|| Volume 3 || Issue 7 || July 2018 || ISSN (Online) 2456-0774

INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH AND ENGINEERING TRENDS

Review on Security Using Keystroke and Mouse Dynamics

Aruna P. Kharat

Asst. Professor, P.E.S college of Engineering, Aurangabad, Maharashtra, India

kharatap.28@gmail.com

Abstract – In today's world, username and password is the most common way to authenticate the person. Stolen username and passwords can be helpful in order to commit suspicious hacking activity. Keystroke biometric authentication provides additional user characteristics which includes typing style to authenticate the user. Pointing device such as touchpad's and mice are getting more importance due to cheap cost and easy availability in behavior based user authentication. Mouse Dynamics focuses on the problem of authentication by verifying the user based on mouse movements which includes single/double clicks, mouse movements. Features are extracted from the mouse dynamics to find out the uniqueness of the user.

I INTRODUCTION

Keystroke analysis is the user's identity through their way of typing on a computer keyboard. Typed key measurements available from most every keyboard can be recorded to determine 'Dwell time' (The time a key pressed) and 'Flight time' (The time between "key down" and the next "key down"). The recorded keystroke timing data is processed through a unique neural algorithm, which determines a primary pattern for the future comparisons. The neural algorithm is provided with Digraph latencies (The elapsed time between the release of the first key and the depression of the second key). The extractions of such features are accepted from the free text provided for the user to create his own profile. Keystroke is a pure software solution. The only required hardware is the standard keyboard that comes with every computer. The system does not require sensors or other additional hardware. Keystroke analysis can completely replace password procedure on the Internet. Users do not have to remember a password. It is highly secure because keystroke behaviour cannot be imitated, stolen, forgotten or misplaced. The assertion that a person's keystroke behavior is exactly as unique as their fingerprint was borne out by scientific research at the University of Regensburg. It is possible to identify a user through the way he types on a keyboard even when the user is entering free text in a language different for the one he used to form his recognition profile. 'Intrusion detection ystem' has an accuracy of limiting the 'False alarms'. The system will not be fooled by the typing rhythms of a language different from the one of the user's profiles used by the Intruder. [1]

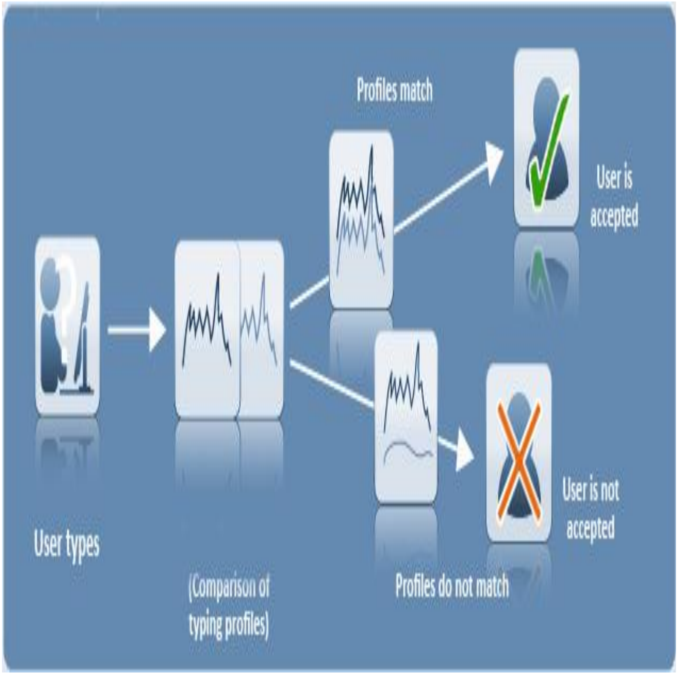

Figure 1 :User Type

Biometric Technology

A biometric system provides automatic recognition of an individual based on some sort of unique feature or characteristic possessed by the individual. Biometric systems have been developed

II LITERATURE SURVEY

Research on keystroke dynamics biometrics has been increasing, especially in the last decade. The main motivation behind this effort is due to the fact that keystroke dynamics biometrics is economical and can be easily integrated into the existing computer security systems with minimal alteration and user intervention. Numerous studies have been conducted in terms of data acquisition devices, feature representations, classification methods, experimental protocols, and evaluations. However, an up-to-date extensive survey and evaluation is not yet available. The objective of this paper is to provide an insightful survey and comparison on keystroke dynamics biometrics research performed throughout the last three decades, as well as offering suggestions and possible future research directions.

Keystroke dynamics refers to the process of measuring and assessing human's typing rhythm on digital devices. Such device, to name a few, usually refers to a computer keyboard, mobile phone, or touch screen panel. A form of digital footprint is created upon human interaction with these devices. These signatures are believed to be rich in cognitive qualities], which is fairly unique to each individual and holds huge potential as personal identifier

In this paper a user re-authentication system that builds a model of a user's behavior directly from their mouse movements. To our knowledge our work is the first to present an accurate re-authentication system based on mouse movements. Shavlik, et al, describe a set of potential features (including mouse data) for profiling users via input devices, but presented results only for keystroke dynamics . the feature set proposed in includes counts of the number of hyperlinks clicked on by the user and the number of scrolling events in a time period ,whereas our feature set models the mouse movement in addition to mouse events (e.g., clicks). Our work is similar to in that we apply supervised learning to detect anomalies, but the learning method employed and in the chosen task of user re-authentication. Finally, similar to other user reauthentication methods we apply a mean later over a window of observations to lower the false positive rate.

