Multi-tiered Framework for User Authentication Based on Multimedia

Monzer M. Qasem

ABSTRACT

With the tremendous development in information technology, the use of technology has become in most areas, and it became the most procedures and electronic transactions, for example: electronic banking and social networking. All these led to the presence of a huge amount of data is one of the privacy for the user, and it must protected by assigning a password to gain unauthorized access to that data, because the Privacy and confidentiality are the most important elements of information security, and it must be for each user to assign a password to gain access to his own data safely and does not even provide an opportunity for illegal access to data. Usually When the user wants to set a password putting in his mind some of the following considerations: Can be alphanumeric password; i.e. (containing letters, numbers and sometimes both), to be an easy password; in order to remember it later, can be semantic or meaningful password; i.e. (family, wife, children and care names) and can be date password; i.e. (date of birth, date of marriage and date of joining job).

All these considerations indicates that the previous password ware sat by the user can be easily known by attackers, because they use software and the dictionaries for the purpose of finding a huge sense of the words to detect passwords. The main goal of a good authentication system is to provide a multilayered of secure password called Multi-tiered Framework for user authentication which based on multimedia password rather than alphanumeric password. This paper presents a Multi-tiered Framework of having an effective authentication system, which provides strong password hard for the attackers to guess and easily remembered graphical passwords for the users with a high level of security. On the other hand, is to reduce the guessing attacks as well as encouraging users to assign a difficult password to guess by the attackers and easy for him to remember it.

KeyWords

Authentication, Computer security, Confidentiality, Graphical password, Guessing attacks, Information technology, Privacy.
1. Introduction

There are many things that are “well know” about passwords; such as that user can’t remember strong password and that the passwords they can remember are easy to guess [1-6]. Password become in recent years a necessary in all electronic transactions, whether it was used to confirm the identity of deals with automated teller machines, or used to access the e-mail or social networking, and others. It has become the need to manufacture passwords encrypted with high reliability and confidence. So that no one can guess or break nor the software can configure to guess passwords. Password is a series of letters, numbers, or symbols, or combination thereof, with the user name used to confirm the credibility and validity of the identity used. Although the development of technology and methods of information security in recent times is still the problem of piracy, and this threatens to primarily large corporations, which fears the confidentiality of their information. It should be noted that the main reason that the password represents the firewall vulnerable to hacking attacks, is its lack of force necessary to repel the attacks, due to the nature of human and his limited ability to remember many and different passwords, which means that most people avoid the problem of forgotten passwords making them very weak which is easy for the attackers to guess.

According to a recent Computerworld news article, the security team at a large company ran a network password cracker and within 30 seconds, they identified about 80% of the passwords [7]. On the other hand, passwords that are hard to guess or break are often hard for user to remember. Studies showed that since user can only remember a limited number of passwords, they tend to write them down or will use the same passwords for different accounts [8, 9]. The alternative authentication method is using both pictures and waves “Graphical password schemes” as a passwords instead of text-based schemes authentication, which humans can remember pictures better than text; psychological studies supports such assumption [10]. The problems of knowledge-based authentication, typically text-based passwords, are well known. Users often create memorable passwords that are easy for attackers to guess, but strong system-assigned passwords are difficult for users to remember [11]. A password authentication system should produce a strong passwords instead of creating weak passwords. The proposed framework allowing users to choose stronger passwords, easy to remember and hard to guess from the attackers side. In fact, this approach makes choosing a more secure password rather than increasing the burden on users to remember a lot for characters, numbers and special characters.

2. Overview of the Authentication Methods

![Figure 1. Classification of Authentication Methods](image)

The following Figure 1: shows that, Current authentication methods can be divided into three main areas: Token based authentication, Biometric based authentication and Knowledge based authentication, the following are the description for each of them:

2.1 Token based authentication techniques:
Such as key cards, bank cards and smart cards are widely used. Many token-based authentication systems also use knowledge based techniques to enhance security. For example, ATM cards are generally used together with a PIN number.

2.2 Biometric based authentication techniques:
Such as fingerprints, iris scan, or facial recognition, are not yet widely adopted. The major drawback of this approach is that such systems can be expensive, and the identification process can be slow and often unreliable and hence not preferred by many. [12,13].

2.3 Knowledge based techniques:
Are the most widely used authentication techniques and include both text-based and picture-based passwords. The picture-based techniques can be further divided into two categories: recognition-based and recall-based graphical techniques. Using recognition-based techniques, a user is presented with a set of images and the user passes the authentication by recognizing and identifying the images he or she selected during the registration stage. Using recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage.
The specific hypotheses with respect to multiple password interferences were:
1) Participants will have lower recall success rates with text passwords than with Pass Points passwords.
2) Participants in the Text condition are more likely than Pass Points participants to use patterns across their own passwords.
3) Participants will recall text passwords more slowly than Pass Points passwords.
4) Participants in the Text condition are more likely than Pass Points participants to create passwords that are directly related to their corresponding accounts.
5) Participants in the Text condition will make more recall errors than participants in the Pass Points condition.

