Three Level Authentication System

[1]Lokesh K, [2]Saba Annamalai V, [3]Jai K

[1]Information Security and Digital Forensics,
[1]Dr.M.G.R. Educational and Research Institute, Chennai, India

Abstract: The project is an authentication system that validates user for accessing the system only when they have enter the correct password. The project involves three levels of user authentication emphasizing the Defense-in-Depth (DiD) mechanism. There are varieties of password systems available, many of which have failed due to bot attacks while few have sustained it but to a limit. It contains three logins having three different kinds of password system. The password difficulty increases with each level. Users have to input correct password for successful login. Users would be given privilege to set passwords according to their wish. The project comprises of text password i.e. pass phrase, image based segmentation password and fingerprint authentication password for the three levels respectively. Hence while creating the technology the emphasis was put on the use of innovative and nontraditional methods.

INTRODUCTION

Authentication is any protocol or process that permits one entity to establish the identity of another entity [5]. Nowadays, we can say password is mostly widely used to verify and authenticate users. For instance, online banking system is important to have high security level to secure user's accounts and protect their asset as well as their personal datum from malicious hands. One of the method to secure system is by using password. Password is a secret word or phrase created by the user in ensuring unauthorized user cannot access the restricted resource. At the same time, it is well known that there is a tension between the security and usability of passwords. Oftentimes, secure passwords tend to be difficult to memorize (i.e., less usable), whereas passwords that are memorable tend to be predictable [7]. Generally, in order for authentication system to be practical, three level authentication is designed to provide additional security. There are many schemes that had been proposed but still have their weaknesses. For your information, the three level authentication is the combination of three existing scheme which is text-based password, image-segmentation and fingerprint authentication to form a better protection. In this, the traditional method used is text- based password. These type of password are strings of letters and digits. In this technique, the password is usually short and easy to predict that lead to malicious activities easily. Hence, to increase the level of security in a system, three level authentication is proposed.

PURPOSE

Three-factor authentication is mainly used in businesses and government agencies that require high degrees of security. The use of at least one element from each category is required for a system to be considered three-factor authentication -- selecting three authentication factors from two categories qualifies only as two-factor authentication (2FA). An additional factor, location, is sometimes employed for four-factor authentication (4FA).

EXISTING SYSTEM

Many password policies require the use of punctuation marks and other special characters, IT often recommends users take words and phrases and replace some letters with those symbols. However, hackers are catching on to those tactics and they can now be accounted for in **password-cracking algorithms**.

PROPOSED SYSTEM

It contains three logins having three different kinds of password system. The password difficulty increases with each level. Users would be given privilege to set passwords according to their wish. The project comprises of text password, image based password and fingerprint authentication for the three levels respectively. This way there would be negligible chances of bot or anyone to crack passwords even if they have cracked the first level or second level, it would be impossible to crack the third one.

OBJECTIVES

The aim of this project is to evaluate the effectiveness of using three level authentication system to improve the security system. The objectives are as follows:

i. To design an implementation of password authentication that give highest security in authenticating users.
ii. To implement the applications/system that more user friendly.
iii. To test and evaluate the authentication scheme in preventing unauthorized access

SYSTEM ARCHITECTURE

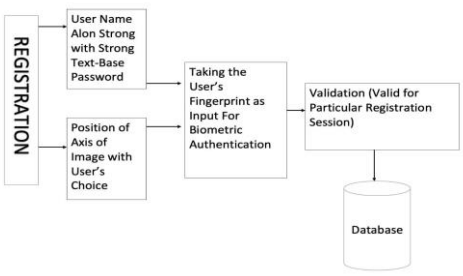

Fig 1.1

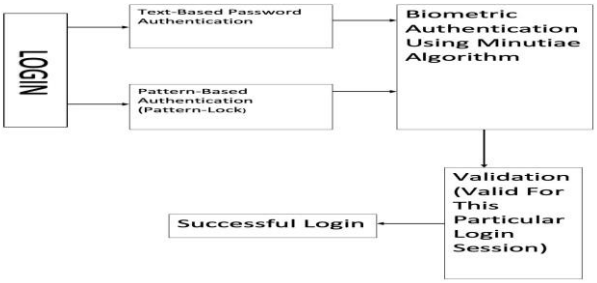

Fig 1.2

METHODOLOGY

Text Password:

In the registration phase in Figure1.1, the user should provide user's details like user name and user conventional textual password which is as strong as much and difficult to guess. This will protect the system from attacker.

Image Based Authentication:

In the registration phase the user has to select minimum 4 images to 40 images for the image axis authentication.

The user then has to select the images in the chronological order for the authentication, which he previously registered.

Fingerprint Authentication:

First, the user have to imprint the finger for impression, which is then converts the retrieved minutiae sets into 2D image spaces. Then the transformation parameters are calculated using phase correlation between two MDMs to align two fingerprints to be matched. The similarity of two fingerprints is determined by the distance between two minutiae sets. User has to provide the impression when prompted for the authentication to login as said in fig1.2.

CONCLUSION

Based on the research, providing a 3-level authentication password scheme is better than a single-factor authentication because it needs to pass through the 3 levels to authenticate successfully. The main reason proposed for this scheme is to enhance the security of computer system. Based on [16], it will certainly be a great enhancement especially in the areas where high security is the main issue and time complexity is secondary. For instance, application of this system at a firm or industry or institute where it will be accessible only to some higher designation holding people, who need to store and maintain the crucial and confidential data secure[17]. However, since this authentication scheme is not yet widely deployed, the vulnerabilities are still not fully understood and user still need training about how to use the 3-level authentication password scheme.

REFERENCES

1. Mughele Ese Sophia, 2015, THREE – LEVEL PASSWORD AUTHENTICATION
2. Babich, A, 2012, Biometric Authentication, Type of Biometric Identifier
3. Gayathiri Charathsandran, Text Password Survey: Transition from First Generation to Second Generation
4. A.T. Akinwale and F.T. Ibharalu, 2009, Password Authentication Scheme with Secure Login Interface
5. Priti Jadhao, Lalit Dole; 2013; Survey on Authenticate Password Technique
6. Cynthia Kuo, Sasha Romanosky, Lorrie Faith Cranor; 2006; Human Selection of Mnemonic Phrase-based Passwords
7. Weining Yang, Ninghui Li, Omar Chowdhury, Aiping Xiong, Robert W. Proctor; 2016; An Empirical Study of Mnemonic Sentence-based Password Generation Strategies
8. Lalu Varghese, Nadiya Mathew, Sumy Saju, Vishnu K Prasad, 2014, 3-Level Password Authentication System
9. Blonder G. (1996) In Lucent Technologies, Inc., Murray Hill, NJ, United States Patent 5559961
10. Aakansha Gokhale, Vijaya Waghmare; 2014 A Study of Various Passwords Authentication Techniques
11. Dr. Swapna Borde, Gauri Satish Tambe, Suchita Ramdas Tambade; 2016; Two Level Password Authentication System
12. Ahmad Almulhem Computer Engineering Department King Fahd University of Petroleum and Minerals Dhahran.Saudi Arabia, A Graphical Password Authentication System.
13. Sayli Chavan, Shardul Gaikwad, Prathama Parab, Govind Wakure; 2015; Graphical Password Authentication
14. Chiasson, S., van Oorschot, P.C., Biddle, R. Graphical Password Authentication Using Cued Click-Cued Click-points. ESORICS 2007.