A Novel Method for Graphical Password Mechanism

Siddharth R. Dharane
Department of Computer Engineering
BVCOE & RI, Nashik
Nashik, India
siddharthdharane@gmail.com

Pradip N. Kakade
Department of Computer Engineering
BVCOE & RI, Nashik
Nashik, India
pradipkakade69@gmail.com

Sapna P. Gaikwad
Department of Computer Engineering
BVCOE & RI, Nashik
Nashik, India
sapna14692@gmail.com

Pooja K. Dokhale
Department of Computer Engineering
BVCOE & RI, Nashik
Nashik, India
pooja.dokhale7@gmail.com

Prof. Ashvini Y. Bhamare
Department of Computer Engineering
BVCOE & RI, Nashik
Nashik, India
bhamare.ashwini17@gmail.com

***Abstract*—** For the verification of authorized users in computer systems, various text based or biometrics methods are used. But these methods have some drawbacks. It is difficult to remember and recall the textual i.e. alphanumeric passwords. To avoid this drawback users prefer to create effortless, short, easy and insecure passwords which are easily guessable by hacker and this makes the system more vulnerable to attacks. On other hand, verification mechanisms based on biometrics offers security to a good extents. But they are quite luxurious for implementation. Cost becomes a key factor in the case of biometrics. Also any injury to the body part used in biometric authorization results in denial of access or performance issues. Graphical password provides another way by providing passwords that are more protected and unforgettable in a reasonable price. In this system, user clicks on images instead of typing passwords for accessing the system. This paper describes and examines usability and security of graphical password mechanism for authentication using graphical passwords. Proposed system describes characteristics for security and performed empirical study comparing Graphical password mechanism with Biometric passwords and alphanumeric password.

Keywords *- Authentication, Empirical study, Graphical password, Usability, Security.*

*****

I. INTRODUCTION

Generally for granting authentication we used knowledge-based authentication schemes involving text-based password, numeric pins or alphanumeric password. All these mechanisms are vulnerable to hacking. Text based password technique is a most popular authentication method, but it has security and usability problems. So alternatives of this method are biometric authentication and token based authentication methods. But they also have their own drawbacks[9][10][11]. Text-based passwords [4] are more prone to attacks and can be easily guessed by the hackers having the details of system or the details of the user. For avoiding this, the system is designed to take long alphanumeric passwords which are difficult to guess for the hacker. On the other hand, these difficult passwords create a challenge for the user to memorize them. As a result user may forget his/her password. The studies of Graphical password states that click point password are hard to guess by attacker and easy to remember for the user. When a secured access mechanism is considered, biometrics can be taken into account. But it has certain drawbacks. Biometrics equipments are costly and therefore cannot be afforded by everyone. Also any temporary or permanent damage to the body part used for authentication may deny users access to the system. The basic principle in Graphical password mechanism is to encourage storage password selection while maintaining the memorability of the user.

Figure 1 Password input mechanism of GPM

The proposed system uses the idea of Graphical password mechanism [3] with a series of images used for accessing the system. System provides graphics for authentication. It gives easy and more secure way for login. The mechanism influences the user to set a random graphical password which is difficult for hacker to guess but easy for the user to remember. In real life situation the same user will required different level of security for different types of system based on their priorities. But the existing system provides the same level of security for all level systems. The strength of the security can be varied by the user depending upon her/his present requirements. To increase the security, support for wrong click can be eliminated so that the hackers cannot guess the right click point path.

II. LITERATURE SURVEY

Now a days, all business, government and academic institutions are investing a lot of money for security of information. A key area in securing important information is authentication. Authentication refers to the process of verifying the identity of communication partner. It determines whether a user is allowed to access a particular system or resource. Today it is a critical area of security research.

The traditional username/password and Personal Identification Number (PIN) based authentication scheme is an example of Token based. Token based is a most popular It is a physical entity which is used for authentication. For example smart card, Driver's license, ATM card, college ID card etc. It allows user to enter their username/password in order to obtain a token which allows them to fetch specific resource without using their username and password. Once their token has been obtained, then the user can offer the token-which allows access to a specific resource for a time period to the remote site[2]. It is a type of knowledge based authentication because sometime in which user need to remember their PIN code. For example in ATM authentication user have a ATM card as token but it also have a PIN code which is need to remember.

