Graphical-Based Password Keystroke Dynamic Authentication System

Prof P. D. Thakare[1], Samiksha Thakur[2]

[1]Professor, Dept. of Computer Engineering, JCOET, Yavatmal Maharashtra, India
[2]Student, Dept. of Computer Engineering, JCOET, Yavatmal Maharashtra, India

Abstract: *Keystroke Dynamics is biometric used to measure the typing rhythm of the user mainly for user authentication when individual types on the keyboard. The aim of this work is to provide 3 level security for the transaction in banking applications. First, we are authenticating by login id and password. After user authentication, he will be shown with a graphical password screen. Graphical passwords have been designed for more secure and that to make passwords more memorable and easy to use by the people. This project proposes a new graphical-based password and Keystroke Dynamic Authentication system for the secure authentication.*

Key Words: Keystroke Dynamics Authentication (KDA); Graphical Password; Cued Click Points (CCP).

1. INTRODUCTION

User authentication is one of the important issues for access restriction, especially to computer systems. Alphanumeric passwords can easily be hijacked later by some malicious user A possible remedy against such a scenario, is to use Keystroke Dynamics. Keystroke Dynamics is biometric used to measure the typing rhythm of the user for user authentication. The functionality of this biometric is to measure the dwell time and flight time for changing keyboard actions. Keystroke dynamics is biometric that aims to identify humans based on the analysis of typing of rhythms on a keyboard.

Firstly user is authenticated by login id and password .user will be shown with a graphical password screen. Graphical passwords have been designed for more secure and that to make passwords more memorable and easy to use by the people. By Using this technique user clicks on the images instead of typing alphanumeric passwords. The user is shown with a sequence of images with 4x4 blocks; the user has to select N blocks from each image. If the user enters an incorrect click-point during login, the next image displayed will also be incorrect.

Unauthenticated users who see an unrecognized image know that they made an error with their previous click point. Conversely, this implicit feedback is not helpful to an attacker who does not know the expected sequence of images. Third, We measure KDA (Keystroke Dynamic-based Authentication) for a password. This project proposes a new graphical-based password and Keystroke Dynamic Authentication system for the secure authentication. The graphical password enlarges the password space size and promotes the KDA utility in touch screen handheld mobile devices.

2. RELATED WORK

Monrose and Rubin authored one of the earliest works on the free text detection of keystrokes [1]. The authors collected, over a period of seven weeks, typing samples from 42 users performing structured and unstructured tasks in various computing environments. In order to reduce the computational cost of the recognition process, they reduced the search time by clustering the collected data using a variation of the maximum- distance algorithm. The typing speed or a number of words typed per minute, in a given profile was used as the clustering criteria. An obvious limitation of using such an approach for clustering is the need to re-cluster the data as the system is used. Several distance measures were used to compute pattern similarities and dissimilarities including Normalized Euclidean distance, and weighted and non-weighted maximum probability measures. The reference profile was constructed by computing the mean and standard deviations for the timing samples. Although Monrose and Rubin obtained a 90% correct classification for fixed text detection, they obtained at best (using the weighted probability measure) only a 23% correct classification for free text detection.

In the approach adopted by Dorland et al.[2] typing samples were collected by monitoring users during their regular computing activities, without any particular constraints imposed on them. A user profile was determined by calculating the mean and standard deviation of digraph latency and by considering only the digraphs occurring a minimum number of times across the collected typing samples. By collecting and analyzing data for five users.

[3] Presents analysis of keystroke dynamics with fixed text (corresponding to keystroked passwords). Publication [5] examines database quality for keystroke dynamics authentication using two databases: the first KDS database remotely collected by the authors and the second Keystroke Dynamics Benchmark Data Set collected with specialized high precision keyboards.

Paper [6] gives Authentication methods based on biometrics techniques and efficient user authentication with keystroke dynamics using non-fixed text of various size. We Author Gives small group of individuals, with data gathered in various ways: over Internet using browser-based WWW application and on local machines using dedicated applications. The obtained results can be used for future keystrokes database creation.

[7]Author gives free text analysis of keystrokes that combines monograph and digraph analysis, and uses a

neural network to predict missing digraphs based on the relation between the monitored keystrokes. This achieves an more accuracy level comparable to the previous related techniques. free text analysis systems, which are based on limited or fixed-text enrollment methods, the enrollment process of the proposed detection system is performed with completely free text sample.

