Password generator Based on Mouse Clicks Signal and Screen Cursor Position

Abdurazzag Ali Aburas and Manal I. Al_Fallah
Electrical and Computer Engineering Department, International Islamic University Malaysia
aburas06@iiu.edu.my, manalalfallah@yahoo.co.uk

Abstract

The passwords are the keys you are using to access personal information that you've stored on your computer and in your online accounts. A strong password should appear to be a random string of characters. Online accounts, computer files, and personal information are more secure when you use strong passwords to help protect them. Unfortunately, it is hard to create easy to use, strong passwords and keep them well protected. In this research, new method of generating complex password based on mouse clicks and cursor coordinates position on screen is presented. Our aims are that use can successfully generate complex and secure password based on computer mouse clicks and cursor position on the screen. Our implemented system can differentiate individuals based on mouse clicks, screen positions and user time. This approach is different from techniques referred to as "voice & text password" which adding the user voice to his/her text password or "keystrokes password" which using the user typing key approach.

Keywords*: password, personal information, mouse clicks, cursor coordinates, text password*

I. INTRODUCTION

Personal Computers have become central in our daily life for many years. Spreading wireless technology has become main part of our PC communications. The users have asked to have password to access different applications such as internet platforms. The user used the traditional and most comment method to great a password which is keyboard. The fewer types of characters in your password, the longer it must be. A fifteen characters password composed only of random letters and numbers is about over thirty thousand times stronger than an eight characters password composed of characters from the entire keyboard. Many systems also support use of the space bar in passwords, so user can create a phrase made of many words a "pass phrase". A pass phrase is often easier to remember than a text continue (no space) password, as well as longer and harder to guess and it is called a blank password (no password at all). If criminals or other malicious users steal this information, they can use your information to open your personal PC or secret database. To prevent the possibility of steal password, this work is introduce a new and secure method of generating user password based on mouse clicks and cursor coordinates position on the screen (monitor coordinates).

The computer mouse is the most popular device have used by user to interact with any soft application. The mouse click detection methodology has been calculated [1][2][3]. The computer mouse itself is a barrier due to lack the fine motor control it requires. Devices that detect electromyographic (EMG) voltage potentials can provide alternative solution for user with disabilities to emulate mouse click events to type its password [1][4]. Many software programmers designer are concentrate of using computer mouse of making the Graphic User Interface (GUI) easy to use. It has a clear implementations commands to help a normal user of getting the best of their produced application [5][6][7][8][9][10]. At present time, it is notice that all advanced and top of the art technology such as 3D colorful graphic user interface which used for Internet applications and a lot of multimedia material have been included password to allowed user to access it via its interface.

In the next section, proposal approach is presented for generating complex password to the most existing software package over personal computer or different Network platform. The idea behind this work is construction of software media used as an invisible interfaced between the computer mouse and the user. This media program first determent the cursor coordinates (locations) on the computer screen monitor which is location of x and y coordinates using mouse click controls of the left click mouse bottom. Section 3, The Interface architecture is described. In section 4, password data code stream generation is explained.

978-1-4244-1692-9/08/$25.00 ©2008 IEEE

Section 5 the proposed online user password setting is discussed. In Section 6, The Analysis of the proposed technique presented and finally, conclusion for the proposed approach is given in Section 7.

II. PROPOSED METHOD

In this section, the discussion of the interesting and motivating factors in building up the invisible interface program for tracing and monitoring user clicks over the computer screen. Our research attention has been given to mouse clicks processes and makes adaptation as sequences of events (types/clicks) from the user with a mechanism of feedback. It can be fast and accurate method for creating sequence of stream equivalent to the sequence of characters used as password and tracing any user identity at any given time. Looking over the problem, the entire password is used to access a computer either individual or over LAN. Thus, the keyboard has been used to enter their password and perform their tasks via graphic interface commands. The mouse clicks in our research work is essential because the mouse provide easy movement, performance and control by the user over the screen interface which reflect the high security of passing the password to the computer system. Hence, it makes the process of generating or typing (entering) invisible password by the proposed approach interfaced program is valid and effective of accessing their private information over different platform. A commitment to quality work that indicates the users cares personally about the best way of accessing the information. Intrinsic motivation takes over for extrinsic motivation for the above reason; invisible media programs have been built as password generator such that the main input to this media program is the mouse click controls, its cursor locations movements over the screen and clicking user time scale. The simulation of the mouse controls and the screen monitor are given because it is very easy and well known its function. The term "invisible" is used as better description for proposed approach.

