DEFENSES AGAINST LARGE SCALE ONLINE PASSWORD GUESSING ATTACKS BY USING PERSUASIVE CLICK POINTS

Chippy.T
chippyrevathy@gmail.com
Dhanalakshmi Srinivasan Engineering College

R.Nagendran
nanonagendran@gmail.com
Dhanalakshmi Srinivasan Engineering College

Abstract

Usable security has unique usability challenges because the need for security often means that standard human-computer-interaction approaches cannot be directly applied. An important usability goal for authentication systems is to support users in selecting better passwords. Users often create memorable passwords that are easy for attackers to guess, but strong system-assigned passwords are difficult for users to remember. So researchers of modern days have gone for alternative methods wherein graphical pictures are used as passwords. Graphical passwords essentially use images or representation of images as passwords. Human brain is good in remembering picture than textual character. There are various graphical password schemes or graphical password software in the market. However, very little research has been done to analyze graphical passwords that are still immature. There for, this project work merges persuasive cued click points and password guessing resistant protocol. The major goal of this work is to reduce the guessing attacks as well as encouraging users to select more random, and difficult passwords to guess. Well known security threats like brute force attacks and dictionary attacks can be successfully abolished using this method.

Index Terms: - Authentication, graphical passwords, guessing attacks, computer security.

INTRODUCTION

There has been a great deal of hype for graphical passwords since two decade due to the fact that primitive's methods suffered from an innumerable number of attacks which could be imposed easily. Here we will progress down the taxonomy of authentication methods. To start with we focus on the most common computer authentication method that makes use of text passwords. Despite the vulnerabilities, it's the user natural tendency of the users that they will always prefer to go for short passwords for ease of remembrance [10] and also lack of awareness about how attackers tend to attacks. Unfortunately, these passwords are broken mercilessly by intruders by several simple means such as masquerading, Eaves dropping and other rude means say dictionary attacks, shoulder surfing attacks, social engineering attacks [10][1].To mitigate the problems with traditional methods, advanced methods have been proposed using graphical as passwords. The idea of graphical passwords firstdescribedby Greg Blonder (1996). For Blonder, graphical passwordshave a predetermined image that the sequence and the tapregions selected are interpreted as the graphical password. Since then, many other

graphical password schemes havebeen proposed. The desirable quality associated with graphicalpasswords is that psychologically humans can remembergraphical far better than text and hence is the bestalternative being proposed. There is a rapid and growinginterest in graphical passwords for they are more or infinitein numbers thus providing more resistance.

The major goal of this work is to reduce the guessing attacks as well as encouraging users to select more random, and difficult passwords to guess.

2. Taxonomy of Authentication

The following Figure 1: is the depiction of currentauthentication methods

Biometric based authentication systems techniquesare proved to be expensive, slow and unreliable and hencenot preferred by many. Token based authentication system is high securityand usability and Accessibility compare then others. Butthis system employ knowledge based techniques to enhancesecurity. But the current knowledge based techniques arestill immature. For instance, ATM cards always go hand inhand with PIN number.