Biometric is the study of automatic methods for uniquely recognizing human being based upon one or more physical or behavioral parts. It is method in which user uses body for authentication. It uses psychological or behavioral characteristic like facial or fingerprints scans and iris or voice recognition to identify users[1]. For example retina scans or finger prints. But when any surgery or any accident happens with the body part used for authorization then problems such as denial of access may occur.

The major drawback of token based and biometric based authentication methods are expensive equipments as they require special devices. Also the user may lose his/her token in some situations. As a result the user is unable to access the system. Or the user should wait for the replacement token.

Knowledge based Authentication is one of the most widely used authentication technique and includes text based and picture based passwords. Knowledge based Authentication is based on "something you know to identify you".

To make the job of attacker more difficult, organizations always encourage their users to use the mixture of uppercase and lowercase characters and also include numbers and special symbols in their password. This may make the guessing of password difficult but the basic problem still remains- user will pick something that is easy for him/her to remember.

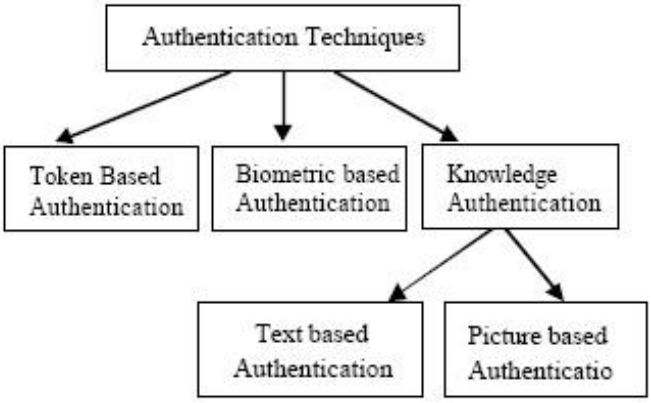

Figure 2 Classification of the authentication techniques.

Graphical password method have been proposed as a potential alternatives to text based techniques, supported partially by the fact that humans can remember images better than the text. Psychologists have confirmed that in both recognition and recall scenarios, the images are more memorable than text. Study on images shows that images are recognized with very high accuracy (up to 98%) after a two hour delay, which is much higher than accuracy for words and sentences. In addition, it has been found that the errors in the recognition of images are only 17% after viewing ten thousand pictures. Studies of recall also confirm that pictures are recalled well than words. Therefore graphical authentication mechanisms have higher usability than other authentication techniques. [14]

In general, the graphical password methods can be classified into two categories: Recall-based graphical techniques[6] and Recognition-based graphical techniques[5]

III. EXISTING SYSTEM

Text based authentication are used most popularly for authentication, but they have security and usability problem. Authentication likes biometric system and tokens have their own drawbacks. Graphical password offer the another alternative in pass points, password consist of a sequence of n number of click-points on a given image. In Pass points, users are free to select any random pixels on the image as click points for check password. For logging in the system, they

 ISSN: 2321-8169
156 - 161

repeat some sequence of clicks in the correct order, within a system defined tolerance radius of the original click points. But having all the points on a single image make it prone for the hacker/attacker cues the pass point sequence. The certain problem with the existing system gave rise to the demand for new system they are:

A. Problem with Biometric:

Bio metric verification consist of mechanism Fingerprints, voice recognition, iris scan, hand geometry etc. But the drawback of this approach is that the systems and equipment used for verifying the authenticity are not only expensive but also the process is slow. However, this technique has a high level of security. Also unfortunately some accident happens with the body part which user uses for authentication any surgery has been performed on it then the system will not provide access to the user unless it is updated with the new details.

B. Problems with Textual passwords:

Users always choose a password that is easy to remember. Generally easier passwords can be the same sequence of characters that they use for it. If the system has an account with user name as ABC, then the first guess for password will be ABC. If this is not working then variations on the same user id can be tried by the hacker. Many times users select the name of their family members, pets or favourite sports player etc for password. Or if numbers are considered then user will select something easy to remember like the individual`s birth year or the date of some other significant event. The key is that the user will always select something easy to remember, so if you know more about the user then there are better chances of discovering their password.

To make the job of attacker more difficult, organizations always encourage their users to use the mixture of uppercase and lowercase characters and also include numbers and special symbols in their password. This may make the guessing of password difficult but the basic problem still remains- user will pick something that is easy for him/her to remember.