III. THE INTERFACE ARCHITECTURE

For simplicity the proposed approach invisible interface media program working on simulated screen monitor which divided into equal four parts, the x and y coordinates axis for screen indexes which are as follows, top-left-coroner at (0,0) to (mid_x, mid_y), right-top-coroner at (0,max_y) to (mid_x, mid_y), left-bottom-coroner at (max_x, 0) to (mid_x, mid_y) and right-bottom-coroner at (mid_x, mid_y) to (max_x, max_y) that is part1, part2, part3 and part4 respectively as illustrated in Figure.1. The program is allocated all the position locations of each application package exist on the simulated screen coordinates based on the mouse clicks activity and it is the only way of determining the sequence of the data steam which would build the password.

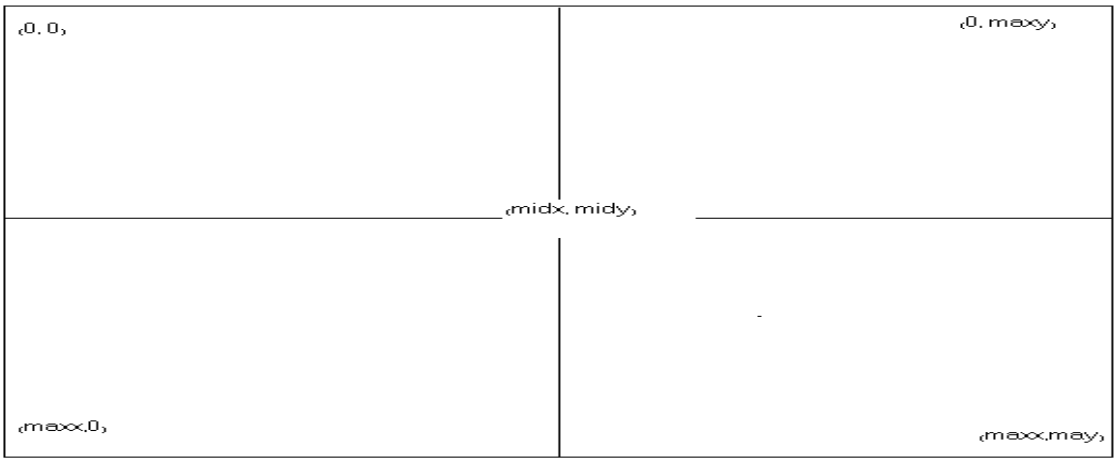

Figure 1 Simulation of the four equal screen parts

The proposed method has three main functions acting for the following purposes:

A. Cursor Locater Function

It is used to compute the mouse left clicks when the user used the mouse as part of his/her single type of entering the password over a particular screen position. This function will indicate the position and the location of the target password

and hence, its indication that what the user is selecting? and is it the right password or not?

B. Time Scale Function

It is used to monitor the user time to finish his/her single data of input password stream sequence over particular screen coordinates, we setup time "timer" to compute the time to finish an entering single password. The invisible interfaced program used pre-computed time scale against the unknown users as a way of verifying user and for user's performance as well. The function (1) used the best known model serving mouse clicks purpose is Fitts' Law[3], commonly expressed in the following form

$$T = a + b\log_2\left(\frac{A}{W} + 1\right) \quad (1)$$

Where T is the acquisition time,
W is width target that lies at distance A, and a, b are constants.

The log is index of the movement difficulty and used as measure of input device (mouse efficiency).

C. Clicks Scale Function

It's working over divided screen area which are four equal parts is illustrated in (Figure.1). This function is returned the cursor coordinates position pointer and the number of clicks on each particular part of the screen. The function is indicates which square have been click it on, As result of determining the active of the screen part (square). It is possible now to determine which part of the screen has been used by the user, and it can known from its cursor position.

By setting up all these four functions in our invisible interfaced program. The proposed method has now controlled all the mouse function and its position pointer that could be hit on the screen monitor. The invisible interfaced program have well structured database which gives a simulating and calculating statistical results about the user behavior to assist our analysis to determine the user password and which software package has been used.

