Research Inventy: International Journal of Engineering And Science
Vol.6, Issue 5 (May 2016), PP -92-95
Issn (e): 2278-4721, Issn (p):2319-6483, www.researchinventy.com

Activity Based Secure Login Mechanism

Prof.MD Sameeruddin Khan[1], AVSM ADISHESHU[2], Prof.GVNKV Subbarao[3],
[1, 2, 3] *Computer Science Engineering Department, Sree Dattha Institute of Engineering & Science*

Abstract: *One of the most imperative topics in information security today is user authentication & authorization. In today's insecure information world any login activity must be secure from hackers who can access the authorized system in an unauthorized manner. Authentication is protecting any system from unauthorized access. Current authentication mechanisms suffer from many flaws. With the express growth of internet and its usage, there is probability for hackers to obtain the textual passwords with ease because most of the users choose their textual passwords which are usually the common words from dictionary or phrases from day to day life; which can be easily obtained by shoulder surfing attack or by guess. To overcome the shoulder surfing attacks we propose an idea that makes use of activity based secure login mechanism which is a pre-defined collection of activities. In activity based login the user needs to select the activity for each login attempt after entering user name and password which is predefined by the user during sign up process. Though the text password is known to the unauthorized user he/she will not be able to login because the unauthorized user is not aware of activity that should be chosen for the current attempt. The user should choose the activity from the activity list as per login attempt. The user may be allowed to choose any number of activity types and any number of activity objects in each activity type during the registration. In the initial development phase of the proposed idea we plan to choose only on activity type and three objects of that activity type.*

Keywords: *Login, Authentication, Authorization, Activity, Activity-Type, Activity-Object.*

I. Introduction

In the present authentication the user's experiences are easy in which individual access to a computer system is controlled by identifying and authenticating the user through the credentials like username and password provided during the registration process. Though a lot of technologies are around, it can be easy for an unauthorized user to steal identity of the user through guess or shoulder surfing attack. Shoulder surfing attack occurs when a user enters details using a keyboard, mouse or any traditional input device a malicious observer may be able to obtain the user's password credentials using direct observation techniques, such as looking over someone's shoulder, PINs and other sensitive personal details.This is a problem that has been difficult to overcome.There are some techniques providing secure image mechanism where user has to choose the single image displayed on the login page after entering username and password. This mechanism fails to avoid shoulder surfing attack.There are some login systems that uses CAPTCHA mechanism which is perceived as a quick and effective way to stop bots from performing abusive actions on a website but this is also unable to avoid the shoulder surfing attack.

The following are some of the security attributes for login:

Authenticity: The authenticity is the state of something being authentic and true. Authenticity is important when the value of something is dependent on where it came from or how it was made.

Integrity: Integrity of information refers to protecting information from being modified by unauthorized parties.

Confidentiality: Confidentiality is whether the information stored on a system is protected against unintentional or illegal access. Since systems are sometimes used to handle sensitive information, Data Confidentiality is often a measure of the ability of the system to protect its data

This paper discusses and implements the proposed technique used for performing login task. The following sections are reserved for discussing: Literature survey in section 2, proposed system in section 3 and results in section 4 by concluding in section 5.

II. Literature Survey

In [1] the authors proposed an idea to make use of 3-D password technique. The advantage of this technique is it provides passwords which are easy to remember and very difficult for intruders to guess and also these passwords can be easily revoked or changed. The disadvantage of this technique is as compared to traditional password approach this approach will take more time to authenticate the user. More storage space is required because it needs to save images which are large binary objects and this mechanism fails to remove shoulder suffering attack. This technique requires devices like web camera, finger print device etc.so it is costly.

In [2] the authors proposed an idea to implement graphical password using different techniques like biometric, smart cards. 3D is based on virtual environment. It concludes that 3D password is somehow free from shoulder

surfing attack and is free from hacking if compared with textual password or graphical password because there is no appropriate sequence of selecting of images as it is used in graphical images. Also this paper describes the idea of implementing 3-D password technique using activity or pass point objects which must be memorable to the user.

In [3] the authors described the watermarking concept and its implementation. This will reduce the efforts expected from the user and thus will provide more luxury. The concept of Watermarking has limited-functionality as Watermarked multimedia objects are not still resilient to attacks rather they are susceptible to attacks because the digital contents can be digitally edited.

In [4] the authors proposed an idea on graphical password techniques. Author classifies technique in two parts one is recognition based and second is recall based. Firstly author discussed about drawbacks of textual password and then discussed the strengths and limitations of each method of graphical password and point out the future research directions in this area.

From all references it is found that various ideas of authentication technique can be used for implementation purpose. The proposed idea for login system can be implemented with multiple activities and due to the use of multiple activities unauthorized user will unable to hack the system because he has to perform different activity as per login attempt.

