International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 6, Issue 2, March - April 2017 **ISSN 2278-6856**

Combining Keystroke and Mouse Dynamics for User Authentication

Swati Gurav[1], Rutuja Gadekar[2] and Snehal Mhangore[3]

[1]Savitribai Phule Pune University, ICEM,
Post Parandwadi, Pune-410506, India

[2] Savitribai Phule Pune University, ICEM,
Post Parandwadi, Pune-410506, India

[3] Savitribai Phule Pune University, ICEM,
Post Parandwadi, Pune-410506, India

Abstract

Biometrics is one of the latest trend to authenticate the users. Most of them use username and password to authenticate the users that is meant to be static authentication. But as they can be easily stolen, here we are going to authenticate the user by applying keystroke dynamics which is a category of behavioral biometrics. Keystroke biometrics can be used as a standalone system for user authentication as well as combined with other pre-existing systems as an added security measure .We are going to capture the keystroke latency while the user is typing the username and password. Keystroke dynamics is focusing on extracting the behavioral features and using it for authentication of the proposed system. Earlier approaches failed to give better results when performed under different screen resolution and mouse pointer speed. Keystroke dynamics is a promising biometric technique to recognize an individual based on an analysis of his/her typing patterns. If the keystrokes are matched with the stored database then the user is authenticated .If the keystroke fails then mouse dynamics is used as second alternative to authenticate the user. Mouse dynamics is also a category of behavioral biometrics. Mouse dynamics is the process of identifying the user based on their mouse operating behavior.

Keywords: keystroke latency, pattern recognition, behavioral biometrics.

1. INTRODUCTION

Simple password is the primary choice of the user when it comes to password selection, such as date of birth, nickname, initials, and regular dictionary words that is either easily guessed or hacked. As we have these information stored on various accounts, license, identity cards it is easy for hackers to steal the password. Such kinds of passwords are easy to identify and such passwords do not provide strong identity check. To overcome this problem and to provide extra security we are going to apply keystroke dynamics and mouse dynamics to authenticate the user while he is typing the password. Authentication is the process of confirming a user's identity and verifying the accessibility of some service or resource to that user. Textual passwords have been the primary means of authenticating users to computers since the introduction of access controls in computer systems. Passwords remain the dominant user authentication technology today, despite the fact that they have been shown to be a fairly weak mechanism for authenticating users. Studies have shown that users tend to choose passwords that can be broken by an exhaustive search of a relatively small subset of all possible passwords. We argue that the use of keystroke rhythm is a natural choice for computer security. This argument stems from observations that similar neuro-physiological factors that make written signatures unique, are also exhibited in a user's typing pattern. When a person types, the latencies between successive keystrokes, keystroke durations, finger placement and applied pressure on the keys can be used to construct a unique signature (i.e., profile) for that individual. For well-known, regularly typed strings, such signatures can be quite consistent. Furthermore, recognition based on typing rhythm is not intrusive, making it quite applicable to computer access security as users will be typing at the keyboard anyway. Keystroke dynamics is the process of analyzing the way a user types at a terminal by monitoring the keyboard inputs thousands of times per second, and attempts to identify them based on habitual rhythm patterns in the way they type. In recent years biometrics is playing a important role in security application. Keystroke dynamics and mouse dynamics are two parts of behavioral biometrics. Keystroke dynamics is a process to recognize an individual based on an analysis of their typing patterns which are unique for every human being. This method uses a prompt for a username and password that is unique to a particular user. Password authentication is the most widely used for authenticating the user. Typing pattern of an individual includes many factors such as the length of time it takes to type the login and password, how long the individual required to depress a key and how long it take to type successive keys. This method uses the natural typing patterns of a user. A user is uniquely identified from his/her typing patterns. Keystroke biometrics can be a technique in standalone system for user authentication as well as combined with other pre-existing systems as an added security measure. Keystroke analysis

is the method of analyzing the keystroke information and deciding whether a user is legitimate or not. The typing rhythm of a user is captured and the extracted features are used to verify users. Timing patterns do not require any extra hardware which is one of the big factor in reduction of cost. The timing patterns are also known as keystroke latencies. Mouse dynamics is also a type of behavioral biometrics. The movements of the mouse like the number of clicks, the movement of mouse in particular direction are captured and recorded. It also includes drag and drop, point and click and silence.