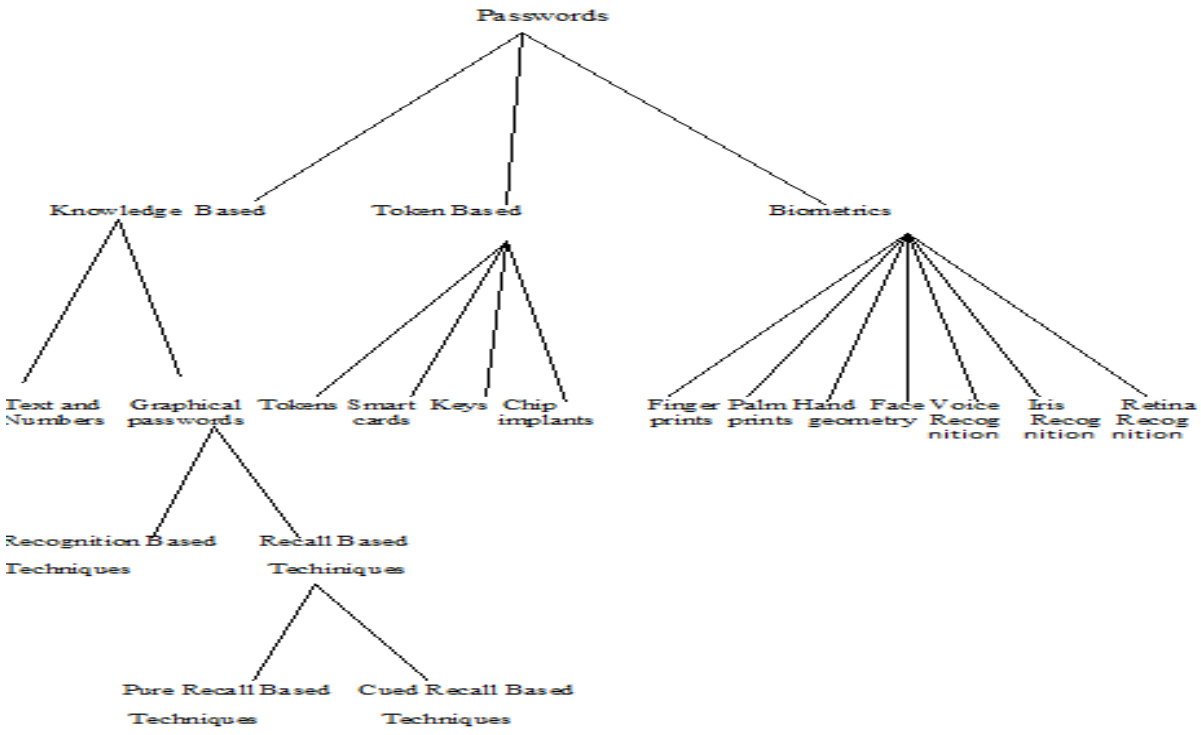

Figure 1: Taxonomy of Password Authentication Techniques

So the knowledge based techniques are the mostwanted techniques to improve real high security.Recognition based & recalls based are the two names by which graphical techniques could be classified.

3. Background on graphical Password Systems

Graphical passwords were first described by Blonder. Since then, many other graphical password schemes have been proposed. Graphical password systems can be classified as either recognition-based (image based scheme, cued recall-based (image based scheme) or pure recall-based (grid based scheme.

3.1 Recognition Based Techniques:3.1.1Dhamija and Perrig

Dhamija and Perrig [4] proposed a graphical authentication scheme based on the Hash Visualization technique. In their system Figure 2: the user is asked to select a certain number of images from a set of random pictures generated by a program later the user will be required to identify the pre selected images in order to be authenticated. A weakness of this system is that the server needs to store the seeds of the portfolio images of each user in plain text. Also, the process of selecting a set of pictures from the picture database can be tedious and time consuming for the user.

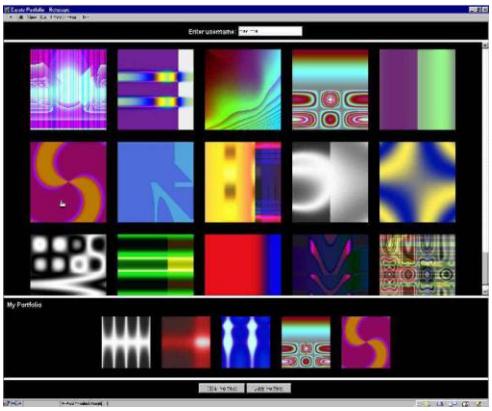

Figure 2: Random images used by Dhamija and Perrig

Akula and Devisetty's algorithm [5] is similar to thetechnique proposed by Dhamija and Perrig .the images willbe converted into hashing code using SHA-1 techniques togive more secure and less memory. In this Techniqueproduces a 20 byte output.Both the above algorithms are prone to shouldersurfing attacks.

3.2.2 Hong's Methods

Hong, et al. [7] proposed another shoulder-surfing resistant algorithm. In this approach to allow the user to assign their own codes to pass-object variants. Figure 3: shows the log-in screen of this graphical password scheme. However, this method still forces the user to memorize many text strings and therefore suffer from the many drawbacks of text-based passwords.