3. Existing Systems

Existing approaches to Users often create memorable passwords that are easy for attackers to guess, but strong system-assigned passwords are difficult for users to remember [14]. Authenticate the user's computer through a user name and password in the form of text, number, or both together, where the most common way that this has become a very well known because the user puts a weak password in order to remember and so they become weak password is easy to guess by hackers.

Studies have shown that users tend to pick short passwords or passwords that are easy to remember. Unfortunately, these passwords can also be easily guessed or broken. According to a recent Computer world news articles, the security team at a large company ran a network password cracker and within 30 seconds, they identified about 80% of the passwords[3]. On the other hand, passwords that are hard to guess or break are often hard to remember. Studies showed that since user can only remember a limited number of passwords, they tend to write them down or will use the same passwords for different accounts, which has several drawback's as follows:

1) The problems of knowledge-based authentication, typically text-based passwords, are well known. Users often create memorable passwords that are easy for attackers to guess, but strong system-assigned passwords are difficult for users to remember.
2) Text passwords are the most popular user authentication method, but have security and usability problems.
3) Users maintaining same password for multiple applications. Because of easy to remember.

4. Problem Statement

A human brain is not good of remembering the alphanumeric password, but it’s a good in remembering the pictures. On the other hand guessing the alphanumeric password become very easy by using specific software and dictionaries, but guessing the graphical password is too difficult. A major goal of this paper is to discover how to create knowledge-based authentication schemes that are memorable, usable, and secure called Multi-tiered Framework for user authentication which based on multimedia password rather than alphanumeric password.

5. Proposed framework

5.1 About proposed framework

To solve the problems with traditional username password authentication, alternative authentication methods, such as Graphical Password have been used which allowing user to choice stronger password by click on images rather than type alphanumeric characters. It’s easy for user to remember his password and too difficult for attackers to guess the password. The proposed framework is a new design and more secure graphical password system, called multi-tiered framework for user authentication.

The proposed framework proposes the concept of creating graphical password to provide secured authentication. This system solves the problem of remembering alphanumeric or several click-points by replacing multiple image sequence with a single window containing a set of images. The visual representation of the images is in form of 4x4 matrix which includes both elements and the non-elements. Since the window frame contains 16 images it is completely impossible for the attackers to guess the sequence of click-points on the images. Additionally the proposed work introduces a sound signature technique that improves the remembrance of the password. Also includes shuffling the sequence of images contained in the window frame. The proposed system performs well in terms of security, accuracy and ease of use.

5.1 Objectives of the proposed framework

1) To prevent an unauthorized user from gaining access to confidential information of an individual or organization and to increase the performance of a knowledge-based authentication mechanism in security systems. Since existing graphical password schemes make use of larger memory space and require long-term password memorabilia, unlike the proposed framework provides higher level of security with reduce chances to guess from attackers.

2) To satisfy the information security triangle (C.I.A):
   a. Confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
   b. Integrity: The property of safeguarding the accuracy and completeness of information's.
c. Availability: The property of being accessible and usable upon demand by an authorized user.

3) The proposed framework allowing users to choice stronger passwords, easy to remember and hard to guess from the attackers side. In fact, this approach makes choosing a more secure password rather than increasing the burden on users to remember a lot for characters and numbers and special characters, it is easier to follow the system’s suggestions for a secure password.

5.3 Features of proposed Framework

1) The probability of guessing the password is relatively low when compared to earlier techniques.
2) The non-elements present in the window also pretends to be as original click-points when an adversary attempts to compromise the system.
3) The viewpoint in existing system is suggested by the system whereas in proposed framework the choice of click-point (selecting images) are user friendly.
4) Access to the system is provided only when the image sequence and audio signature are synchronized.
5) The system finds its application in protecting confidential information of an individual or an organization as a whole.

6. Implementation

6.1 Implementation module

The implementation has mainly three modules: New user registration, Existing user Login and Recovering Password.

The new users should give user-ID, then answer for some unique security questions, which is based on his personal details. The Audio was played by the user before selecting the images, duration of playing, user must select the eight click-points on images out of sixteen click-points and then click register button. The actual time taken from the first click-point to the eighth click-point is consider on authentication process.

Users select their own click-based graphical passwords without guidance, hotspots will remain an issue. By adding shuffling feature encourages users to select less predictable passwords, and makes it more difficult to select passwords where all eight click-points are hotspots. The viewpoint is positioned randomly, rather than specifically to avoid known hotspots, since such information might allow attackers to improve guesses and could lead to the formation of new hotspots.