Click Based Graphical Password Algorithm:

Graphical Password Mechanism is a type of knowledge based authentication that attempts to take the advantage of human memory for remembering visual information.

The cued click point purpose five click point on one image. The points are scattered randomly on the single image making it more vulnerable to attacks. Also it makes it mandatory to follow the sequence of clicks.

IV. PROPOSED SYSTEM

A. Graphical Password:

The alternative to existing alphanumeric passwords is Graphical Password. In graphical passwords, instead of typing an existing alphabetical or numerical password, user clicks on images prior to the graphical password which is an alphanumeric word known to the computer and the user.

The result of a recent survey shows that 92% of large businesses in India still use passwords to authenticate users. But users have many problems with the alphanumeric passwords like difficulty in remembering complex, pseudo-random passwords over time. Generally, a good password has some characteristics like including numbers, alphabets (both capital and small) and special symbols, words not present in dictionary and not only that it must be long enough to stand against different attacks. As a general rule of thumb, a strong password should have no less than eight characters. Such pseudorandom passwords lack meaningful content and can be learned only by rote memorization, which is a weak way of remembering.

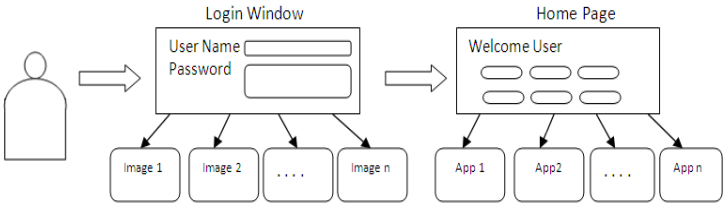

Figure 3 Graphical Model of system

Studies have shown that users mostly tends to pick short passwords or passwords that are easy to remember, like alphabetic-only passwords consisting of personal names of family or friends, names of pets etc. Such passwords are easy to crack using dictionary attacks or attacks based on the knowledge of the user. According to Computer World news article, a team of security engineers ran a password cracker in a network and within 30 seconds, they cracked 80% of the passwords.

People often forget their passwords. If a password used less frequently it will be even more susceptible to forgetting. If the password is hard to guess, it is hard to remember. Psychological theories have identified decay over time and interference with other information in long term memory as underlying reasons for forgetting .Another complicated issue is that users have many passwords for computers, networks and e-mails. Remembering a complex and long password is difficult. But Studies shows that human brain can better recall images than text. Further study on images shows that images are recognized with very high accuracy (up to 98%) after some time, which is much higher than accuracy for words and

 ISSN: 2321-8169
156 - 161

sentences. In addition, it has been found that the errors in the recognition of images are only 17% after viewing ten thousand pictures. Studies of recall also confirm that pictures are recalled well than words, and this has led to the "picture superiority effect".[12][13]

B. *Graphical password mechanism Algorithm:*

Graphical password mechanism (GPM) is prepared alternative to pass points. In GPM, users click on one point on each of n = 5 images rather than on five points on one image[7] .It offers cued-recall. It also makes attacks based on hotspot analysis more challenging.

Each click results next-image it leads users down a "path" as they click on their sequence of points [8]. A wrong click leads down an incorrect path, with an explicit indication of authentication failure after the final click.

Each new click revert to a distinct level image. During the password creation process a de authorization method is used to determine click points tolerance, that is every margin for clicks and corresponding grid. The capability improvement being cued to recall one point on each image appears easier than remembering an ordered sequence of the points on one *image*.

C. *Advantages:*

The proposed graphical password mechanism provides a more secured and easy way to login in an inexpensive manner. It also provides an easy way to remember and recall password. GPM provides greater security by providing passwords that are less prone to any kind of hacking. It increases the workload by attackers and makes the hacking difficult by increasing strength of system and has large key space that reduces the likelihood of successful attacks using traditional techniques such as brute force attack or dictionary attacks. GPM has advantages over pass point in terms of usability, security and memorable authentication mechanism.[15].

V. EXPERIMENTAL RESULT

We conducted a survey with 100 participants. We provided them with three login systems, one based on alphanumeric authentication method, one based on Bio-metric and the other one based on Graphical Password Mechanism. Participants were asked to create a login in all three systems and login in it. Participants were asked to follow few basic rules for creating passwords. After the experiment, participants were asked about which system they will prefer more in daily basis. And 97% participants voted for Graphical Passwords.

