IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727
PP 11-14
www.iosrjournals.org

A Review of Behaviometric Techniques for User Authentication

Princy Ann Thomas, Lakshmi Priya A, Dr. Suvanam Sasidhar Babu
Dept. of CSE (Cyber Security) Sree Narayana Gurukulam College of Engineering Kadayiruppu, Kerala, India
Dept. of CSE (Cyber Security) Sree Narayana Gurukulam College of Engineering Kadayiruppu, Kerala, India
Dept. of CSE Sree Narayana Gurukulam College of Engineering Kadayiruppu, Kerala, India

Abstract: *Biometrics is an authentication mechanism classified into physical biometrics and behavioural biometrics. Physical biometrics uses the physical attributes of the individual to verify the claimed identity. Behavioural Biometrics or behaviometrics uses measurable behavioural patterns of device usage to verify the identity of the individual. Physical biometrics would require a special hardware device to capture the characteristics of the claimed identity for verification purposes but behaviometric does not require one in most cases. Keystroke dynamics and mouse dynamics have been researched most frequently for the purpose of static authentication, periodic authentication and continuous authentication of users. In this paper we make a comparative survey on the effectiveness of keystroke dynamics, Keystroke sound, mouse dynamics and mouse gesture dynamics individually as a defense-in-depth mechanism for authentication purposes.*

Keywords: *Behavioural Biometrics, Keystroke Dynamics, Mouse Dynamics, Static Authentication, Continuous Authentication, Equal Error Rate (EER).*

I. INTRODUCTION

User Authentication is the process by which a device or application is able to verify the identity of an individual user or claimed identity. This allows privilege assignment and authorization according to user requirements. In the authentication process the credentials provided by the user are compared to stored values. If a match occurs the process is completed and user is granted authorization for access. Authentication mechanisms are generally categorized into three types. Type 1 is based on something the user knows like passwords. Type 2 is based on something the user has as in the case of credit cards or ATM cards. Type 3 is based on something the user is or something that is unique about the user. Biometrics falls in the Type 3 category.

Biometrics is further categorized into physical biometrics and behavioural biometrics. Physical Biometrics uses the physical characteristics of an individual for authentication like fingerprint, iris, facial, retina, hand geometry, voice and vein pattern. Behavioural Biometrics is also referred to as behaviometrics. Behaviometrics is based on the behavioural pattern of an individual when using specific devices. These patterns are unique to the individual and can be used to verify the identification of the user.

The most commonly researched techniques for authentication using behaviometrics are keystroke dynamics [1], [6] and mouse dynamics [10], [11], [12] as they are less vulnerable to effects of physical environmental changes. Added benefits of using these methods are that they do not require any additional equipment to capture the behavioural pattern.

This paper focuses on recent techniques using keystroke dynamics and mouse dynamics for authentication. We compare research on the use of keystroke dynamics [3], keystroke sound [7], mouse dynamics based on mouse clicks [12] and mouse gesture dynamics [13]. Current research reports the results in terms of Equal Error Rate (EER) or False Acceptance Rate (FAR) and False Rejection Rate (FRR).

The remainder of this paper is organized as follows. In Section II, we present an introduction on the behavioral biometric techniques that are reviewed for authentication in this paper. In Section III, we present findings from most recent work done in behaviometric authentication. In Section IV, we make a comparative study on the different research work presented. In Section V, we give our conclusions.

II. Behaviometric Methods

Behavioural biometrics makes use of measurable behavior patterns to recognize the identity of an individual. Most of these methods work in two stages such as enrollment stage and identification stage. In both data capture is followed by feature extraction using different algorithms or methods.

In the enrollment stage, after feature extraction the data is stored into a database or as a template of the user profile. In the case of identification stage instead of storing the extracted features it is matched with the stored template. If a match occurs the user is authenticated.

A. Keystroke Dynamics

Keystroke dynamics is the process of capturing the typing rhythm and mannerism of a user on the keyboard. Since users generally use the keyboard this method is well suited for computer biometrics. In addition it could offer a high level of security as it would be very difficult to duplicate an individual's innate behavioural pattern.

This method is based on key press, key flight and key sequence. Key press refers to the time taken for a single button on the keyboard to be pressed and released. Key flight is the difference between the time taken to press two consecutive keys. Key sequence is the time taken to type a full word.

