ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2014

Adding Persuasive Features in Graphical Password to Increase the Capacity of Knowledge Based Authentication Mechanism

Divyashree v[1], Gaurav Dutt Sharma[2], NancyA[3], A.Rosline Mary[4]

U.G. Student, Department of Computer Science & Engineering, Vemana Institute of Technology, Bangalore, India[1]

U.G. Student, Department of Computer Science & Engineering, Vemana Institute of Technology, Bangalore, India[2]

U.G. Student, Department of Computer Science & Engineering, Vemana Institute of Technology, Bangalore, India[3]

Asst Professor, Department of Computer Science & Engineering, Vemana Institute of Technology, Bangalore, India[4]

ABSTRACT: The existing authentication system has certain drawbacks for that reason graphical passwords are most preferable authentication system where users click on images to authenticate themselves. An important usability goal of an authentication system is to support users for selecting the better password. User creates memorable password which is easy to guess by an attacker and strong system assigned passwords are difficult to memorize. So researchers of modern days gone through different alternative methods and conclude that graphical passwords are most preferable authentication system. The proposed system combines the existing cued click point technique with the persuasive feature to influence user choice, encouraging user to select more random click point which is difficult to guess.

KEYWORDS:Authentication, graphical passwords, images

I. INTRODUCTION

Authentication is the process of positively verifying the identity of a user, device, or other entity in a computer system, often as a prerequisite for allowing access to resources in the system [2]. There are three types of authentications:

1) Knowledge-Based are characterized by secrecy or obscurity. This type includes the memorized password. It can also include information that is not so much secret as it is “obscure,” which can be loosely defined as “secret from most people”. Mother’s maiden name and user’s favourite colour are examples of this category. A security drawback of secrets is that, each time it is shared for authentication, it becomes less secret.**2) Object-Based** are characterized by physical possession. Physical keys which are called metal keys to distinguish them from cryptographic keys are tokens that have stood the test of time. A security drawback of a metal house key is that, if lost, it enables its finder to enter the house. This is why many digital tokens combine another factor, an associated password to protect almost all stolen token.**3) ID-Based** are characterized by uniqueness to one person. A driver's license, passport, credit card, university diploma, etc., all belong in this category. So does a biometric, such as a fingerprint, eye scan, voiceprint, or signature. For both ID documents and biometrics, the dominant security defence is that they are difficult to copy or forge. However, if a biometric is compromised or a document is lost, they are not as easily replaceable as passwords or tokens.

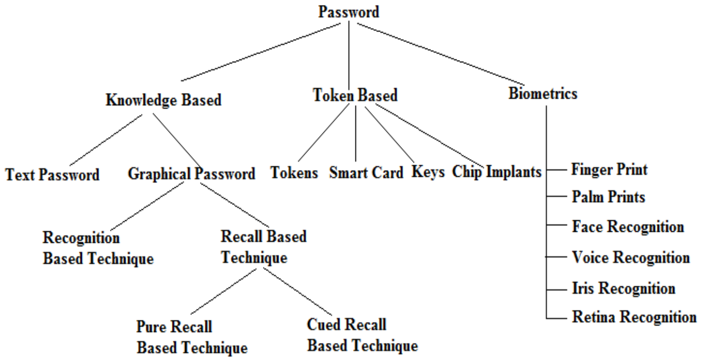

Figure 1. Categorization of Password Authentication Techniques

The above Figure 1.shows the representation of current authentication methods. The problem with text based password is that user creates memorable password which can be broken easily and also the text password has limited length which means that password space is small. Biometric based authentication techniques are somewhat expensive, slow and unreliable and thus not preferred by many.

The objective of this paper is to support users to selecting the better password.The goal of an authentication system is to support users in selecting the superior password. The problem of Knowledge based authentication mechanism (KBAM) typically text based password are well known. An alternative to alphanumeric password is the graphical password. Graphical password uses images or representation of an image as password. Human brains easily recognize pictures than the text. Most of the time, user create memorable password which is easy to guess but strong system assigned password are difficult to remember.

An authentication system should allow user choice while influencing user towards stronger passwords. An important usability goal of Knowledge based authentication system is to support users in selecting password of higher security with larger password space. Basically persuasion is used to control user choice in click based graphical password, encouraging user to select more random click point which is difficult to guess.

Token based authentication system has high security and usability and accessibility then the others. Also the system uses the knowledge based techniques to enhance the security of token based system. But the problem with token based system is that if token gets lost, the security also gets lost.

Therefore the Knowledge based authentication techniques are most preferable technique to improve the real high security. Graphical Password is one of the knowledge based technique and it is categorized into Recognition based and Recall based. In Recognition based technique user has to recognize or reproduce the things during the login where as in case of recall based technique user has to recall the things during the login in such a way that whatever they selected during the password creation they have to recall it in the same manner.

