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

MEASURING THE USER'S MOUSE ACTIONS FOR CONTINUOUS RE-VERIFICATION

Karun Madan

Surya World Institute of Engineering & Technology

Bapror, Punjab, India

E-mail : karanmadan99@gmail.com

Abstract

From decades, the most widespread approach for secure systems is to employ a password. Unfortunately, passwords, suffer from hurdle like password cracking and password theft. By only offering one-time verification, the verified end-users are still susceptible to both session hijacking and the exposing of the confidential information. To keep one safe all the times, more frequent end-user verification is needed. These repeated verifications are also called re-authentication.

For re-authentication, trend favours the biometric approaches. Nowadays, various biometric approaches are prevalent. Various Physiological biometrics like fingerprints and retinal scans, offer one-time authentication accurately but demand specialized hardware which may be quite expensive or unavailable on all end-users' machines. On the other hand, recent trend is of action based biometrics such as keystroke and mouse based action schemes. In keystrokes scheme, the system would record first the end-user's passwords, end-user names, and other sensitive information. On the opposite side, in mouse based action schemes no information about end-user credentials gets saved. Our approach concentrates on tiny-points angle-oriented metrics, which can differentiate an end-user accurately with very few mouse clicks. In fact, a end-user's mouse based action schemes is a continuous process, making it much more difficult to forge than a signature. Unlike forging a signature, which only has to be done once, the benefit of our verification system is that it would need to mimic the true end-user's mouse patterns continuously for the entire length of the session.

Introduction

Almost in every field nowadays, authenticating an end-user before login, is the most important topic concerned with security solutions. Existing end-user verification methods only offer one-time verification, and the verified end-users are still in danger to even nasty session hijacking[1]. To achieve a well-timed information to an account crack, more frequent end-user verification is needed. In addition to physiological biometrics, action based biometrics has proven very useful in authenticating a end-user.

Mouse based action schemes, with their unique patterns of mouse movements, is one such action based biometric. In this paper, we present an end-user verification system using mouse based action schemes, which is both accurate and competent enough for future usage. Unfortunately, a physical entity such as a key or an ID card can be lost or stolen.

Similarly, a conventional memorized password could be forgotten or divulged to some malicious end-users. On the contrary, a biometric-based approach relies on inherent as well as unique characteristics of a human end-user being authenticated. The biometrics can never be lost or forgotten, nor can any end-user easily steal or acquire them.

This method is robust across different operating platforms, and no specialized hardware is needed. The main feature of our approach is to exploit the point-by-point angle-oriented metrics of mouse movements, which are relatively unique from individual to individual and independent of any computing platform, for end-user verification. Our approach focuses on tiny-point angle-oriented metrics, which have two benefits over previously studied metrics. First, angle-oriented metrics can distinguish a end-user accurately with very few mouse clicks. Second, angle-oriented metrics are relatively independent of the operating environment of an end-user, making them appropriate for online re-authentication.

Action Based Biometric Approaches

As this system can verify an end-user in an accurate and timely manner, and induced system operating cost is minor. Since our verification system records end-users' mouse movements and clicks, privacy concerns may come up. However, compared to keystroke based action schemes, the amount of any kind of personal information included in mouse based action schemes is minimal. In the course of recording keystrokes[2], the system would record the end-user's passwords, end-user names and other receptive textual information.

By contrast, recording mouse based action schemes only expose the physical movements of a mouse and its clicks within a specific period of time, giving away minute to no information about end-user credentials. In general, mouse-based action

schemes re-authentication techniques are hearty against online forgery[3].

An individual's unique mouse based action schemes are similar to its signature, and like a signature, it is very tricky to mimic even with the total knowledge of the original. In fact, an end-user's mouse based action schemes is a continuous process, making it much complicated to forge than a signature[4]. Unlike forging a signature, which only has to be done once, the benefit of our verification system would need to mimic the true end-user's mouse patterns continuously for the whole length of the session. It is very tricky for one end-user to force itself to consistently move the mouse in such a mechanical way that it match up with specific angles, even if those metrics are known much earlier.

Characterization of end-user's mouse movements

We can deliberately set a normal environment for the end-users and instruct them to behave as naturally as it is possible. Mouse movement data can be recorded during their normal routine computing proceedings. These activities may range within word processing software, using the Internet, programming something, online chatting sessions and playing some games. We can make use of a logging tool RUI [5] to trace their mouse movement activities. For the field set, more than 1,000 unique forum end-users' mouse movements are recorded by JavaScript code, and submitted passively via AJAX requests to the web server[5]. In spite of this, there is no guarantee on the amount of data gathered for a specific end-user.

An end-user could be logged in for a much long time with frequent mouse activities, or could achieve just one click and then leave. On the other hand, the width of this corpus of end-users is utilized to serve up as the base profile for both the training and the testing purposes[6]. The raw mouse movements are correspond to tuples of timestamp and the pairs of Cartesian coordinate[7]. Each tuple is in the kind of action-type, t, x, y where action-type is the mouse action type (a mouse-move or mouse-click), this t is the timestamp of the mouse action, the 'x' is the x-coordinate, and 'y' is the y-coordinate. Timestamps in our data collection are collected in few milliseconds.

Continuous mouse movements are chain of mouse movements with tiny or no pause between each adjacent step. Within the ith point-and-click act for an end-user c, we symbolize the jth mouse move record as mouse-move, ti, xi, yi c, j ,where ti is actually the timestamp of the ith mouse movement. On the basis of record that belongs to each point-and-click act, we calculate angle-oriented metrics. The purpose of preprocessing is to identify every point-and-click act, which is defined as the continuous mouse movements and followed by a click.

