International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

A Review of the Graphical Password Based Authentication Schemes

Shraddha S. Banne[1], Prof. Kishor N. Shedge[2]

[1]Student, Master of Engineering, Dept .of Computer Engineering, Sir Visvesvaraya Institute of Technology, Chincholi, Sinner

[2]Assistant Professor, Dept .of Computer Engineering, Sir Visvesvaraya Institute of Technology, Chincholi, Sinner

Abstract*: Using the graphical password for providing the security is the heart of the modern security system. It has gained a lot of popularity in the last decade. In this paper, we present a comprehensive survey of all the modern graphical password providing mechanisms. We have also provided a classification of the existing password protection schemes. This survey also discusses the merits and the demerits of the existing password protection techniques.*

Keywords: Graphical Password, Security primitives

1. Introduction

In recent years, Network security is the most describing problem. Information stored in the database are much more precious for the user. To remember the password:

1) Should be easy to remember
2) Should be quickly and easily executable
3) Should be changeable

User may forget the password if it is too long and complicated. The text based password can be stolen by any powerful software. Phishing is another serious threat to text based password. Phishing is the action of getting secured information such as username, password and other further details by masquerading. Graphical password may be solution to the text based password vulnerabilities. One of the most constrain reasons for exploring the use of a graphical password scheme that humans ability for recalling pictures, whether they are line drawings or real objects. [1]

User authentication is a major problem in every system providing secure access to confidential information and personalized services. Although, today there exists numerous ways to authenticate a person [1, 2], the most popular method amongst them is with passwords. In this knowledge based authentication scheme, user authenticates herself by presenting the knowledge of a secret string of alphanumeric characters. The secret string is called as password and it is assumed to be known only to the claimed identity and hence her identity gets verified. However, in practice, anyone who knows or guesses the password is also able to authenticate as the legitimate user. Passwords represent simple, cost effective and user friendly authentication solution since its usage requires no special hardware or training and passwords can be easily distributed, maintained and updated via telephone, fax or email. However, passwords are effective only if following two conflicting requirements are satisfied simultaneously [3].

2. Literature Survey

As we know graphical images are more easily recalled then text. In this selection so graphical password system based on recognition and recall based are discussed.

1) ***Recognition-Based Technique***: In this type of technique, users will select pictures, logos or any symbols from prestored image. For authentication process user need to recognize the image, which he choose as a password.
2) ***Recall-Based Technique***: Again recall-based password authentication are categorize in two parts [2] : i) Pure Recall Based Technique ii) Cued Recall Based Technique

Recognition based technique require the user to identify and recognize the secret, or part of it, that the user selected before. Generally during password creation the users are required to memorize a series of images, and then must recognize their images from among decoys to log in. Phishing attacks are somewhat more difficult with recognition-based systems as a correct set of images must be presented to the user before password entry. Shoulder-surfing seems to be of particular concern in recognition-based systems when an attacker is standing behind the user and sees or observes the images selected by users during login.[3][4] Various recognition based password schema are explained below:

a) ***Passfaces***: The recognition-based system studied most extensively to date is Passfaces . Generally during setting a password the user selects a set of human faces. A panel of candidate faces is presented during his/her login. Among the given set of decoys the user must select the faces he/she selected during setting the password. Passfaces simply works by having the user select a subgroup of x faces from a group of k faces. For authentication, the system shows p faces and one of the faces belongs to the subgroup q. The user has to do the selection many times to complete the authentication process. [5]
b) ***Story***: The Story scheme, which requires the selection of pictures of objects (people, cars, foods, airplanes, sight-seeing, etc.) to form a story line. Story was proposed by

Davis, Monrose and Reiter [2004] as a comparison system for passfaces. Users create a story by selecting a series of pictures. To log in, users are presented with one panel of images and they must identify their story images from among set of fake images. Images used for the story scheme can be everyday objects, places, or people. Story introduced a sequential component: users must select images in the correct order. To aid remembrance, users were instructed to mentally construct a story to connect the images in their set.[3][4]

Another recognition-based graphical password system is Déjà Vu proposed by Dhamija and Perrig, which authenticates the users by choosing pictures among the set of fake pictures. These pictures are presented in a random manner. Each picture is derived from an initial seed and no need to store the pictures pixel by pixel so only the seeds need to be stored in the server. Therefore, an authentication server does not need to store the whole picture; it simply needs to store the initial seed. [4][5]

DAS, introduced by Jemyn is recall based graphical password schema and, is simply a grid in which the user draws their password using a stylus or a mouse. The user's drawings, which consist of one continuous or preferably many pen strokes using a stylus or a mouse are considered to be the user's password. The password space depends on the size and the complexity of the grid. Larger grid sizes increases the password space which becomes difficult for the attacker to crack the password. However, there are limitations in grid complexity due to human error. To recall where the middle points were becomes very hard to guess for the user if we have verylarge grid sizes. [1][6]

Cued-recall based password history is mostly dominated by passpoints. In passpoints the user needs to click on the five different positions or areas of the same image. Hence it is clicked based graphical password. The click is mouse based and user must remember the correct sequence or series of click points on that predetermined image for the next successful login[2][9]. It is a click-based scheme where users select one click-point on each of 5 images in sequence, one at a time; this provides one-to-one cueing. During the next login the user must remember that particular click point on the given image to unlock the next correct image, if the click is wrong the next opened image will be a fake one and not from the chosen series of images. This will stop current user authentication [7].

