A Survey on Behavioral Biometric Techniques: Mouse vs Keyboard Dynamics

Monika Bhatnagar
Associate Professor
NIRT Bhopal
(RGPV University)

Raina K. Jain
MTech, CSE
NIRT Bhopal
(RGPV University)

Nilam S. Khairnar
ME, COMP
S.R.E.S COE, Kopargaon
(Pune University)

ABSTRACT

With hundreds of people using computers and mobile devices all over the globe, these devices have an established position in modern society. Nevertheless, most of these devices use weak authentication techniques with passwords and PINs which can be easily hacked. Thus, stronger identification is needed to ensure data security and privacy. In this paper, we give a survey on two of behavioral biometric techniques to computer. We also propose an authentication scheme for desktop that uses characteristics of interaction of user with the input devices viz. keyboard and mouse.

General Terms

Behavioral biometrics.

Keywords

Biometric, authentication, classification, data mining.

1. INTRODUCTION

Identity theft has since long been dealt with by many techniques. The most commonly used are logins and passwords. With time came different techniques, use of smartcard based authentication increased. Three factor authentication or biometric authentication was a great leap in research. Biometric refers to identification of users by their characteristic. These features are unique to each individual and hence they prove useful to identify a user. [1] classified biometrics into two categories: a)physiological biometrics, are based on a person's physical characteristics which are assumed to be relatively unchanging such as fingerprints, iris patterns, retina patterns, facial features, palm prints, or hand geometry, audio tone. You know what they look like and sound like so you are usually able to recognize them when you see them or hear them. Turning the characteristics into reproducable electronic data is quite an art however and no perfect system has yet been developed that is absolutely foolproof - although some are pretty good. b)Behavioral biometrics are related to the behavior of a person, including but not limited to: typing rhythm, gait, and voice. These systems does not require any expensive sensors and other hardware devices. Behavioral biometric data can be, thus collected without the knowledge of the user. These systems use the human traits of interaction with the input devices and later on use these profiles to verify the identity of the user. Even though these types of biometric systems depend upon the consistency of human interaction, but still the results have shown sufficiently high accuracy.

2. RELATED WORK:

Recently a number of researches were conducted to explore the utilization of machine learning techniques in different biometric systems. Several works on keystroke biometrics have already adopted approaches based on different metrics, sampling methodologies and data analysis techniques. In [4], there is a general discussion on different authentication schemes. According to [4], biometric based authentication techniques are best to uniquely characterize an individual , than text based(i.e. passwords and PIN) and physical (i.e. smartcards etc). [1] has stated that behavioral biometric techniques can be categorized based on different types of categories such as type of learning: implicit or explicit.

But the focus of this paper is based on two techniques i.e. mouse vs key dynamics. Roman Yampolski, Venu Govindraju has given classification and properties of behavioral biometrics [2]. The generalized algorithm for behavioral biometrics is also stated in [2]. According to [2], behavioral biometric share a number of characteristics and can be analyzed using seven properties of good biometrics by Jain et al(1999,2004d). According to [2], the properties of good biometrics are uniqueness, universality, permanence, collectability, performance, acceptability, circumvention. According to [2], most common behavioral biometrics verification techniques are based on: (a) mouse dynamics.(b) keystroke dynamics and (c) software interaction.

In [1], we get a general idea on how mouse based authentication methods work which will be explained in following sections. [1] has also stated the basic metrics to measure the performance of behavioral biometric devices as follows:

Table 1: Metric to evaluate performance of the type of behavioral biometrics[1]

Metric	Explanation
FAR	Measures the ratio between the number of attacks that were erroneously labeled as authentic interactions and the total number of attacks.
FRR	Measures the ratio between the number of legitimate interactions that were erroneously labeled as attacks and the total number of legitimate interactions.
ROC	A ROC curve is a graphical representation of the tradeoff between the FAR and the FRR for various threshold values.
AUC	Measures the area under the ROC curve.
EER	The rate at which both acceptance and rejection error rates are equal. Low EER values indicate an accurate authentication system.

In this table:
FAR => False Acceptance Rate
FRR => False Rejection Rate
AUC => Area under Curve
EER => Equal Error Rate

3. NEED AND SIGNIFICANCE OF PROPOSED RESEARCH WORK

There are three mechanisms of security: text based, physical authentication and biometric authentication. Traditionally, passwords have been used as a means of security. But authentications of passwords and PINs have long since been proven to be vulnerable to hackers. Also, other credentials such as smartcards can be robbed and misused. The best proven authentication scheme until now is biometric system which offers highest degree of security since it uses those features of an individual which are unique.