These newly- described metrics are different from the conventional metrics, like speed and acceleration, and can accurately characterize an end-user's unique mouse moving behaviors, independent of its running platform. To examine the mouse movement data, three tiny-point angle-oriented metrics can be: direction, angle of curvature, and curvature distance.

The direction is the angle between that line AB and the horizontal[8]. For any two successive saved points A and B, we record the direction traveled along the line AB from the very first point to the second. For any three successive recorded points A, B, and C, the angle of curvature is angle ∠ABC; i.e., the actual angle between the line from A to B and the line from B to C. This metric is in fact unit-less because it is the ratio of two distances only. The curvature distance is in fact the ratio of the length of AC to the perpendicular distance from the specific point B to the line AC. For any of the three recorded points A, B, and C, think about the length of the line connecting A to C. As a comparison, we present the two traditional mouse movement metrics, speed and the pause-and-click. In case of first metric Speed, we compute the speed as the ratio of the total distance traveled for that act divided by the total time taken to complete the act for each point-and-click act.

In case of Pause-and-Click, this metric analyzes the amount of time exhausted pausing between pointing to an entity and actually clicking on it. We compute the amount of time between the finish of the movement and the click event for each point-and-click action.

Influence of End-user Environment

The entire end-user's environment can influence its data: the OS used, size of screen and its resolution, font size, sensitivity of mouse pointer, brand of mouse, type of mouse and even the amount of vacant space available on the desk close to the mouse-pad[9]. Metrics such as speed and acceleration are weak choices for comparison between end-users of arbitrary platforms. This is because these two metrics can be twisted by differences in screen resolution and pointer sensitivity as well. Conversely, metrics such as pause-and-click are totally dependent on the content, that an end-user is reading[10]. For example, an end-user be likely to pause longer before clicking a link on a loaded content page such as a wiki article etc, and be reluctant for a much shorter time before clicking a button like "submit".

This problem we face in analyzing our data , "it may be tuff or meaningless to compare two end-users who are using very different types machines", is actually reasonable one. This makes a nice reason to use angle-oriented metrics for arbitrary end-user comparison instead.

Similarly, curvature distance is a ratio of the actual distances on the screen, and so self-

adjusts for the end-user's specific environment.

A ratio can be compared to another end-user's ratio across different platforms. Direction and angle of curvature are not at all based on screen size or any other similar element of the end-user's environment, and so are relatively platform-independent.

Conclusion & Future Work

The actual notion of biometric-based end-user authentication is centered on "who you are", as it is totally dissimilar from conventional end-user authentication approaches, which are primarily based on either "what you have" or may be on "what you know". We compared action based biometrics using mouse based action schemes with keystrock based action schemes. However, today, the on hand mouse-based end-user verification approaches have either resulted in unacceptably low accuracy or have need of an unacceptably long amount of time to reach at a decision, making them totally unsuitable for online re-authentication. In contrast to previous research work on this area, our approach establishes a novel way—tiny-point angle-oriented metrics—to characterize and differentiate end-users' mouse movements, which appreciably reduces verification time while keeping high accuracy intact. This system is fairly independent of the operating environment, and capable of uniquely identifying and differentiate individual end-users. Graphical passwords are another kind of end-user verification, relying totally on pointing device to authenticate an end-user. Mouse based action schemes differ in that they actually differentiate between end-users by how the end-users move and click the mouse, instead of where the end-users click. Systems such as these are not independent as they are complementary to our approach, and can be deployed together with it. For instance, one can utilize a graphical password system while passively recording an end-user's mouse based action schemes

One problem may relate with this mouse based action based biometric and in-fact also relate with keystroke based biometric. This problem is termed as "the scalability problem", which is a general problem for almost all types of action based biometrics approaches. As the no. of end-users increases at rapid rate, there is more chance that two end-users share the similar mouse movements. On the other side, in face recognition technique, there are very less chances that two end-user's faces are similar and could make the system to fail. So researchers can, work on the problem of this action based biometric, in future.

References

[1] S. Chiasson, P. van Oorschot, and R. Biddle. A usability study and critique of two password managers. In USENIX Security Symposium, 2006.

[2] T. Buch, A. Cotoranu, E. Jeskey, et al. An enhanced keystroke biometric system and associated studies. In Proceedings of Student-Faculty Research Day, CSIS, Pace University, pages C4.2–C4.7, 2008.

[3] C.-C. Chang and C.-J. Lin. LIBSVM: a library for support vector machines, 2001. Software available at http://www.csie.ntu.edu.tw/~cjlin/libsvm.

[4] DTREG. SVM - Support Vector Machines. http://www.dtreg.com/svm.htm, Feb 2011.

[5] U. Kukreja, W. E. Stevenson, and F. E. Ritter. RUI: Recording user input from interfaces under windows and mac os x. Behavior Research Methods, 38(4):656–659, 2006.

[6] D. Florencio and C. Herley. A large scale study of web password habits. In Proceedings of WWW 2007, 2007.

[7] T. Joachims. Text categorization with support vector machines: Learning with many relevant features. In Proc. of European Conference on Machine Learning, pages 137–142, 1998.

[8] Z. Jorgensen and T. Yu. On mouse dynamics as a behavioral biometric for authentication. In Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, ASIACCS ’11, pages 476–482, 2011.

[9] S. Chiasson, A. Forget, E. Stobert, P. van Oorschot, and R. Biddle. Multiple password interference in text passwords and click-based graphical passwords. In ACM Conference on Computer and Communications Security (CCS), 2009.

[10] S. Chiasson, P. C. V. Oorschot, and R. Biddle.Graphical password authentication using cued click-points. In 12th European Symposium On Research In Computer Security (ESORICS), 2007. Springer-Verlag, 2007.