International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 02 | Feb 2019 www.irjet.net p-ISSN: 2395-0072

GRAPHICAL PASSWORD TO AVOID SHOULDER SURFING

Sumedh Kadge[1], Sanskar Pant[2], Moosa Khan[3], Yusuf Siddiqi[4]

[1,2,3,4]*Diploma in Computer Engineering, Thakur Polytechnic, Maharashtra, India*

ABSTRACT:- *Graphical password can be seen as one of the easy and secure solutions for computer security as opposed to textual passwords. Graphical passwords are said to be easy to access and remember which is why they are more preferable than textual passwords. It is also said to be the best alternative for alphanumeric passwords. In this paper, we are going to state a technique of graphical password to avoid shoulder surfing.We are going to propose an algorithm based on password selection of a different form or method so that it is not accessible or understandable to another person rather than you.There are a lot of methods of choosing a graphical password including images,graphical texts, different structures (grid,card etc)and according to these techniques, the password authentic level is declared.*

Key Words: shoulder surfing, graphical password, colour, clockwise and anticlockwise.

1.INTRODUCTION:

In this today's world computer has become a essential part of human life. We use computers in many places such as our mobile phones as well as banking system and highly confidential places too such as big company locker rooms etc. These worksites also used the textual passwords depends on their strength relate to their organisation but, these passwords can easily face attacks like intruders, spy, social engineering these are well known .The another schema of graphical passwords is biological passwords like retina scanner, fingerprint, eye scanner these are very secure than all the password techniques but, the major disadvantage of this system is that we cannot use this system everywhere because its costly and not anyone could afford it.

So, we are proposing a graphical password which will be used for highly confidential worksites and will be very cost efficient. By this technique the spy or a shoulder surfing attacker would not able to understand what's happening. That's why to protect the applications we are proposing a graphical password technique called GRAPHICAL PASSWORD TO AVOID SHOULDER SURFING which is more secure and cost efficient too.

1.1 SHOULER SURFING

Shoulder surfing, as defined in computer security, is a social engineering technique which is primarily used to obtain information, like for example, personal identification numbers (PINs), passwords and other confidential data by the means of looking over the individual's shoulder. This type of an attack or breach can be conducted either at a close range, that is, directly by looking over the particular individual's shoulder or at a longer range, that is, by using binoculars or another such hardware device as a means to obtain information. To be able to device such an attack, the attacker does not require any particular technical skills. The only resources the attacker needs are keen observation skills of the victim and his surroundings as well as the victim's typing speed and pattern. Shoulder surfing can be easier and more likely to conspire in crowded places. Apart from the threats that arise to passwords or PIN entry, it can also be used in day to day situations to unearth private information on devices such as mobile phones. Shoulder surfing is an issue that may lead to the leakage of sensitive personal and private information.

1.2 GRAPHICAL PASSWORD

Graphical password is seen as an important discovery and a very different yet easy option to passwords wherein the individuals are provided with a particular challenge to click on certain images as a way of authentication of themselves as opposed to typing their alphanumeric letters which are more prone to thefts. The graphical passwords are also said to be easier to remember, as it has been proved by the means of experimentation and study by science as well as psychological researches on the brain and memory functioning of humans that visual stimuli like pictures or other images are more easily retained in a person's memory as opposed to learning and remembering complex and lengthy letters set in an irregular pattern found in alphanumeric passwords.Thus, graphical or pictorial passwords are excellent techniques to be used as a means to overcome the limitations set by number or letter password techniques, pictures being easier to remember and recall. This is called as 'picture superiority effect.'

2. AIMS AND GOALS OF PROJECT:

Our aim with graphical password entering system is to provide security against shoulder surfing. We want that the secrecy of the confidential information of user should be maintained. User should not have to worry about people or camera devices while entering password. With this password entering system one can feel safe while entering the password even if there are untrustworthy people in the same room. The procedure of entering password will confuse the unwanted party and they can't figure out the password even if they are looking right at the pc screen.

