International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 08 | Aug-2016 www.irjet.net p-ISSN: 2395-0072

Graphical Password Authentication for Secure Online Services

Prashanthi Muddam, D.Raman

Dept.of CSE, Vardhaman College of Engineering Affiliated to JNTUH, Hyd
mpr.prashanthi@gmail.com
Professor, Dept. of CSE
Vardhaman College of Engineering, Affiliated to JNTUH, Hyd
d.raman@vardhaman.org

Abstract - : *The most common way of access to computer systems is based on alphanumeric passwords where combination of alphabets, numbers and special characters are used as password. But the issue with alphanumeric passwords is the passwords that are strong and reliable for attacks are hard to remember and passwords that are short, simple and easy to remember are not secure and are easily breakable. Graphical password is a new password scheme where a set of images are given to the user and asked to click on certain point and that is set as password. Cracking graphical passwords is more difficult compared to alphanumeric passwords hence the security of the system will be very high and working with graphical passwords is easy where a sequence of clicks on images gives us password. Graphical passwords are mainly divided into two categories they are recognition-based and recall-based technique.*

Key Words: **Graphical Password, Authentication, Brute Force Attack, Pass points, Recognition-based, Recall-based technique.**

1. INTRODUCTION

Authentication is a process of determining a user whether he is allowed to access a particular system. Passwords are used for a system or a website to authenticate a user and provide security but using traditional alphanumeric password has some issues like passwords that are strong enough are hard to remember and on other hand passwords that are easy to remember are easy to guess as well and mostly users write down the password or use common password for several sites to reduce the their memory load risking security .Replacement of traditional alphanumeric passwords by a more secure means of authentication is both necessary and imminent. Authentication through biometrics can be alternative solution to overcome issues in alphanumeric but biometric systems are more complex and expensive

Graphical passwords have been proposed to overcome the disadvantages of alphanumeric and biometric based authentication. Surveys have proved that human beings can remember images better compared to text. In addition the complexity of graphical password scheme is less compared to biometric system. Graphical password is an authentication technique where a user is given with set of images, sequential clicks on images is considered as password .The main idea behind graphical passwords is, using images which results in more memorability and they are easy to work with as user has nothing to type like text based password.

2. RELATED WORK

Providing secured authentication has been always a tedious work. Many types of authentication techniques have been implemented till now and still research is going on for new techniques. The authentication can be done in three ways:

a. By something a user knows: The information a user knows like a text password, a PIN(Personal Identification Number) or a graphical password.
b. By something a user has: A smart card or a security token is used.
c. By something a user is: Biometrics characteristics such as finger prints, iris etc.

A brief discussion on different types of authentication systems is given below:

1. Alphanumeric
2. Biometric
3. Graphical Password

2.1 Alphanumeric: It is the traditional solution for security issues proposed in the early stages of authentication problem solving. As the name indicates alphanumeric is a combination of alphabets, numerical and special characters. These passwords provide good security only if they are complicated. Usually the passwords should have minimum of 8 characters and combination of at-least a special character to provide better security.

The major disadvantage of this type of authentication is remembering the passwords, as usually human tends to forget. The passwords are usually the words related to the users like their names, date of birth which are

easy to remember but it would be a major issue as they can be cracked easily. A password which is strong is hard to remember as they are complicated and a password which is simple is easy to remember but can be cracked easily. Another major drawback is dictionary attack. In order to easy remembrance most users use common words or names as passwords. There are many tools that allow a user to crack passwords by automatically testing of random words which occur in dictionary.

2.2 Biometric

Biometric authentication is a type of authentication which is hard to spoof or forge where biological characters of an individual are used to provide authentication. Biometric identifiers are mainly characterized as physiological and behavioral characteristics where physiological characteristics relate to shape of a body like fingerprints, palm veins, etc. and behavioral characteristics include voice, gait, etc. The most common biometric technique is finger prints where fingerprints are stored in database initially and are compared whenever a user try to authenticate to provide access.

This type of authentication provides high security but is used rarely because of its disadvantages. The major disadvantage is its high cost. Different biometric systems use different devices that have a high range of cost. Using biometric devices is complex and time consuming. A denial of service is also an issue in biometric system which occurs when a system does not recognize a legitimate user or when a system recognizes unauthorized user as authorized one.