Figure 3: Hong's al 's Shoulder surfing resistant

3.3 Recall based techniques:

In this section we discuss recent there types of click based graphical password techniques:
1. Pass Points (PP)
2. Cued Click Points (CCP)
3. Persuasive Cued Click- Points (PCCP)

3.3.1 Pass point (PP)

Based on Blonder's original idea [7], Pass Points (PP) [7] is a click-based graphical

password system where a password consists of an ordered sequence of five click-points on a pixel-based image as shown inFigure.4 To log in, a user must click within some system-defined tolerance region for each click-point. The image acts as a cue to help users remember their password click-points.

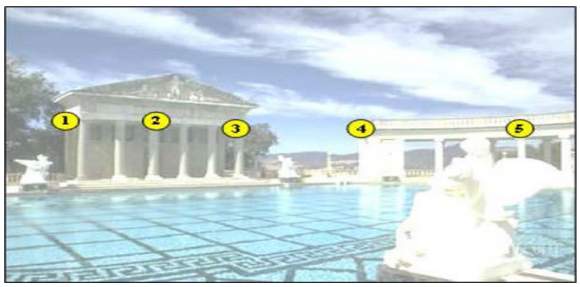

Figure: 4 Pass Points

3.3.2 Cued Click Points (CCP)

CCP [1] was developed as an alternative click based graphical password scheme where users select one point per image for five images Figure.5: The interface displays only one image at a time; the image is replaced by the next image as soon as a user selects a click point. The system determines the next image to display based on the user's click-point on the current image. The next image displayed to users is based on a deterministic function of the point which is currently selected. It now presents a one to-one cued recall scenario where each image triggers the user's memory of the one click-point on that image. Secondly, if a user enters an incorrect click-point during login, the next image displayed will also be incorrect. Legitimate users who see an unrecognized image know that they made an error with their previous click-point. Conversely, this implicit feedback is not helpful to an attacker who does not know the expected sequence of images.

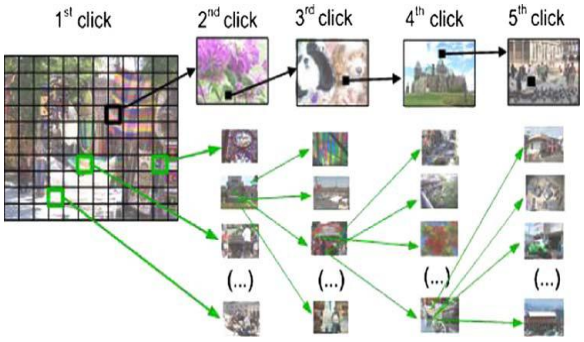

Figure 5:-Cued Click point.

3.3.3 Persuasive Cued Click- Points (PCCP)

To address the issue of hotspots, PCCP was proposed [7]. As with CCP, a password consists of five clickpoints, one on each of five images. During password creation, most of the image is dimmed except for a small view port area that is randomly positioned on the image as shown in Figure. 6. Users must select a click-point within the view port. If they are unable or unwilling to select a point in the current view port, they may press the Shuffle button to randomly reposition the view port. The view port guides users to select more random passwords that are less likely to include hotspots. A user who is determined to reach a certain click-point may still shuffle until the view port moves to the specific location, but this is a time consuming and more tedious process.

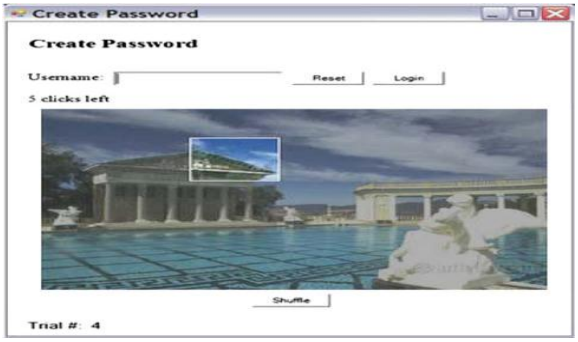

Figure 6: the PCCP password creation interface

4. Discussion:

"Will Graphical passwords circumvent Text basedpasswords?"