IV. PASSWORD DATA CODE STREAM GENERATION

A single implementation task of generating a single password for each user has been provided by selecting random volunteers' using a prototype Personal Computer. The user is free to create the password in any order of sequence as long as s/he finished its task within time frame set by the proposed invisible password algorithm. The computed user time will be used for verifying the entry of individual user password as second level of security. The password generated using the left mouse clicks. The numerical values are obtained from each mouse left click as in equation (2)

$$clicks = \begin{cases} 1 & leftclick \\ 0 & otherwise \end{cases} \quad (2)$$

The valid numerical value of the click (i.e. left) will be count to generate the password which is '1'.

The proposed algorithm is exams the valid user click to set the pair code. The pair code for each part of the screen is illustrated in Table 1. The user has to aim on the screen part (location) using mouse cursor and click. The pair code(s) are used to build the stream code of the user favorite password.

TABLE 1 PAIR CODE FOR SCREEN PARTS

00	01
10	11

The screen coordinates generates codes for the password in following sequences. If mouse cursor is clicked on the first square (left top corner of the screen) then the pair code is n= 00, If mouse cursor is clicked on the first square (right top corner of the screen) then the code is n= 01, If mouse cursor is clicked on the first square (left bottom corner of the screen) then the code is n= 10 If mouse cursor is clicked on the first square (right bottom corner of the screen) then the code is n=11. The complete sequence of the selected pair codes could be set by any length, starting range from two which is the simplest password to eight which is normal length of secure enough to maximum limited time allowed by the algorithm to generate complex long binary numbers based on the complexity degree of the user selection of password. The length of the pair code of the password is determined by the following formal (3)

$$\text{Pair code} = n^S \quad (3)$$

Where n is defined pair code and
s is screen parts (s= 4, 8 or 16)

The user is allowed to set his/her password by clicking any number of sequences on screen within given time frame. the screen position coordinates are the password roadmap illustrated in Figure 2. The code sequence (stream) is saved with its time from the in the system database. Also the diagram shows also the user pair coding area over the screen (i.e. at any part of the screen) that indicates undirected way of the position and location of the user password sequences.

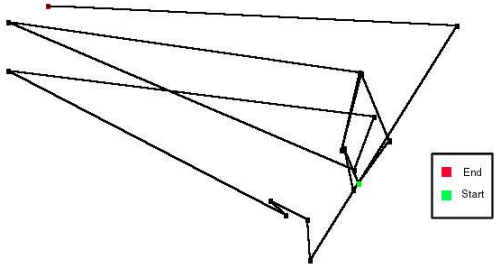

Figure 2 Roadmap of the cursor clicks and its movements

V. Online User Password Database Setting

The proposed technique creates advanced database. The proposed database consists of tables as for each new user. The database is divided into number of fields such as password, roadmap, user time and number of clicks. The proposed algorithm takes variables (sequence of codes) of the screen coordinates location and determined the code for the data sequence of the proposed password. The proposed technique is producing two other values, which are the total time, and the total clicks. The timer started as soon as the user hit (use) the mouse left clicks on the appropriate part on the screen monitor. It indicates how long the user will spent time clicking (typing) his/her own password and how long s/he takes time to completed? Calculating the user time is used as a secret key which helps the proposed technique to authenticate user's password.

VI. The Analysis of the Proposed Technique

The users are selected from different gender, age, education levels and without any pre-user training. The experimentation gives very good results of generating a different password for each user. The user's random generating passwords from starting and finishing cursor clicks positions over his/her screen working area. In Figure 3, indicates direct notation of which part of screen area has been hit. The complete sequences of clicks can be redrawing fully based on the user behavior for password roadmap database. This sequence of pair codes will help the proposed technique to make decision of who is the user?. The proposed technique gives a complete history for each user whom trying to guess the password for further possible decisions. The second analysis of database's proposed method is the values of the total time and the total clicks of the user. Those two values shows the user whom is s/he s creating a password over the screen and it could be compute out the total time to see is it the same values for a user whom trying to get into the computer system?. The time scale is the advanced level of security for the proposed method, which has been added to the proposed database system. The user total time and total clicks (pair codes) could be used over the particular investigation and could lead or help the administrators of the organization to put a new strategy for future work of modifying or increasing level of security for special packages of database or classified information over the network.