[8] Paper gives the graphical passwords scheme to manage the difficulty level of guessing it along with the biometric authentication which is very suitable and efficient method by acquiring low resolution images of nail plate surface. This is highly secure authentication scheme by using user name with graphical password using persuasive cued click points along with biometric authentication using finger nail plate. The scope of the scheme is limited to three fingers and it is used for high security purpose where it is very important to keep tight security.

3. THE PROPOSED SYSTEM

After login by the user at registration time keystroke parameter are registered by using DU, DD, UD, UU, DU2. User allows for selecting N unique images. User Select cued click point on each image and the points are stored in database. After login display images in a sequence. User have to select Select cued click point on each image and Check register ccp .not , if ccp points are same then display next right image else display image from other images.

The dynamics are extracted by measuring the dwell time (the length of time a key is held down) and fly time (the time duration from key released to the next key pressed) for each keyboard. The action can be described by the key code as well as the dwell time. A fig 2 represents a typing action performed by the user from a specific key to another key on the keyboard. The figure action is described by the two key codes of the from/to keys and the fly time between these key.

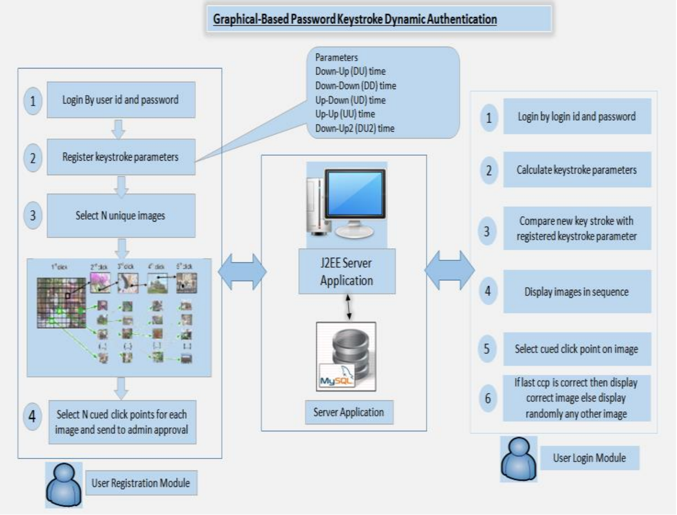
Graphical-Based Password Keystroke Dynamic Authentication
1 Login By user id and password
2 Register keystroke parameters
3 Select N unique images
1st click
2nd click
3rd click
4th click
5th click
4 Select N cued click points for each image and send to admin approval
User Registration Module
Parameters
Down-Up (DU) time
Down-Down (DD) time
Up-Down (UD) time
Up-Up (UU) time
Down-Up2 (DU2) time
J2EE Server Application
MySQL
Server Application
1 Login by login id and password
2 Calculate keystroke parameters
3 Compare new key stroke with registered keystroke parameter
4 Display images in sequence
5 Select cued click point on image
6 If last ccp is correct then display correct image else display randomly any other image
User Login Module

Fig - 1: Architecture of Keystroke Dynamic Authentication System

A. Measuring of KDA Parameters

A touch event includes the on touchdown and up, producing five features DU, DD, UD, UU, DU2 defined as follows. Down-Up (DU) time: DU time is the interval between the same click being pressed and being released Down-Down (DD) time: DD time is the interval between the click being pressed and the next click being pressed

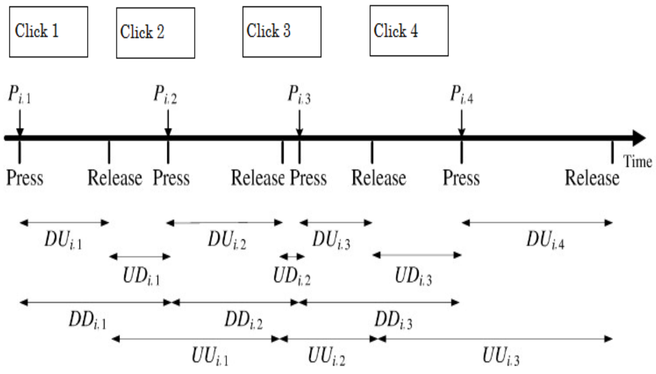

Fig -2: A touch event includes the on touchdown and up

Up-Down (UD) time: UD time is the interval between the click being released and the next click being pressed. Up-Up (UU) time: UU time is the interval between the click being released and the next click being released.Down-Up2 (DU2) time: DU2 time is the interval between the click being pressed and the next click is released.

B. Authenticating User based on KDA parameter:

At the time of registration, user will keystroke dynamic authentication parameters in Database.

