THE INTERNATIONAL JOURNAL OF SCIENCE & TECHNOLEDGE

Multilevel System Security Using Graphical Password and Pair Based Authentication Scheme

Shashank Sawant
Student, Department of Computer Engineering, SIES GST, Nerul, Navi Mumbai, India
Aishwarya Shetty
Student, Department of Computer Engineering, SIES GST, Nerul, Navi Mumbai, India
Payal Pawar
Student, Department of Computer Engineering, SIES GST, Nerul, Navi Mumbai, India

Abstract:
Passwords are used for authentication (the process of determining whether someone or something is, in fact, who or what it is declared to be), authorization (the process used to decide if the authenticated person is allowed to access specific information or functions) and access control (authentication & authorization are a part of restriction of access). Currently available schemes include textual password but they are highly vulnerable to attacks because they follow predictable patterns which the hackers can easily guess. Multilevel authentication scheme is a combination of many other authentication schemes consisting of cued click points, pair based authentication system & audio or video play pause techniques. This scheme is user friendly & quite hard to break. We have contributed in making multilevel authentication technique to become more secure & user friendly to users of all the categories.

Keywords: *Secret pass, PBAS, cued click point*

1. Introduction

Text based passwords were invented in the year 1960s and today many systems use this type of passwords. These passwords suffer from much vulnerability such as dictionary attacks which is the common way used by the intruders to hack the system. Another problem with these passwords is that it is difficult to remember these passwords. If dictionary words are not used to set a password then they become difficult to memorize. Recent studies from Dhamija et al (2000) showed that humans are only capable to memorize a limited number of passwords, because of this syndrome, they often to write down, share and use the same passwords for different current accounts. Graphical password can be used as an alternative to text based password. It overcomes the weakness of current password authentication schemes. Graphical passwords are easier to use, easier to remember and at the same time very secure. Based on the two assumptions; first, humans can remember pictures better than alphanumeric characters and second, a picture is worth a thousand passwords. [5] Some psychological studies and company software seem to agree with these assumptions. The current graphical password schemes suffer from the problem of shoulder surfing attacks, it thus becomes important to find a way which removes shoulder surfing problems from the system.

2. Problem Definition

There are not many secure authentication systems available which provide high level security for applications like nuclear, navy army and other defense purposes. The current system has many loopholes which need to be addressed. So we trying to devise a system which combines the advantages of three techniques and at the same time eliminates the disadvantages present in the current system. At the same time we are trying to implement a system that helps to generate revenue and one of the techniques available in the system can be independently used for the people who are visually challenged.

3. Literature Survey

3.1. Biometrics

Biometrics is a method by which a person's authentication information is generated by digitizing measurements of a physiological or behavioral characteristic. [6] Just like other technologies, biometrics also has some disadvantages. One disadvantage of biometrics is cost. The devices used by Different biometric technologies have a range of costs. Also the use of these biometric devices may be time consuming. People are concerned they will have to wait in line to get scanned or finger printed to gain access to a building or school.

Another disadvantage is the fact that people are concerned they might have to touch a device that someone else has to touch which could cause the spread of germs. Disadvantages from the iris-scan is the fact that it is difficult to capture some individuals. Also, eyelashes, eyelids, lens and reflections from the cornea can easily obscure the iris. There is also a lack of existing data which deters the ability to use for background or watch list checks. The disadvantages of face recognition are that the face can be obstructed by hair, glasses, hats, scarves, etc. A third disadvantage related to face recognition is that people's faces change over time. In order for face recognition to be accurate, it is important to face the camera properly furthermore the user's face must be lit evenly, preferably from the front This is not always possible and can be very hard to do in some environments. Biometric technologies like voice, signature, and hand geometry verification also have some drawbacks. With voice verification the surrounding noise interference must be minimum or the spoken phrase will not be registered accurately. The problem with signature verification is when people change their signatures over a period of time change over time so the consistency is not maintained. And lastly, hand geometry verification is very costly and needs a large device to carry out the task.

3.2. Tokens

The problem with tokens is that tokens are used in the form of credit cards and ATM cards. It is an efficient means of authentication, but it can be stolen and hence can be misused. Furthermore, it involves additional costs such as the cost of token and any replacement fees. It always needs to be carried and can be easily stolen and misused. Software tokens based on asymmetric encryption with keys generated locally are extremely vulnerable to malware attacks.

