RESEARCH ARTICLE OPEN ACCESS

An Improving Method of Grid Graphical Password Authentication System

M.Thirunavukkarasu
Department of Computer Science and Engineering SCSVMV University,

ABSTRACT
Security in the computer is largely supported by passwords for authentication process. Alphanumeric passwords still remain as the most common Authentication method. This conventional authentication method has been shown to be susceptible security threats such as phishing attack, brute force attack, dictionary attack, spyware attack etc. To overcome the vulnerabilities of traditional methods, a numerous graphical password authentication systems have been designed. These graphical passwords are usually seen as complex and time consuming. Furthermore, the existing graphical passwords are susceptible to spyware and shoulder surfing attacks. In this system we propose this 2 step random colored grid graphical password scheme to abolish the above mentioned well known security threats. Considering the drawbacks of the existing graphical password systems, we have proposed a robust graphical password scheme, which is highly adaptable for traditional desktop systems, smart phones and other web applications
Keywords: Graphical Password.

I. 1.INTRODUCTION

The main objective of this system is to introduce a process by which system verifies the identity of a user. Authentication is the main step of any security system. Text passwords remain the most common method for several reasons. Graphical password authentication is a technique in which graphics (images) are used instead of alphanumerical passwords Graphical passwords are much easier to remember, they provide high level of security. We applied this approach to propose a novel two step authentication graphical password scheme. This can be achieved by asking the user to select patterns from an image rather than typing characters as in alphanumeric password approaches.

II. EXISTING WORK

User authentication is a fundamental component in most computer security contexts. It provides the basis for access control and user accountability. While there are various types of user authentication systems, Alphanumerical passwords are required to satisfy two contradictory requirements. They have to be easily remembered by a user, while they have to be hard to guess by impostor.

Users are known to choose easily guessable and/or short text passwords which are an easy target of dictionary and brute-forced attacks. Enforcing a strong password policy sometimes leads to an opposite effect, as a user may resort to write his or her difficult to remember passwords on sticky notes exposing them to direct theft .Several techniques have been proposed to reduce the limitations of alphanumerical password. Graphical passwords refer to using pictures as passwords. In theory, graphical passwords are easier to remember, since humans remember pictures better than words. Also, they should be more resistant to brute force attacks, since the search space is practically infinite. In general, graphical passwords techniques are classified into two main categories:

1. Recognition-based and
2. Recall based

In recognition-based techniques, a user is authenticated by challenging him/her to identify one or more images he or she chooses during the registration stage.

In recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage.

2.1 DRAWBACKS OF THE EXISTING SYSTEM

In this systema robust graphical password scheme, which is highly adaptable for traditional desktop systems, smart phones and other web applications? This random coloured grid graphical password authentication scheme shows promise as a usable and memorable authentication mechanism.
Graphical password authentication can be achieved by asking the user to select patterns from an image rather than typing characters as in alphanumeric password approaches. In future it has great scope. It can be used everywhere instead of text-based password .We can increase the security of this system

by increasing the number of levels used, the number of tolerance squares used.

III. PROPOSED SYSTEM

Our proposed system consists of 2 phases. The first phase is the user registration phase and the second phase is the authentication phase.

Phase 1:

In this registration phase user enters his desired username and an alphanumeric password. After that user need to another password called pattern password. In that user need to enter the password in capital letters. Both the passwords should contain minimum six characters. Along with the setting up of passwords user need to answer for security questions, useful in case of forgotten case.

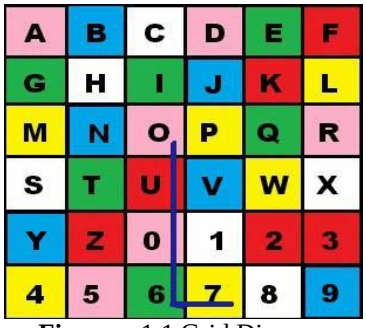

Figure – 1.1 Grid Diagram

Phase 2:

In this phase (authentication phase) user will be authenticated in 4 steps.

Step 1: User enters his username

Step 2: A 6*6 grid is shown to the user. User has to enter the first letter of the colour of the squares in which his password letters lie.

Step 3:In this step another 6*6 grid is shown to the user. User has to enter the first letter of the colour of the squares through which his imaginary pattern line passes.