2.3 Graphical Password

Graphical password is a knowledge based authentication technique where a user is asked to produce or recall something which he selected earlier. Majorly there are two different types of graphical passwords techniques

a. Recognition based technique

b. Recall based technique

Recognition Based Technique: In this recognition based technique user is asked to select certain number of images which are produced by the system during registration and asked to identify preselected images to allow authentication. This technique was proposed by Dhamija and Perrig. Success rate of authentication of this technique is high compared to text based password.

Weinshall and Kirkpatrick has designed several authentication techniques, such as picture , object, and pseudo word recognition, and conducted a number of user studies. In the picture recognition technique, a user is trained to recognize a large number of images selected from a database. After few months, users in their study were able to recognize over 90% of the images in the training set. This proved that pictures are the most effective among picture recognition, object recognition, and pseudo word recognition technique.

Pass face is one of the recognition based authentication technique where a user is provided with an image which is a grid of nine faces. User has to select particular face from a grid and reproduce or recognize the same during the authentication. This technique is said to be easy to work as people can recall human faces easily then other images

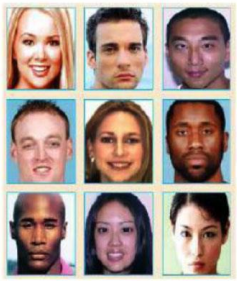

Fig 1: Example of pass face

Recall Based Technique: Recall based technique is a sequence of invariant points of object. There are two type of recall based techniques

Draw a secret: It is a pure recall based technique where user is provided with rectangular box of size n x n and asked to draw a simple image on a 2D grid , every cell in the image is denoted with coordinates(x, y)

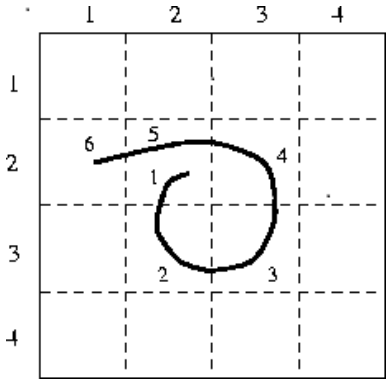

Fig 2: Example of Draw a secret

Syukri Algorithm is one of the pure recall, draw a secret based technique where user signature is drawn using mouse and it is used as password. The major advantage of this technique is there is no need of remembering a password as it is users signature itself and it is hard to forge , but the drawback with this technique is not all the users can use mouse a writing device

Fig 3 Example of signature scheme

Pass points:

In Pass point password scheme user selects sequence of clicks on an image and has to remember the same click points for authentication, as clicking on same click point in an image is not always possible so to overcome that the system allows for system tolerance near the click point i.e small variation in the click point will be accepted

Fig3 :Example of pass point scheme

3. SAFETY

An authentication system must provide adequate security, otherwise it fails to meet its primary task, research is still going on to study the difficulty of cracking a graphical password. Let's discuss different types of attacks in comparison to text based password.

3.1 Brute Force Attack: In this type of attack attacker try as many passwords as possible until the correct password is guessed, short passwords are highly vulnerable to brute force attack. Compared to text based password graphical password are less affected by this type of attacks as password space of graphical passwords is high. Password space of text based password is 94^N, where N is number of characters in a password and 94 is no of printable characters, whereas for an image password it depends on number of images being used more no of images gives larger password space and high security from brute force attack

3.2 Dictionary Attacks: It is a type of attack where every possible string such as in dictionary is used to break the password. Graphical passwords are not much affected by dictionary attacks as the input for graphical passwords is given by clicking mouse rather than keyboard like text password.so graphical password are less vulnerable to dictionary attacks compared to text based password

3.3 Shoulder Surfing Attacks: It is an observation technique where an intruder looks over ones shoulder to get the password Unfortunately graphical passwords are highly vulnerable to shoulder surfing attacks only few recognition based techniques are shoulder surfing attack resistant, using some techniques like two phase authentication where both graphical and textual based are combined together to provide authentication may provide security against shoulder surfing attacks.

3.4 Malware: Spyware is software that gains information about user without their knowledge. Breaking graphical password using spyware is highly difficult as mouse motion alone is not enough to crack graphical password.

3.5 Social Engineering: Social engineering is manipulating a user psychologically to obtain confidential information. Compared to text based password graphical passwords are hard to give away.

4. PROPOSED WORK

We propose and examine the usability and security of Cued Click Points (CCP), a cued-recall graphical password technique. Users click on one particular point or a pixel per image in a sequence of pictures. Successive image relies on the previous click-point , it appears only if the previous click point is correct. Using more number of images increase password space and also provides more security but decreases usability.

