. In graphical passwords, if the image is 1024x752, with the click point of 20x20 pixels, and with passwords consisting of 5 clicks, the password space will have size 2.6x1016. As graphical passwords depends upon pointing devices for their input and as graphical password scheme has no pre existing searchable dictionaries, dictionary attacks are insurmountable.

In graphical password, registration and login process takes longer time than alphanumeric password scheme. A number of shoulder surfing-resistant graphical password schemes have been proposed, but they offer little security against of shoulder surfing attack. A successful graphical password scheme must prevent successful shoulder-surfing attacks and it must also be easy to learn and use. As graphical password authentication also has some drawbacks therefore researchers developed some hybrid schemes based on graphic and text was developed. The main objective of this scheme is to achieve higher security with compromising user-friendliness and procure a considerable improvement in terms of system security.

2. Methodology Used

In this section, we illustrate five articles in which are shoulder surfing text based graphical schemes are proposed.

We also illustrating the problems, methods used outcomes and finally future plan if any.

2.1 Problem 1

In computer system and information system, alphanumeric password is frequently used authentication approach. This method takes username and textual passwords as input. This approach secure to some degree but it has some drawbacks such as if user selects short password then it is easy to guess for attacker and if user selects too long hard password then it is difficult to remember[1].

2.1.1 Methodology Used

Due to these drawbacks, researchers have been developed new password scheme which uses images, pictures as a password known as graphical password scheme. This scheme is used as alternative to alphanumeric password. In this paper, an extensive survey of existing graphical password techniques up to 2005 is carried out. In this paper, in the beginning they explained the traditional text based authentication scheme and their limitations, and then they explained graphical password scheme and their attacks. They introduced the current authentication methods and categorized into three main areas: Token based authentication, Biometric based authentication, Knowledge based authentication. In addition to this, they presented a comparison of current graphical password techniques. Then they classified graphical password schemes into two categories viz. recognition-based and recall based approaches. They explained briefly each scheme with example and show their advantages and limitations. They finally presented the future scope in research direction. They also explain in brief some of the feasible techniques for breaking graphical passwords and compared it with text-based passwords as the answer for question: “Is a graphical password as secure as text based password?”They also strive to find the answer to the question: “What are the major design and implementation issues for graphical passwords?” This study is useful for the researchers who is interested in graphical password methods and wants to find the alternatives to overcome the susceptibility of it [1].

2.1.2 Outcomes / Findings

They drew preliminary analysis that it is harder to break graphical passwords using the traditional attack methods such as brute force search, dictionary attack, or spyware. Overall, the current graphical password techniques are still immature. Much more research and user studies are needed for graphical password techniques to achieve higher levels of maturity and usefulness [1].

2.2 Problem 2

Traditional passwords include password hacking as selected password is short and forgetting passwords as selected password is difficult and choice of weak passwords. Researchers have been proposed advanced password-based authentication systems depends on graphical passwords which have better memorability and improved password space. Graphical password-based authentication schemes are generally vulnerable to shoulder-surfing attack [2].

2.2.1 Methodology Used

In this paper, researcher has proposed two authentication schemes using graphical passwords viz. Pair Pass Char (PPC) and Tricolor Pair Pass Char (TPPC). These both the schemes support two modes of input: keyboard entry and mouse clicks. In this method, the first mode used is the text mode and the next mode as the graphical mode. The input image composed of a 10x10 grid of cells each of which represents the basic character set. The basic character set consist of characters A-Z, a-z, 0-9 and other printable characters which are padded with spaces in a single color and randomly spaced on the grid. In PairPassChar (PPC) scheme only basic character set is used. In PairPassChar (PPC) each character randomly spaced in a 10x10 grid. In PairPassChar (PPC) rules have been proposed which manage the allowable input corresponding to each pass-character pair. In the PPC scheme, the pass- characters are examined one pair at a time, starting with the first pass-character and shifting to the right until the last pass-character in the password becomes the first pass- character in a pass-character pair. Each pass-character pair is then first converted into the mapped character pair and the rules of the PPC schemes are applied.

In Tricolor Pair Pass Char (TPPC) scheme the tricolor version of the same character set is used. In Tricolor Pair Pass Char (TPPC) each character appears in three colors: red, green and blue randomly spaced in a 17x17 grid. The special case rules are proposed for TPPC scheme. In Tricolor Pair Pass Char (TPPC) scheme same as the PPC scheme the pass-characters are examined one pair at a time, starting with the first pass-character and shifting to the right until the last pass-character in the password becomes the first pass- character in a pass-character pair. Each pass-character pair is then first converted into the mapped character pair and the rules of the PPC schemes are applied and then the special case rules of TPPC are applied to which results in the rectangle [2].

2.2.2 Outcomes / Findings

As an experiment is carried out it was found that the average login times increase as the password length increases in both schemes. Supplementary, the login times for the TPPC scheme are higher than the PPC scheme for the same password length. Also in the study found that the rules for the TPPC scheme to be difficult to apply than the PPC scheme.PPC scheme provides the password as much as that offered by conventional password systems and it is greatly enhanced in the TPPC scheme because of the use of the same 96-character set in three colors[2].

2.3 Problem 3

The graphical password has been proposed as an alternative to alphanumeric password scheme as it is vulnerable to shoulder-surfing, hidden camera and spyware attacks. The graphical password scheme achieves memorability and security to certain extent but it is captured by direct observation or by recording login session called shoulder surfing attack. Thus graphical password scheme is also is vulnerable to shoulder-surfing attack [3].

