IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

Graphical Password based Authentication System

Anitha H.B[1], Adithi Reddy[2], Irudaya Mary S[3], Vidya V[4]

Abstract: Most of the existing authentication system has certain drawbacks for that reason graphical passwords are most preferable authentication system where users click on images to authenticate themselves. Access to computer systems is most often based on the use of alphanumeric passwords. However, users have difficulty remembering a password that is long and random-appearing. Instead, they create short, simple, and insecure passwords. Graphical passwords have been designed to try to make passwords more memorable and easier for people to use and, therefore, more secure. Using a graphical password, users click on images rather than type alphanumeric characters. We have designed a new and more secure graphical password system, called gSign. An important usability goal of an authentication system is to support users for selecting the better password. User creates memorable password which is easy to guess by an attacker and strong system assigned passwords are difficult to memorize. So researchers of modern days have gone through different alternative methods and concluded that graphical passwords are most preferable authentication system. The proposed system combines the existing cued click point technique with the persuasive feature to influence user choice along with image steganography techniques, encouraging user to select more random click point which is difficult to guess. Image steganography, the art of hiding data within an image is used to improve the security of the authentication system. Textual passwords are stored within the images using the steganography techniques.

Index Terms: Graphical password, Steganography, Image steganography.

INTRODUCTION

The problem of Knowledge based authentication mechanism (KBAM) typically text based password are well known. The goal of an authentication system is to support users in selecting the superior password. An alternative to alphanumeric password is the graphical password. Graphical password uses images or representation of an image as a password. Human brains easily recognize pictures than the text. Most of the time user create memorable password which is easy to guess but strong system assigned password are difficult to remember. An authentication system should allow user choice while influencing user towards stronger passwords.

An important usability goal of Knowledge based authentication system is to support users in selecting password of higher security with larger password space. Basically persuasion is used to control user choice in click based graphical password, encouraging user to select more random click point which is difficult to guess. In the proposed system, the task of selecting weak password which is easy for an attacker to guess is more tedious; discourages users from making such choices. In consequence, this approach chooses the more secure password the path of least confrontation. Instead of increasing the burden on users it's easier to track the system suggestions for a secure password which is the feature lacking in most of the schemes. Here persuasive feature is combined with previous cued click point technique which uses one click point on five different images. The next image to be displayed is based on previous click-point

Here the password entry becomes a true cued recall scenario wherein each image triggers the memory of corresponding click-point. For valid users it provides implicit feedback such that while logging if user is unable to recognize the image then it automatically alters the user that their previous click-point is incorrect and user can restart the password entry whereas explicit indication is provided after the final click point.

RELATED WORK

To understand the introductory concepts related to authentication system various books have been referred [1,2, 3] which gave a thorough knowledge about the basic concepts. This introductory books leads the user through a clear, step-by-step, screen-by-screen approach to learning the authentication methods. Alphanumeric and graphical passwords are the two commonly used authentication techniques.

In alpha numeric password the password are:

- The password should be at least 8 characters long.
- The password should not be easy to relate to the user.
- The password should not be a word that can be found in dictionary or public dictionary [4].

Because human beings live and interact in an environment where the sense of sight is predominant for most activities, our brains are capable of processing and storing large amounts of graphical information with ease. While we may find it very hard to remember a string of fifty characters, we are able easily to remember faces of people, places we visited, and things we have seen. These graphical data represent millions of bytes of information and thus provide large password spaces. Thus, graphical password schemes provide a way of making more human-friendly passwords while increasing the level of security [5][6].

Authentication schemes such as sessions method authenticate the user by session passwords which are used only once. Once the session is terminated, the session password is no longer useful. For every login process,

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

users input different passwords. The session passwords provide better security against dictionary and brute force attacks as password changes for every session. But in this same problem occurs that every time user has to enter password again and again. It is too hard to remember password and as the session password is only for a particular time .

To remove the drawback of textual password removed by graphical password schemes which provide a way of making more user friendly passwords, while increasing the level of security, they are vulnerable to shoulder surfing .Here text was combine with image and color to generate the session password and every time user have to enter new password as session ends[4].

