International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 01 | Jan 2019 www.irjet.net p-ISSN: 2395-0072

Graphical Password Authentication

Mohini Patil

Department of Computer Engineering, Xavier Institute of Engineering (Affiliated to Mumbai University), Mumbai, India

---

Abstract - *The most widely recognized authentication method is for a user to submit a user name and a text password. The vulnerabilities of this method have been well known. One of the fundamental issues is the trouble of recollecting passwords. Normally users will in general pick short passwords or passwords that are anything but difficult to recall. Unfortunately, these passwords can also be easily guessed or broken. In this paper, we propose a Financial graphical password authentication system. We describe its operation with some examples, and highlight important aspects of the system.*

Keywords: Graphical password, Authentication, Security, Text-based password, Recognition, Pictures

1. INTRODUCTION

The work of Graphical passwords was originally proposed by BLONDER in 1996. In the graphical password authentication system, the user selects from certain set of the images, in a specific order, presented in a graphical user interface (GUI). It also sometimes called as a graphical user authentication (GUA). Graphical password is easy to remember compared to regular text-based password. Graphical passwords provide better security than text-based passwords because many people, in an attempt to memorize text-based passwords, use plain words (rather than the recommended complex set of characters). It is easy for the hacker to enter into the system by the dictionary search on the other hand It is difficult to break into the system if hacker has to choose series of the selectable images which is used on successive screen pages. If there are many images then hacker has to try each and every combination which is bit tedious.

1.1 Problem Definition

In order to Satisfy the shortcomings of the existing Text based Password Systems and to make the systems more secure from hacking and predictability we are developing a new generation of passwords that are based on images that cannot be easily predicted or hacked.

Solution to above mentioned limitation of existing system.

- In order to Satisfy the shortcomings of the existing Text based Password Systems and to make the systems more secure from hacking and predictability we are developing a new generation of passwords that are based on images that cannot be easily predicted or hacked.
- They cannot be written in any form so there no scope for stealing.

1.2 Research Motivation

When we look up to alternative to the traditional username and authentication, such as biometric authentication like face recognition, voice recognition, iris recognition, fingerprints, palm prints, hand geometry and retina recognition. Each of these biometric recognition scheme has its advantages and disadvantages based on a number of factors, including consistency, uniqueness and acceptance. One of the important limitations that it is based on the user's personal characteristics. Also, retina biometrical acknowledgment plans require the client to willingly expose their eyes to a low-force infrared light. Moreover, many biometric systems require a special scanning device to authenticate users, which remote and Internet users cannot access.

Graphical password schemes have been proposed as a possible alternative to other authentication schemes, inspired somewhat by the way that people can recollect pictures effectively. Pictures are generally easier to be remembered or recognized.

2. Graphical Password Authentication

Human variable factors regularly viewed as the weakest connection in a computer security system. Patrick, et al. call attention to that there are three main areas where human computer interaction is essential: confirmation, security tasks, and creating secure systems. We are focusing on authentication problem. Current authentication methods can be divided into three fundamental areas:

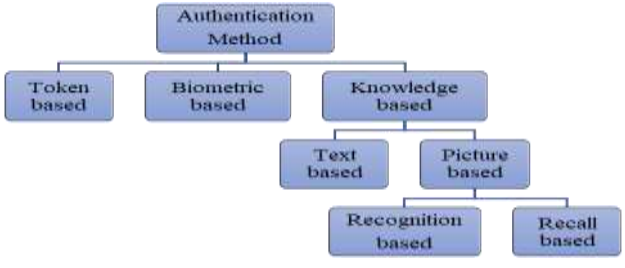

Figure 2.1 : Types of Graphical Password Authentication

2.1 Token Based authentication:

Token based Techniques, for example, scratch cards, bank cards are widely used. Numerous token-based verification Techniques additionally use information-based methods to improve security. For instance, ATM cards are commonly utilized together with a PIN number. Although token-based authentication is a strong authentication technique, it has important drawbacks, suggested in a Microsoft article. Authentication software must be installed on a centralized database and the software needs to be deployed on each user's external device. Moreover, users may lose the device and replacing it can be costly for the company.

2.2 Biometric based authentication:

Biometric based validation strategies, for example, fingerprints, facial acknowledgment or iris examine are not yet broadly adopted. The significant downside of this methodology is that such approach can be costly, and the recognizable proof process can be moderate and frequently inconsistent.

2.3 knowledge-based authentication:

Knowledge based techniques are the most widely used validation techniques. They include both text-based and picture-based passwords. According to the analysis of the security researchers there is rise in the malware attack, a spyware built to capture login names and passwords and to send them to the attackers. The hacker can easily attack Text-based passwords. Therefore, picture-based techniques are more useful.

2.3.1 Recognition based techniques:

Using acknowledgment-based methods, a user is given a certain set of images and the user passes the validation by perceiving and recognizing the pictures the person while the registration phase. There are mainly two types of recall-based techniques.

