International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:268
Vol.3, No.2, February 2014 DOI:10.15693/ijaist/2014.v3i2.42-45

A Survey Of Authentication Based On Mouse Behaviours

Dr.P.M.BALAGANESH,[1]
Asso.Prof /Department of CSE
Anna University, Chennai, India

A.SONIYA[2]
PG Scholor /Department of CSE
Anna University, Chennai, India

[1] Asso.Professor, Dept of CSE/Sembodai Rukmani Varatharajan Engineering college
[2] PG Scholar of Sembodai Rukmani Varatharajan Engineering college

Abstract*-Behavior-based user authentication with pointing devices, such as mice or touchpads, has been gaining attention. As an emerging behavioral biometric, mouse dynamics aims to address the authentication problem by verifying computer users on the basis of their mouse operating styles. This process represents a simple and efficient user authentication approach based on a fixed mouse-operation task. For each sample of the mouse-operation task, both traditional holistic features and newly-defined procedural features are extracted for accurate and fine-grained characterization of a user's unique mouse behavior. Distance-measurement and eigenspace-transformation techniques are applied to obtain feature components for efficiently representing the original mouse feature space. Then a one-class learning algorithm is employed in the distance-based feature eigen space for the authentication task.*

Index Terms:
Mouse dynamics, ,mouse behavior based security, Mouse movement operations, user authentication.

I INTRODUCTION

The quest for a reliable and convenient security mechanism to authenticate a computer user has existed since the inadequacy of conventional password mechanism was realized, first by the security community, and then gradually by the public. As data are moved from traditional localized computing environments to the new Cloud Computing paradigm, the need for better authentication has become more pressing. Recently, several large-scale password leakages exposed users to an unprecedented risk of disclosure and abuse of their information. These incidents seriously shook public confidence in the security of the current information infrastructure; the inadequacy of password-based authentication mechanisms is becoming a major concern for the entire information society. Of various potential solutions to this problem, a particularly promising technique is mouse dynamics. Mouse dynamics has attracted more and more research interest over the last decade.

Most existing approaches for mouse-dynamics-based user authentication result in a low authentication accuracy or an unreasonably long authentication time. Either of these may limit applicability in real-world systems, because few users are willing to use an unreliable authentication mechanism, or to wait for several minutes to log into a system. Moreover, previous studies have favored using data from real-world environments over experimentally controlled environments, but this realism may cause unintended side-effects by introducing confounding factors (e.g., effects due to different mouse devices) that may affect experimental results. Such confounds can make it difficult to attribute experimental outcomes solely to user behavior, and not to other factors along the long path of mouse behavior, from hand to computing environment.

It should be also noted that most mouse-dynamics research used data from both the impostors and the legitimate user to train the classification or detection model. However, in the scenario of mouse-dynamics-based user authentication, usually only the data from the legitimate user are readily available, since the user would choose her specific sequence of mouse operations and would not share it with others. In addition, no datasets are published in previous research, which makes it difficult for third-party verification of previous work and precludes objective comparisons between different approaches.

Faced with the above challenges, our study aims to develop a mouse-dynamics-based user authentication approach, which can perform user authentication in a short period of time while maintaining high accuracy.

II RELATED WORK

Architecture Diagram

The mouse dynamics function is explained from the different kind of processes in the system architecture.

This Architecture diagram enhances the holistic features and procedural features are extracted from the fixed mouse-operation task to accurately characterize a user's unique behavior data. Then distance-based feature construction and parametric eigenspace transformation are applied to obtain the predominant feature components for efficiently representing the original mouse feature space.