SYSTEM OVERVIEW

The graphical password based authentication system is based on click based graphical password system that not only guides and helps the user for password selection but also encourages the user to select more random distributed password. The proposed system is based on Persuasive Technology which motivates and influence people to behave in a desired manner. The system model is as given below:

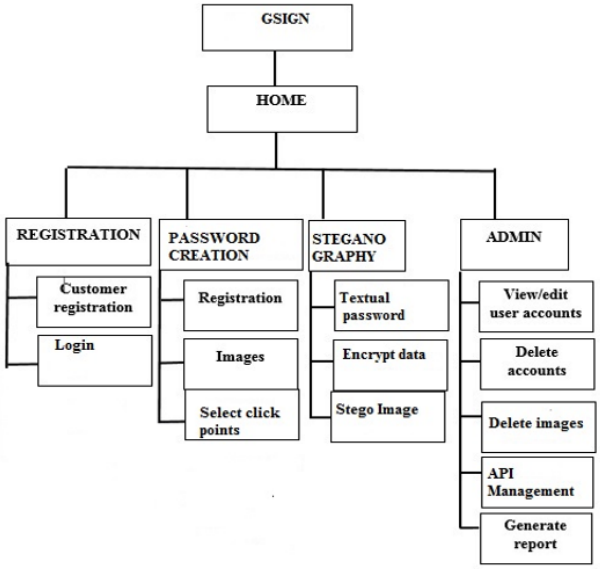

Fig 1. System Model

The proposed system combines the Persuasive features with the cued click point to make authentication system more secure. Basically during password creation the part of an image which is less guessable is highlighted and user has to select the click-point within the highlighted portion and if the user is unable to select the click-point then he can move towards the next highlighted portion by pressing the shuffle button. The highlighted part of an image basically guides users to select more random passwords that are less likely to include hotspots. Therefore this works encouraging users to select more random, and difficult passwords to guess. During Login, images are displayed normally and user has to select the click point as chosen at the time of password creation but this time highlighted portion is not present as it only provides the system suggestion. An important usability goal of proposed system is to support users in selecting password of higher security with larger password space. The proposed system removes the pattern formation attack and Hotspot attack (it is an area of an image where most of the user is selecting it as the click-point).Also it removes the shoulder surfing attack. The user is also given an option to store a text password which will then be encrypted in the images selected by the user through the technique of steganography. Image steganography is an art of hiding data within an image. The system also is a utility tool for authentication with the implementation of the API module.

SYSTEM ARCHITECTURE

The architecture used in this project is a three tier architecture, which comprises of the presentation tier, logical tier and the data tier. Below is the architecture diagram of the system:

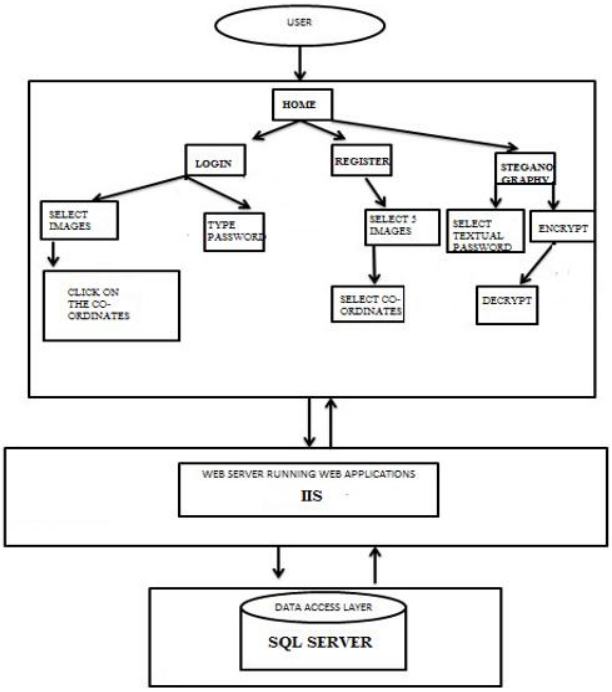

Fig 2. System Architecture

Registration

The users of the system have to firstly register with the application before going ahead and logging into it. The registration consists of firstly choosing the set of images that the user desires for setting the password, out of each those images the user selects the area in the image which least likely guessable. For more security the user also gives a text password which will in turn be hidden in the set of images that the user had selected before this will be done by the concept of image steganography.

