ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 1, January 2014

Mechanism To Deny Password Guessing Attacks

Mr.S.D.Samleti[1], Prof.B.S.Satpute[2]

Assistant Professor, Information Technology, Army Institute of Technology, Pune, India[1]

Assistant Professor, Computer Engineering, Pad. Dr.D.Y.Patil College, Pune, India[2]

Abstract: Usability has many security threats concern with user friendliness. Hence, normal Human-machine interactions are not applicable. Major objective of user friendliness lies selecting better passwords. Normally, users create easier passwords so that they remember it & recall it. If user creates easier passwords then they can be easily cracked by some people with malicious intent. So create passwords with better security measures. If you create better password it has to be more secure. Passwords are normally mix of letters, alphabets, numbers. Other options is to select password with images or graphs. Normally human brain is better in recalling image based things. There are different graphical password schemes or graphical password software in the market. However, very less research has been done to examine that are still not strong. Hence it combines persuasive cued click points and password guessing resistant protocol. The major objective of this work is to bring down the guessing attacks as well as encouraging users to select more stochastic, and different passwords to imagine.

Keywords: Authentication, Graphical Passwords, CCP, Attacks

I. INTRODUCTION

In recent times there is a huge hype for graphical passwords since last few years due to the fact that text based passwords are very much vulnerable for different class of attacks like brute force, dictionary based attack, shoulder surfing attack etc.,

In spite of such vulnerabilities users are tend to select short guessable passwords. Unfortunately, such passwords can be break-down easily by third party. To avoid this problem, the idea of graphical based or image based passwords were first introduced by greg blonder in the year 1996. Blonder assumed that graph based passwords have a preset collection of images with click regions which acts as password. After initial blonder proposed this scheme, there were so many password schemes were developed. Basic feature of image based password is that human beings can easily recall images as compared to boring images. Hence, it is assumed to be a better alternative to the images based passwords

A major advantage of Persuasive cued click point scheme is its large password space over alphanumeric passwords. There is a growing interest for Graphical passwords since they are better than Text based passwords, although the main argument for graphical passwords is that people are better at memorizing graphical passwords than text-based passwords.

Cued Click Points (CCP) is a proposed alternative to PassPoints. In CCP, users click one point on each of images rather than on different points on one image. It offers cued-recall and introduces visual cues that instantly alert valid users if they have made a mistake when entering their latest click-point at which point they can cancel their attempt and retry from the beginning. It also makes attacks based on hotspot analysis more challenging.

II. CLASSIFICATION OF PASSWORDS

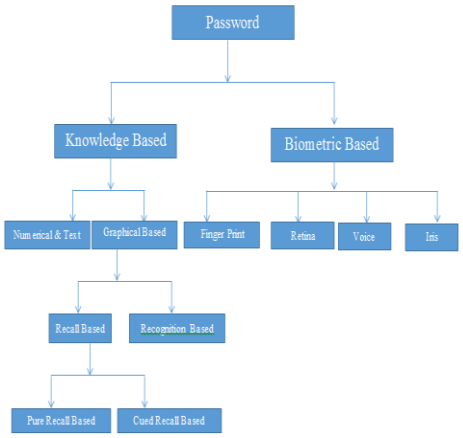


Fig. Classification Of Passwords

Fig shows current authentication mechanism. Normally password can be classified into Knowledge based & Biometric Based techniques. Biometric based authentication strategies take into of the human body part to authenticate the user.

For Example: Finger Print, Iris Scan or Retina Scan. Such mechanism seems to be quite expensive in terms of money & you need to install the hardware for the same authentication procedure.

Now-a-days, Knowledge based passwords are quite most wanted techniques because knowledge based techniques can improve high security. Normally, Graphical Based Passwords can be classified into Recall Based & Recognition Based techniques.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 1, January 2014

History Of Graphical Based Password Scheme:

Graphical password based techniques were first coined by Greg Blonder in the year 1996. After that so many other graphical based password were introduced. Graphical password system can be categorized as Recognition & cued Recall of images based or Pure recall based schemes. At present most of the existing systems depends on Recognition.

Recognition Based System:

Recognition based technique was first proposed by Dhamija & Perrig in their work on Deja Vu: A User Study Using Images for Authentication. This work was based on Hash Visualization Technique. Their work was on making authentication process easier, reliable & user friendliness to use. In additional to this, system use to prevent users from selecting weaker passwords & making them to choose strong passwords. Hence, making it tougher task for user to note it down passwords or secret words & hence making it pass the passwords to other users.

Drawback of the recognition based system was server or database would need to store the images. Hence, making it a difficult task of selecting a particular image from the database & again this process use to take huge amount of time.