The possibility of adding keystroke features in mobile will enhance the security concern. Widely used mobile applications can run without the fear of hacking. Hackers will automatically get captured at the time of unauthorized login on the system.

The challenge in keystroke biometric is to calculate the pressure applied by the user at the time of entering into the system. Future work will cover combining another biometrics with keystroke mechanism to enhance the security. This technique will increase the security parameters and help to catch the imposter.

Disadvantages existing Modes of Authentication:

-The password has to be changed regularly (Password Aging)

-Old passwords should not be re-used after a password change (Password History)

-Trivial passwords and easy-to-guess words like names or car code plates should be prevented

-After a small number of wrong inputs the access has to be blocked for at least a limited time

III SYSTEM ARCHITECTURE

Biometric systems work by first capturing a sample of the feature, such as recording a digital sound signal for voice recognition, or taking a digital colour image for face recognition. The sample is then transformed using some sort of mathematical function into a biometric template. The biometric template will provide a normalized, efficient and highly discriminating representation of the feature, which can then be objectively compared with other templates in order to determine identity. Most biometric systems allow two modes of operation. An enrolment mode for adding templates to a database, and an identification mode, where a template is created for an individual and then a match is searched for in the database of pre-enrolled templates.

Support Vector Machine:

1. More Accurate classifier
2. Supervised Learning models
3. Analyze Data and Recognize Patterns
4. Classification and Regression analysis.

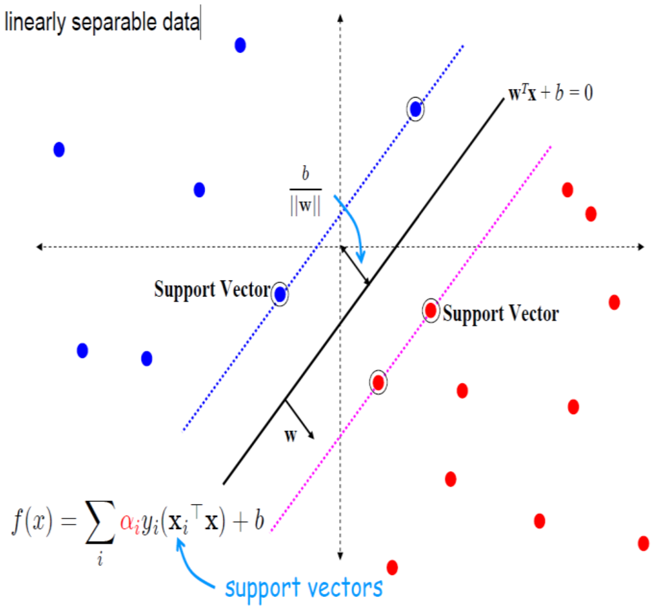
linearly separable data
$\mathbf{w}^T\mathbf{x} + b = 0$
$\frac{b}{||\mathbf{w}||}$
Support Vector
Support Vector
w
$f(x) = \sum_i \alpha_i y_i (\mathbf{x}_i^\top \mathbf{x}) + b$
support vectors

Figure 2: Support Vectors

IV CONCLUSION

A new technique for user authentication based on keystroke dynamics and Mouse dynamics has been proposed by the author. The focus of the technique is to provide maximum level of authentication with less cost. This technique achieve the high level of authentication using a cheap device such as keystroke and mouse dynamics with the high accuracy.

This new methodology can be used anywhere where user name and password is typed by the user. This new methodology can be applied to any application when only a group of trusted users should log in to the system and where

REFERENCES

1. S. J. Shepherd, "Continuous authentication by analysis of keyboard typing characteristics," inProceedings of the 1995 European Convention on Security and Detection, pp. 111–114, May 1995.
2. M. Karnan and M. Akila, "Identity authentication based on keystroke dynamics using genetic algorithm and particle swarm optimization," in Proceedings of the 2nd IEEE International Conference on Computer Science and Information Technology (ICCSIT '09), pp. 203–207, August 2009.

3. P. S. Teh, A. B. J. Teoh, C. Tee, and T. S. Ong, “A multiple layer fusion approach on keystroke dynamics,” Pattern Analysis and Applications, vol. 14, no. 1, pp. 23–36, 2011.

4. B. Ngugi, B. K. Kahn, and M. Tremaine, “Typing biometrics: impact of human learning on performance quality,” Journal of Data and Information Quality, vol. 2, no. 2, article 11, 2011.

5. B. Ngugi, M. Tremaine, and P. Tarasewich, “Biometric keypads: improving accuracy through optimal PIN selection,” Decision Support Systems, vol. 50, no. 4, pp. 769–776, 2011.