New Security System for Preventing Data over Shoulder Surfing Attacks

ATMURI NAGA SOWJANYA [#1] & Y.SRINIVASA RAJU [#2] & D.D.D.SURIBABU [#3]
[#1] M.Sc Student, Master of Computer Science, D.N.R. College, P.G.Courses & Research Center, Bhimavaram, AP, India.
[#3] Assistant Professor, Master of Computer Science, D.N.R. College, P.G.Courses & Research Center, Bhimavaram, AP, India.
[#3] Head & Associate Professor, Dept of CSE, D.N.R. College of Engineering, Bhimavaram, AP, India.

Received: January 09, 2019 Accepted: February 14, 2019

ABSTRACT: *In recent days security plays a very major role in each and every domain including IT, insurance, banking, shopping, online services and so on. Hackers are becoming more and more advantage in finding sensitive information illegally by hacking others accounts. Some of the hacking techniques which are used by hackers are password based attacks, shoulder surfing attacks and dictionary attacks. Hence text based passwords are easy to guess and break that graphical based passwords. Hence in this proposed thesis we try to design graphical passwords (GP's) which consists of either click events or drag events on pictures. So with this new type of authenticated passwords, it is the new option to overcome the problems that arise while using text-based passwords system. In this paper, a graphical password system with a supportive sound signature to increase the remembrance of the password is discussed. In proposed work a click-based graphical password scheme called Cued Click Points (CCP) is presented. In this system a password consists of sequence of random images in which user can select one grid per image. By conducting various experiments on our proposed mechanism, we finally came to a conclusion that this approach is very best suited to achieve data integrity.*

Key Words*: Click Points, Sensitive Information, Graphical Passwords, Guess Attacks, Randow Signatures.*

I. Introduction

As we all know that there was a lot of research work done on this security systems and as per the research work, it clearly tells that there was mainly three important areas where human computer interaction is important. They are as follows

1) Authentication
2) Security Operations, and
3) Developing secure systems.

In the field of information security (IS) the primary element for any user is nothing but authentication of user. Authentication is the process of allowing /accepting or denying/restricting access to an individual's who claim with their identity. Authentication process asks users to memorize/remember the valid login passwords and recall them during log-in time process [1].

In order to do authentication of system most of the users select text based passwords as the userid and password which was maximum predictable in nature [2]. User try to choose a remember able passwords which are mostly memorable and easy to remember, unfortunately this is the easy way where hackers are easily attacking the systems by breaking the predictable passwords. While this predictability problem can be solved by not allowing users choice of giving his/her own passwords [3].

Text Based Passwords are majorly used for:

(a) **AUTHENTICATION**
It is a Process of identifying the user credentials are correct or wrong. This is one of the major feature used for authenticating each and every individual user.

(b) **AUTHORIZATION**
This process is mainly used in order to find out the person is valid user or not.

(c) **ACCESS CONTROL**
This is the last feature in which the access control can be provided for access-includes authentication & authorization.

II. Background Knowledge

In this section we mainly try to discuss about the background work that is carried out in order to identify the individual functionalities of each and every module.

Main Motivation

Cued Click Points (CCP) is a proposed alternative to Pass Points. In CCP, the users use the techniques in very different and new way when compared with existing graphical password methodology. Here in this new proposed technique users click one point on each of 3 individual images rather than like clicking on three points on one image. During this process, the attack that was based on hotspot analysis is also a more challenging task for this method implementation. Figure 1, clearly shows that each click results in showing a next-image, in effect leading users down a "path" as they click on their sequence of points until last point is reached in last image.

By combining both textual and graphical based password authentication schemes, it is possible to design an authentication technique that is resistant to all of the following attacks:

Key Loggers Attack

A key logger is a type of surveillance software that has the capability to record every keystroke the user makes, into a log file. Usually, banks and other organizations provide their customers with a unique, short-length Personal Identification Number (PIN) which is used as a password for online login. But, such short length passwords are easier for the attacker to memorize through keystroke monitoring or shoulder surfing. Even if the password is of a longer length, for example, in systems like Email, it is not a big task for the attacker to capture keystrokes using key loggers.

Shoulder Surfing Attack

Shoulder surfing attack refers to using direct observation techniques, such as looking over someone's shoulder, to get information.

Dictionary Attacks:

A dictionary attack is a method of breaking into a password-protected computer or server by systematically entering every word in a dictionary as a password.