2. PROPOSED SYSTEM

2.1 Keystroke Dynamics

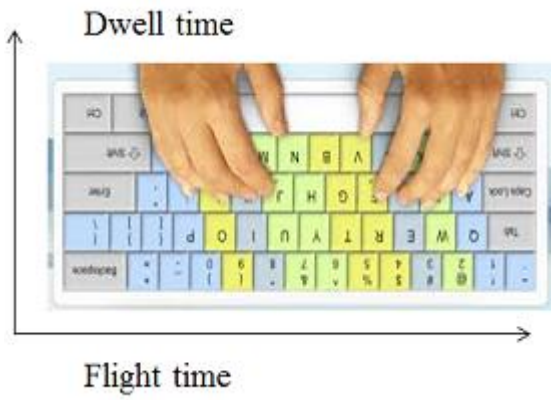
There are two stages to distinguish between genuine and impostor user.

- Enrollment Stage
- Authentication Stage

At the enrollment stage user sign up their login details such as user name and password which is retyped for several times. The system takes the user dynamic keystrokes ten times for each enrollment, extracts the features, then collected features are stored in the database as templates. At the authentication stage, the user enters the login details to be matched with user's reference template which is already stored in the database. This phase consists of collecting user dynamic keystrokes, feature extraction, and feature matching with reference template in a database (i.e) the current probe sequence gets compared with the stored gallery sequence. At last the verification process yields two kinds of action: accepted or rejected user access.

The features are extracted from the user's keystroke for formation of template and later for verification. Two features were extracted during the keystroke: keystroke duration and keystroke latency. Keystroke duration is the interval of time that a key is pressed and liberated. Keystroke latency is the interval of time the pressed of between two consecutive keys interval of time to liberate a key and press the key successor, which is known as flight time, dwell time.

- Flight time- The time take between releasing the key and pressing the next key.
- Dwell time-The time taken to press a key.



The Classifier is responsible for deciding the authentication .The user gets accepted or rejected, based on Criterion of Separation (Threshold).The Classifier verifies the similarity between the pattern to be verified and the template of the prototypes, using the Distance Pattern between the vector of feature of the pattern and the prototype.

2.2 Mouse Dynamics

In the proposed system, the mouse dynamics is used as an alternative method for authentication. Following are the ways we converted the raw mouse events into four different actions.

1. Mouse Single Click Action: The feature is similar to a Single Key Action, i.e. the time duration between mouse button press and release.

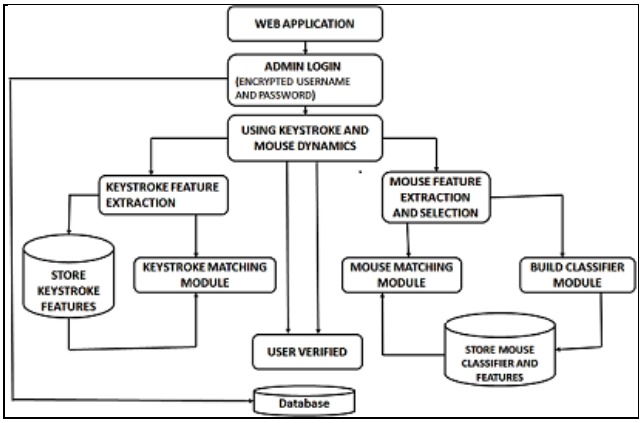
2. Mouse Double Click Action: The features are the same as those of a Key Digraph Action. Two consecutive mouse clicks are considered to be a double click when total time duration,(say) $i < 1000ms$.

3. Mouse Move Action: This action was formed by the sequence of mouse move events.

4. Mouse Drag-Drop Action: This action is very similar to the Mouse Move Action, but for this action first here has to be a mouse click down event followed by mouse move sequences and then mouse click up event.

3.SYSTEM ARCHITECTURE

In this section, we describe our system architecture. The proposed system will have a usual authentication reference for the administration login. A fixed and encrypted username and password will be assigned for the same. Now here on, for additional security behavioral biometrics are implemented. Behavioral biometrics are defined to be unique characteristics of an individual. The keystroke and mouse usage of every individual is variable. The user authentication will be noted by the keystroke dynamics or mouse dynamics. Keystroke dynamics is defined as the characteristics of the usage of keyboard by a particular individual. The key latencies would be monitored to analyze the typing behavior of the individual. In the same way, the movement of mouse will be captured. For every method, feature extraction module is generated. Here, the features of the defined method will be analyzed and a particular feature is worked on. Then after classifier models are generated. These models are nothing but the results of the training data classified with respect to the algorithm. These classifier models and other features are stored in the database and used to process the next level of authentication.



3.1 Modules

3.1.1 Login Module : The administrator needs to login to access the confidential data. This is the first module that is encountered by the user. The provision of authentication by keystroke dynamics or mouse dynamics is decide by this module.