Research until now suggests different biometric techniques, such as physiological and behavioral as explained above. The drawback of physiological techniques is that they require expensive sensors and other hardware devices which are not always affordable. Another drawback is that the data collection phase is very complicated whereas in behavioral biometric techniques data can even be collected without the knowledge of the user. Also these techniques can be easily assimilated with desktops of any platforms.

4. BEHAVIORAL BIOMETRIC

4.1 General architecture of behavioral biometric system:

The figure 1 shows the general architecture of behavioral biometric system which consists of following components:

- Events acquisition
- Feature extraction
- Classifier
- Signatures database

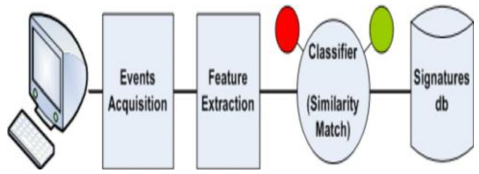

Fig. 1: A typical architecture of behavioral biometric system. [1]

Roman V. Yampolskiy-Venu Govindaraju have generalized the algorithm in few steps which can be stated as follows:

Step 1: Break the behavior (viz. human trait to interact with input devices) into number of atomic operations.

Step 2: Determine frequencies of component actions for each user

Step 3: Combine results into a feature vector profile

Step 4: Apply similarity measure function to the stored template and current behavior.

Step 5: Experimentally determine a threshold value
Step 6: Verify or reject user based on the similarity score comparison to the threshold value.

4.2 Behavioral biometric techniques:

As such there are many techniques that recognize an individual by his behavior viz. interaction with input devices, audit logs, car driving style, gait or stride etc. these features are captured and treated as raw data which are used to characterize an individual.

In this paper, we focus on two techniques: a) user interaction with mouse b) user interaction with keyboard. The general idea is that timing, movement direction and clicking actions are used to build a profile of a user, which is then used for authentication purposes. Most system relies on a continuous monitoring process, or require the user to interact with a program (such as a game) in order to derive sufficient statistical information regarding their mouse dynamics.

The behavioral biometric of keystroke dynamics uses the manner and rhythm in which an individual types characters on a keyboard or keypad. The keystroke rhythms of a user are measured to develop a unique biometric template of the users typing pattern for future authentication. Raw measurements available from most every keyboard can be recorded to determine Dwell time (the time a key pressed) and

Flight time (the time between "key up" and the next "key down"). The recorded keystroke timing data is then processed through a unique neural algorithm, which determines a primary pattern for future comparison. Similarly, vibration information may be used to create a pattern for future use in both identification and authentication tasks. Data needed to analyze keystroke dynamics is obtained by keystroke logging. Normally, all that is retained when logging a typing session is the sequence of characters corresponding to the order in which keys were pressed and timing information is discarded. When reading email, the receiver cannot tell from reading the phrase "I saw 3 zebras!" whether:

- that was typed rapidly or slowly
- the sender used the left shift key, the right shift key, or the caps-lock key to make the "i" turn into a capitalized letter "I"
- the letters were all typed at the same pace, or if there was a long pause before the letter "z" or the numeral "3" while you were looking for that letter
- the sender typed any letters wrong initially and then went back and corrected them, or if he got them right the first time

With keystroke dynamics the biometric template used to identify an individual is based on the typing pattern, the rhythm and the speed of typing on a keyboard. The raw measurements used for keystroke dynamics are dwell time and flight time.

Dwell time is the time duration that a key is pressed

Flight time is the time duration in between releasing a key and pressing the next key

When typing a series of characters, the time the subject needs to find the right key (flight time) and the time he holds down a key (dwell time) is specific to that subject, and can be calculated in such a way that it is independent of overall typing speed. The rhythm with which some sequences of characters are typed can be very person dependent. For example someone used to typing in English will be quicker at typing certain character sequences such as 'the' than a person with French roots.

4.3 Some behavioral biometrics

According to [2] some behavioral biometrics are Audit logs, Biometric sketch, Blinking, Call-stack, Calling behavior, Car driving style, Command line lexicon, Credit card use, Dynamic facial features, E-mail behavior, Gait/stride, Game strategy, GUI interaction,, Handgrip, Haptic, Keystroke dynamics, Lip movement, Mouse dynamics, Network traffic, Painting style, Programming style, Signature/handwriting, Registry access, Soft behavioral biometrics, Storage activity.

4.4 Keystroke dynamics

Differences in the typing patterns make verification of people as experienced typists utilize the touch-typing method, and others utilize the hunt-and-peck approach which uses only two fingers. For verification, a small typing sample such as the input of user’s password is sufficient, but for recognition, a large amount of keystroke data is needed and identification is based on comparisons with the profiles of all other existing users already in the system[2].

Keystroke features are based on time durations between the keystrokes, inter-key strokes and dwell times, which is the time a key is pressed down, overall typing speed, frequency of errors (use of backspace), use of numpad, order in which user presses shift key to get capital letters and possibly the force with which keys are hit for specially equipped keyboards (Ilonen, 2006; Jain et al., 1999).