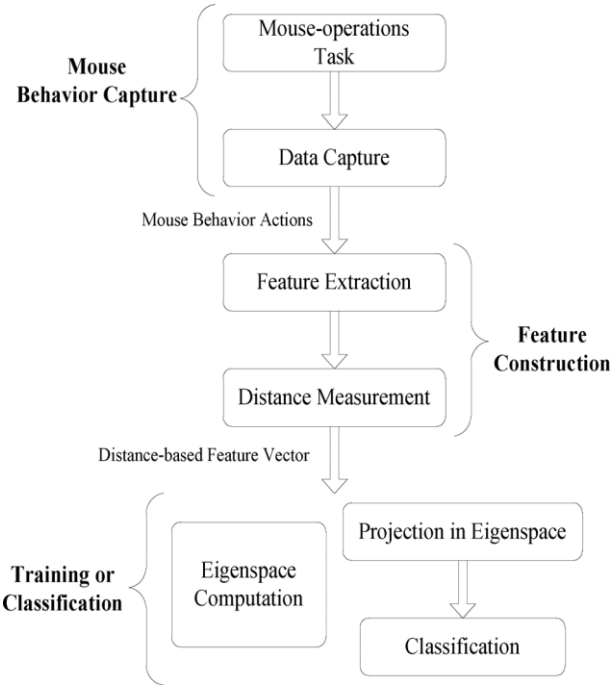

Figure 2.1 Architecture Diagram

III PROPOSED SYSTEM

Mouse dynamics measures and assesses a user's mouse-behavior characteristics for use as a biometric. Compared with other biometrics such as face, fingerprint and voice, mouse dynamics is less intrusive, and requires no specialized hardware to capture biometric information. Hence it is suitable for the current Internet environment. When a user tries to log into a computer system, mouse dynamics only requires her to provide the login name and to perform a certain sequence of mouse operations. Extracted behavioral features, based on mouse movements and clicks, are compared to a legitimate user's profile. A match authenticates the user; otherwise her access is denied. A simple and efficient approach that can perform the user authentication task in a short time while maintaining high accuracy. Holistic features and procedural features are extracted from the fixed mouse-operation task to accurately characterize a user's unique behavior data. Then distance-based feature construction and parametric eigenspace transformation are applied to obtain the predominant feature components for efficiently representing the original mouse feature space. Finally, a one-class classification technique is used for performing the user authentication task.

Mouse Operation Task

For preparing training set users are requested to perform a mouse-operation task.During data collection, the application displayed the task in a full-screen window on the monitor, and recorded.The three operations are, the corresponding mouse operations (e.g., mouse-single-click), the positions at which the operations occurred, and the timestamps of the operations. When collecting data, each subject was invited to perform a mouse-operations task on the same desktop computer free of other subjects; data collection was performed one by one on the same data-collection platform. To reduce behavioral variations due to different mouse-operation sequences, all subjects were required to perform the same sequence of mouse operations. We designed a mouse-operation task, consisting of a fixed sequence of mouse operations, and made these operations representative of a typical and diverse combination of mouse operations. The operations were selected according to (1) two elementary operations of mouse clicks: single click and double click; and (2) two basic properties of mouse movements: movement direction and movement distance.

Feature Extraction

The data collected training set are sequences of mouse operations, including left-single-clicks, left-double-clicks, and mouse-movements. Mouse features were extracted from these operations, and were typically organized into a vector to represent the sequence of mouse operations in one execution of the mouse-operation task. Mouse behavior based on two basic types of mouse operations, mouse click and mouse movement. Each mouse operation was then analyzed individually, and translated into several mouse features. This dynamic process divided these features into two categories:

1) Holistic features: features that characterize the overall properties of mouse behaviors during interactions, such as single-click and double-click statistics;

2) Procedural features: features that depict the detailed dynamic processes of mouse behaviors, such as the movement speed and acceleration curves.

Client Phase

A one-class classification technique is used for performing the user authentication task. In the scenario of mouse-dynamics-based user authentication, a login user is required to provide the user name and to perform a specific mouse-operation task which would be secret, like a password. Each user would choose their own mouse-operations task, and would not share that task with others. Thus, when building a model for a legitimate user, the only behavioral samples of her specific task are her own; other users' (considered as impostors in our scenario) samples of this task are not readily available. In this scenario, therefore, an appropriate solution is to build a model based only on the legitimate user's data samples, and use that model to detect impostors. This type of problem is known as one-class classification or novelty/anomaly detection.

Distance Measurement

The raw mouse features cannot be used directly by a classifier, because of high dimensionality and behavioral variability. Therefore, distance-measurement methods were applied to obtain feature-distance vectors and to mitigate the effects of these issues. In the calculation of distance measurement, first used the Dynamic Time Warping (DTW) distance to compute the distance vector of procedural features.