6.1.2 Existing user Login:

Existing users should give user-ID and play Mp3 player. The Audio was played by the user, duration of playing, user must be select the eight click-points and then click on login button. The actual time taken from the first click-point to the eighth click-point in registration process. The user must select the click-points on during the play audio, if not, the user not entered correctly. If user done above things correctly he or she enter into database.

6.1.3 Recovering Password:

The user could retrieve password (the sequence of selected eight images) by using the security question that he entered during the registration process. The user retrieve password by getting the current shuffled picture matrix value they assign into the matrix value then get the user password and assign to the current password hidden format in the matrix value.

6.2 Data Flow Diagram

1) DFD is a simple graphical formalism that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data is generated by this system.
2) DFD is used to model the system components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system.
3) DFD shows how the information moves through the system and how it is modified by a series of transformations.
4) DFD may be used to represent a system at any level of abstraction. It may be partitioned into levels that represent increasing information flow and functional detail.
Figure 3. Data Flow Diagram

- **New User**
  - Admin Authentication
  - Registration Process
    - Create user ID
    - Selecting Require mp3 time
    - Select Image Sequence
      - Set security questions
        - Register
          - Create user profile vector
    - User profile vector
- **Forget Password**
  - User Login
    - User ID
      - Play Audio and Image Sequence
        - Compare with Registered Profile
          - Request
            - Yes: Correct
              - Login
                - Logout/shuffle
            - No: Terminate
  - Answer the security question
  - Detect the Password image sequence

6.3 UML DIAGRAM

UML stands for Unified Modeling Language. UML is a standardized general-purpose modeling language in the field of object-oriented software engineering. The standard is managed, and was created by, the Object Management Group. The goal is for UML to become a common language for creating models of object-oriented computer software. In its current form, UML are consisted of two major components: a Meta-model and a notation. In the future, some form of method or process may also be added to; or associated with, UML.

The Unified Modeling Language is a standard language for specifying, Visualization, Constructing and documenting the artifacts of software system, as well as for business modeling and other non-software systems. The UML represents a collection of best engineering practices that have proven successful in the modeling of large and complex systems. The UML is a very important part of developing objects oriented software and the software development process. The UML uses mostly graphical notations to express the design of software projects.

The Primary goals in the design of the UML are as follows:
1) Provide users a ready-to-use, expressive visual modeling Language so that they can develop and exchange meaningful models.
2) Provide extensibility and specialization mechanisms to extend the core concepts.
3) Be independent of particular programming languages and development process.
4) Provide a formal basis for understanding the modeling language.
5) Encourage the growth of OO tools market.
6) Support higher level development concepts such as collaborations, frameworks, patterns.
7) Integrate best practices.

6.4 Use Case Diagram:

A use case diagram in the Unified Modeling Language (UML) is a type of behavioral diagram defined by and created from a Use-case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases. The main purpose of a use case diagram is to show what system functions are performed for which actor. Roles of the actors in the system can be depicted.

6.5 Implementation Procedure

The project is developed in .NET Framework in the support of C#.NET as front end. SQL server 2010 as back end and the development tool used is Microsoft Visual Studio 2010. The Home page is first designed with required backgrounds and texts. The other user interfaces are developed with text boxes, labels, buttons, images, sound files according to the requirements for increasing knowledge based-authentication. The project consists of three pages for accessing. They are: New user Registration page, Existing user page, Recovering the Password. The User registration page consists of details required for a user to register to the application. The existing user page is accessed by users who are already registered. The required coding for the project is done and back-end database created in MS SQL Server with the required data and the front end is linked and configured with the back-end database. After completion of the designing, coding and configuration with the back-end the project is executed. The various steps of implementation for the proposed framework are:

Step-1: Registration of the New User
  - Click the images as password
  - Set the sound file

Step-2: Login of the Registered User
  - User name
  - Play Mp3
  - Authentication through images

Step-3: Recovering the password
  - Security questions
  - Correct Sequence Matrix
6.6 System Architecture

**Figure 5. Proposed System Architecture**
Conclusion

The most common computer authentication method is for a user to submit a user name and password consisting of text, numbers or together even with special characters. The vulnerabilities of this method have been well known for attackers to guess, because the users often create memorable passwords that are easy for attackers to guess, but strong system-assigned passwords are difficult for users to remember. The use of strong passwords reduces the risk of unauthorized access, and difficult task of trying to break all the password. This paper gives an idea of having a secured effective authentication system, which provides strong and easily remembered graphical passwords with dynamic security level.

A major advantage of this proposed framework, is to large password space over alphanumeric passwords. There is a growing interest for Graphical passwords since they are better than Text based passwords, although the main argument for graphical passwords is that people are better at memorizing graphical passwords than text-based passwords.

References