2.3.1 Methodology Used

S3PAS is designed to be used in client/server environments as most password authentication system. In S3PAS scheme two kinds of passwords are generated viz. original password and session password. The original password is created when

creating their account. User inputs different session passwords in every login process. So that they can protect their original password from releasing. To login, the user must find all his/her original passcharacters in the login image and then make some clicks inside the invisible triangles which are called "pass-triangles" created by 3 original pass-characters following a certain click-rule. Otherwise, the user can input/type a textual character chosen from inside or on the border of the passtriangle area instead of clicking by mouse. Such character is known as "session pass-character". For that reason, the final inputs could be either several session pass-clicks or several session pass-characters. These session pass-clicks or session pass-characters is a user's "session passwords". In this scheme, click rule is also defined. This scheme introduced "change image" technique to defend against the brute-force search. In this "change image" technique, if a user fails in clicking the correct areas, or a user inputs wrong session password for I times, the client automatically changes the session login image [3].

2.3.2 Outcomes / Findings

There are still some minor drawbacks in this system similar to other graphical password schemes. The major issues in S3PAS schemes include slightly more complicated and longer login processes. The detailed click-rule for three set scheme will be presented in future publications .The future plan is to design a simplified version of S3PAS with a little lower security level to ease its adoption[3].

2.4 Problem 4

As the graphical password scheme have been proposed to overcome drawbacks of traditional password schemes but it was found that users are more familiar with textual passwords rather than pure graphical passwords so that text based graphical password scheme has been proposed[4].

2.4.1 Methodology Used

This proposed scheme is based on texts and colors. In this scheme the alphabets are used which consist of 64 characters including 26 upper case letters, 26 lower case letters, 10 decimal digits, and symbols "." and "/".There are two phases are presented viz. authentication phase and registration phase. In this scheme user has to select set his textual password K of length L ($8 \leq L \leq 15$) characters and also pick one color as his passcolor from 8 colors assigned by the system. The colors not pick by the user are his decoycolors. The user has to register his/her valid email address to re-enable his/her disabled account. The textual password is stored in the user's entry in the password table after encrypted by system key. After registration phase there is login phase in which user request to login system and system displays circle. This displayed circle is composed of eight equally sized sectors. Each sector having different color and each sector is identified by its color. At the beginning 64 characters are positioned randomly in the sectors and then displayed characters are rotated either clockwise or anticlockwise by clicking on the button "clockwise" or "anticlockwise", otherwise just by scrolling the mouse wheel. After completing the login process if login is not successful for three successive times then account will be disabled and system will send the secret re-enable link to registered email address to the valid user. In this way user can re-enable his/her account by using this secret link and attacker can't access it [4].

2.4.2 Outcomes / Findings

The operation of the proposed scheme is simple and easy to learn for users. Without using any physical keyboard or on-screen keyboard, the user can easily and efficiently to login the system. Finally, we have analyzed usability and the resistances of the proposed scheme to shoulder surfing and accidental login [4].

2.5 Problem 5

In addition to textual password, graphical password is another memorable authentication method for authorization. Graphical password is memorable, but it is inherently vulnerable to shoulder surfing attack [5].

2.5.1 Methodology Used

In this paper Painting Album Mechanism is proposed. This mechanism having characteristics of both recognition and recall graphical techniques. The Painting Album Mechanism involves two phases viz. registration phase and authentication phase. The registration phase involves three steps. In first step the user has to choose one picture as theme picture. Then using Swipe Scheme, Color Scheme, or Scot Scheme each user has to register their new password. Finally user has to click on the 'register' button to complete registration process. The lengths of Password should be greater than eight), otherwise password is not accepted. The authentication phase involves two steps. In the first step, user has to select pictures, colored boxes, or both of these two things, which user have selected in registration phase. Finally clicks on "log-in" button to complete authentication phase. It is important that selected pictures colored boxes are in same sequence as in the registration phase [5].

2.5.2 Outcomes / Findings

In this scheme respondents are able to recall theirs passwords under acceptable duration of time, and they were fast in learning this mechanism [5].

3. Conclusion

In this paper we studied on near about ten graphical password schemes and then selected five schemes which are resistant to shoulder surfing attack. For each paper we studied the problems, their methodology used to overcome problem, their analysis and finally future plan. We explained each methodology based on security and usability parameters. As there are various proposed schemes to shoulder surfing problem but still it is needed to improve these schemes in order to achieve more secure graphical password schemes. This survey will be useful for researchers who are interested in developing secure graphical password schemes.

References

[1] Xiaoyuan Suo, Ying Zhu G. Scott. Owen, "Graphical passwords: a survey", 21st Annual Computer Security Applications Conference, 2005.
[2] M. K. Rao and S. Yalamanchili, "Novel shoulder-surfing resistant authentication schemes using text-graphical passwords,", *International Journal of Information & Network Security,* vol. 1, no. 3, pp. 163-170, Aug. 2012.
[3] Huanyu Zhao and Xiaolin Li, 'S3PAS: A Scalable Shoulder- Surfing Resistant Textual-Graphical Password Authentication Scheme', 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW) ,2007.
[4] Yi-Lun Chen, Wei-Chi Ku, Yu-Chang Yeh, "A Simple Text-Based Shoulder Surfing Resistant Graphical Password Scheme," IEEE 2nd International Symposium on Next-Generation Electronics (ISNE), February 2013.
[5] Lim Kah Seng, Norafida Ithnin and Hazinah Kutty Mammi, "An Anti-Shoulder Surfing Mechanism and its Memorability Test", International Journal of Security and Its Applications Vol. 6, No. 4, October, 2012.

Author Profile

Miss. Mokal Pranita H. received the B.E. in Information technology Department from AVCOE Sangamner and perusing M.E. from AVCOE Sangamner.

Prof. Devikar R.N. received M. Tech in Computer department, Pursuing PhD and working as Assistant Professor in AVCOE Sangamner.