Multifactor Graphical Password Authentication

Shubhangi Agarwal

***Abstract*— Alphanumeric Passwords have been used since decades for gaining access to any system. The major problem with alphanumeric passwords is that they are confusing, random appearing. People tend to forget these easily. So create short, simple, and insecure passwords which can be remembered. From studies it has been found that they are vulnerable to attacks. In this paper we discuss Graphical passwords which have been designed to make passwords more memorable, easier for people to use. These are found to be safer and less vulnerable Using a graphical password, users click on images rather than type alphanumeric characters. We have designed a two level authentication system in which the user creates a graphical password as well as a code is generated and sent to the handheld device for authentication. User must clear both levels .Our approach can be leveraged by many organizations as it is more secure due to two level authentication with both levels being equally hard to crack.**

***Index Terms*— Graphical Password, Handheld Device, Two level authentication**

I. INTRODUCTION

Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. System security can be provided by identification and authentication of a person. This is implemented by password system. Here comes the common password problem, which says, firstly, passwords should be easy to remember and secondly, they should be secure, i.e., they should appear random and should be hard to guess; and should be different on different accounts of the same user and they should be changed frequently, They should not be written down or stored in plain text.

Classical studies have shown that, human users tend to choose and handle alphanumeric passwords very insecurely .Graphical passwords provide a promising alternative to traditional alphanumeric passwords. Graphical passwords are more likely to be recognized and remembered by the human brains as they are presented as pictures rather than as words.
Multifactor authentication is provided by a module for sending a code to handheld device which is a text .A user is logged in if and only if both levels are passed.

II. BACKGROUND

The problems with alphanumeric passwords is that people tend to forget the password. If the account is not used frequently then the password is more susceptible to forgetting.

Manuscript received May 04, 2014.
Shubhangi Agarwal,*VIT University*

Studies reveal people keep name of their family members, pets, Date of birth as their passwords which are easily guessable. They give least priority to security. If the users keep long and hard passwords they tend to forget. Hence, they keep simple, easy, and short passwords which can be easily cracked by keyboard sniffers and using dictionary attacks.

Graphical Passwords with multifactor authentication provides a solution to this problem. Studies have shown graphical passwords are easy to remember comparatively. A sequence of pictures is easy to remember as compared to remembering a sequence of random characters. Pictures are independent of users surrounding and hence difficult to guess. There do not exist yet special dictionaries for a dictionary attack and it is very difficult to be constructed.

(Especially for graphical passwords that have a very large password space). Automated attacks are difficult to take place.

Graphical password Techniques

1. Dhamija and Perrig proposed a graphical authentication scheme based on the Hash Visualization technique. In their system, the user is asked to select a certain number of images from a set of random pictures generated by a program.
2. Sobrado and Birget developed a graphical password technique that deals with the shoulder-surfing problem. To be authenticated, a user needs to recognize pass-objects and click inside the convex hull formed by all the pass-objects.
3. In their second algorithm, a user moves a frame (and the objects within it) until the pass object on the frame lines up with the other two pass-objects. The authors also suggest repeating the process a few more times to minimize the likelihood of logging in by randomly clicking or rotating. The main drawback of these algorithms is that the log in process can be slow.

III. OUR APPROACH

Password Generation- The graphical password interface allows the user to choose an image of his choice. User is given a checkbox list from where he can choose image of his choice. This level employees three steps, in each step the user is supposed to choose an image and a point on that image. The user has the freedom of changing the image after selection of even one point per image. This makes the system more secure. A confirmation code is sent to the handheld device. For the second level of authentication the user is supposed to enter a confirmation code. If the entered code

matches with the generated code then the user is logged in to the system.

Account authentication-For accessing the account, firstly the user is supposed to provide his correct username. If the username is found registered then the image is displayed to the user. The user is supposed to click in the region, if the point clicked lies in the region then the next image is displayed and the process is repeated three times. After the first level of authentication is cleared, user has to enter a confirmation code which has been sent to handheld device. If they match then the account is authenticated.

IV. Implementation

1. As a proof of concept, we developed a web-based authentication system based on Microsoft .NET technology.
2. The clickable areas are implemented using widely deployable browser-independent server-side HTML.
3. Every point that is clicked, the coordinate of the point is recorded for future purpose. The points help in generation of password.

We implemented a prototype of the direct communication .When the image is displayed and the authentication login is done, verification code is sent to the email id/phone of the authenticator which secures the login of the user.

LoginPage

Registration Page

V. Usability

This model can be implemented anywhere on any webpage that wants a user interaction in safe and secure manner by multi-level authentication. It is designed in a user friendly format it can be used by social networking sites, blogs, any kind of online accounts .It can be run on local networks as well.

VI. Research work and future scope

The core element of computational trust is identity. Currently many authentication methods and techniques are available but each with its own advantages and shortcomings. There is a growing interest in using pictures as passwords rather than text passwords but very little research has been done on graphical based passwords so far. In view of the above, we have proposed authentication system which is based on graphical password schemes. Although our system aims to reduce the problems with existing graphical based password schemes but it has also some limitations and issues like all the other graphical based password techniques. To conclude, we need our authentication systems to be more secure, reliable and robust as there is always a place for improvement. In future some other important things regarding the performance of our system will be investigated like User Adoptability and Usability and Security of our system.

1. We can make users upload their own image of password creation
2. User can be given a choice for creation of his/her own technique

A) Pass point
B) Face recognition
C) Creating a secret code and generating a private or public key for better security

3. Implementation on other devices as well.

VII. Conclusion

In this brief paper, we have considered the nature of graphical passwords, and how they might be adapted for greater accessibility. We have introduced a new technique to graphical password creation with a multi factor authentication process. We have used handheld device for second level authentication which provides a very secure way of authentication. These features are the ease of use and creation which means that the use of the system to choose the password can be done easily and the creation of the password is easy also that indicate that the password chosen can be done without any complication such as using the mouse or keyboard to choose the password and navigation throw the system easily done and the user should be satisfied by using the new system to create the password, where the second feature is the ease to memory or to memorize the password that the user have chosen which mean that the user can easily memorize the faces or pictures used as password. The proposed method is more secure and reliable than alphanumeric password authentication. Automated attacks are difficult to take place. It is more difficult to break this graphical password authentication using the traditional attack methods such as: Brute force search, dictionary attack or spyware.

References

1. http://www.slideshare.net/akhilrocker143/558-11294069

2.http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5749855