The reasons for this choice are that procedural features (e.g., movement speed curve) of two data samples are not likely to consist of the exactly same number of points, whether these samples are generated by the same or by different subjects; DTW distance can be applied directly to measure the distance between the procedural features of two samples without deforming either or both of the two sequences in order to get an equal number of points. The Manhattan distance to calculate the distance vector of holistic features. The reasons for this choice are that , this distance is independent between dimensions, and can preserve physical interpretation of the features since its computation is the absolute value of cumulative difference;final one is previous research in related fields (e.g., keystroke dynamics).

Eigenspace Computation:

It is usually undesirable to use all components in the feature vector as input for the classifier, because much of data will not provide a significant degree of uniqueness or consistency. The eigenspace transformation technique to extract the principal components as classifier input.

One-Class Classifier

User authentication is still a challenging task from the pattern-classification perspective. It is a two-class (legitimate user vs. impostors) problem. In the scenario of mouse-dynamics-based user authentication, a login user is required to provide the user name and to perform a specific mouse-operation task which would be secret, like a password. Each user would choose her own mouse-operations task, and would not share that task with others.

An appropriate solution is to build a model based only on the legitimate user's data samples, and use that model to detect impostors. This type of problem is known as one-class classification or novelty/anomaly detection. We thus focused our attention on this type of problem, especially because in a real-world situation we would not have impostor renditions of a legitimate user's mouse operations anyway.

IV CONCLUSION

Mouse dynamics is a newly emerging behavioral biometric, which offers a capability for identifying computer users on the basis of extracting and analyzing mouse click and movement features when users are interacting with a graphical user interface. Mouse dynamics based user authentication process is developed a simple and efficient approach that can perform the user authentication task in a short time while maintaining high accuracy.

REFERENCES

[1] Abe .S and Aksari .Y Support Vector Machines for Pattern Classification, Springer, NY, 2005.

[2] Ahmed A. A. E and Traore .I , "A new biometric technology based on mouse dynamics," IEEE Trans. Depend. Secure Comput., vol. 4, no. 3, pp. 165-179, Jul-Sep. 2007.

[3] Ahmed A. A. E and Traore .I , "Anomaly intrusion detection based on biometrics," in Proc. IEEE Information Assurance Workshop, West Point, NY, pp. 452-453, 2005.

[4] Aksari .Y and Artuner .H , "Active authentication by mouse movements," in Proc. 24th Int. Symp. Computer and Information Science, Guzelyurt, pp. 571-574, 2009.

[5] Bengio S. and Mariethoz .J , "A statistical significance test for person authentication," in Proc.

Speaker and Language Recognition Workshop, Toledo, Spain, pp. 237-244, 2004.
[6] Berndt D.J and Clifford .J , "Using dynamic time warping to find patterns in time series," Advance in Knowledge Discovery in Database: Papers from the 1994 AAAI Workshop, pp. 359-37, Jul. 1994.
[7] Biddle .R, Chiasson .S, and Van Oorschot .P.C , "Graphical passwords: learning from the first twelve years," ACM Computing Surveys, vol. 44, no.4, 2012. (to appear).
[8] P. Bours and C. J. Fullu, "A login system using mouse dynamics," in Proc. 5th Int. Conf. Intelligent Information Hiding and Multimedia Signal Processing, Kyoto, Japan, pp. 1072-1077, 2009.
. [9] R. Brooks, T. Arbel, and D. Precup, "Anytime similarity measures for faster alignment," J. Computer Vision and Image Understanding, vol. 110, no. 3, pp.378-389, Jun. 2008.
[10] CENELEC, "European Standard EN 50133-1: Alarm systems. Access control systems for use in security applications," Part 1: System requirements, Standard Number EN 50133-1:1996/A1:2002, Technical Body CLC/TC 79, European Committee for Electrotechnical Standardization (CENELEC), 2002.

AUTHORS PROFILE

Dr.M.Balaganesh completed his Master Degree from Anna University, Chennai, India. Currently working Associate Professor in Sembodai Rukmani varatharajan Engineering college, Anna University Chennai, India. His research interest includes Network Security,Theory of computation,compiler design and Image processing.

A.soniya. received the M.C.A degree in computer science from the E.G.S.P College of Engineering, Nagapattinam, Anna University, Chennai, India. Currently doing M.E. in Computer Science Engineering in Sembodai Rukmani varatharajan Engineering college, Anna University chennai, India. Her research interest includes network security, forensic communication Neural Networks and fuzzy logic, and Data Mining.