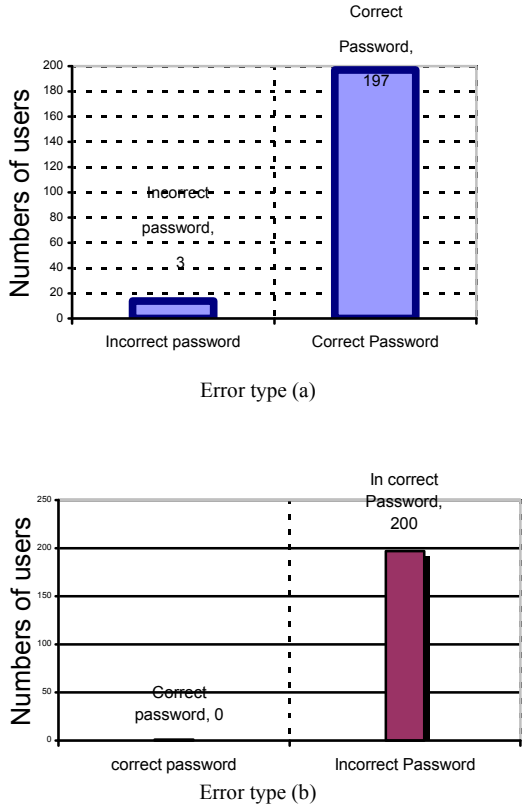

Figure 3 illustrated the two types of possible errors (a) and (b)

The proposed technique has been heavily tested over different users and the errors that could be occur are mainly two types of errors which are as follows:

(a) The first type of error is user has typed (clicks) correct number of clicks over correct coordinates but spent longer time. The total percentage is less than 1%

(b) The second error type is users did not type the total number of the correct sequence (clicks) over the correct screen position within the time scale. The total percentage is less than 3%

Both errors were minimum compare to the existing and traditional method of password generator systems [1][6]. Figure 3 illustrated the two types of possible errors (a) and (b) respectively.

VII. CONCLUSION

New and intelligent invisible password system generator is introduced. The proposed technique main functions have been described. The proposed approach has shows sold levels of security to increase the level of security is by dividing the screen into smaller parts and could be implemented to guarantee different types of complex passwords (paircodes). The proposed algorithm has shown good performance over tested user passwords. The new technique is very easy to use and could be implemented to any hardware computer platform system and running as hidden program. Clearly for users do not use the mouse, this method will success to detect an intruder. Future devolvement of the new method is to be implemented over wireless applications for disable users.

REFERENCES

[1] Prinz, R.; Zeman, P.M.; Neville, S.; Livingston, N.J.; (2006). Feature Extraction Through Wavelet De-Noising of Surface EMG Signals for the Purpose of Mouse Click Emulation, Canadian Conference on Canadian Conference on Electrical and Computer Engineering CCECE06, May 2006 Page(s):1454 – 1457

[2] LAMBIE, T., STORK, A. and LONG, J. (1998). The Coordination Mechanism and Cooperative Work. In Proc. Ninth European Conference on Cognitive Ergonomics (ECCE9), Limerick, Ireland, 24-26 August 1998, T.R.G. Green, L. Bannon, C.P. Warren and J. Buckley (eds). France: EACE. 163-166

[3] Accot, J. & Zhai, S. (1997). Beyond Fitts' law: models for trajectory-based HCI tasks. Proceedings of ACM CHI'97 Conference on Human Factors in Computing Systems, pp 295 302

[4] Brain Actuated Technologies Inc. (2004) BRAINFINGERS USER MANUAL V5.9. Yellow Springs, Ohio, USA: Brain Actuated Technologic Inc.

[5] Delsys, (2000) EMGworks Signal Acquisition and Analysis Software User Manual. P.O. Box 15743 Boston, MA http://www.passwordportal.net/ : accessed 4/09/2007

[6] WHITEFIELD, A. and HILL, B. (1994). A Comparative Analysis of Task Analysis Products. Interacting with Computers, 6 (3), 289-309.

[7] UIGNAN, K. and LIFE, M.A. (1997). Disclosing Differing Interpretations of User Needs: An Application of Soft Systems Methodology. In Contemporary Ergonomics, Proc. Annual Conference of the Ergonomics Society, Grantham, UK, 15-17 April 1997, S.A. Robertson (ed). London: Taylor & Francis, pp.498-503.

[8] D. B. Skillicorn, Teaching Computer Scince Using Hypermedia (1995). External Technical Report, ISBN – 0836-0227-95-386