B. Mouse Dynamics

Mouse dynamics uses user mouse movement patterns for verifying a claimed identity. The characteristic for a user may be mouse movements or mouse clicks or a combination of both. The captured mouse data would include mouse coordinates, movement angles, consecutive mouse movement timing, mouse click timing and drag and drop actions.

C. Gesture Dynamics

Human motion is used to identify the individual. This method is normally used in mobile devices. Mobile devices have sensors inbuilt that can capture data with comparative accuracy and continuously, such as pressure, gesture, accelerometer, and gyroscope.

Mathematical algorithms are used to interpret human gestures. Gestures are commonly captured from facial expressions or hand movement. In addition identification and recognition of posture, gait and other human behaviors may also be used in gesture dynamics.

III. Existing Authentication Techniques

A. Authentication via Keystroke Dynamics

Keystroke dynamics has increased in importance because of the rising risks in cyber security and computer network security. Research done in this area focuses mostly on static text authentication. Static text authentication requires a predetermined string to be designated. There are limited studies on free text verification. Free text would be more suitable for continuous authentication.

Keystroke dynamics features are usually extracted using the time a key is pressed or released and the latency between two key presses or releases. Digraph and trigraph information may also be used, which are the latency between two or three consecutive keystrokes respectively. It has been shown that word specific digraphs give better accuracy.

Different distance metrics like Euclidean distance, Mahalanobis distance and Manhattan distance have been compared [4]. It has been found that by combining the benefits of Mahalanobis distance and Manhattan distance the limitations of Euclidean distance can be overcome. It is reported that the EER has been reduced from 8.4% to 6% for advanced classifiers like K-Nearest Neighbour [3].

B. Authentication via Keystroke Sound

In this method the sound emanating from a user typing on the keyboard is captured by a microphone and then techniques similar to audio feature extraction is used to extract features. These features will then be stored as templates for testing against probe signals for verification.

The benefits of this technique have been discussed in the work of Roth et al [7]. External sensors are not required, it is a non-intrusive technique, key logging is avoided and it has a shorter verification time compared to the keystroke dynamics technique. The limitation is that accuracy is affected by environmental noise and processing of the raw sound stream could use better feature extraction and classification algorithm for improved performance. An EER of 11% has been observed in this work.

C. Authentication via Mouse Dynamics

Mouse dynamics can be easily incorporated into a continuous authentication framework with existing infrastructure. A stream of mouse events is compared to stored values to generate a match. Medvet et al [12] describe a technique where continuous reauthentication is performed without specific software being installed on client machines.

The features extracted in their research are based on position, speed, acceleration and so on. Each time there is a pause in mouse movement of at least 500ms a new feature vector of a small amount of preceding events is generated. This vector is then used for evaluation of the user identity. An alert is generated on a non match exceeding a particular threshold.

Each mouse related event consists of a timestamp, position co-ordinates and type of event (click or movement). Results on varying size of training data set and number of positive classifiers show that false acceptance rate and false rejection rate are minimum when number of classifiers is more. This study shows an Equal Error Rate (EER) of 0.08 [12].

D. Authentication via Mouse Gesture Dynamics

Sayed et al [13] present a mouse gesture analysis framework that authenticates a user statically. A learning neural network using vector quantization is used as classifier to analyze the captured gestures. In mouse gesture the software recognizes the command as a group of mouse movements and clicks.

In their work, at the enrollment stage user makes several gestures on a computer monitor and the features are extracted, analyzed and an hierarchical procedure is used to train the neural network for matching. For verification, the user will be required to make different types of gestures selected from the set of gestures used during the enrollment phase.

The experimental evaluation results observed in this work show that when the numbers of participants increase the false acceptance rate (FAR) and the false rejection rate (FRR) approach 0% giving an equal error rate (EER) of 0% [13]. Gamboa and Fred [15] show that EER progressively tends to zero when more strokes are recorded.

IV. Comparison

The following table gives a summary and comparison on keystroke dynamics, keystroke sound, mouse dynamics and mouse gesture techniques for user authentication.

