Behavioural Biometrics for Multi-Factor Authentication in Biomedicine

Anna Schlenker[1,2], **Milan Šárek**[3]

[1] EuroMISE Centre, Institute of Computer Science AS CR, Prague, Czech Republic

[2] Institute of Hygiene and Epidemiology, First Faculty of Medicine, Charles University, Prague, Czech Republic

[3] CESNET z.s.p.o., Prague, Czech Republic

Abstract

Objectives: The goal of this work is to suggest an improved authentication method for biomedicine based on analysis of currently used behavioural biometric methods.
Methods: A brief definition of identification, authentication and biometric characteristics is provided. The main part of the work focuses on keystroke dynamics, its advantages, disadvantages and applications in biomedicine. Keystroke dynamics is then proposed as an interesting behavioural biometric characteristic for use in computer security not being widely used so far.
Results: The result of the work will be a new set of methods, which allows optimal multi-factor authentication method regarding its comfort, cost and reliability.
Conclusions: The purpose of this paper is to focus on the available information about keystroke dynamics.

Keywords

Biometrics, anatomical-physiological biometrics, behavioural biometrics, multi-factor authentication, keystroke dynamics, mouse dynamics

Correspondence to:

Anna Schlenker
EuroMISE Centre, Institute of Computer Science, AS CR, v.v.i.
Address: Pod Vodarenskou vezi 2, Prague 8, Czech Republic
E–mail: schlenker.anna@gmail.com

EJBI 2012; 8(5):19–24
recieved: August 15, 2012
accepted: September 20, 2012
published: November 22, 2012

1 Introduction

A wide range of authentication methods have accompanied us through during the whole existence of human society. One group of these methods is directly associated with human physiognomy. This corresponds to the initial recognition of persons by body, face, eyes or voice. It was a system that allowed identification of people in a relatively narrow group, where everyone knows each other. This method obviously has its weaknesses, one can for example temporarily change his/her physical appearance (wigs, fake beards, haircut, glasses etc.) or similar-looking individuals (doubles) may be contained in the group. When comparing only one physiological characteristic, a mistake may occur in simple characteristics such as face shape. In the case of scanning more than one characteristic or complex characteristics (iris or retina), the processing may be slow and uncomfortable for users.

On the other hand, we can use some external attributes, whether it is formal clothing (uniforms), seal rings or passwords. One major weakness of this system is that the external attribute may by stolen by unauthorized person. And it is no matter whether it is a seal ring or token[1].

Based on the shortcomings of single-factor authentication methods presented above, only multi-factor authentication seems adequately reliable to securely eliminate unauthorized access. It can be for example combination of anatomical or behavioural features with an external attribute or password.

2 Identification and Authentication

In biomedicine there is a need to protect information and data. There are two necessary conditions to assure

[1] A security token may be a physical device that an authorized user of computer services is given to ease authentication [18].

that only the authorised person can access or modify the data [4]:

1. identification and
2. personal authentication,

which both together assure the control of the access to the information.

The process of *identification* establishes who the person is. It happens during the initial login to the system, while the *authentication* confirms or denies the personal identity. It also demands a proof of identity to obtain the certainty that the person is really who is affirming to be [4].

Basically, there are three ways in which a person can be authenticated to the system [11, 13]:

1. The first method of authentication is based on something that the person knows, e.g. password or Personal Identification Number (PIN), called a *knowledge factor*.
2. The second method of authentication is based on something that the person has, e.g. a magnetic strip card or a secret key stored on a smart card, called a *possession factor*.
3. The third method of authentication is based on the fact that the person itself has a unique set of measurable characteristics that can be used to verify or recognize the identity of the person. This is called a *biometric factor*.

Security measures belonging to the first two categories are inadequate because possession or knowledge may be compromised without discovery – the information or article may be retrieved from its rightful owner. Therefore, attention is being shifted to reliable identification by biometric techniques that encompass the third class of identification (i.e. biometrics) as a solution for more foolproof methods of identification. For the foreseeable future, these biometric solutions will not eliminate the need for I.D. cards, passwords and PINs. The use of biometric technologies will rather provide a significantly higher level of identification than passwords and cards alone, especially in situations where security is paramount [13].

2.1 Multi-Factor Authentication

Multi-factor authentication is a security system in which more than one form of verification is used in order to prove the identity and allow access to the system. In contrast, single factor authentication involves only one form of verification, most frequently a combination of user ID and password [17].

Additional authentication methods that can be used in multi-factor authentication include biometric verification such as fingerprinting, iris recognition, facial recognition and voice verification. In addition to these methods, smart cards and other electronic devices can be used along with the traditional user ID and password [17].

3 Biometric Characteristics

In the context of authentication, biometrics have several advantages over traditional authentication techniques that verify identity based on something one knows (e.g. a password) or something one has (e.g. a hardware token). In particular, biometric characteristics cannot be forgotten, stolen, or misplaced [9].

Biometric systems recognize a living person (see [19]) and encompass both physiological and behavioural characteristics. Physiological characteristics such as fingerprints are relatively stable physical features that are unalterable without causing trauma to the individual (see [19]). Behavioural traits, on the other hand, have some physiological basis, but also reflect a person's psychological qualities. Unique behavioural characteristics such as the pitch and the amplitude of one's voice, the way of signing names, and even the way of typing, form the basis of non-static biometric systems [13].