Keystroke dynamics is probably the most researched type of HCI-based biometric (Bergadano et al., 2002; Monrose and Rubin, 2000), with novel research taking place in different languages (Gunetti et al., 2005), for long text samples, (Bartolacci et al., 2005; Curtin et al., 2006) and for e-mail authorship identification (Gupta et al., 2004).

In a similar fashion Bella and Palmer (2006) have studied finger movements of skilled piano players. They have recorded finger motion from skilled pianists while playing a musical keyboard. Pianists’ finger motion and speed with which keys are struck was analysed using functional data analysis methods. Movement velocity and acceleration were consistent for the participants and in multiple musical contexts. Accurate pianists’ classification was achieved by training a neural network classifier using velocity/acceleration trajectories preceding key presses[2].

4.5 Mouse dynamics

A unique profile can be generated by monitoring all mouse actions produced by the user during interaction with the GUI, which can be used for user re-authentication (Pusara and Brodley, 2004)[2].

Mouse actions of interest include general movement, drag and drop, point and click, and stillness. From those a set of features can be extracted for example, average speed against the distance travelled and average speed against the movement direction (Ahmed and Traore, 2005a; 2005b). Pusara and Brodley (2004) describe a feature extraction approach in which they split the mouse event data into mouse wheel movements, clicks, menu and toolbar clicks. Click data is further subdivided into single and double click data.

Gamboa and Fred (2003; 2004) have tried to improve accuracy of mouse-dynamics-based biometrics by restricting the domain of data collection to an online game instead of a more general GUI environment. As a result, applicability of their results is somewhat restricted and the methodology is more intrusive to the user. The system requires around 10–15 minutes of devoted game play instead of seamless data collection during the normal game play to the user human computer interaction. As far as the extracted features, x and y coordinates of the mouse, horizontal velocity, vertical velocity, tangential velocity, tangential acceleration, tangential jerk and angular velocity are utilised with respect to the mouse strokes to create a unique user profile.

4.6 Mouse dynamics Vs keystroke dynamics:

Mouse and keystroke dynamics are related and complement to each other. Mouse is very important GUI, while keyboard is a command line [6]. Compared to traditional technique mouse and keystroke based authentication scheme allows passive and dynamic verification of users throughout the sessions.

User identity verification by mouse dynamics largely depend upon hardware input devices whose interactions are to be captured, these are different types of mice devices which may work differently so sometimes it become difficult to capture events. Also human behavior is prone to errors and user may vary his style. So a user needs to be trained to give proper sequence during data collection and authentication. Optical mice may introduce noise [1] as they cannot track movement on glossy, transparent surfaces.

A significant drawback of mouse-based verification in comparison to keyboard-based verification is the variety of mice, mouse pads and software configurations which may influence the performance of the verification [1].This problem does not exist in keyboard-based verification techniques since the keyboard is an integral part of the laptop.
According to [5], pros of keystroke dynamics are- No additional hardware, Non intrusive and wide user acceptance and minimal training to the user. While cons are-Low accuracy and narrow range of applications.
The style of interaction with mouse is captured in mouse dynamics where in keystroke dynamics the measure is skill. There are many attributes which can be captured in keystrokes whereas mouse provides only a limited set of attributes such as latency, clicks, distance and direction of mouse movement.

Thus, each one i.e. keystrokes and mouse dynamics have their own pros and cons. To eliminate these cons we propose a novel multimodal technique which combines information from two sources i.e. keyboard and mouse.

5. ACKNOWLEDGMENTS

Our thanks to the experts who have contributed towards development of this paper.

6. REFERENCES

[1] Clint Feher [a,*], Yuval Elovici [a], Robert Moskovitch a, Lior Rokach [b,1], Alon Schclar [c] User identity verification via mouse dynamics.

[2] Roman V. Yampolskiy*, Venu Govindaraju* Behavioral biometrics: a survey and classification.

[3] Enzhe Yu, Sungzoon Cho Keystroke dynamics identity verificationdits problems and practical solutions.

[4] Hafiz Zahid Ullah Khan “Comparative study of authentication techniques” International Journal of Video & Image Processing and Network Security IJVIP0opl;NS Vol: 10 No: 04 9

[5] Sushil Chauhana, A.S. Arorab, Amit Kaula “ A survey of emerging biometric modalities”, Procedia Computer Science2(2010)213–218,ICEBT 2010.

[6] Ahmed Awad E. Ahmed, Issa Traore”Mouse Dynamics biometric Technology”, DOI:10.4018/978-1-60566-725-6.ch010

[7] Chien Le, ”A Survey of Biometrics Security Systems”