II.LITERATURE SURVEY

G.E.Blonder [1] said that a graphical password arrangement displays a predetermined graphical image and requires a user to “touch” predetermined areas of the image in a predetermined sequence, as a means of entering a password. The password is Set by allowing the arrangement to display the predetermined areas, or “tap regions”, to a user, and requiring the user to position these tap regions in a location and sequence within the graphical image, with which the user desires the Password to be set at. These “tap regions” are then removed from the display, leaving the

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2014

original image by itself. The arrangement then waits for an entry device (user) to select the "tap regions", as described above, for possible access to a protected resource.

The method correspondingly comprises the steps of displaying a predetermined image, selecting locations in the displayed image under user control, determining whether the selected locations correspond to a predetermined number of predetermined positions in the predetermined image that are stored as a password, and denying the user access to the resource in response to a determination that correspondence is lacking between the selected locations and the predetermined positions.

L. O'Gorman [2]said thatthe password has been the standard means for user authentication on computers for decades. However, as users are required to remember more, longer, and changing passwords, it is evident that a more convenient and secure solution to user authentication is necessary. This model examines passwords, security tokens, and biometrics which are collectively referred as authenticators and compares these authenticators and their combinations.

S. Wiedenbeck, et al [3], Graphical passwords are an alternative to alphanumeric passwords in which users click on images to authenticate themselves rather than type alphanumeric strings. Expansion of human factors testing by studying the effect of tolerance, or margin of error, in clicking on the password point and the effect of the image used in the password system is have been studied in this model. In this tolerance study, results show that accurate memory for the password is strongly reduced when using a small tolerance (10 x 10 pixels) around the user's password points. This may occur because users fail to encode the password points in memory in the precise manner that is necessary to remember the password over a lapse of time. In the image study user performance on four everyday images was compared. The results indicate that there were few significant differences in performance of the images. This preliminary result suggests that many images may support memorability in graphical password systems.

III. CUED CLICK POINT

The proposed system is based on click based graphical password system that not only guides and helps the user for password selection but also encourages the user to select more random distributed password [4]. The proposed system is based on Persuasive Technology which motivates and influence people to behave in a desired manner. The proposed system combines the Persuasive features with the cued click point to make authentication system more secure. The below Figure 2shows the architecture of cued click-point technique.

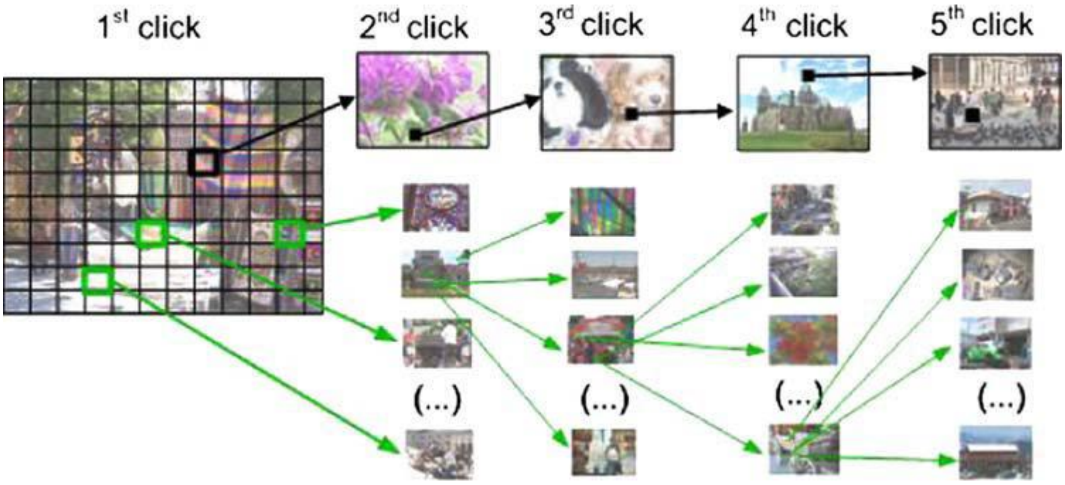

Figure 2. Cued click Point

In the proposed system, the task of selecting weak password which is easy for an attacker to guess is more tedious, discourages users from making such choices. In consequence, the more secure password is chosen which the path of least confrontation is. Instead of increasing the burden on users, it's easier to track the system suggestions for a secure password which is the feature lacking in most of the schemes. Here persuasive feature is combined with cued click point technique which uses one click point on five different images. The next image to be displayed is based on previous click-point and on the user specific random value. Here the password entry becomes a true cued recall scenario wherein each image triggers the memory of corresponding click-point. For valid users it provides implicit feedback such that while logging, if user is unable to recognize the image then it automatically alerts the user that their previous click-point is incorrect and user can restart the password entry whereas explicit indication is provided after the final click point.

During password creation the part of an image which is less guessable is highlighted and user has to select the click-point within the highlighted portion and if the user is unable to select the click-point, then the user can move towards the next highlighted portion by pressing the shuffle button. The highlighted part of an image basically guides users to select more random passwords that are less likely to include hotspots. Therefore this encourages users to select more random, and difficult passwords to guess. During Login, images are displayed normally and user has to select the click point as chosen at the time of password creation, but this time highlighted portion is not present as it only provides the system suggestion.