III. Proposed System

The proposed system aims to make use of activity based login mechanism to avoid shoulder surfing attack. The proposed idea in this paper is about to make use of activity based secure login system with a pre-defined collection of activities. In activity based login mechanism the first step is sign up process in which user need to enter his/her credentials and number of activities according to his/her login attempts per day.After this the user needs to choose the activity type for each login attempt and objects for each activity type,this will act as password for that activity type. Once this process is successfully completed user will get one message of activity sequence on his mobile number provided during sign up process.This will be helpful at the time when user forgets the activity type and its sequence,so that he can use this message to perform the correct activity and login to system.Then the next step is login process in which user needs to select the activity after entering user name and password which is predefined by the user during sign up process. Once the correct activity type is selected user need to select objects for that activity type which user had set during sign up process after this user can successfully logged in to the system. The proposed system prototype limits the login attempts per day as user has to set the number of login attempts as many times he wants to login to system in one day.When the number of login attempts exceeds then the activities will follow the circular path like it will go to the first activity for that login attempt number and so on. If the textual password is known to the unauthorized user he/she will not be able to login because the unauthorized user is not aware of activity type that should be chosen for the current login time and if he/she tries for more than two times to login to system then he will be blocked and one message about this will be sent to authorized user.The overall goal of this mechanism is to enhance the login process and to make it more secure by incorporating the activity based login mechanism and avoid shoulder surfing attack. At intial phase of development of proposed idea we plan to choose only one activity type and objects of that activity type.Once the object is selected for particular activity, our tool will authenticate it and crosscheck with the information in database. In this case, we are applying various activities data so that it is rendered safe from the shoulder surfing attack. One additional feature of this proposed idea is user can update the activity type and activity sequence.Also user can update the objects for each activity type as per his/her choice.

The following are some of the activity types that will be performed in this mechanism:

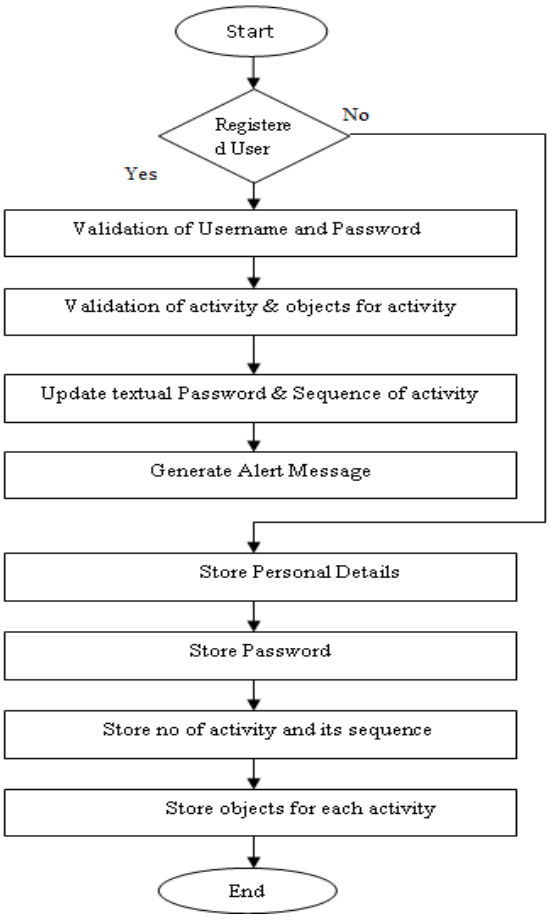
1) Security question
2) Sequence of images
3) Play an audio
4) Play the video
5) Selecting a single image
6) Selecting sequence of numbers
7) Captcha
8) Opening Microsoft word or any other in built application

Activity based secure login mechanism is divided into four modules as follows:

1. User: User is one of the modules who have to perform activities for authentication and login purpose.
2. System: This is the functional module of activity based secure login mechanism.
3. Activity: Activity is the module that interfaces the user and system**.**
4. Database: This module is used to store and retrieve the data that is entered by the user.

5. The proposed idea is about to create one tool which will demonstrate activity based secure login mechanism. As this project is related to security, JAVA technology will be used.
6. Database is required for storing and retrieving personal and security related information about user.

Flow Chart for system:
This diagram shows the flow of activities that are carried out by the user and system. The following flow chart is for both registered and non registered user.



IV. Results

This section contains the results obtained after the implementation of activity based secure login mechanism. This following figure shows the first page of proposed login mechanism. User may first fill the login form if he is registered otherwise he/she must perform sign up process.

Fig1. Home page of Activity based Secure Login Mechanism

The following diagram shows the actual working of proposed idea about selecting activity from activity list.

Fig 2. Selecting activity from activity list for activity based secure login mechanism

V. Conclusion

In this paper we explored the concept of activity based secure login system. This concludes that this system is free from shoulder surfing attack and is free from hacking with the help of multiple activities as per sequence for each login number.

References

[1.] Shubham Bhardwaj, Varun Gandhi, Varsha Yadav, Lalit Poddar "New Era of authentication: 3-D Password" , in International Journal of Science, Engineering and Technology Research (IJSETR) Volume 1, Issue 5, November 2012.

[2.] Banita Chadha Dr. Puneet Goswami "Cryptanalysis to Secure System" in: International Journal of Advanced Research in July 2014

[3.] Rahul Ingle, Mayuri Bawane, Karishma Dudhbade, Reena Tijare, Prof. Sneha Ramteke "A Secure Recognition Based Graphical Password by Watermarking",in:International Journalof Advanced Research in Computer Science and Software Engineering Volume 4, Issue 3,March 2014

[4.] Xiaoyuan Suo, Ying Zhu, G.Scott. Owen "Research paper on Graphical Passwords: A Survey", Department of Computer Science, Georgia State University.