	Keystroke Dynamics	**Keystroke Sound**	**Mouse Dynamics**	**Mouse Gesture Dynamics**
Static/Dynamic Authentication	Both	Both	Both	Static
EER	0.09	0.11	0.03	0
Accuracy	91 %	89 %	97 %	99.6 %

As shown in the table we see that static authentication gives better accuracy than any of the methods that could implement both static and dynamic or continuous authentication. Just as in other research work, sound has the problem of filtering unwanted noise when the keystrokes are being recorded. This causes sound to be the least likely option, except in environments where background noise would be steady like that of a fan or air conditioner. Each of the above methods could benefit from better feature extraction techniques when being used for continuous authentication of a claimed identity.

V. Conclusion

Behaviometric techniques could be a powerful tool to authenticate a user periodically once login is accomplished. The percentage of EER suggests that at present they could be deployed as a defense-in-depth strategy. To accomplish continuous authentication a combination of the above methods could be used with feature extraction and matching techniques that provide the best performance. Keystroke sound would be a good option in quiet environments where confidentiality is of high priority since it avoids the need for key logging. Mouse gesture shows highest efficiency. These techniques could be used in Cyber forensics to log suspicious events on a system and create a trail of evidence. In this paper, we review the common techniques used in behaviometric authentication and compare their effectiveness.

REFERENCES

[1] F. Monrose and A.D. Rubin, "Keystroke Dynamics as a Biometric Authentication", Future Generation Computing Systems, vol. 16, no. 4, pp. 351-359, 2000.
[2] F. Monrose and A.D. Rubin, "Authentication Via Keystroke Dynamics", Proceedings of the 4th ACM conference on Computer and communications security, Pages 48 – 56, ACM New York, NY, USA ©1997.

[3] Y Zhong, Y Deng, A Jain, "Keystroke Dynamics for User Authentication", Computer Vision and Pattern Recognition Workshops (CVPRW), Pages 117-123, IEEE Computer Society Conference 2012.
[4] J Kalina, A Schlenker, P Kutilek, "Highly Robust Analysis of Keystroke Dynamics Measurements", IEEE 13th International Symposium on Applied Machine Intelligence and Informatics, Pages 133-138, SAMI 2015.
[5] S Mondal, P Bours, "Continuous Authentication in Real World Settings", Advances in Pattern Recognition (ICAPR), Pages 1-6, IEEE Eighth International Conference 2015.
[6] F. Bergadano, D. Gunetti, and C. Picardi, "User Authentication through Keystroke Dynamics," ACM Trans. on Information and System Security, vol. 5, no. 4, pp. 367–397, 2002.
[7] J Roth, X Liu, A Ross, D Metaxas, " Investigating the Discriminative Power of Keystroke Sound ", Information Forensics and Security, IEEE Transactions on Biometrics Compendium, Vol:10 No. 2, Pages 333 - 345, Feb 2015.
[8] J. Roth, X. Liu, and D. Metaxas, "On continuous user authentication via typing behavior," IEEE Trans. Image Process., vol. 23, no. 10, pp. 4611–4624, Oct. 2014.
[9] D. Asonov and R. Agrawal, "Keyboard acoustic emanations," in Proc. IEEE Symp. Secur. Privacy, May 2004, pp.3–11.
[10] 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.
[11] S. Mondal and P. Bours, "Continuous authentication using mouse dynamics," in Int. Conf. of the Biometrics Special Interest Group (BIOSIG'13), 2013, pp. 1–12.
[12] E Medvet, A Bartoli, F Boem, F Tarlao, " Continuous and Non-Intrusive Reauthentication of Web Sessions based on Mouse Dynamics", Availability, Reliability and Security (ARES), Pages 166-171, IEEE 2014 Ninth International Conference.
[13] B Sayed, I Traore, I Woungang, M Obaidat, "Biometric Authentication Using Mouse Gesture Dynamics", Pages 262-274, IEEE Systems Journal, Vol. 7 No. 2, June 2013.
[14] Rautaray, A Agrawal, "Design of gesture recognition system for dynamic user interface", Technology Enhanced Education (ICTEE), Pages 1-6, 2012 IEEE International Conference.
[15] H Gamboa, A Fred, " A Behavioural Biometric System based on Human Computer Interaction.", in Proc. Conf. Biometric Tech. Human Indentification, vol. 5404, 2004, pp. 381-392.