ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 10, October 2014

User Authentication by Typing Pattern for Computer and Computer based devices

Ankur Kumar[1], Abhijeet Patwari[2], Sagar Sabale[3]

Department of Network and Communication Engg, IIIT Bangalore, Bangalore, India [1]

Department of Network and Communication Engg, IIIT Bangalore, Bangalore, India [2]

Department of Network and Communication Engg, IIIT Bangalore, Bangalore, India [3]

Abstract: User access to the most computer systems is secured through possession of a login ID and password combination. Once the login details have been exposed, an unauthorized user has complete access to the computer system. This paper focuses on a powerful authentication system that captures the typing style of a user and detects the change of user based on the typing pattern. The basic idea is to compare a reference set of typing characteristics of the authenticated user with a test set of a user operating the system. The difference between these two sets should be below a certain threshold or else the user change is detected. Moreover on the basis of training sample it has been found that flight time give much better authenticated results when compared with dwell time and words per minute.

Keywords: Dwell time; Flight time; Typing speed; Clustering of keys; Keystroke dynamics;

I. INTRODUCTION

This paper describes the recent advancement in the field of keystroke dynamics for the computer user authentication. The keystroke biometric system makes a set of typing characteristics which is unique for each person. In comparison to other biometrics, amount of space and the money incurred in using typing characteristics for authentication are comparatively less. As the security mechanism is not visible, the unauthorized users can't have an idea of the security measure. An attempt is to develop a more powerful authentication system, with low cost and good acceptance by users. Therefore, an authentication mechanism has been proposed based on information of human typing pattern. While typing on a keyboard a user can be authenticated not only through (user name & password), but also through keystroke dynamics (i.e. how he/she types). So initially a set of typing characteristics of authenticated user has been saved, which are then compared with a test set of current user operating the system. Hence, keystroke biometrics provides a foolproof authentication solution.

II. RELATED LITERATURE

The idea of typing pattern for user authentication came into picture when people used to communicate over long distances via telegraph. While sending messages each telegraph operator was noticed to have unique signature. Therefore rather than using traditional password authentication this solution can help us to know whether the actual user is using the system or not.

Keystroke dynamics can be used for authentication of computer and computer based devices. Figure 1 shows

keystroke dynamics (which include several different measurements) that can be detected when the user presses t keys on the keyboard. Various keystroke parameters which we have considered for authentication purpose are :

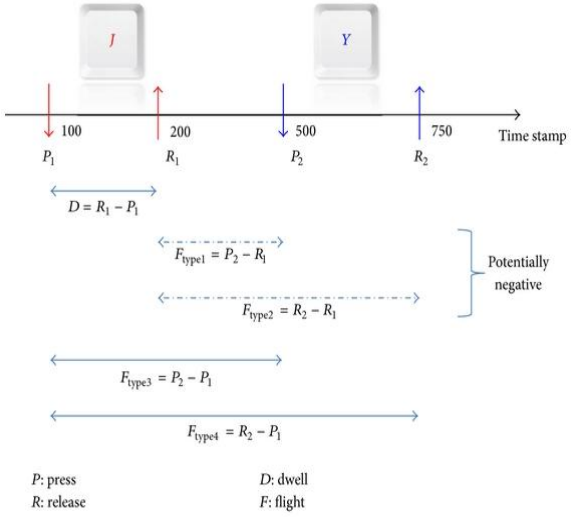

Figure1: Flight and dwell time measurement

A. Flight Time

It is the latency between consecutive keystrokes or the time between two consecutive keys.. The inter stroke interval between the keys is measured in milliseconds. Flight time can be calculated by the formula:

$$F_{type1} = P_i - R_{i-1} \quad \text{(i)}$$

$$F_{type2} = R_i - R_{i-1}$$

where,

P_i is i^{th} key down time and R_i & R_{i-1} is key up time

Figure 1 shows calculation of flight time between consecutive keys

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 10, October 2014

B. Dwell time

It is the time interval between the key down event and the key up event or in other words the time for which each key is being pressed. It can be calculated by the formula:

$$D_i = R_i - P_i \quad \text{-(ii)}$$

where,

P_i is i^{th} key down time and R_i is i^{th} key up time.