Keystroke Module

a) Keystroke template storage : The administrator will be prompted to provide ten keystroke templates as per his choice and design.

b) Keystroke dynamics secure login : User is prompted to enter the password in the memorized format.

c) Keystroke dynamics feature extraction : Current typing behavior will be compared to the saved templates in the database. And will further provide access to the confidential data.

3.1.2 Mouse Module

a) Mouse dynamics feature : A feature with saved number of pixels over an image to authenticate the administrator.

b) Mouse dynamics authentication : Once the area with correct pixels is detected, the administrator is given access.

4.ALGORITHM USED

Algorithm : Forward Selection Algorithm

Input : Features: 1) Dwell Time, 2) Flight Time Latency, 3) Words Total Time Duration.
Output : The best subset feature values.

Step 1: Start with the empty set.
Step 2: Compute weights of all features using criterion function.
Step 3: Select the best single feature and add it to the Generated pool of candidate feature subset.
Step 4: Repeat steps 2 to 3 until a predefined number of features are selected or until no possible single feature addition would cause an increase in a higher evaluation of the criterion function.

Input parameters include dwell time, flight time latency and words total time duration. Dwell time is the time the key is pressed in. Flight time latency is the time take between releasing the key and pressing the next key. Words total time duration is the total time calculated from the press time to release time. The total time calculation is stored in the database in millisecond(ms) format.

Words total time duration (WT) = endTime – startTime

Where,
endTime = key release time,
startTime = key press time.

5. APPLICATIONS

Keystroke dynamics has many applications in the computer security arena. One area where the use of a static approach to keystroke dynamics may be particularly appealing is in restricting root level access to the master server hosting a key database. Any user accessing the server is prompted to type a few words or a pass phrase in conjunction with his/her username and password. Access is granted if his/her typing pattern matches within a reasonable threshold of the claimed identity. This safeguard is effective as there is usually no remote access allowed to the server, and the only entry point is via console login. Alternatively, dynamic or continuous

monitoring of the interaction of users while accessing highly restricted documents or executing tasks in environments where the user must be alert at all times (for example air traffic control), is a ideal scenario for the application of a keystroke authentication system. Keystroke dynamics may be used to detect uncharacteristic typing rhythm (brought on by drowsiness, fatigue etc.) in the user and notify third parties. Keystroke dynamics can be used for authentication, then it is used mostly together with user ID / password credentials as a form of multifactor authentication. There are several home software and commercial software products which claim to use keystroke dynamics to authenticate user. Also mouse dynamics is used to provide more security to the system along with the keystroke feature.

6. CONCLUSION

A new keystroke data representation model based on potential functions is proposed to allow keeping information about order, times and key values of keystroke actions in a single fixed size feature vector. In this sense the proposed representation model dramatically differs from existing representation models that are referred to as complex. The proposed model based on "press-release" times for each key can store information about keystrokes. On the other hand complex representation models such as n-grams can keep information about keystroke sequences, but the feature space size grows exponentially to the length of analyzed sequences. As a result the obtained authentication models based on such an approach are usually over-trained and computationally expensive. The proposed in this paper representation model is an attempt to overcome these disadvantages. The system is lightweight as it is only implemented for the administrator. Future work would include generating keystroke models for other users too along with other possible behavioral features like face recognition, gait analysis and other features.

References

[1] I. Traore, I. Woungang, M. Obaidat, Y. Nakkabi, and I. Lai. "Combining mouse and keystroke dynamics biometrics for risk-based authentication in web environments", 4th International Conference on Digital Home, pages 138–145, 2012.

[2] Alaa Darabseh and Akbar Siami Namin,"On accuracy of classifcation-based keystroke dynamics for continuous user authentication," 2015 International Conference on Cyberworlds, 978-1-4673-9403-1/15, 2015.

[3] Vladislav Kaganov, Andrey Korolyov, Mikhail Krylov, Igor Mashechkin, Mikhail Petrovskiy, "Hybrid method for active authentication using keystroke dynamics," 978-1-4799-7633-1/14 2014 IEEE

[4] C. Feher, Y. Elovici, R. Moskovitch, L. Rokach, and A. Schclar, "User identity verification via mouse dynamics," Information Sciences, vol. 201, pp. 19-36, 2012.

[5] L. Araujo, J. Sucupira, L. H. R., M. Lizarraga, L. Ling, and J. B. T. Yabu-Uti, "User authentication through typing biometrics features," IEEE Trans. on Signal Processing, vol. 53, no. 2, pp. 851-855, 2005.