POSTER: Can It Be More Practical? Improving Mouse Dynamics Biometric Performance

Chao Shen[1] Zhongmin Cai[1, ‡] Xiaohong Guan[1, 2]

[1]MOE KLNNIS Lab and SKLMS Lab, Xi'an Jiaotong University, Xi'an, China

[2]Center for Intelligent and Networked Systems and TNLIST Lab, Tsinghua University, Beijing, China

{cshen, zmcai, xhguan}@sei.xjtu.edu.cn

ABSTRACT

Mouse dynamics is the process of verifying the identity of computer users on the basis of their mouse operating characteristics, which are derived from the movement and click events. Some researchers have explored this domain and reported encouraging results, but few focused on applicability in a realistic setting. Specifically, many of the existing approaches require an impractically long verification time to achieve a reasonable accuracy. In this work, we investigate the mouse dynamics of 26 subjects under a tightly-controlled environment. Using procedural features such as speed and acceleration curves to more accurately characterize mouse activity, and adopting distance metrics to overcome the within-class variability, we achieved a promising performance with a false-acceptance rate of 8.87%, a false-rejection rate of 7.16%, and an average verification time of 11.8 seconds. We find that while this level of accuracy comes close to meeting the requirements of identity verification, a tradeoff must be made between security and user acceptability. We also suggest opportunities for further investigation through additional, controlled experimental environments.

Categories and Subject Descriptors

K.6.5 [**Computing Milieux**]: Security and Protection—*authentication, unauthorized access*

General Terms

Design, Experimentation, Security

Keywords

Mouse dynamics biometric, authentication, identity verification, human computer interaction

1. INTRODUCTION

As the internet becomes increasingly powerful and convenient, more and more computer applications allow people to access information and resources globally and ubiquitously. Growing with the development of internet is the thirst for a reliable and convenient security mechanism to authenticate a computer user. This thirst becomes much stronger as more and more important data are moved to the Cloud (e.g. Dropbox), which is accessible to anyone with a registered account. Of the various potential solutions to protect the security of internet identity, one technique that has attracted more and more interest is mouse dynamics – the procedure for measuring and evaluating a user's mouse operating characteristics. These measures, based largely on movements and clicks of the mouse, are compared to a legitimate user's profile; a match or non-match can be used as a biometric to identify or verify the user. Revett et al. provide a review of this field [1].

While previous studies show promising results in mouse dynamics, the proposed approaches may require a long verification time to collect and analyze enough mouse activity data before a reasonably accurate identity verification can be made [2, 6]. For instance, the approach of [2] achieved an average EER of 3% but with the verification time around 17 minutes. This limits the applicability for a large scale deployment in real systems, since more than 3 minutes is too long to authenticate a user in a login process, while for identity monitoring even a few minutes is enough for an adversary to compromise a system. This study, by adopting procedural features, such as speed and acceleration curves, allows one to more precisely characterize the nature of mouse behavior. Moreover, we employed the edit distance [9] to overcome within-class variability and to preserve between-class differences.

Previous studies have favored using data from real-world environments. This introduced unintended side-effects (different mouse devices, operating environments, etc.) as complicated confounding factors that can influence experimental outcomes [10]. This investigation, by using a tightly-controlled experimental environment, isolates the inherent behavioral characteristics as the principle factor in analysis of the behavioral data, and also greatly reduces the effects of external confounding factors introduced by variance in operating environments. Based on our approach, we achieved an encouraging improvement with a false-acceptance rate of 8.87%, a false-rejection rate of 7.16%, and an average verification time of only 11.8 seconds, which approaches a practical standard for identity verification.

2. DATA COLLECTION

2.1 Controlled Environment

In this study, we set up a desktop machine to collect the data, and we developed a Windows application that prompts a subject to conduct the pre-fixed mouse-operating pattern under instructions.

The research is supported in part by NFSC (60921003, 60905018), National Science Fund for Distinguished Young Scholars (60825202), 863 High Tech Development Plan (2007AA01Z464), Research Fund for Doctoral Program of Higher Education of China (20090201120032) and Fundamental Research Funds for Central Universities (xjj20100051).

‡ Corresponding author

CCS'11, October 17–21, 2011, Chicago, Illinois, USA.
ACM 978-1-4503-0948-6/11/10.

We could only collect data from one subject at a time; we made every effort to control software and hardware factors from having any unintended influence on the subject's recorded mouse behavior. The desktop was an HP workstation with a Core 2 Duo 3.0 GHz processor and 2GB of RAM; it was equipped with a 17" HP LCD monitor (set at 1280×1024 resolution). We equipped the computer with a USB HP optical mouse, running the Windows XP operating system. We chose to sacrifice some amount of realism so we could use this carefully-controlled data-collection apparatus. The reason for this decision is that we wanted to make the environment as consistent as possible for all subjects.