Devisetty & Akula[6] proposed similar technique as Perrig & Dhamija[5] the images shall be converted into SHA-1 which use to give more secure system. Their work was not pure graphical based password system. It was mixed with text. They were used text based passwords with images to enhance security which were vulnerable to the Shoulder Surfing attacks.

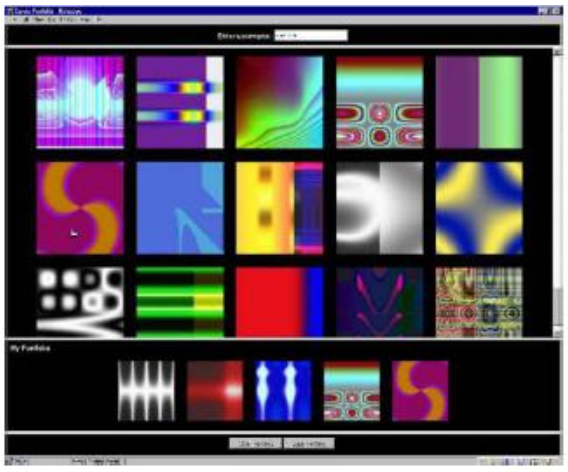


Fig. Random Images Used by Dhamija & Perrig.

Hongs Approach:

Hong et Al., proposed another shoulder surfing resistant algorithm. In this approach to allow user to assign their own codes to pass object variants. Fig. shows the login screen snapshot of this graphical password scheme. However this method still forces user to remember to remember many text string and hence suffer from the many drawbacks of text based passwords.

Fig Hongs Shoulder Surfing Resistant Algorithm

1. Pure Recall Based Technique:

Here we discuss pure recall based strategy to authenticate the system.It uses the following techniques:

i) Pass Pointsw
ii) Cued Click Points
iii) Persuasive Cued Click Points (PCCP)

i) Pass Points :

As proposed by Greg Blonder's original idea Pass Points are nothing but a Click-Based Graphical Password system where password include an ordered set of sequence of four to six click-points on a pixel based image.
To get login process, user is supposed to click on some system defined tolerance region for each click point.
Image behaves as a reminder to help user in their password entering process.

1.1 Cued Click Points:

CCP was considered as an alternative to the Click Based Graphical Password scheme in which user is suppose selects single point from each image for next 5 images. Fig shows this procedure in details.

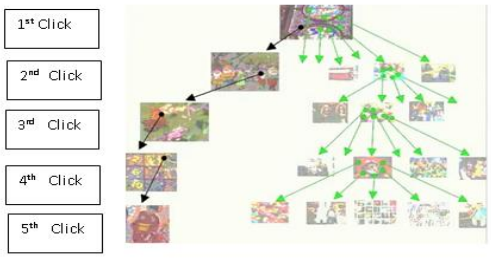
In this process, the user interface is supposed to present one image at a given time, the present image is replaced by the next image no sooner user selects a click point.
Here system determines the next image to image to be displayed based on the present image which user has selected.

At this point, user selects images based on the previous images which were selected one after the other image here we are following cued based recall technique in which each image initiates the user's memory to click on the image.

Next thing is if user selects wrong click point during login process the image or graph to be displayed is wrong image. Original user who see the wrong image come to know that they encounter an error with their last click. Reversely this inexplicit feedback is no helpful to the intruder as he/she does know the exact sequences of the images.

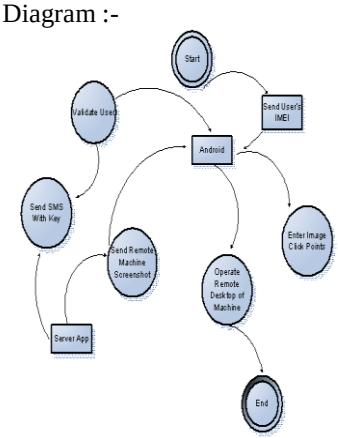
ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 1, January 2014



Activity Diagram For Proposed System:

DFD Diagram :-



Algorithm Design:

1. Send User's IMEI number of the mobile phone.
2. Validate against Android System.
3. Enter Click point on image.
4. Operate Remote Desktop of the Image.
5. Validate at server side.
6. Send request to user.
7. Send Remote machine screenshot
8. Allow to access as remote machine.

Explanation of algorithm:

1) User opens the application on the Android Phone.
2) In response to this system validates the IMEI address in database.
3) User is taken to the login screen for the login purpose.
4) Automatic SMS is sent to the phone that is connected to the central server.
5) User is validated
6) User is shown with 5 different images as part of CCP authentication.
7) Each image is divided into 5x5 split of matrix.
8) System checks the image blocks on server if it matches then preference is send to android based phone.
9) Remote desktop App is shown user can operate remotely.
10) Enjoy the system securely without security threats.