III. Proposed Grid Based Image Authentication

In our proposed work we try to propose an grid based image authentication in which image is mainly divided into various small blocks and each and every individual block takes the co-ordinates from X and Y axis. The image is mainly divided into multiple parts like 12 * 12, with height and width as 0.5 cm and 1 cm.For more security we try to use multiple images in order to give more and more security for the data, where 3 random images are taken as input and each and every individual image takes one input and on a combination of three images gives three random click points in order to store and access the data[4].The partition of image is treated as detailed vector and this is explained as follows:

Detailed Vector

Based on the master vector data, the detailed vector with the following parameters is converted and displayed as

(Image, Click Points)

As an example of vectors

Master vector (DNRStudent, 2689, 50)

Detailed Vector for the user Profile DNR Student is

Image	Click points
I_1	(123,678)
I_2	(176,134)
I_3	(450,297)
I_4	(761,164)

Figure. 1 Represents a Random of Three Images with Individual Image selected with one Grid

From the above figure 1, we can clearly identify each and every image is choosing with one selected grid, and a random of three images with three individual grids is selected. These three corresponding values will be stored into the database and once if any user who need to verify the identities then he/she will be identified based on these grids and if all the three grids are matched correctly then the account can be login success[5]. If the same user try to attempt any three wrong attempts then the account will be automatically blocked.

IV. Implementation Modules

Implementation is a stage where theoretical design is automatically converted into programmatically manner. For this the application is divided into number of modules. The application is mainly divided into 5 modules, they are as follows:

1. Multi Layer Image Authentication
2. Grid Image Authentication
3. Login / Register
4. Upload Data
5. Download the Data

1) Multi Layer Image Authentication

Here in this module the image is mainly divided into small blocks in order to maintain security[6]. Each and every block is known as grid in which user need to choose individual grid at the time of registration and login in order to enter into their accounts.

2) Grid Image Authentication

In this type of authentication multiple images can be provided to the user, the user has the select the image that he can to log in, this will they provide more security.

3) Login / Register Module

Here the user need to register first with all the above details along with image as security and the same details he/she need to substitute at the time of login into the system[7].

4) Upload Data

Here the admin try to upload the data for the users and those users who successfully registered or login need to enter their details correctly in order to download the data from the admin.This module is mainly used to provide data for the end users.

5) Download the Data

Here the data users try to download the data once after successfully verifying all the login credentials and image as a security. During the image authentication if any user try to do 3 wrong attempts for downloading the data, the user account will be automatically blocked by the system and the same account can be activated again by the admin only[8].

V. Conclusion

In this paper we finally implemented a new authentication approach for password authentication which uses grid based authentication along with text based password authentication. Till today, there was no implementation of such a kind of system which is helpful for any user to store and access the data in a secure manner. By this application for the first time we have achieved highest level of data integrity for the data what we want to store or retrieve securely.

VI. References

1. Luis von Ahn, Manuel Blum, Nicholas Hopper, and John Langford. CAPTCHA: Using Hard AI Problems for Security. In Proceedings of Eurocrypt, Vol. 2656 (2003), pp. 294-311.
2. Bergmair, Richard (January 7, 2006). "Natural Language Steganography and an "AI-complete" Security Primitive". CiteSeerX: 10.1.1.105.129. (unpublished?)
3. Birget, J.C., D. Hong, and N. Memon. Graphical Passwords Based on Robust Discretization. IEEE Trans. Info. Forensics and Security, 1(3), September 2006.
4. R. N. Shepard, "Recognition memory for words, sentences, and pictures," Journal of Verbal Learning and Verbal Behavior, vol. 6, pp. 156-163, 1967.
5. D. Weinshall and S. Kirkpatrick, "Passwords You'll Never Forget, but Can't Recall," in Proceedings of Conference on Human Factors in Computing Systems (CHI). Vienna, Austria: ACM, 2004, pp. 1399-1402.
6. Blonder, G.E. Graphical Passwords. United States Patent 5,559,961, 1996.
7. Chiasson, S., R. Biddle, R., and P.C. van Oorschot. A Second Look at the Usability of Click-based Graphical Passwords. ACM SOUPS, 2007.
8. Davis, D., F. Monrose, and M.K. Reiter. On User Choice in Graphical Password Schemes. 13th USENIX Security Symposium, 2004.
9. R. Curtmola, J.A. Garay, S. Kamara, and R. Ostrovsky, "Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions,"Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06), 2006.
10. Y.-C. Chang and M. Mitzenmacher, "Privacy Preserving Keyword Searches on Remote Encrypted Data," Proc. Third Int'l Conf. Applied Cryptography and Network Security, 2005.
11. A. Hiltgen, T. Kramp, and T. Weigold. Secure internet banking authentication. IEEE Security and Privacy, 4:21–29, March 2006.