2.2 Mouse-operation Design

To make a mouse-operating pattern that is representative of a typical combination of mouse actions, we designed a fixed mouse-operating pattern based on two commonly used properties in mouse movement: movement direction and movement distance; and two basic characteristics in mouse click: single click and double click [5]. In this pattern, eight directions are considered, and each of them covers the movements performed within a 45-degree area. In addition, three distance intervals are contained in this pattern, ranging from 0 pixels to 200 pixels, from 200 pixels to 600 pixels, and from 600 pixels to 800 pixels, respectively. The choice of movement distance and direction is based on the results in the literature [2, 5], which covers the most common and discriminative mouse actions in users' daily mouse-operation. Based on these properties, we constructed a typical and representative mouse-operating pattern containing eight types of mouse movements with a variety of movement directions and distances, and two types of mouse click actions (single-click and double-click). During data collection, every two adjacent movements are separated by mouse click actions, and all of these actions are required to be repeated twice to obtain one sample of the mouse-operating pattern.

2.3 Running Subjects

We recruited 26 subjects, many from within our lab, but some from the university at large. We required subjects to conduct the data collection at least 2 repetitions of the pattern every time, and wait at least 24 hours for next collection (ensuring that some day-to-day variation existed within our sample). All 26 subjects remained in the study, contributing 150 samples.

3. FEATURE EXTRACTION

3.1 Feature Extraction

To extract features determining an individual user's mouse behavioral characteristics and thus validate his/her identity, we first characterized mouse behavior based on two basic types of mouse actions: click and movement. Each action was further analyzed individually, and translated into several mouse features. This study divides these features into two categories: static features and procedural features. Static features characterize the constituents of mouse actions during interactions, containing single-click statistics, double-click statistics, movement offset, and movement time. Procedural features characterize the efficiency, agility and motion habits of individual mouse actions, including movement speed and acceleration. It should be noted that by using the procedural features, such as speed and acceleration curves, one can more precisely characterize the nature of mouse behavior.

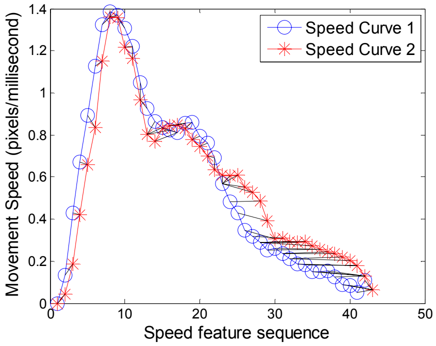

Figure 1. Distance metric between movement speed features

3.2 Distance Measurement

The raw mouse feature data cannot be used directly by a classifier, given the behavior variability and large dimensionality. Instead, we adopted several distance metrics to obtain feature-distance vectors, which can not only overcome within-class variability of mouse behavior, but can also preserve between-class differences of mouse behavior. First, we generated the reference vector using mean distance among training samples. Then, we computed distance metrics between the mouse feature vector and the reference vector using edit distance [9] (for comparing procedural features such as speed and acceleration curves) and absolute distance (for comparing static features such as single-click statistics and double-click statistics) respectively. Finally, we obtained the feature-distance vector for every sample. An example of the edit distance between two movement speed features is shown in Figure 1. The two speed curves are for the same subject.

In this paper, we used all of mouse features defined in Section 3.1 to generate the distance vector. There are 10 click-related features, 16 distance-related features, 16 time-related features, 16 speed-related features, and 16 acceleration-related features, which taken together and then transformed to form 78-dimentional feature-distance vector, representing a repetition of the pattern.

4. COMPONENT, CLASSIFIER AND TRAINING

4.1 Component Analysis

It is usually undesirable to use all components in the feature vector as input of the classifier, because much of data will not provide a significant degree of uniqueness or consistency. Therefore, we used Kernel Principal Component Analysis (*KPCA*) to extract the principle components of the feature-distance vector as input for the classifier.

4.2 Classifier

We used a two-class Support Vector Machine (2-class *SVM*) classifier, which is an effective machine learning method to find an optimal hyper-plane to maximally separate the two classes in the training set. The decision function takes the value "+1" in a "small" region capturing most of the normal data points, and "-1" elsewhere.

4.3 Training and Testing Procedure

We started by designating one of subjects as the legitimate user, and the rest as impostors. We train and test the classifier as follows:

Step1: We trained the classifier on the first 75 samples of the legitimate user and 75 samples of each impostor to build a profile of that user.

Step2: We tested the ability of the classifier to recognize the user himself by generating anomaly scores for the remaining patterns conducted by the user. We record these to calculate FRR.

Step3: We tested the ability of the classifier to recognize impostors by generating anomaly scores for the remaining patterns typed by impostors. We record these to calculate FAR.