TABLE I EXPERIMENT RESULTS

	Graphical	Textual	Biometric
Total no. of votes	97%	2%	1%

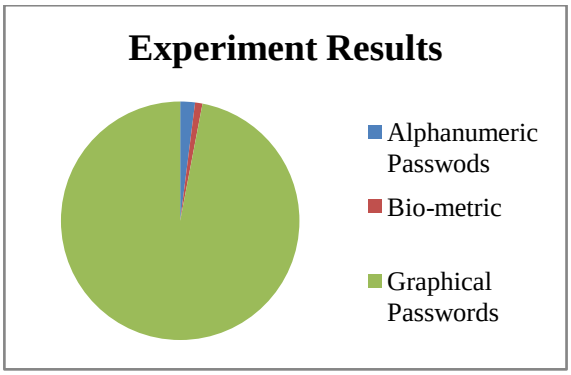

Figure 4 Experiment Results

The survey showed that people mostly go for simple, short and easy to remember passwords. In this case biometrics and Graphical passwords fulfill their requirements. But when it comes to cost, Graphical Passwords becomes their first choice. Participants found Graphical Password Mechanism, an easy to remember and cost effective alternative to Text based passwords and Biometrics. Most participants chose it because they find in universally applicable to any system and to people of any age and any background, no matter technical or non technical.

While manipulating the Alphanumeric Password authentication system and Graphical Password authentication system, participants were asked to follow the following steps:

1. Creating a new login: Create a pair of username and password, in Graphical method, by clicking on one point on each of five images which were presented in sequence. In Alphanumeric authentication system, participants were asked to create complex and random passwords as per standard guidelines.
2. Confirming the password: The participants were asked to re-enter the same password correctly in the same sequence.

The accuracy of the participants with the Graphical passwords were far better than alphanumeric passwords. Only 8 participants out of 100 required a restart for Graphical passwords whereas for alphanumeric passwords 86 participants required a restart. Even for Biometric system, participants were finding trouble in properly placing the physical part twice and restarts were required. The total number of restarts for it was 48. The success rates for Graphical password system were high for all phases than alphanumeric password system and Biometric systems.

TABLE II TOTAL NUMBER OF RESTARTS AND SUCCESS RATES

	Graphical	Textual	Biometric
Total no. of Restarts	8	86	48
Success Rate	92%	14%	52%

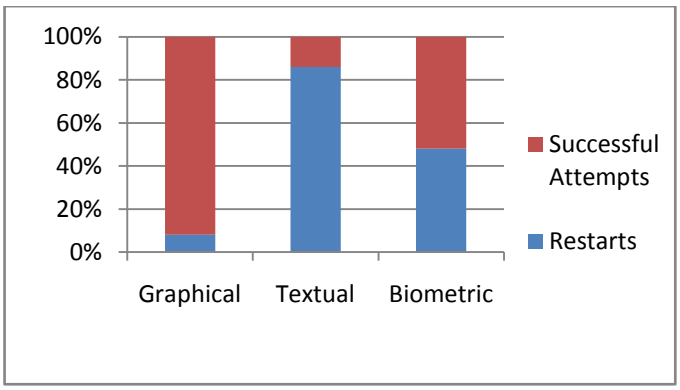

Figure 5 Accuracy for each mechanism

Participants were very accurate while re-entering their passwords in Graphical password authentication system than the other two systems. They were also considering the cost aspect with the security aspect when asked for the views in terms of purchasing point of view.

VI. CONCLUSION

In this thesis, the general goal was to increase the memorability and security of knowledge-based authentication schemes. The focus was on click-based graphical passwords. Successfully, the designing of innovative schemes that improved memorability was created and that were more secure than existing alternatives. The proposed Graphical Password Mechanism scheme is promising as an usable and memorable authentication mechanism. By taking advantage of users' ability to recognize images with greater accuracy, GPM has an advantage over Pass Points in terms of usability. As each image appears and the user has to remember only one click-point per image, it becomes easier than remembering an ordered series of clicks on one image.GPM increases the workload for attackers by forcing them to conduct hotspot analysis on each of these images. In addition, the system's suppleness to increase the overall number of images in the system allows us to arbitrarily enlarge this workload.