IV.SYSTEM ARCHITECTURE OF PERSUASIVE GRAPHICAL PASSWORD SYSTEM

The system architecture of the persuasive graphical password system shown in Figure 3. It is 3 tier architecture. User registers with the persuasive graphical password system by giving the relevant details and clicking on 5 different images with highlighted portion retrieved randomly from the database. Based on the click-points given by the user a hash code is generated and is stored in the database.

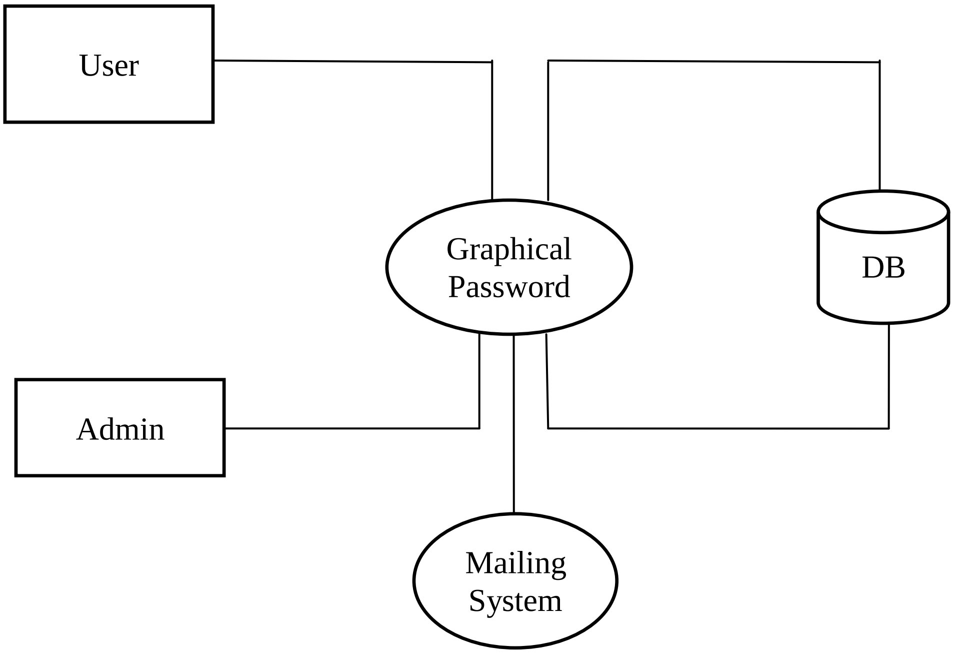

Figure 3. System Architecture of Persuasive Graphical Password System

During login, the user has to enter the user id and text password, if these input matches the value stored in the database, set of 5 images corresponding to that particular user is retrieved from the database and displayed to the user. The user has to repeat the same set of click-points (approximately) as done during registration. A new hash code for these click-points is generated and compared against the hash code already stored in the database while registration. If both the hash codes matches then only user can enter the home page and can utilize the benefits of secure intranet mail system.

The secure intranet mail system consists of inbox, sent item and composes mail options. Secure intranet mail provides users to communicate with each other within the same application.

Admin is the super user of the application who can view the details of the users present in the system, edit their details (one user at a time), delete the users, can also view his own profile, and change his password.

V. CONCLUSION

A major advantage of proposed scheme is that it provides larger password space then the alphanumeric passwords. For Graphical passwords there is a rising interest is that they are better than the Text based passwords, while the important argument for graphical passwords are that people are better at memorizing graphical passwords than text-based passwords. Also it removes the pattern formation and hotspot attack since it provides the system suggestion. Also the proposed system removes the shoulder surfing attack.

REFERENCES

[1] G. E. Blonder, "Graphical passwords," in Lucent Technologies, Inc., Murray Hill, NJ, U. S. Patent, Ed. United States, 1996

[2] L. O'Gorman, "Comparing Passwords, Tokens, and Biometrics for User Authentication", Proc. IEEE, vol. 91, no. 12, pp. 2019 2020, Dec. 2003.Mr. Rajesh H. Davda1, Mr. Noor Mohammed, " Text Detection, Removal and Region Filling Using Image Inpainting", International Journal of Futuristic Science Engineering and Technology, vol. 1 Issue 2, ISSN 2320 – 4486, 2013

[3] S. Wiedenbeck,J.Waters, J. Birget, A.Brodskiy,and N. Memon,"Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice," Proc. First Symp. Usable Privacy and Security (SOUPS), July 2005

[4] S. Chiasson, P. van Oorschot, and R. Biddle, "Graphical Password Authentication Using Cued Click Points," Proc. European Symp. Research in Computer Security (ESORICS), pp. 359-374, Sept.2007.

[5]S. Chiasson, J. Srinivasan, R. Biddle, and P.C. van Oorschot "Centered Discretization with Application to Graphical Passwords," Proc. USENIXWorkshop Usability, Psychology, and Security (UPSEC), Apr. 2008