This method provides protection against online password-guessing attacks and related denial-of-service attacks. The owner is granted with administrative privileges and is referred to as administrator. Only the owner registers with the application provider other user accounts are created by using a Web interface. Each user logs in with three credentials rather than the usual two. A user id which is known only to the user and administrator, a password known only to the user, and saved in an encrypted form in database. If an intruder tries to attack the password after a certain number of consecutive bad guesses against a password, the account is locked out. Bad guesses are considered to be consecutive if there is no successful login to the user's account in between. All the consecutive bad guesses must be against the same password; counting starts over if the password is changed. A user who has been locked out is allowed to log in again once his password has been reset.. This method provides protection against online guessing attacks and related denial-of-service attacks and other security attacks.

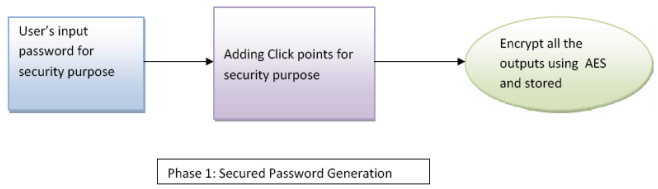

Fig 5:Password Generation

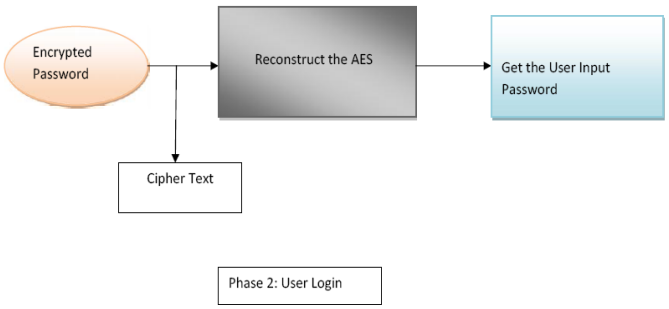

Fig 6:Login

5. CONCLUSION

Textual passwords are still the most common method used for authentication. Many years ago Morris and Thompson identified textual passwords as a weak point in information system security. So Graphical password is possible alternative to provide security, but graphical passwords are still underexplored, more research and studies are needed for graphical password techniques. Graphical passwords are more secure compared to textual password due to its large password space and users have to click on image rather than typing like textual password. Graphical passwords are less vulnerable to security attacks like online guessing attacks, brute force attacks and dictionary attacks

Graphical passwords are still not in use due to some of its problems like they require large amount of storage space to store images and working with graphical passwords during registration is time taking when compared to textual passwords

References

[1] D.S. Jeslet et al. "Survey on Awareness and Security Issues in Password Management Strategies." IJCSNS, vol. 10, no.4. April, 2010.

[2] S.M. Furnell et al., "Authentication and Supervision: A Survey of User Attitudes." Computers & Security, vol.19 no.6, pp 529-539, 2000.

[3] R.J. Sutton, Secure Communications: Applications and Management. Chichester: John Wiley & Sons, Ltd. 2002.

[3] E.F. Gehringer, (2002) "Choosing Passwords: Security and Human Factors." IEEE, 0-7803-7824-0/02/$10.00 8.

[4] S. Farrell, "Password Policy Purgatory." IEEE Computing Society. pp. 84-87, 2008.

[5] M.I.U. Adeka, J.S. Shepherd, and R.A. Abd-Alhameed, "Cryptography and Computer Communications Security: Social and Technological Aspects of Cyber Defence," Ongoing PhD Research Work, School of Engineering, Design and Technology, University of Bradford, Bradford (UK), (Ongoing: 2011-)

[6] A. S. Patrick, A. C. Long, and S. Flinn, "HCI andecurity Systems," presented at CHI, Extended Abstracts (Workshops). Ft. Lauderdale, Florida, USA.2003.

[7] A. Adams and M. A. Sasse, "Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures," Communications of the ACM, vol. 42, pp. 41-46, 1999.

[8] K. Gilhooly, "Biometrics: Getting Back to Business," in Computerworld, May 09, 2005.

[9] R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in Proceedings of 9th USENIX Security Symposium, 2000.

[10] M. Kotadia, "Microsoft: Write down your passwords," in ZDNet Australia, May 23, 2005.

[11] A. Gilbert, "Phishing attacks take a new twist," in CNET News.com, May 04, 2005.

[12] A. Jain, L. Hong, and S. Pankanti, "Biometric identification," Communications of the ACM, vol. 33, pp. 168-176, 2000.