Goals:

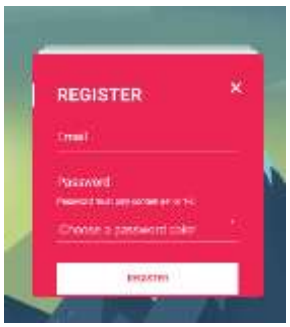
a. The user interface should be efficient and user friendly.
b. The password field should be accurate towards its specific username.
c. The colour selection mechanism should work properly.

3. PROPOSED SYSTEM:

Our group, while aiming to find a solution, thought of developing an application for confidential purposes like for example, banks or a company's confidential data. For a more secure level of protection of confidential information it is better to use a different kind of technique called graphical password rather than the traditional textual data. The Graphical password consists of a colour choosing mechanism and the architecture is mentioned below:

3.1 Architecture:

My project includes a registration window which will further include a username field, password field and a colour choosing field. And then only you can login to the system. Our method of entering the graphical password consists of a wheel which is further divided into 2 parts: inner circle which is circumcised inside an outer circle. Our wheel is divided into 8 equal parts. Each of these parts will contain 2 characters; one in the inner wheel and another one in the outer wheel. This wheel will contain randomly arranged numbers from 1-26 and alphabets A-h. Each party will be initially associated with a unique colour. We will be also having 4 buttons below the wheel. First 2 buttons will be controlling the rotation of colours from left to right and right to left. And other 2 buttons will be used to navigate between inner circle and outer circle.



4. IMPLEMENTATION METHOD:

To enter the password text user will already have a colour decided. User will place that colour on the character he has to enter with the help of the buttons provided below the wheel. If the user has to choose the character present in the inner

circle then he will have to press the 'inner circle' button and the same for outer circle. For placing the colour on the desired character the user will move the colour in the clock wise or anti clock wise direction with the help of 'Rotate Clock wise' and 'Rotate anti clock wise' button which are present below the wheel. By pressing 'Rotate clock wise' button all the colours will shift to the next segment of the wheel in the clock wise direction without changing their sequence and 'rotate anti clock wise' will do the same but in the anti clock direction. This will provide user a way for placing the colour in the same segment in which their character is present. Now after placing the colour in the same segment of the character the user have to choose that whether the character is present in the inner circle or outer circle. If the character is present in the inner circle, the user will press 'inner circle' button and the character whichever in present in the inner part of that segment will be entered. And if the desired character is present in the outer part of the segment then the user will press the 'outer circle' button to enter the character present in the outer part of the segment.

5. CONCLUSION:

In conclusion we would like to state that shoulder surfing is a great threat to one's security. Anyway we should always be careful while entering confidential data or it may get misused. We need to introduce more similar methods to prevent potential hacking. We as a provide look forward to make our users life safer and easier. Ideas like this can be very useful as more and more cases occur related to cyber security around the world to make it a safer environment for the user to access his/her private data.

6. REFERENCES:

[1] Uma D. Yadav, Prakash S. Mohod "Adding Persuasive features in Graphical Password to increase the capacity of KBAM" International Conference on Emerging Trends in Computing, Communication and Nanotechnology(ICECCN 2013) IEEE 2013.

[2] "A Review of Vision Based Hand Gestures Recognition" International Journal of Information Technology and Knowledge Management, July-December 2009, Volume 2.

[3] Yi-Lun Chen, Wei-Chi Ku, Yu-Chang Yeh, and Dun-Min Liao "A Simple Text-Based Shoulder Surfing Resistant Graphical Password Scheme" 2nd International Symposium on Next-Generation Electronics (ISNE) IEEE 2013.

[4] Rohit Jagtap, Vaibhav Ahirrao, Vinayak Kadam, Nilesh Aher "Authentication schemes for session password using color and special characters" International Journal of Innovations Advancement in Computer Science IJIACS ISSN 2347 8616 Volume 3, Issue 2 April 2014.