Securing password against online password guessing attacks using graphical password.

Miss.Poonam M.Khairnar¹, Miss.Kirti K.Nagare², Miss.Ritika V.Agrawal³ & Miss.Ashwini U.Mahale⁴
¹,²,³&⁴Pune Vidyarthi Griha’s College of engineering (P.V.G.C.O.E) Nasik, Pune, India.

Abstract

Today’s remote login services are widely spread and ever increasing. So the different security issues are also increased, different attacks may increase like brute force attacks, dictionary attacks. Preventing such attack is a difficult problem. Automated Turing Test (ATT) is effective approach to minimize such attacks. But sometimes it may create inconvenience to the legal user; so to avoid such inconvenience we propose a new Password Guessing Resistant Protocol(PGRP), derived upon revisiting prior proposals designed to avoid such attacks. The Persuasive Cued Click Points (PCCP) password scheme which provides high level of security important goal of the authentication system is to provide support to users in selecting better passwords thus it increases security by expanding password space. Our method significantly decrease the disadvantages of the current authentication method that is being used.

Keywords: PGRP, Brute Force Attack, Dictionary Attack, ATT, Authentication.

1. Introduction

Now-a-days, all business, government, and private organizations are spending lots of money, time, efforts and computer memory for the security of data. Online password guessing attacks have been known since the early days of the Internet, there is literature on prevention technology. This paper deals with guessing attacks like brute force attacks and passive attacks. In that we propose system is a click-based graphical password. During the password creation time, there is a small view port area that is randomly generated on the image. Users must select a click-point within the view port area. If they are unable to select a point in the view port, they may press the Shuffle button to randomly rehanged the view port area. The view port gives idea to users to select more different passwords that are less to include hotspots. Therefore this works encouraging users to select more various, and difficult passwords to guess. Brute force and dictionary attacks on password-only remote login services are now largely spread and also increasing. Enabling convenient login for legal users while preventing such attacks is a difficult problem. This project propose a new Password Guessing Resistant Protocol (PGRP), based upon revisiting prior proposals designed to avoid such attacks. While PGRP limits the total number of login attempts from unknown remote system (hosts). This proposed system also prevents the key logger spy ware. Since, computer mouse is used rather than the keyboard to enter our graphical password; this prevents the password from key loggers.

We propose is to decrease the guessing attacks as well as motivate users to select more random and difficult passwords to guess. The proposed system work by using persuasive cued click points and password guessing resistant protocol.

2. Objective

- To identify System(Unknown and Known system)
- To provide Security using Graphical password
- To validate the user using authentication system
- PGRP protocol should make brute force and dictionary attacks ineffective for opponents.
- The major objective of this work is to decrease the guessing attacks as well as encouraging users to select more random, and difficult passwords to guess

3. Existing System

Existing approaches to users often create small and easy passwords that are easy for attackers to guess, but system-assigned passwords are very difficult for users to remember hence generally user choose simple password. Despite the vulnerabilities, it’s the user natural tendency of the users that they will always prefer to go for simple passwords for ease of memorizing, thats why the small passwords are easily crack by attacker and
also lack of awareness about how attackers tend to make attacks. This password are easily crack by several simple means such as masquerading (pretend), Eaves dropping and other dictionary attacks, shoulder surfing attacks, social engineering attacks. Also Pinkas algorithm allows attackers to eliminate 94 percent of the password space without answering any ATTs.

4. Proposed System

![Proposed Architecture]

5. System Modules
   a. Password Guessing Resistant Protocol (PGRP)
   b. Points (PP)
   c. Cued Click Points (CCP)
   d. Persuasive Cued Click-Points (PCCP)
   e. Audio Graphical Password (AGP)

   a. Password Guessing Resistant Protocol (PGRP)
   This protocol reduces users inconvenience in the login process. This protocol has a white list of IP addresses for known user. If a user sees that unauthorized person has tried to log in to his account and have made failed login attempts then the administer can add that IP address to the blacklist. This list may be made only by tracking the log information. This protocol also checks the number of failed login attempts from unknown system. If the login attempts are more then it blocks the user.

   b. Pass point (PP)

   ![Pass Point]

   Pass Points (PP) is a click-based graphical password system. In this a password consists of sequence of five click-points on a pixel-based single image. To log in, a user must click within some system-defined tolerance value/area/region for each click-point. The image more easy to help users remember their password click-points. The tolerance region is the degree of closeness to the actual click point. Users must click on that nearby point to get actual click point.

   c. Cued Click-Point (CCP)

   ![Cued Click Point]

   CCP was developed as an optional click based graphical password technique. In which users select one point on each image. This displays only one image at a time; the image is replaced by the
next image when a user selects a correct click point. The system generates the next image to show on the basis of user’s click-point on the current image. The next image displayed to users is based on an accurate function of the click point which is currently selected by user. If a user enters an incorrect click-point during the login process, the next generated image will also be incorrect. Legal users who see an unrecognized (incorrect) image able to understand that they made an error with their previous click-point on image.

d. Persuasive Cued Click-Points (PCCP)

This proposes to indicate the drawback of hotspots. As in the CCP, a password consists of five click points, one on each of five images. During the password creation process, most of the image is mad except for a small view port area that is different positioned on the image.

Users must select a click-point within the view port area. If they are not able to select a point in the current view port area, they may press the Shuffle button to randomly change the view port. The view port gives idea to users to select more random passwords that are less likely to include hotspots. A user whose goal is to reach a particular click-point may still exchange until the view port moves to the particular location, but this method is so time consuming and more inconvenient process.

The overall studies of the PCCP method show that remembrance of the graphical password is much easier than the text-based passwords method.

e. Audio graphical password(AGP)

In this method, User Select the Audio as password like any song. In this we playing the audio or song at time of registration of user at that time we have play button. If We click on that play button then song is playing, after some period of time, click on start button then we get First starting point after that clicking on stop button we get end point. Doing this entire thing, there is shuffle button, if we click on that the new image display and select four click points on that image. It means that the AGP algorithm is also uses the PCCP protocol for selecting click point as password.

6. Conclusion

Persuasive cued click point scheme is effective for large password space over alphanumeric passwords. In that we also show the working of Pass points, Cued Click points, and Audio graphical passwords. There is a increasing 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 decades. In contrast, PGRP is more restrictive against Active attacks and passive attacks while safely allowing a large number of free failed attempts for legitimate users. PGRP is more efficient in preventing password guessing attacks, it also increase more convenient login experience.

7. References