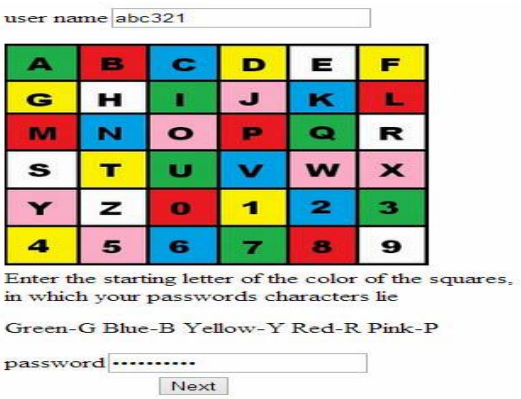

Figure – 1.2 Grid Diagram for User Name

Step 4:In this step verification of the password and security code is carried out by conducting a comparison in the background . For every login attempt step 2 and step 3 are carried out for the original password and security code which were set at registration phase. If the starting letters of the colours of the squares entered by the user matches with the starting letters of the colours of the squares generated in the background for the same grids, user will be granted access.

The squares of 6*6 grids shown to the user contain 26 alphabets and 0-9 numerals. The squares of the grids are randomly colored using 6 different colors (Red, Blue, Green, Yellow, White and Pink).

For each login attempt the colors squares of the grid are randomized, but the letters and numbers are places in an order for the convenience of the user. As the user enters the first letters of the colors there is no chance of phishing and shoulder surfing. Even if the intruder knows the color of the square through phishing or some spyware, he can't identify the exact password and security code since there will 6 same colored grids containing different characters. To increase the security levels the user is supposed to choose passwords which are at least 6 characters long.

3.1 ADVANTAGES OF PROPOSED SYSTEM

Dictionary Attacks

Graphical passwords are less vulnerable to dictionary attacks. In our proposed system, as the user enters only the starting letters of the colours, it will be impractical to carry out dictionary attacks against this graphical password method.

Guessing Attacks

Guessing attack is another eminent strategy used by the intruders. Even if the attacker tries to guess the password, the security code used in our proposed system makes our system resilient against guessing attacks since user has a chance to select an imaginary pattern of his own choice. Even if the attacker tries on guessing the colors it would be of no use since the colours of the squares get changed for every login attempt. Hence the probability of guessing attacks is very low.

Spyware attacks

Excluding a few exception, key loggers and screen loggers cannot be used to attack against this method. By using a key logger if the attacker knows the colours of the squares in which the password characters lie, it would be of no use to him since there will be another 5 characters lying inthe same colours. The colours of the squares of the grid will be randomized for the next attempt he tries. Hence our proposed system is resistant to spyware attacks.

Shoulder surfing

Unlike recognition based graphical passwords, recall based graphical passwords are more resistant to shoulder surfing. In the proposed system, even if the peepers observes the colours of the square in which the password character lies, he cannot identify the exact password character since the user enters the first letter of the colours of the square (not the actual character).Thus proposed system is resilient to shoulder surfing attacks.

Social Engineering

Compared to ordinary alphanumeric passwords, it is inconvenient for a user to give his graphical password to another person. Hence graphical passwords are less susceptible to social engineering attacks.

Phishing Attacks

Phishing attacks are easily done in web applications. A phishing website can easily copy the login page from a legitimate site, including the area for entering the graphical password. In the proposed system when the users enters their username and the starting letters of the colours of the squares in the phishing site this entire information is sent to the attacker. Even if the attacker knows the colours of the grids he cannot identify the exact code since there will be 5 other characters residing in the same coloured grid.

IV. SYSTEM DESIGN STRUCTURE

It is a three-tier (layered) architecture is a client-server architecture in which the user interface and data storage and data access are developed and maintained as independent.The Architecture of Outing pass management system is based on three-tier architecture. The three logical tiers are

- Presentation tier - HTML Web forms.
- Middle tier – JSP.
- Data tier- Database.