The design intent of the randomized viewport positions is to flatten the distribution of click-points across multiple users, to reduce the effects of hotspots[8].Two authentication techniques are based on text and colors proposed for PDA in this they generate the session passwords and resistant to dictionary attack[2].Drawback of this paper is that every time they generate the session password and it is difficult to remember new password to the user. Two new authentication schemes authenticate the user by session passwords which are used only once. Once the session is terminated, the session password is no longer useful. For every login process, users input different passwords. The session passwords provide better security against dictionary and brute force attacks as password changes for every session. But in this same problem is occur that every time user has to enter password again and again. It is too hard to remember password and as it is the session password it is for the particular time only[1]. To remove the drawback of textual password removed by graphical password schemes which provide a way of making more user friendly passwords, while increasing the level of security, they are vulnerable to shoulder surfing .Here text was combine with image and color to generate the session password and every time user wants to enter new password as session ends . Two authentication techniques (pair-based authentication scheme and hybrid textual authentication scheme) for engendering the session passwords. Same problem is here too as previously comes. Drawbacks associated with the textual passwords such as brute-force and dictionary attacks and same this problem held with graphical passwords which includes shoulder-surfing and are very expensive to implement. Two authentication techniques (pair-based authentication scheme and hybrid textual authentication scheme) for engendering the session passwords [3].

3. Objective and Scope

This research aims to study the existing graphical password schemes and to design and develop an improved graphical password scheme, to empirically test its security & usability, and to compare it with existing alphanumeric and graphical password schemes. The extent of previously discussed problems and their effect on individuals and organizations give raise to a number of research questions:

- What is the security and usability performance of graphical password schemes in actual use? How can the performance of graphical password schemes be measured?
- Are graphical password schemes as secure as alphanumeric passwords? What are the causes of good or bad performance of alphanumeric and graphical password schemes?
- What are the major design and implementation issues for graphical password schemes? And ultimately, what interventions can be made to improve the security and usability performance of graphical password schemes?

This research provides secure, usable and cost effective user authentication mechanisms to help mainly the computer users those are working on untrustworthy computers, Internet, and unsafe networks.

4. Conclusion

In this paper, a survey over existing graphical password protection techniques has been presented. A review over the merits and demerits of the password protection techniques is also presented. This survey will help us in developing more secure & efficient graphical password based authentication schemes to provide the better security to the user data.

References

[1] Fawaz A. Alsulaiman and Abdulmotaleb El Saddik, *Three-Dimensional Password for More Secure Authentication*, School of Information Technology and Engineering, University of Ottawa, *VOL. 57, NO. 9, SEPTEMBER 2008*

[2] Chippy. T and R. Nagendran, *Defences Against Large Scale Online Password Guessing Attacks By Using Persuasive Click Points*, International Journal of Communications and Engineering, *Volume 03– No.3, Issue: 01 March2012*

[3] Sonia Chiasson, Alain Forget, Elizabeth Stobert, P.C. van Oorschot, Robert Biddle, *Multiple Password Interference in Text Passwords and Click-Based Graphical Passwords*, School of Computer Science, Department of Psychology Carleton University, Ottawa, Canada, ACM CCS'09, *November 9–13, 2009*

[4] Robert Biddle, Sonia Chiasson, and P.C. van Oorschot, *Graphical Passwords: Learning from the First Twelve Years*, Carleton University, Ottawa, Canada, ACM, *September 27, 2010*

[5] Amirali Salehi-Abari, Julie Thorpe, and P.C. van Oorschot, *On Purely Automated Attacks and Click-Based Graphical Passwords*, Annual Computer Security Applications Conference, IEEE, *Version: Sept.15, 2008*

[6] Sonia Chiasson, Robert Biddle, P.C. van Oorschot, A Second Look at the Usability of Click-Based Graphical Passwords, Symposium On Usable Privacy and Security (SOUPS) *2007, July 18- 20, 2007, Pittsburgh, PA, USA. Volume 2, Issue 9, September 2013*

[7] Elizabeth Stobert, Alain Forget, Sonia Chiasson, Paul van Oorschot, Robert Biddle, *Exploring Usability Effects of Increasing Security in Click-based Graphical Passwords*, ACSAC '10 Austin, Texas USA *Copyright 2010 Dec. 6-10, 2010, ACM 978-1-4503-0133-6/10/12*

[8] Sonia Chiasson, Elizabeth Stobert, Alain Forget, Robert Biddle, and Paul C. van Oorschot, *Persuasive Cued ClickPoints: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism*, IEEE, VOL. 9, NO. 2, MARCH/APRIL 2012

[9] Susan Wiedenbecka, Jim Watersa, Jean-Camille Birgetb, Alex Brodskiyc, Nasir Memonc, *PassPoints: Design and longitudinal evaluation of a graphical password system*, International Journal of Human-Computer Studies 63 (2005) 102–127

[10] Aman Darren Davis Fabian Monrose Michael K. Reiter, *On User Choice in Graphical Password Schemes*, Usenix, The Advanced Computing Systems Association, *Volume 13 pages 11-11 27 July 2004*

Author Profile

Shraddha S. Banne received the B.E. degree in Computer Science & Engineering from D.K.T.E Textile & Engineering Institute in 2012.