This process is then repeated, designating each of the other subjects as the legitimate user in turn. In addition, for choosing parameters of interest, 5-fold cross validation is employed.

5. RESULTS AND ANALYSIS

Table 1 shows results for FAR, FRR and verification time using direct classification and our proposed approach, and also presents some relevant results from the mouse dynamics literature to judge the tradeoff between security and usability.

Our first observation is that direct classification of the original feature-distance space produced a FAR of 10.25% and a FRR of 9.37%. This result is promising compared with previous results reported, since our samples are subject to more variability compared with previous work, which represent activities in a longer period of observation. Moreover, we observe that the classification result was FAR=8.87%, FRR=7.16% by our approach, which is impressive and better than direct classification. These results may be due to the detailed characterization of mouse behavior by using procedural features, and also demonstrate the effectiveness of a distance metric and component analysis technique in dealing with variable behavior data. Note that the results do not yet meet the European standard for commercial biometric technology (0.001% false acceptance rate and 1% false rejection rate) [4]. However, with further investigation and improvement, it seems possible that mouse dynamics could be used as, at least, an auxiliary authentication technique such as an enhancement for conventional password mechanism.

Our second observation is that the average verification time in our study is 11.8 seconds with a FAR of 8.87% and FRR of 7.16%. The approach of [2] obtains an average EER of 3%, but with verification time around 17 minutes. This limits the applicability for a large scale deployment in real systems. The verification time of 11.8 seconds in our study shows that we can perform mouse dynamics analysis quickly enough to make it applicable to identity verification for most login processes. The significant decrease of verification time is due to procedural features providing much more detailed information about each mouse movement than previous approaches, and the introduction of edit distance accommodating the accompanying within-class variability.

6. CONCLUSION

This work performs an objective experimental study of the true applicability of mouse dynamics under a tightly-controlled environment. We adopted procedural features such as speed and acceleration curves to more precisely characterize mouse activity and we employed edit-distance metrics to overcome within-class variability. The empirical results show that our approach significantly reduces verification time compared with previous research, with acceptable accuracy. At this amount of verification time, we believe mouse dynamics suffice to be a practical auxiliary authentication mechanism such as enhancement for a conventional password mechanism. Of course, more investigation should be performed to improve the accuracy of the method.

Table 1. Results of Identity Verification

Approach	FAR	FRR	Average Verification Time
2-class SVM	10.25%	9.37%	11.8 seconds
KPCA + 2-class SVM	8.87%	7.16%	11.8 seconds
Distance-based[8]	15%	15%	20 seconds
Probabilistic Model[3,7]	2%	2%	50 seconds*
Decision Tree[6]	0.43%	1.75%	96 seconds
Neural Network[2]	2.46%	2.46%	1033 seconds*

7. REFERENCES

[1] K. Revett, H. Jahankhani, S. T. de Magalhes, and H. M. D. Santos. A survey of user authentication based on mouse dynamics. In *Proceedings of 4th International Conference on Global E-Security*, 2008, pages 210-219.

[2] A. A. E. Ahmed and I. Traore. A new biometric technology based on mouse dynamics. *IEEE Transactions on Dependable and Secure Computing*, 2007, 4(3): 165-179.

[3] H. Gamboa and A. Fred. Web biometrics: user verification via web interaction. In *Biometrics Symposium*, 2007, pages 1-6.

[4] 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, 2002.

[5] D. A. Schulz. Mouse curve biometrics. *Biometrics Symposium: Special Session on Research at the Biometric Consortium Conference*, 2006, pages 1-6.

[6] M. Pusara and C. E. Brodley. User re-authentication via mouse movements. In *Proceedings of the 2004 ACM Workshop on Visualization and Data Mining for Computer Security*. Washington DC, USA, 2004, pages 1-8.

[7] H. Gamboa and A. Fred. A behavioral biometric system based on human-computer interaction. *Proceedings of SPIE*, 54:4-26, 2004.

[8] S. Hashia, C. Pollett, and M. Stamp. On using mouse movements as a biometric. In *Proceedings of International Conference on Computer Science and its Applications*, 2005.

[9] A. Marzal and E. Vidal. Computation of normalized edit distance and applications. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 1993, 15(9):926–932.

[10] Zach Jorgensen and Ting Yu. On mouse dynamics as a behavioral biometric for authentication. In *proceeding of the 6th ACM Symposium on Information, Computer and Communication Security*, 2011, pages 476-482.

*The verification time was not explicitly stated in [2, 3, 7]; however, it can be calculated from the data collection process. For example, it is stated in [2] that an average of 12 hours 55 minutes of data were captured from each subject, representing an average of 45 sessions. We therefore assume that average session length is 12.55×60/45=17.22 minutes=1033 seconds.