International Journal of Computing and Business Research
(IJCBR)
ISSN (Online) : 2229-6166
Volume 4 Issue 1 January 2013

EXPERIMENTAL ASSESSMENT OF ACTION-ORIENTED POINTING DEVICE BASED VERIFICATION SCHEMES

Karan Madan, Surya World Institute of Engineering & Technology, Bapror

Abstract

In the recent past, action based biometrics begin to get more recognition over the traditional verification procedures like password, or some entity in the form of some cards or hardware or may be some gestures. While verification with keystroke based schemes as action based biometrics has been studied extensively over some time, pointing device based schemes has just recently begun to gain interest as well. The main reason behind this transformation is that pointing device based schemes seems to hold promise as a verification method, with some recently proposed approaches reporting error rates superior or comparable to other well-established biometrics such as voice as well as face recognition. As far as the approaches for these action based biometrics are concerned, the road is going well but the purpose of this study is to shed light on the shortcomings in the experimental assessments of these procedures. As recent work on the assessment of these emerging procedures is not satisfactory, few concerned points or areas are as: many of the existing approaches have need of an impractical amount of pointing device data to be collected before a verification decision can be made with realistic accuracy. We have also observed that in many of the past assessments, environmental variables that can potentially influence pointing device based schemes were not properly controlled. These limitations in the experimental assessments can be eliminated by few refinements.

Introduction

In the beginning, the word verification means only password or some pin etc. After that so many interrelated verification procedures explored like some token or hardware, cards. Then comes the category of biometric verification. In this biometric verification, generally three broad categories are prominent; face, voice and gestures. In recent past, action based biometrics

emerged and two new procedures evolve; keystroke based schemes and pointing device based schemes. So we can say that among these procedures, the pointing device based schemes is the youngest member. As the breach chances are very low in this case. But the assessments of these pointing device based action based biometrics could not carefully control environmental variables of the procedures. We have also experienced that in many of the past assessments, environmental variables that can potentially influence pointing device based schemes were not properly controlled from one test subject to the next.

As a consequence, it is unclear whether the results of those assessments actually reflect detectable differences in pointing device behavior among test subjects, or differences among their computing environments.

We study the feasibility of utilizing pointing device based schemes for verification in remote access scenarios, such as web-based applications. In contrast to the local access scenario, it is common for a user to remotely access the same application from different computers, which may impact verification accuracy.

Impact of Environment variables and remote access scenarios

We review existing verification approaches based on pointing device based schemes and identify several hazards in the experimental style used to evaluate these procedures. For instance, we show that environmental variables (including pointing device type) were not properly controlled across test subjects in some of the assessments, which can significantly impact the results. This work argue that, while promising, pointing device based schemes based verification is not yet suitable for some practical deployment.

Existing Approaches

Continuous Verification Approaches

In an method by Ahmed and Traore, point-and-clicks or drag-and-drops, characterized by action type, distance, duration and direction [1], [2] are used. Consecutive actions over some time frame can be grouped into sessions, over which many pointing device based schemes-related features are computed. Pusara and Brodley Features such as frequency, angle, distance and speed are extracted for each type of window. They presented an method in which raw pointing device data is preprocessed and grouped into data points, each corresponding to a summing up of pointing device events over a window of configurable size[3].

Gamboa and Fred launched the movement events occurring between two clicks [4], [5]. Each stroke is characterized by many spatial, temporal and statistical issues, though this feature space is reduced to the best subset of features, for each user through a greedy type of feature selection process.

International Journal of Computing and Business Research
(IJCBR)
ISSN (Online) : 2229-6166
Volume 4 Issue 1 January 2013

A statistical model make use of the Weibull distribution as the parametric model was utilized for classification and verification decisions were in-fact based on the average classification outcome of a sequence of individual type of strokes.

Static Verification Approaches

Pointing device movements are gathered through javascript embedded in some web page and are sent to a verification server, which concede access based on the entered credentials as well as the corresponding pointing device movements[6]. In one of the schemes given by Gamboa et al., an verifying user enters his username and pin number via an common on-screen virtual keyboard embedded in the particular login web page, using only the pointing device[7]. Gamboa et al. extended their continuous verification approach into a static verification scheme for web-based applications.

Features figured out from the user's movement between each pair of dots consist of the enrollment signature. Hashia et al. present a method in which enrollment involves moving the pointing device pointer between pairs of specific dots shown sequentially on the screen [8]. Verification involves the same sequence of dot-to-dot movements, which are match up against the enrollment signature. Bours and Fullu suggested a static approach in which the authenticating user utilizes the pointing device to trace a winding maze-sort of path while pointing device movements are recorded and used to calculate velocity vectors for each segment of the path [9]. This edit distance is used to match up the verification data to the enrollment data in the scheme proposed by Bours and Fullu.