Here we briefly exam some of the possible techniques for breaking graphical passwords and try to do a comparison with text-based passwords.

• Dictionary attacks

Since recognition based graphical passwords involve mouse input instead of keyboard input, it will be impractical to carry out dictionary attacks against this type of graphical passwords. For some recall based graphical passwords [11], it is possible to use a dictionary attack but an automated dictionary attack will be much more complex than a text based dictionary attack. More research is needed in this area Overall; we believe graphical passwords are less vulnerable to dictionary attacks than text-based passwords.

• Guessing

Unfortunately, it seems that graphical passwords are often predictable, a serious problem typically associated with text-based passwords. More research efforts are needed to understand the nature of graphical passwords created by real world users.

• Shoulder Surfing

Like text based passwords, most of the graphical passwords are vulnerable to shoulder surfing. At this point, only a few recognition-based techniques are designed to resist shoulder-surfing.

• Spy ware

Except for a few exceptions, key logging or key listening spy ware cannot be used to break graphical passwords. It is not clear whether "mouse tracking" spy ware will be an effective tool against graphical passwords. However, mouse motion alone is not enough to break graphical passwords. Such information has to be correlated with application information, such as window position and size, as well as timing information.

• Social engineering

Comparing to text based password, it is less convenient for a user to give away graphical passwords to another person. For example, it is very difficult to give away graphical passwords over the phone. Setting up a phasing web site to obtain Graphical passwords would be more time consuming.

5. Proposed System

Now-a-days, all business, government, and academic organizations are investing a lot of money, time and computer memory for the security of information. Online password guessing attacks have been known since the early days of the Internet, there is little academic literature on prevention techniques. This project deals with guessing attacks like brute force attacks and dictionary attacks.

This project proposes a click-based graphical password system. During password creation, there is a small view port area that is randomly positioned on the image. Users must

select a click-point within the view port. If they are unable or unwilling to select a point in the current view port, they may press the Shuffle button to randomly reposition the view port. The view port guides users to select more random passwords that are less likely to include hotspots. Therefore this works encouraging users to select more random, and difficult passwords to guess.

Brute force and dictionary attacks on password-only remote login services are now widespread and ever increasing. Enabling convenient login for legitimate users while preventing such attacks is a difficult problem. Automated Turing Tests (ATTs) continue to be an effective, easy-to-deploy approach to identify automated malicious login attempts with reasonable cost of inconvenience to users.

This project proposes a new Password Guessing Resistant Protocol (PGRP), derived upon revisiting prior proposals designed to restrict such attacks. While PGRP limits the total number of login attempts from unknown remote hosts, legitimate users in most cases (e.g., when attempts are made from known, frequently-used machines) can make several failed login attempts before being challenged with an ATT.

This proposed system also provides protection against key logger spy ware. Since, computer mouse isused rather than the keyboard to enter our graphicalpassword;this protects the password from key loggers.