A. Dhamija and Perrig Method:

Dhamija and Perrig proposed a graphical authentication scheme which uses Hash Visualization technique. In their system, the program generates certain number of the images and user is asked to select number of images from a set of random pictures generated by a program. Later, the user will be required to identify the pre-selected images in order to be authenticated

B. Sobrado and Birget method:

Sobrado and Birget developed a graphical password technique that based on the shoulder-surfing problem. In the first scheme, the system will display a number of pass-objects (pre-selected by user) among many other objects. A user needs to recognize pass-objects and click inside the convex hull formed by all the pass-objects for the authentication.

C. Man, et al. Method:

Man, et al. proposed another shoulder-surfing resistant algorithm. In this algorithm, a user selects a number of pictures as pass-objects. Each pass-object has several variants and each variant is assigned a unique code. During authentication, the user is challenged with several scenes. Each scene contains several pass-objects many decoy-objects. Recall Based.

D. Jansen et al Method:

Jansen et al is a graphical password mechanism works on mobile device during the registration stage, a user selects a theme (e.g. sea, trees, cat etc.) which comprises of thumbnail photographs and afterward registers a sequence of pictures as a password.

E. Pass face Technique:

The user will be asked to pick four pictures from human appearances from a face database as their future password. In the validation stage, the user sees a grid of nine faces, comprising of one face recently picked by the client and eight fake faces. The user perceives and clicks anyplace on the known face. This system is repeated for a few rounds

2.3.2 Recall based techniques:

Using recall-based procedures, a client is requested to recreate something that the person in question made or selected earlier during the stage.

3. Implementation

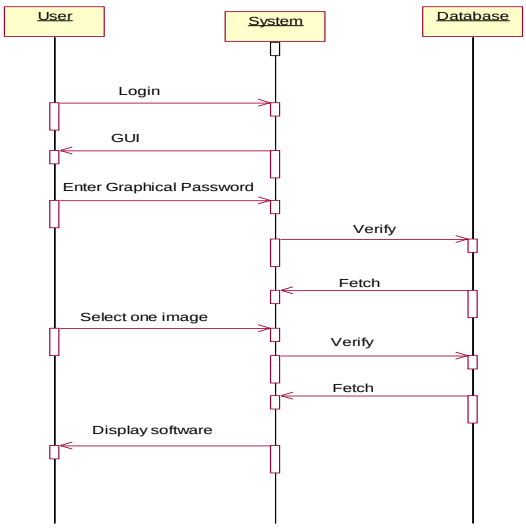

Fig 3-1: Sequence Diagram

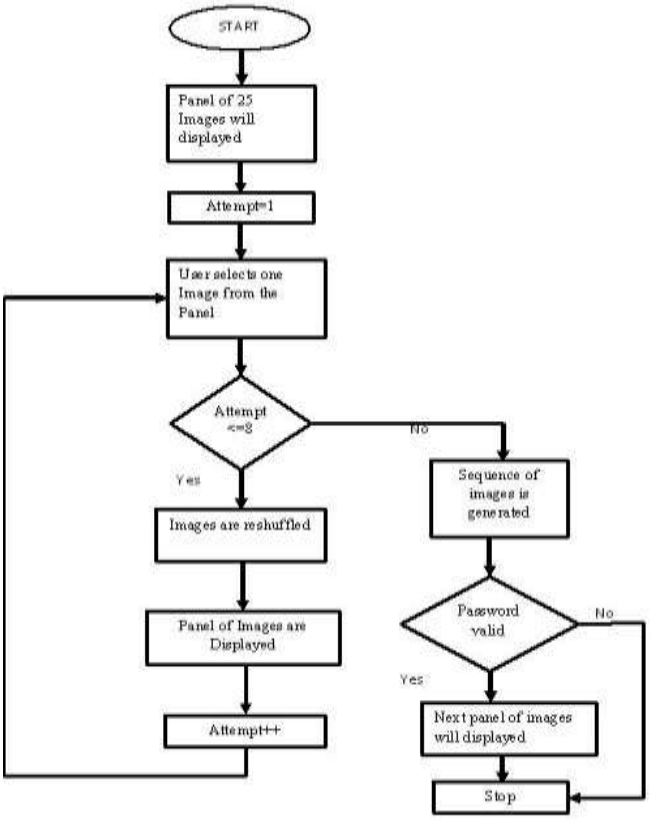

Figure 3-2: Flowchart

This flowchart demonstrates the flow of our project which first includes the panel of 25 images displayed on the screen the user selects 1 image from the panel. In this way there are 8 panels displayed, user selects 1 image from each panel. After every image selection the reshuffling of images takes place. The sequence of images is generated. If password is valid then proceed with the software and stop. If password is not valid then the process will stop.