Shortcomings of the Existing Work

Verification Time Unfeasible

The first Shortcoming that we notice is that many of the existing methods, particularly those offering continuous verification, require a significant amount of pointing device data to be captured before a rationally accurate verification decision can be made. This is undoubtedly not practical for any online system.

Environmental Variables are Uncontrolled

The style has been to collect pointing device data from test subjects by installing some recording software on each subject's personal computer [2], [7], [3]. The problem with using an entirely different type of machine for each subject is that each test machine could differ with respect to any type and no. of software-related variables like screen resolution, actual pointer speed and some acceleration settings, and last but not least, pointing device polling rate, etc.

Remote Access Scenario

Pointing device based verification procedures must have the provision to be used in remote access applications, such as web-based applications. In reality, a given user may access a single web-based application from any no. of computers. This could result in the situation in which the enrollment data for a end-user is gathered under a different computing environment than the data used for the verification.

Recommendations for refinement of current pointing device based action-oriented biometrics

The realism of pointing device based verification systems depends not only on the low error rates, but also depends significantly on achieving a reasonably shorter verification time. There is significant need for the creation of a common, publicly accessible data set for use by researchers in this area, it would significantly trim down the overhead for new researchers in this field. Strategies for minimizing or handling false rejections in a elegant manner might also increase the practicality of Pointing device based verification systems. One possibility might be to combine pointing device based schemes with other types of action-oriented biometrics, such as keystroke based schemes ([9]) to improve verification accuracy. We have revealed in this paper that certain environmental variables like pointing device type may significantly impact pointing device performance if the state of these variables is somehow different at enrollment time than at the verification time. Other such variables that could be explored includes the following: software-level variables such as screen resolution, pointing device speed and its acceleration settings in the OS, much important pointing device polling rate, features of the surface on which the pointing device is being used, and last but not least, the psychological condition of the user like the user may be fatigued, distracted or distressed in some way. The effects of such variables on one's pointing device performance are generally unexplored.

Future Work & Conclusion

There is no doubt that action based biometrics specifically pointing device based schemes seems to possess much more potential as verification method. As the error rates are very much low as comparable to other conventional verification procedures like passowords or OTP etc or even better than other well-established biometrics such as voice and face recognition as well. But the assessments of these pointing device based action based biometrics did not carefully control environmental variables of the procedures. In lack of accurate assessments, the real applications of these procedures doesn't get much recognition. This study would try to find whether the low error rates reported in the text were due to

firmly detectable action based differences among individuals or in-fact due to differences in their computing environments. The results of this study established that there are detectable action based differences among individuals but neglected or poor attention given controlled environmental variables in these past testing assessments likely add up to the low error rates. One more issue moved up in this study is that when signed up data and verification data for the same user are gathered under two different pointing devices, existing procedures are not likely to be able to accurately verify the user's identity somehow. It means pointing device based schemes may not be a good choice for verification specifically in web-based applications or other remotely accessed applications. Study also suggests that there are indeed detectable action based differences among users, even when environmental variables are in-fact tightly controlled.

These results recommend that pointing device hardware itself exhibits an influence on pointing device based schemes strong enough to overshadow the unique action based patterns of most of the users.

A lot of work can be done on the improvement in assessment procedures of these pointing device based or some other action based biometric procedures. The study also suggested many recommendations for refinement of current pointing device oriented action based biometrics.

References

[1] A. A. E. Ahmed and I. Traore. Anomaly intrusion detection based on biometrics. In IEEE Workshop on Information Assurance and Security, pages 452–453, 2005.

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

[3] M. Pusara and C. E. Brodley. User re-authentication via mouse movements. In C. E. Brodley, P. Chan, R. Lippman, and W. Yurcik, editors, Workshop on Visualization and Data Mining for Computer Security (VizSEC/DMSEC 2004), 29 October 2004, Washington DC, USA, pages 1–8. ACM, 2004.

[4] H. Gamboa and A. Fred. An identity authentication system based on human computer interaction behaviour. In 3rd International Workshop on Pattern Recognition on Information Systems, pages 46–55, 2003.

[5] H. Gamboa and A. Fred. A behavioural biometric system based on human computer interaction. In SPIE 5404 - Biometric Technology for Human Identification, pages 381–392, Orlando, FL USA, 2004.

[6] H. Gamboa, A. L. N. Fred, and A. K. Jain. Webbiometrics: User verification via web interaction. In Proceedings of Biometrics Symposium, pages 1–6, 2007.

[7] D. A. Schulz. Mouse curve biometrics. In Biometric Consortium Conference, 2006 Biometrics Symposium, pages 1–6, 2006.

[8] S. Hashia, C. Pollett, and M. Stamp. On using mouse movements as a biometric. In Proceeding in the International Conference on Computer Science and its Applications, volume 1, 2005.

[9] F. Monrose and A. D. Rubin. Keystroke dynamics as a biometric for authentication. Future Generation Computer Systems, 1:351–359, 2000.