5.1 Proposed System Architecture

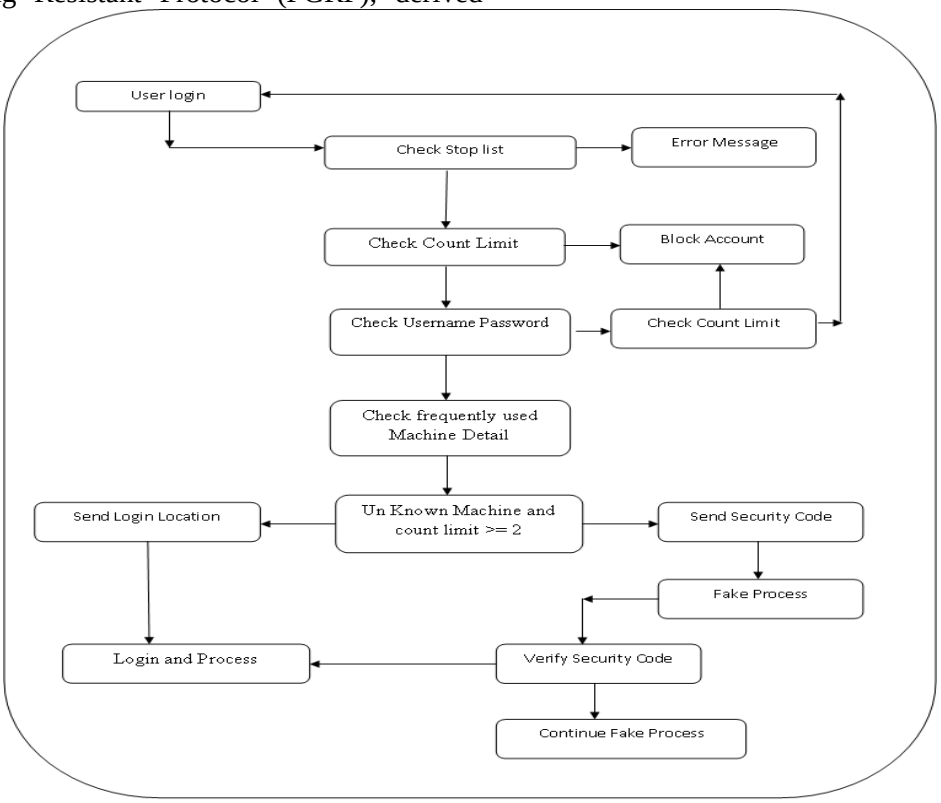

Figure: 7System Architecture

6. Conclusion and future work

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. Online password guessing attacks on password-only systems have been observed for decade's .Present-day attackers targeting such systems are empowered by having control of thousand to million node botnets. In previous ATT-based login protocols, there exists a security-usability trade-off with respect to the number of free failed login attempts (i.e., with no ATTs) versus user login convenience (e.g., less ATTs and other requirements). In contrast, PGRP is more restrictive against brute force and dictionary attacks while safely allowing a large number of free failed attempts for legitimate users. PGRP is apparently more effective in preventing password guessing attacks (without answering ATT challenges), it also offers more convenient login experience, e.g., fewer ATT challenges for legitimate users. PGRP appears suitable for organizations of both small and large number of user accounts.

REFERENCES

[1] Sonia Chiasson, P.C. van Oorschot, and Robert Biddle, "Graphical Password Authentication Using Cued Click Points" ESORICS , LNCS 4734, pp.359-374,Springer-Verlag Berlin Heidelberg 2007.

[2] Manu Kumar, Tal Garfinkel, Dan Boneh and Terry Winograd, "Reducing Shoulder-surfing by Using Gazebased Password Entry", Symposium On Usable Privacy and Security (SOUPS) , July 18-20, 2007, Pittsburgh,PA, USA.

[3] 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

[4] R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in *Proceedings of9th USENIX Security Symposium*, 2000.

[5] S. Akula and V. Devisetty, "Image Based Registration and Authentication System," in *Proceedings ofMidwes Instruction and Computing Symposium*, 2004.

[6] L. Sobrado and J.-C. Birget, "Graphical passwords," *The Rutgers Scholar, An Electronic Bulletin forUndergraduate Research*, vol. 4, 2002.

[7] Sonia Chiasson, Alain Forget , Robert Biddle, P. C. van Oorschot, "User interface design affects security: patterns in click-based graphical passwords", Springer-Verlag 2009.

[8] 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 USENIXSecurity Symposium*, 1999.

[9] S. Man, D. Hong, and M. Mathews, "A shoulder surfing resistant graphical password scheme," in *Proceedingsof International conference on security andmanagement*. Las Vegas, NV, 2003.

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

[11] 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 USENIXSecurity Symposium*, 1999.

[12] Alain Forget, Sonia Chiasson, and Robert Biddle,"Shoulder-Surfing Resistance with Eye-Gaze Entry in Cued-Recall Graphical Passwords", ACM 978- 1-60558-929-9/10/04, April 10 – 15, 2010.