It is independent of keyboard layout because some keyboard layouts have more space in between the keys and some are close enough. Generally dwell time is very less. Sometimes even long key press occurs but in real life they are very rare.

C. Typing speed

Typing speed is one of the features used for typing pattern recognition. Following factors need to be considered to calculate typing speed**:**

- Words per minute is used to measure the typing speed, is abbreviated as WPM.
- Each word is standardized to be five characters or five keystrokes long, including spaces and punctuation. For example, the phrase "I run" counts as one word, but "rhinoceros" and "let's talk" both count as two.
- Characters per minute, or CPM, is equal to the WPM measurement times five.
- Based on the speed of user, the typists are divided into "fast," "moderate" and "slow" groups.

III. APPROACH

The system consists of a front end application for data capture (Includes parameters like dwell time, flight time etc), and a back end application for both data capture and authentication classification (based on various parameters). Below are various parameters which we have considered for user authentication:-

A. Keystrokes Capturing

In real-time program, all keystrokes pressed by user are captured. As the user types, the device captures each keystroke and saves it in text file in computer hard disk. The hook functions are used for capturing the keystrokes. The hook functions are called whenever a key is pressed. The typing parameters are evaluated based on the time at which these hook functions are called. The key is captured and its parameters are stored in text file. But for rare cases when more than one key is pressed at a time, the calculation of typing parameters becomes tedious. So, whenever a key is pressed it is added at the end of the linked list and when it is released it is deleted from the linked list. These hook functions are called when a key is pressed.

B. Clustering of keys

This has been designed to capture user's preferences for using particular group of keys. Each user has a unique style the way he/she presses the keys associated with function keys. Few users use left Shift key with other keys and right Shift key with other. Similar is the case with function keys like left and right CTRL and ALT keys. The clustering of such keys need to be done properly. The keys pressed with left Shift, right Shift, left CTRL, right CTRL are stored in separate file. Moreover this user-focussed approach improves performance by taking into account the clustering of the clustering of the individual user's samples.

C. Accurate calculation of typing speed

The accuracy of typing speed has been increased by considering the errors and excluding the function keys like Shift, Caps lock, ALT and CTRL. While calculating the typing speed the function keys like Shift, Caps lock, ALT and CTRL are not considered since these are used to make a character Upper case or various other functions.

D. Calculation of mean and standard deviation

The mean and the standard deviation can be determined by using the relationship given below:

$$\text{Mean} = 1/n(\Sigma x(i))$$

$$\text{Standard Deviation} = \text{Sqrt}\{[\Sigma x(i) - \text{Mean}]2/n\}$$

where,

x(i) is the i^{th} key parameter and n is the no. of readings collected till i^{th} key press.

In order to find mean and standard deviation of different parameters like dwell time, flight time and wpm(words per minute), fetch the data from different text files. The statistical measures of mean and standard deviation are quite useful whenever there is long text input. But in case few samples are there, computation of mean and standard deviation requires special handling. As the number of samples increases, the mean and standard deviation become more accurate and stable.

E. Identity of authenticated user

The identity of authenticated user has been created by following various steps:

- Typing the paragraph contained in the text area
- A user can start typing only after clicking on Start button. Once the start button is pressed, all the keystroke parameters are recorded to create identity.

It provides platform in which a user can type the given one or multiple paragraphs. The sample paragraphs are selected such that they cover almost all keys necessary to create users identity.

F. GUI Interface

Here user has to type the same text as per rectangular box. If he/she types something wrong it will be marked as red otherwise blue (if it is correct). Once the user press Start button and start typing it will start retrieving the keystroke dynamics and make the identity of user.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 10, October 2014

Figure 2

G. Data Collection

During this phase we asked the users to type paragraphs consisting of approximately 5-10 lines. The typing patterns of 5 users were collected and their identity was created. The paragraphs were selected such that the text has all the keys along with common words.. The keystroke dynamics (includes dwell time, flight time and words per minute) in 90% cases is found different from the authenticated user, hence it detects the change of user. Figure3 shows the dialog box which will appear whenever unauthorised user tries to access the computer and computer based devices.