3.3. Text based password

As the multi-user operating systems were being developed text based passwords were introduced to tackle the security issues that became evident. An alpha-numeric password is simply a combination of letters and digits. Although almost any combination can serve as a password, they can only offer good security as long as they are complicated enough so that they cannot be deduced or guessed. People have devised ways to create pseudo-random passwords as it is best to have a password which is completely random. One such method is to perform certain actions on a common word. However, it is very difficult to remember a complicated password. Alpha-numeric password is also prone to dictionary attack. Most users tend to choose a common word or name or date of birth or a phone number which can be easily cracked by some tools that allow an individual to crack passwords by automatically testing all the words that occur in dictionaries or public directories. Studies have shown that this attack has a high success rate in finding valid passwords of some users of a given system.

4. Proposed System

Our system is proposed as an alternative to other password based techniques. The current system present for authentication has several loop holes .We are trying to eliminate password guessing through dictionary attacks, brute force attack and guessing attacks. Our objective is to overcome the known weakness of traditional passwords. It is also designed to make the passwords more memorable, easier for people to use and therefore more secure. [2] Based on the two assumptions; first, humans can remember pictures better than alphanumeric characters and second, a picture worth a thousand words[2]; some psychological studies and company software seem to agree with these assumptions that a picture based password is better than a text based password. Our objective is to make the system more secure and hence by combining three techniques we have introduced levels. This is for making the system hard to break.

Basically, in our model we are using three techniques, namely pair based authentication scheme, cued click point and audio/video password. At the same time we are introducing a password scheme, i.e. video password that can be used for generating revenue and audio password that can be used for physically disabled people with blindness.

5. Implementation

Three levels in the system are Pair based authentication scheme, cued click point and video password. Instead of video password, we can use audio password depending upon the user who is using the system.

5.1. Pair Based Authentication Scheme (PBAS)

During registration, user has to submit his password which actually looks like a combination of alphabets and numbers i.e. alpha numeric password. An important condition on this password is that is should always be even. In case it is not even then the system will reject the password. This password entered by the user is known as secrete pass.[3]At the time of login when the user enters his username a grid is displayed which comprises of alphabets from A to Z and numbers from 0 to 9.The size of the grid is 6x6 and the elements present are in random order. When the user refreshes the page, the order of the grid automatically gets changed. Following figure shows the user interface for the grid.

