ISSN: 2321-7782 (Online)
Volume 4, Issue 3, March 2016
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Online Security Based On Graphical Authentication and Persuasive Cued Click Points

Prasad Baban Panmand[1]
B.E (Computer Engg)
G.H.Raisoni COEM,
Ahmednagar, India

Sandeep Vilasrao Shitole[2]
B.E (Computer Engg)
G.H.Raisoni COEM,
Ahmednagar, India

Mahesh Ashok Kakade[3]
B.E (Computer Engg)
G.H.Raisoni COEM,
Ahmednagar, India

Devndra Pandurang Thombare[4]
B.E (Computer Engg)
G.H.Raisoni COEM,
Ahmednagar, India

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 goal for authentication systems is to support users 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 now days researchers have develop alternative methods where in 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, Graphical Authentication 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.

Keywords: Access protection, displays and images, Graphical user Interface Languages, Security Services, Graphical or visual Password, Authentication.

I. INTRODUCTION

To start with we tend to target the most common computer authentication methodology that creates use of text passwords. Despite the vulnerabilities, it’s the user natural tendency of the users that they're going to forever prefer to select short passwords for easy remembrance and also lack of awareness regarding however attackers tend to attacks. To mitigate the issues with ancient strategies, advanced strategies have been projected using graphical as passwords.

II. MOTIVATION

User-name password is one amongst the foremost wide used authentication system for long. During this system, end user provides user-name and password at the login screen and system varies an equivalent. Outcome of the system may be binary either true or false, authenticated or not authenticated, success or failure. Different to username and password primarily authentication system is biometric system and smart card based system. Biometric system provides higher security however needs a further hardware which will increase the value. This additionally raises the question regarding a day usability and attractiveness. Additionally some biometric systems like iris scan are intrusive in nature to capture authentication knowledge.

Other different may be a smart card primarily based system. However smart card is often simply lost or purloined. So several good cards primarily based systems use data based authentication systems to forestall impersonation through loss of card or larceny of card. In spite of common use and recognition of user-name and password primarily based system, its multiple shortcomings. Since the authentication information is often fashioned from a group of characters like combination of upper-case letter, lowercase, numerals, special characters etc., it's subjected to brute force attack or dictionary attack. Choice of password plays an awfully necessary role for providing strength to the protection of the system. If the password selected is dictionary word like apple or some common passwords like pass123 etc., password are often simply guessed by the attacker and system are often simply compromised. To overcome this downside several organizations have password policy that enforces the principles for the formation of strong password and regular amendment of password. In several things this has unsuccessful as a result of users merely build a variation of recent password or write down password or swap them with their friends or family. All this solutions don't remedy the most explanation for password insecurity that is the human limitation in terms of memory for secures passwords.

Many times people communicate or share their password with others for multiple reasons. This weakens the protection of the organizations. Hence, the passwords are expected to comply with 2 convicting needs, namely:

1. Passwords ought to be simple to recollect, and also the user authentication protocol ought to be feasible quickly and simply by humans.

2. Passwords should be secure, i.e., they must look random and may be exhausting to guess; they must be modified frequently, and may totally different on different accounts of an equivalent user; they must not be written down or hold on in plain text.

Meeting these convicting needs is nearly not possible for humans, with the result that users compensate by creating weak passwords and handling them in an insecure method. Several issues that users have with alphamerical passwords are associated with memorability of secure passwords. In an attempt to form additional unforgettable passwords, graphical password systems have been devised. In these systems authentication is based on clicking on pictures instead of typing or writing alphanumeric strings. Many forms of graphical passwords are fabricated. Here we've created a replacement reasonably graphical password system, referred to as Persuasive Cued Click Points and Graphical Authentication and have used it as an authentication mechanism into the system.

III. Literature Survey

Sr. No.	Title	Author	Publication	Year
1.	”Defence Against Large Scale Online Password Guessing Attacks By Using Persuasive Click Points”	Abdul Rasheed. Madhava Naidu	International Journal of Engineering Science & Advanced Technology	2014
2.	Persuasive Cued Click-Points: Design, implementation, and evaluation of a knowledge-based authentication mechanism	Sonia Chiasson, P.C. van Oorschot, Robert Biddle	IEEE	2011
3.	Authentication Schemes for Session Passwords using Colour and Images	M Sreelatha , M Shashi, M Anirudh, MD Sultan Ahamer, V Manoj umar	IJNSA	2011
4.	Secure User Authentication & Graphical Password using Cued Click-Points	Miss. Saraswati, B.Sahu, Prof. Angad Singh	IJCTT	2014

TABLE I: Literature Survey

IV. Problem Statement

There has been a good deal of hype for graphical passwords since two decade as a result of the actual fact that Primitives strategies secured from Associate in Nursing numberless range of attacks that may be obligatory easily. Here we are going to progress down the taxonomy of authentication strategies. To begin with we tend to specialize in the most common computer authentication methodology that creates use of text passwords. Natural tendency of human in case of choosing text password is short in length also easy to remember. By choosing such type of text password it can be easily crack by using dictionary attacks, shoulder surfing attacks, social engineering attacks. To solve such type of issues with old strategies, advanced strategies are planned using graphical as passwords.