IV. CONCLUSION

The typing parameters like flight time, dwell time, typing speed and clustering of keys is used to create identity of authentic user.

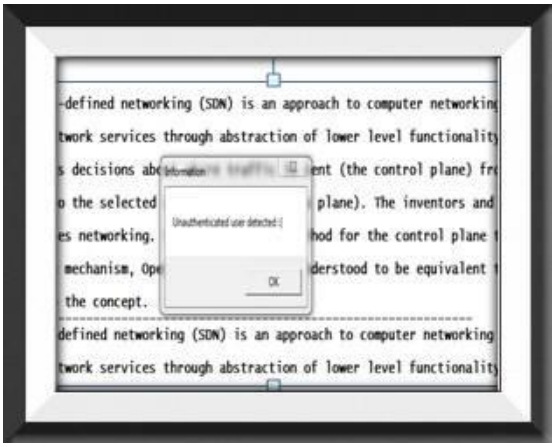

Figure 3

This identity is used for authentication of system. The authenticated user's identity is created using few sample paragraphs. The user detection system is successfully implemented with lowest possible amount of irritations of authentic user while creating users identity. Continuous typing gives better results. The project can be used in enhancing the banking security. The keystrokes based authentication can be used in crucial areas like defence.

V. FUTURE WORK

The data captured is stored in the text file in the project. Stream database can be used for storing the captured data as keywords pressing are also a type of stream data. Accessing the data would become easy and data retrieval time would decrease significantly. This will increase the efficiency of project in computational speed and make the project more robust. Database is also easy from analysis point of view. Time required to detect unauthenticated user can be reduced.. Lesser is the time for detection more useful it will be in critical areas like accessing confidential data. More typing parameters can be added to make the system more secure. Parameters like specific words which user types at relatively high speeds can be monitored and used as a parameter for user identity. Keystrokes dynamics can also be used in human stress detection.

VI. ACKNOWLEDGEMENT

We are extremely grateful to those who have helped, contributed and supported us during the project. Our deepest thanks to our advisor Prof. Poonacha P G for his continuous encouragement, for explaining many scenarios where the project can be used and suggestions throughout the course of this work. It was our pleasure to work under his guidance.

REFERENCES

[1] Toshiharu Samura, Yoshitomo Matsubara and Haruhiko Nishimura, "Performance Assessment in Keystroke Dynamics by Combined Profile Documents for Free Text Typing", Department of Electrical and Computer Engg, Akashi National College of Technology, Akashi, Japan, 2013.

[2] Giroux, Wachowiak-Smolikova, Man and Cybernetics, "Keystroke based authentication by key press intervals as a complimentary behavioral biometric",SMC 2009, IEEE International Conference , 2009.

[3] Sunghoon Park ,Seoul Nat. Univ., Seoul, Jooseoung Park ,Sungzoon Cho, " User Authentication based on Keystroke analysis of long free texts with a reduced number of Features", Second International Conference, 2010.

[4] S.J.Shepherd,"Continuous Authentication by Analysis of keyboard Typing", European Convention on security and detection, 1995.

[5] T.Shimshon, R.Moskovitch, L.Rok Y.Elovici, "Clustering di-graphs for Continuously Veifying Users According to their Typing patterns" Electrical and Electronic Engineers in Israel, 26th IEEE Convention, 2010.

[6] E. Lau, X. Liu, C. Xiao and X. Yu, "Enhanced user authentication through keystroke biometrics," in Computer and Network Security, Massachusetts Institute of Technology, 2004.

[7] R. Joyce and G. Gupta, "Identity authentication based on keystroke latencies," Communications of the ACM, vol. 33, no. 2, pp. 168-176, 1990.