3.1 Description of the Software:

Front End: ASP.net
Back End: Microsoft SQL Server

- **About SQL Server**

Microsoft SQL Server is comprehensive, integrated data management and analysis software that enables organizations to reliably manage mission-critical information and confidently run today's increasingly complex business applications. SQL Server allows companies to gain greater insight from their business information and achieve faster results for a competitive advantage.

- **Computer Hardware Specification**
  - 4th Generation Intel® Core™ i7-4770 Processor (8M Cache, up to 3.9 GHz)
  - Windows 7 64bit, English
  - 4 GB Dual Channel DDR3 SDRAM at 1600MHz
  - 1TB 7200 RPM SATA Hard Drive 6.0 Gb/s
  - NVIDIA® GeForce® GTX 645 1.0GB GDDR3

3.2 Implementation Results:

- We expect our project to provide maximum security to any applications to which it is applied, as in the above case it is financial software for a stock broking firm.
- Our project also takes care of the hacking of passwords through keyboards using any software as the user has to only select the images from a pool given to him/her. There is no question of pressing any key on the keyboard.
- Interactive user interface on PC
- Portability
- Efficiency

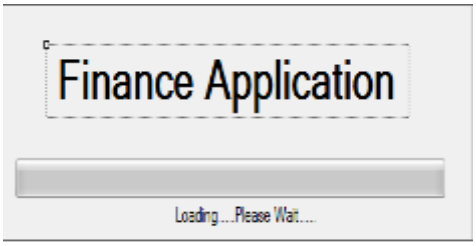

Figure 3.1 : Application Start

Figure 3.2 : Graphical Login

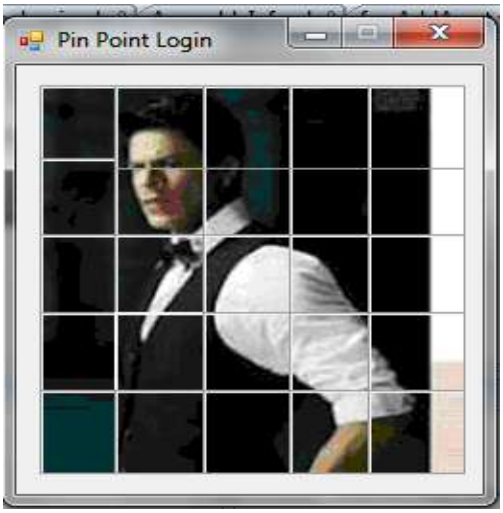

Figure 3.3 : Pass face Login

This is the first Graphical login page that is displayed at the start of the application. On this page there is a panel which includes 25images.In this way there are total 8 number of panels used which includes 25 images each. For setting the password the user needs to select any one image from the panel. While selecting this image, reshuffling of images takes place. The user has to remember the sequence of selection of images which he or she had selected as their password. After selecting 8 images from the 8 respective panels the user clicks on the login button. After clicking on the login button one single image panel will be displayed, the user needs to select any part of the image as a password. Thus, the user's graphical password gets stored which consist of 8 random images and 1 single part of the whole image. After clicking on ok the user's password is saved & the finance application is opened for the user to work in it or perform task as he or she requires.

4. Conclusions

As known, text-based passwords are still dominating the security systems. However, this traditional system has its own drawbacks, like retaining the password. Because people cannot easily remember the random generated long textual password, they tend to choose short and easy textual passwords which are open to attacks. The main motivation behind the graphical passwords is that the people can recall or recognize graphical objects easier. It is observed that with traditional attacks it is hard to crack the graphical security systems. Concept-Based method which is based on the user's concept preference allows users to correlate themselves with the passwords by which they can easily remember their passwords later in time. Also making a story with the categories they pick during registration would help the users to remember the password later on. In addition, the probability of the guessing attacks could be lowered by increasing the number of random pictures shown in each round, number of rounds and number of categories.

Statics shows Graphical Passwords are difficult to crack for hackers. Here in this system we will ask user to create a graphical password by choosing 8 pictures in a particular order from a set of 50*8 pictures.

Graphical password security is required to a very high security demanding software like the one we will develop, "Financial Application". All the data in Financial Application will be Guarded by Graphical Password. This software can be used by any Financial Broker who wants to guard the high security financial information of his/her clients.

REFERENCES

1] Graphical Password Existing Recognition Base Graphical Password Usability. Proceedings of International conference on security and management. Las Vergas, NV.

[2] Graphical Passwords: A Survey Concept-Based Graphical Password Authentication MethodİbrahimBumin Kara Department of Computer Science Engineering Isik University Istanbul, TURKEY

[3]A Design and Analysis of Graphical Password Georgia State UniversityDigital Archive @ GSU .Computer Science Theses Department of Computer Science.

[4] Real User Corporation. The science behind Pass faces. http://www.realusers.com.

[5] An Ample-Range Survey on Recall-Based Graphical Password Authentication Based On

Multi-Line Grid and Attack Patterns International Journal of Science and Modern Engineering (IJISME) ISSN: 2319-6386, Volume-1, Issue-5, April 2013