V. Goals and Objectives

An important usability goal for authentication systems is to support users in choosing better passwords. Users often produce unforgettable passwords that are simple for attackers to guess, however strong system-assigned passwords are troublesome for users to recollect. Therefore we've gone for different strategies whereby graphical footage is used as passwords. Graphical passwords basically use pictures or illustration of pictures as passwords. Human brain is sweet in remembering image than matter character. The main goal of this work is to cut back the dead reckoning attacks further as encouraging users to pick additional random and difficult passwords to guess. Well known security threats like shoulder surfing attacks, brute force Attacks and lexicon attacks are with success abolished using this technique.

1. Human brain is sweet in remembering image than matter character that's why we tend to develop the Graphical password pattern.

2. Guessing the graphical password is just too tough.

VI. Proposed Approach

Now days in most of all fields investing a lot of money, time and computer memory for the security of information. This project deals with guessing attacks like brute force attacks and dictionary attacks. This project proposes a click-based and pixel matching graphical password. 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. Also in previous PCCP system there is pass point system were present.

In that case it is not easy to remember. To overcome such remembrance problem we are developing new system called as Graphical Authentication system.

VII. Modules of the System

A. Graphical Authentication

Graphical Authentication is new method of graphical password. It allows you to use a combination of (0 to9) number and picture to unlock your device instead of typing a password. You'll be show a picture and a grid of random number which is created on transparent image. To unlock system, tap anywhere on screen and drag number grid until your number is on top of selected spot on normal image. In this we are going to match the two image's grid coordinate with each other and whenever the appropriate match will found the system gets unlocked. We are providing to user a grid of numbers with transference image to see background image. When user matching the selected position of images with number on transparent image then database check coordinate of grid in normal image with number. If the match found then and then only the system is getting unlocked. For matching two images we are providing the transparent image to move over the background image.

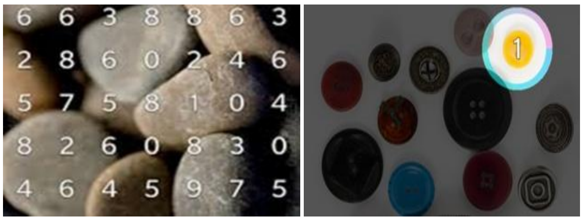

Fig. 1:Sample Image

B. Cued Click Points Module

Cued Click Points (CCP) was developed as click based graphical password theme wherever users choose one purpose per image for 3 pictures. The interface displays just one image at a time; the image is replaced by subsequent image as soon as a user selects a click point. The system determines subsequent image to show, supported the users click-point on the present image. Subsequent image exhibited to users is based on a settled perform of the purpose that is presently selected. It currently presents a one to-one cued recall situation wherever every image triggers the user’s memory of the one click-point on that image. Secondly, if a user enters an incorrect click-point throughout login, subsequent image displayed will be incorrect. Legitimate users who see an unrecognized image recognize that they created a mistake with their previous click-point. Also at each click show combination of alphabet, number, symbols due to that it is easy to remember the click.

C. Persuasive Cued Click- Points Module

To address the problem of hotspots, Persuasive Cued Click Points (PCCP) was planned. Like CCP, a password consists of three click points, one on every of three pictures. Throughout password creation, most of the image is dimmed except for a little view port space that's randomly positioned on the image. Users should choose a click-point inside the view port. If they're unable or unwilling to pick out some extent within the current view port, they will press the Shuffle button to randomly reposition the view port. The view port guides users to pick out a lot of random passwords that are less seemingly to incorporate hotspots. A user who is decided to succeed in an exact click-point should shuffle till the view port moves to the specific location, however this is a time intense and a lot of tedious process.

VIII. Conclusion

The goal of a good authentication system is to supply a maximized of effective and secure password space. We are combining these three modules to achieve high security. Here during this system the click point on the image has the scope of the view port area and since the view port can't be exploited, the password created is going to be strong. The graphical click point and Graphical Authentication are a lot of random and robust, in order that no hacker will guess it, however simple to recollect. The safety strength is determined by the user himself, depending upon the requirement a significant advantage of Persuasive cued click point scheme and Graphical Authentication is its massive password space over alphanumeric passwords. There’s a growing interest for Graphical passwords since they're better than Text primarily based passwords, though the most argument for graphical passwords is that people are better at memorizing graphical passwords than text-based passwords. On-line password guessing attacks on password-only systems are observed for many years.

References

1. Abdul Rasheed, MadhavaNaidu.V and D.sunitha “Defence Against Large Scale Online Password Guessing Attacks By Using Persuasive Click Points” International Journal of Engineering Science & Advanced Technology 2014

2. Sonia Chiasson, P.C. van Oorschot, and Robert Biddle “Persuasive Cued Click-Points: Design, implementation, and evaluation of a knowledge-based authentication mechanism”, publications [1]–[5]. Copyright held by the IEEE.2011

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. M. Sreelatha, M. Shashi, M. Anirudh, MD Sultan Ahamer, V. Manoj umar “Authentication Schemes for Session Passwords using Colour and Images” at IJNSA 2011.

5. S. Akula and V. Devisetty “Image Based Registration and Authentication System,” in Proceedings of Midwes Instruction and Computing Symposium, 2004.

6. L. Sobrado and J.-C. Birget “Graphical passwords”, The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4, 2002.