At the time of login, system will compare registered parameter of keystroke and login time keystroke parameter if it match then open graphical password authentication window.

C. Authenticate user by Graphical Authentication Using Cued Click- Points (CCP).

At the time of registration, The user will give checkpoint for each image i.e. for example for a particular image split is 3 then that image will get divided into a 3x3 matrix and then checkpoint can be a combination of row and column e.g. (1,2),(2,2)etc. Images and the respective checkpoint is get stored in the database. At the time of login, 1st of all user will give his unique user-id then, will enter click point (which is given at the time of registration) then the system will check the database using CCP if checkpoint for each image matches with checkpoints stored in the database then user login is successful.

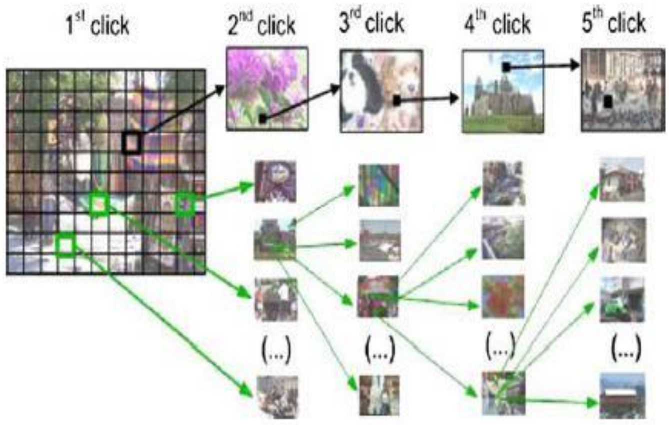

Fig-3: Cued Click Point

4. CONCLUSIONS

In this paper, we presented a new authentication technique keystroke dynamics. this system provides. By using this we would improve security by using keystroke dynamic authentication and graphical authentication in banking applications. High security for authentication. Graphical based authentication scheme and keystroke authentication. It is Easy to remember password using ccp. It Provides high-speed application to a user and friendly application.

REFERENCES

[1] F. Monrose and A. Rubin, "Authentication via keystroke dynamics, in Proc. Fourth ACM Conf. Comput. Commun. Security, pp. 48–56,Apr. 1997.

[2] P. Dowland, S. Furnell, and M. Papadaki, "Keystroke analysis as a method of advanced user authentication and response," inProc. IFIPTC11 17th Int. Conf. Inform. Security: Visions Persp., May 7–9, 2002,pp. 215–226.

[3] M. Rybnik, M. Tabedzki, and K. Saeed, A keystroke dynamics based system for user identification, Computer Information Systems and Industrial Management Applications CISIM 2008, pp. 225 - 230, 2008.

[4] M. Rybnik, P. Panasiuk, and K. Saeed,User Authentication with Keystroke Dynamics using Fixed Text , International Conference on Biometrics and Kansei Engineering – ICBAKE 2009, pp. 70 - 75, 2009.

[5] M. Rybnik, P. Panasiuk, and K. Saeed "Advances in the Keystroke Dynamics: the Practical Impact of Database Quality", Lecture Notes in Computer Science (LNCS), Vol. 7564,Computer Information Systems and Industrial Management, Proceedings of 11th IFIP TC 8 International Conference, CISIM 2012, pp. 203-214, Venice, Italy, September 26-28,2012.

[6] Mariusz Rybnik,Marek Tabedzki, Marcin Adamski,Khalid Saeed,"An Exploration of Keystroke Dynamics Authentication using Non-fixed Text of Various Length",2013 International Conference on Biometrics and Kansei Engineering.

[7] Ahmed A. Ahmed and Issa Traore,"Biometric Recognition Based on Free-Text Keystroke Dynamics",IEEE TRANSACTIONS ON CYBERNETICS, VOL. 44, NO. 4, APRIL 2014.

[8] Ushir Kishori Narhar,Ram B. Joshi,"Highly Secure Authentication Scheme",2015 International Conference on Computing Communication Control and Automation.

[9] K. Killourhy and R.A. Maxion. (2009, June29).Key stroke Dynamics - Benchmark Data Set [Online]. Available: http://www.cs.cmu.edu/ keystroke/

[10] K.S. Killourhy and R.A. Maxion, The Effect of Clock Resolution on Keystroke Dynamics. In Proc. of the 11th International Symposium on Recent Advances in Intrusion Detection,(RAID-08), Cambridge, MA, 2008.