Mathematical Approach:

At this point we can compare various protocols with PGRP by facing some of the questions :-

Q1. what is the chances that opponents with "n" different users name's can guess a password without answering ATT Challenges?

Q2 what is the possibility that correct guess for an opponent's knowing "n" users and willing to answer ATTs?

$$\frac{nr_2+s}{M} > \frac{s}{q.M}$$

$$n > \frac{s}{r_2}\left(\frac{1}{q} - 1\right)$$

Formal Discussion on Future of Graphical Passwords:

Can Text Based Passwords will be replaced by Graph Based Passwords [1] :

Not surely, in future all the text based passwords shall be replaced by the graphical image based passwords. But to replace we need to have more complex system in terms of software interface & novice user should be given more training. At this point we will discuss the possible attacks on graph based passwords and try to correlate with the text based passwords.

Brute Force Attacks [1] :

To defend against brute force attack we must have huge pool or collection of passwords. Text based passwords has a 94N password space where N is the length of the password where 94 is number of printable characters which are available on keyboard without SPACE BAR. Few image based password techniques shown to provide a password strategies has been shown to give password space same as or greater than that of textual passwords. Recognition based graphical passwords tend to be smaller password spaces than recall based methods. It is quite difficult to have Brute Force Attacks on Image or Graph Based Passwords than textual passwords.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 1, January 2014

Dictionary Attack:
It is quite tougher to have dictionary attacks on graph based system as graph based passwords take into consideration of mouse click instead of keyboard interfaces.

Shoulder Surfing Attacks:
Similar to the text based attacks graph based attacks are more vulnerable to the shoulder surfing attacks.

Guess Work Attacks [1]:
Graphical Passwords can be more predictable as compared to the text based passwords. In graphical password system, people normally select weaker and easier passwords. Thorpes and Nali study revealed similar predictability among graphical passwords developed with DAS strategy.

Message Passing Attacks:
It can also be considered as social engineering attacks. Social Engineering attacks people normally pass message over telephonic conversation. People cannot distribute the passwords on phone etc., Phishing website cannot detect such graphical passwords.

Malware Spyware or Hacking Attacks:
Spyware uses software that collect information from remote user without the knowledge of the people whose machine has been attacked by spyware. So such attacks are not possible using graphical password system.
Still some work needs to prevent attacks like Shoulder Surfing attacks. Sometimes shoulder surfing attacks can break the graph based passwords which are more vulnerable to shoulder surfing attacks. Shoulder Surfing attacks makes graphical passwords weaker candidates.
We can use some advance techniques to prevent such attacks like 3D graphical concepts which makes this graphical passwords somewhat strong resist attacks.

III.CONCLUSION

Problem with the click based password system is to find the exact position of click point.
User may get confused with the exact location of the click point where user to click. In future we can develop or enhance the system with click point by adding some clue based system.
Here disadvantage is that the user may get confused with click point as image is divided into 4x4 matrix.

Future Enhancement:
To avoid the confusion of the point of click the user can add color the location of correct point of click.
This will act as the clue for the user.
To increase the security further the some 2 or 3 images can be brought under one canvas and customize the number of images on that.

REFERENCES

[1] "Revisiting Defenses Against Large Scale Password Guessing Attacks" By Mansour Alsaleh, Mohammed Mannan & P.C. Van Oorschot.
[2] Xianyuan Suo,Ying Zhu,G.S.Owen "Graphical Password : A Survey"
[3] Manu Kumar, Tal Garfinkel, Dan Boneh and Terry Winograd "Reducing Shoulder-surfing by Using Gaze based Password Entry": Symposium On Usable Privacy and Security (SOUPS) , July 18-20, 2007, Pittsburgh USA.
[4] Zhi Li, Qibin Sun, Yong Lian, and D. D. Giusto "An association-based graphical password design resistant to shoulder surfing attack International Conference on Multimedia and Expo(ICME), IEEE 2005
[5] R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in Proceedings of 9th USENIX Security Symposium,2000.
[6] S. Akula and V. Devisetty "Image Based Registration and Authentication System" in Proceedings of Midwes Instruction and Computing Symposium, 2004.
[7] L. Sobrado and J.-C. Birget "Graphical passwords" The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4, 2002.
[8] Sonia Chiasson, Alain Forget , Robert Biddle, P. C. Van Oorschot User interface design affects security: patterns in click-based graphical passwords Springer-Verlag 2009.
[9] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A.D. Rubin "The Design and Analysis of Graphical Passwords" in Proceedings of the 8th USENIX Security Symposium, 1999.
[10] S. Man, D. Hong, and M. Mathews "A shoulder surfing resistant graphical password scheme" in Proceedings of International conference on security and management. Las Vegas, 2003.