Image Steganography

Image steganography is performed during the registration and login process of the application. It is the process of hiding a data within another. If any type of data such as image, text etc. are hidden within an image, it is known as image steganography. During registration process, a textual password is asked from the user, which is then

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

stored within the images. While the login process, the user is asked to re-enter the password, which will then be compared with the one retrieved from the image. If the retrieved password matches with the one stored during the login process, the user is considered authenticated.

Login Process

During logging in the user is asked to type the text password which is matched to the text which will be retrieved from the images which was stored during the registration. Along with the text, the images that the user had selected during the registration will be displayed out of which the user will have to click on the same areas that were clicked before.

EXPERIMENTAL RESULTS

The proposed method is practically experimented to demonstrate the working model of the same. As mention in the system architecture the first step is the registration process. Given below are the screen shots taken while a user is registering with the system:

Fig 3. Registration Process

Here the user will enter the email address, user name, and then selects the images for setting the password. Given below are the images for setting the password:

Fig 4. Selecting the pixel on image 1

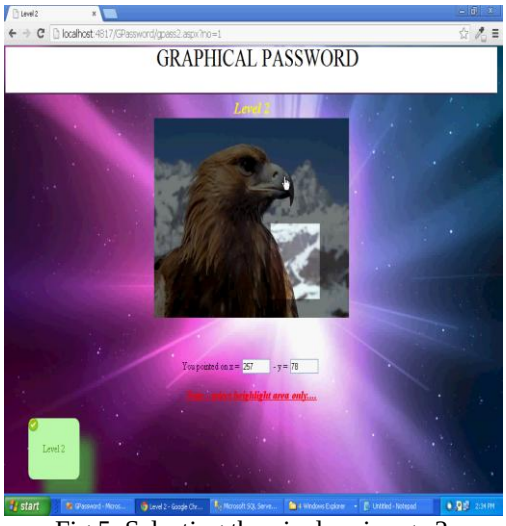

Fig 5. Selecting the pixel on image 2

Selecting the pixel: The highlighted area on the images is the area from which the user can select the pixel for setting the password. This area is mathematically calculated and projected as the least guessable area. This highlighted area will be different for different users and images.

CONCLUSIONS AND FUTURE SCOPE

Picture passwords are an alternative to textual alphanumeric password. Most of the existing authentication system has certain drawbacks for that reason graphical passwords are most preferable authentication system where users click on images to authenticate themselves. As authentication techniques generate passwords but they have to face attacks like dictionary attacks, brute force attacks, shoulder surfing. An important usability goal of an authentication system is to support users for selecting the better password. User creates memorable password which is easy to guess by an attacker and strong system assigned passwords are difficult to memorize. So researchers of modern days have gone through different alternative methods and concluded that graphical passwords are most preferable authentication system. By implementing encryption algorithms and hashing for storing and retrieving pictures and points, one can achieve more security. The proposed system combines the existing cued click point technique with the persuasive feature to influence user choice, encouraging user to select more random click point which is difficult to guess. Picture password is still immature more research is required in this field.

REFERENCES

[1] Diffie, W., and Hellman, M.E., New Directions in Cryptography, IEEE Transactions on Information Theory, vol. 22, no. 6, November 1976, pp.
[2] Garret, Paul. Making, Breaking Codes: An Introduction to Cryptology. Upper Saddle River, NJ: Prentice-Hall, 2001
[3] Hoffstein, Jeffery, Pipher, Jill and Silverman, Joseph H. NTRU: A Public Key Crypto http://grouper.ieee.org/groups/1363/lattPK/submissions.html#NTRU1.
[4] Priti Jadhao and Lalit Dole, "Survey on Authentication Password Techniques", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-2, May 2013
[5] L.Sobrado and J.C. Birget, "Graphical Passwords", The Rutgers Schloar, An Electronic Bulletin for Undergraduate Research, vol 4, 2002.
[6] G. E. Blonder. Graphical passwords. United States Patent5559961, 1996.

DOI 10.17148/IJARCCE.2016.5236