VII. ACKNOWLEDGEMENT

We would like to pay our sincere gratitude to Prof. C. K. Patil, Principal, BVCOE&RI, who provided us an excellent platform for studies and research activities. We are also thankful to Prof. H. D. Sonawane, HOD, BVCOE&RI for his constant and unconditional support to this explicitly knowledgeable work. Last but not the least we also thank to our Faculty members, Staff and friends for being instrumental towards the completion of this paper.

VIII. REFERENCES

[1] Neil Yager and Ted Dunstone ―The Biometric Menagerie‖ IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol 32, No. 2 February 2010

[2] Wazir Zada Khan, Mohammed Y. Aalsalem and Yang Xiang ―A Graphical Password Based Systems for Small Mobile Devices, IJCS Issues, vol 8,Issue 5, No. 2, September 2011.

[3] A. Forget, S. Chiasson, P. van Oorschot, and R. Biddle, "Improving Text Passwords through Persuasion," Proc. Fourth Symp. Usable Privacy and Security (SOUPS), July 2008.

[4] S. Chiasson, A. Forget, E. Stobert, P. van Oorschot, and R. Biddle, "Multiple Password Interference in Text and Click-Based Graphical Passwords," Proc. ACM Conf. Computer and Comm. Security (CCS), Nov. 2009.

[5] Sadiq Almuairrfi, Prakash Veeraraghavan and Naveen Chilamkurti ―Implicit Password Authentication System ― 2011 Workshops of International Conference on Advanced Information Networking and Applications.

[6] Xiaoyuan Suo Ying Zhu and G. Scott. Owen ―Graphical P password ds : A Survey.

[7] S Chiasson, A. Forget, R. Biddle, and P. van Oorschot, "Influencing Users towards Better Passwords: Persuasive Cued Click- Points," Proc. British HCI Group Ann. Conf. People and Computers: Culture, Creativity, Interaction, Sept. 2008.

[8] X.S. Zhou and T.S. Huang, ― Relevance feedback For Image Retrieval: A Comprehensive Review, Multimedia systems, vol.8, no. 6 Apr. 2003.

[9] L. Jones, A. Anton, and J. Earp, "Towards Understanding User Perceptions of Authentication Technologies," Proc. ACM Workshop Privacy in Electronic Soc., 2007. IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 1, March, 2013 ISSN: 2320 - 8791

[10] L. O'Gorman, "Comparing Passwords, Tokens, and Biometrics for User Authentication," Proc. IEEE, vol. 91, no. 12, pp. 2019-2020, Dec. 2003.

[11] A. Jain, A. Ross, and S. Pankanti, "Biometrics: A Tool for Information Security," IEEE Trans. Information Forensics and Security (TIFS), vol. 1, no. 2, pp. 125-143, June 2006.

[12] S.Chiasson, E.Stobert, A.Forget, R.Biddle,and P.van Oorschot," Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism", IEEE DEPENDABLE AND SECURE COMPUTING, March/Arril 2012.

[13] S. Chiasson, R. Biddle, and P. van Oorschot, "A Second Look at the Usability of Click-Based Graphical

Passwords," Proc. ACM Symp. Usable Privacy and Security (SOUPS), July 2007.

[14] S. Chiasson, A. Forget, R. Biddle, and P.C. van Oorschot, "User Interface Design Affects Security: Patterns in Click-Based Graphical Passwords," Int'l J. Information Security, vol. 8, no. 6, pp. 387- 398, 2009.

[15] J. Yan, A. Blackwell, R. Anderson, and A. Grant, "The Memorability and Security of Passwords," Security and Usability: Designing Secure Systems That People Can Use, L. Cranor and S. Garfinkel, eds., ch. 7, pp. 129-142, O'Reilly Media, 2005.

Author's Profile

Siddhartha R. Dharane Pursuing BE Degree in Computer Engineering from BVCOE&RI, Nashik, India. Area of Interest: Network Security

Pradeep N. Kakade Pursuing BE Degree in Computer Engineering from BVCOE&RI, Nashik, India. Area of Interest: Network Security

Pooja K. Dokhale Pursuing BE Degree in Computer Engineering from BVCOE&RI, Nashik, India. Area of Interest: Network Security

Sapna P. Gaikwad Pursuing BE Degree in Computer Engineering from BVCOE&RI, Nashik, India. Area of Interest: Network Security

Ashvini Y. Bhamare, Assistant Professor, Department of Computer Engineering, BVCOE&RI, Nashik, India. Qualification: M.Tech (Computer Engineering), Area of Interest: Network Security and Image Processing.