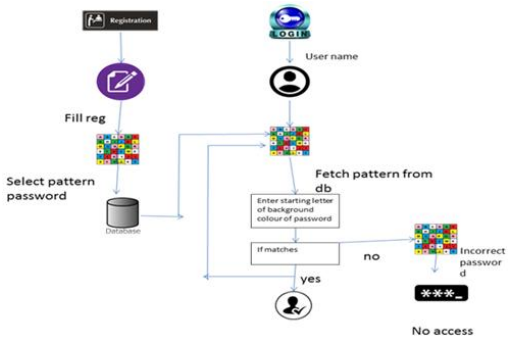

Fig.4.1 System Architecture

V. SAMPLE SCREENS

5.1 WELCOME PAGE

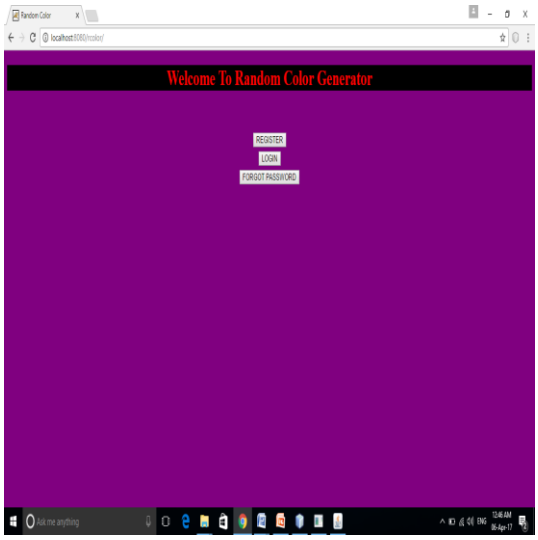

Fig 5.1 Welcome Page

5.2 REGISTRATION PAGE

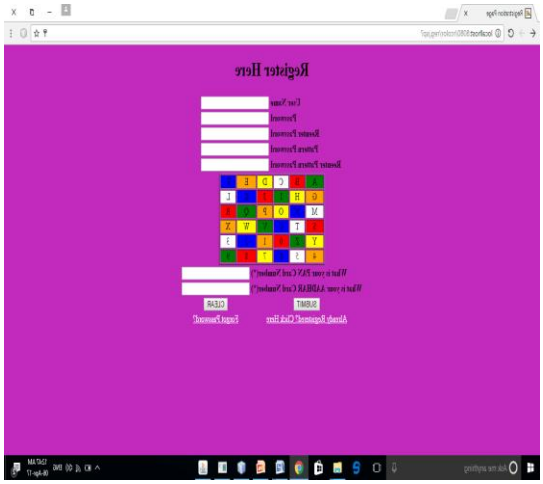

Fig 5.1 Registration Page

5.3 LOGIN PAGE

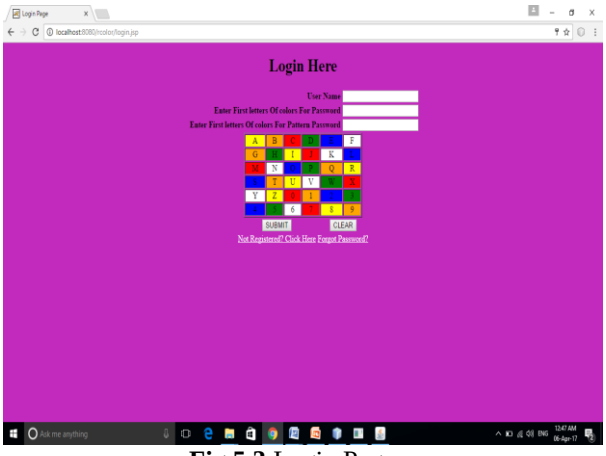

Fig 5.3 Login Page

VI. CONCLUSION

The expected product for this system is graphical password systems that are resistant to shoulder surfing. The objective of this system would be to strive to identify and study the pros and cons of existing graphical password system and to come out with a more comprehensive graphical passwords authentication system. It is also hopeful that the new system would be able to address the four problem identified earlier, which are difficulty in remembering of strong password, vulnerability of current method to shoulder surfing, insufficient passwords space or complexity and vulnerability of password to dictionary attack for easy to guess passwords. Other than the graphical passwords system, a printed user manual will also be provides as part of this system package into the one single application and in the local dialect of the rancher, then it is anything but difficult to use it.

VII. SCOPE OF THE SYSTEM

Graphical password authentication can be achieved by asking the user to select patterns from an image rather than typing characters as in alphanumeric password approaches. It can be used everywhere instead of text-based password. We can increase the security of this system by increasing the number of levels used, the number of tolerance squares used

REFERENCES

[1] K. Renaud, "Guidelines for designing graphical authentication mechanism interfaces," International Journal of Information and Computer Security, vol. 3.
[2] A. De Angeli, L. Coventry, G. Johnson, and K. Renaud, "Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems," International Journal of Human-Computer Studies, vol. 63, 2005
[3] S. Chiasson, P. van Oorschot, and R. Biddle, "Graphical password authentication using Cued Click Points," in European Symposium on Research in Computer Security (ESORICS), LNCS 4734, September 2007.
[4] Brostoff S. and Sasse M.A. *In People and Computers XIV – Usability or Else: Proceedings of HCI*. Sunderland, U.K, 2000.
[5] SobradoL&BirgetJ.(2007) *http://rutgersscholar.rutgers.edu/volume04/sobrbirg/sobrbi rg.htm*.
[6] Kerbroes: A Network Authentication System by Brain Tung.
[7] Adaptive Approach towards Authentication System by Papri Ghosh, Ritam Dutta
[8] http://www.jsptut.com/
[9] http://en.wikipedia.org/wiki/JavaServer_Pages
[10] http://www.oracle-dba-online.com
[11] Real User Corporation (2014) PassfacesTM, *http//:www.realuser.com*.