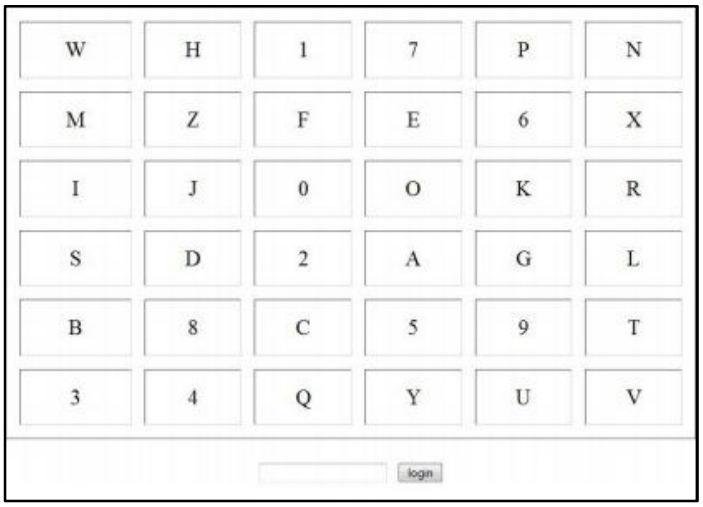

Figure 1: Login interface

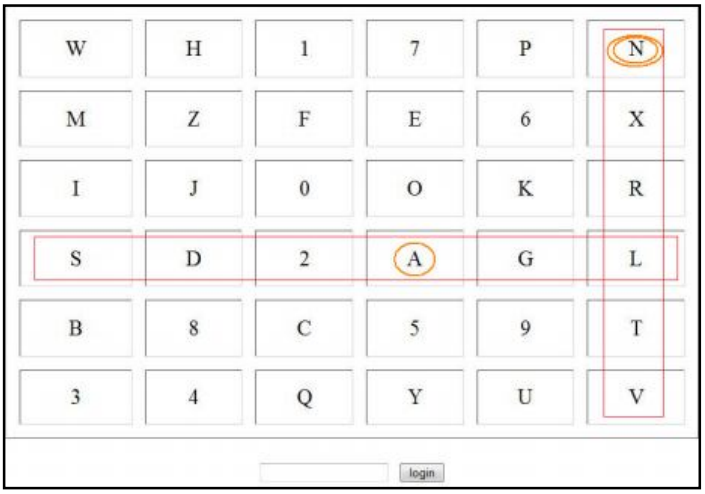

Figure 2: Intersection letter for the pair AN

User has to consider his pass in terms of pairs. The first letter in the pair is considered for the row and the second letter in the pair is considered for the column. The intersection letter for the row and column is the session password. This is repeated for all pairs of secret pass. Fig. 2 shows that L is the intersection symbol for the pair "AN". The password entered by the user is verified by the system. If the secret pass comprises of 8 elements, the password generated will have size 4. The grid size can be increased to include special characters in the password. This technique prevents shoulder surfing attack, dictionary attack and brute force attack. [1]

5.2. Cued click point

Cued click point provides cues to the user for remembering the password. The system comprises of five images which is placed one, besides the other. The user can click anywhere on each image. The point which the user clicks on the image becomes his password i.e. the image has x and y axis and the corresponding xy point becomes the first point of the password. User has to repeat this for all the images present. Five is the optimal number of images as points in five images are easy to remember and the combination of passwords available with this scheme is sufficient enough to prevent guessing attacks.

5.3. Video/Audio password

5.3.1. Video Password

Video passwords require the user to watch and remember the parts of the video. It can be used as a means to generate revenue for the business firm that uses this technique.Video-passwords require a user to select parts of a video as his or her password. The scenes, movement, and sounds in a video work as cues in particular parts of a video. A video is at the timeline that consist of many timestamps along the timeline. [4] Each time stamp can be used as the user's password.These timestamps can be selected and remembered based on the scene, movement, and/or sound events that occur. Basically after we load the video we have to play the video form random amount of time and pause it. We can play and pause the video for a number of times and the final value becomes the user password.

5.3.2. Audio Password

Audio password is similar to video password with the only difference that it doesn't comprise of visual data and just audio data. The concept of play and pause present in audio password is exactly same in case of audio password. Audio password can be used for people who are visually challenged. Using both audio and video password doesn't make much sense and so either of them can be used in the system depending upon the requirement of the user.

5.4. Encryption and Decryption

Encryption and decryption play an important role in any system. Any data stored in the database should be present in any encrypted form so as to prevent the system form database attack. We are using Rijndael algorithm for encryption, decryption purpose.

6. Conclusion

Thus, this scheme provides a high level of security in terms of guessing and dictionary attack. At the same time it can be used as a means of generating revenue as is the case with video password and can be used for visually challenged people as is the case with audio password. This model is easy to use and at the same time difficult to break by intruders.

7. Future Scope

It can be used for very high level defense systems which requires more security. Further, it can also be modified to be used in various other fields like banking, commerce by using individual modules presented in this paper. The number of modules can be changed depending upon the level of security required by the system.

8. Acknowledgement

We express our deepest sense of gratitude and sincere thanks to our guide Mrs. Prachi Shahane for her excellent guidance throughout our work. Her prompt and kind help led to the successful completion of our work.

We would like to thank our Hon. Principal Dr. Alka Mahajan, Hon. Dean Academics Mr. Ashok Tagalpallewar and H.O.D (Computer) Prof. Mr. Rajesh Kadu for giving us this opportunity and all the necessary facilities to present this report and providing us with the opportunity to learn.

We would like to extend our gratitude to the entire team for their co-operation and unity they have shown.Last but not the least we would like to thank the college staff for providing us with facilities and sources that we needed.

9. References

1. Passwords in practice and usability survey, May 2011
2. Graphical password usable password prototype, May 2005
3. Authentication Schemes for Session Passwords using Color and Images, May 2011
4. Video password advertising while authenticating, May 2012
5. Graphical Password: Usable Graphical Password Prototype, May 2009
6. http://www.e-authentication.gov.hk/en/professional biometric.htm