Biometric technologies are defined as "automated methods of verifying or recognizing the identity of a living person based on a physiological or behavioural characteristic" [12]. Biometric technologies are gaining popularity because when used in combination with traditional methods for authentication they provide an extra level of security.

3.1 Anatomical-Physiological Biometric Characteristics

Some examples of biometric features used in identification systems include include [19, 5]:

- fingerprints – patterns found on the fingertip, including the location and direction of ridge endings and bifurcations,
- palm prints – a larger-scale version of the fingerprint biometrics,
- hand geometry – shape of the hand including height and width of bones and joints in the palm and fingers,
- blood vessel patterns in the hand – vein and capillary patterns on the palm or the back of the hand,
- patterns in the face – facial characteristics such as position and shape of nose and position of cheekbones, eye sockets and mouth (but not hairline area, which is prone to change),
- patterns in the retina – layer of blood vessels in the back of the eye,

- patterns in the iris – inherent radial pattern and visible characteristics (e.g., freckles, rings, furrows, corona) of the iris.

Today, a few devices based on these biometric techniques are commercially available. However, some of the currently deployed techniques are easy to fool, while others (like iris pattern recognition) are too expensive and uncomfortable for users [19].

3.2 Behavioural Biometric Characteristics

Behavioural biometric characteristics have the advantage of being less obtrusive than other biometric characteristics and do not require special hardware in order to capture necessary biometric data [9]. They are also cheaper and easier to use.

The most known examples of behavioural biometrics are [15]:

- signature dynamics – measurement of combination of appearance, shape, timing and pressure during the writing of user's signature,
- voice verification – tone, pitch and cadence of voice,
- mouse dynamics – measurement of mouse movement distance, speed and angle during the work,
- keystroke dynamics – the duration of each key-press and the time between keystrokes.

4 Keystroke Dynamics

Keystroke dynamics analysis utilizes the way a user types at a terminal to identify users. The identification is based on habitual typing rhythm patterns [13] and realized by constant monitoring the keyboard inputs. It has already been shown that keystroke rhythm is a good sign of identity [10].

Moreover, unlike other biometric systems which may be expensive to implement, keystroke dynamics is almost free – the only hardware required is a keyboard [13, 8].

The application of keystroke rhythm to computer access security is relatively new, but there has been some sporadic work done in this area. Joyce and Gupta [10] present a comprehensive review on the progress in this field prior to 1990. The brief summary of these efforts and examination of the research, that has been undertaken since then, can be found in [13].

Keystroke verification techniques can be classified as either *static* or *continuous* [13].

- *Static verification* approaches analyse keystroke verification characteristics only at specific times, for example, during the login sequence. Static approaches provide more robust user verification than simple passwords, but do not provide continuous security – they cannot detect a change of the user after the initial verification.
- *Continuous verification*, on the contrary, monitors the user's typing behaviour throughout the course of the whole interaction.

Keystroke dynamics allows so-called continuous (dynamic) verification, which is based on the use of keyboard as a medium of continuous interaction between user and computer [3]. This offers a possibility of constant monitoring over the whole time the computer is being used. This method is useful in situations when there is a risk of leaving a computer without control for a certain period of time [6].

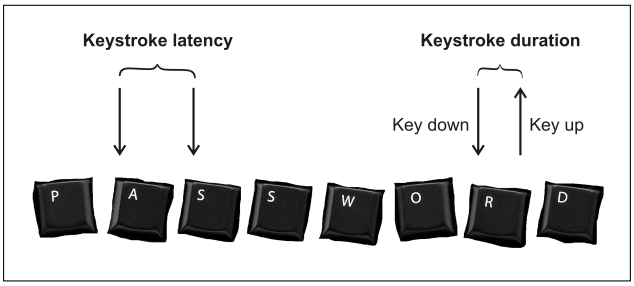

Figure 1: Keystroke duration and keystroke latency.

Some features can be extracted from the keystroke rhythm, for example [4, 19]:

- the period time a key is held for (keystroke duration) – see figure 1,
- the time between individual keystrokes (keystroke latency) – see figure 1,
- frequency of errors,
- style of writing of capital letters,
- speed of the keystroke,
- placement of the fingers and
- pressure that the person applies when pressing a key (pressure keystroke).

The latter three types requires a special keyboard that allows the force of the push to be measured. All other methods can be evaluated by a special program without any modification of hardware [13, 8].

The history of keystroke dynamics can be found in [13, 10] or in [4].

We must also mention that there might be a large difference in typing characteristics depending on the current type of user's activity, for example when chatting with friends compared to writing a program in Java [2]. You need to think more, to analyse and then to type when you are writing a Java program. The set of frequently used characters may also differ (you use more special characters when programming, for example). For more details about this problem, see [2].

4.1 Advantages of Keystroke Dynamics

1. The ultimate goal is ability to continually check the identity of a person as they type at a keyboard [13, 3].
2. Neither login nor verification affect the regular work flow because the user would be typing the needed text anyway. Easy to use for example with login and password during a logon process [21].
3. Unlike other biometric systems, keystroke dynamics is almost free. The only hardware required is the keyboard [13, 8].
4. Time to train the users is minimal and ease of use is very high [21].
5. Public acceptability is very high. There are no prejudices such in a case of fingerprint verification or discomfort such as retina pattern scanning [19].
6. Keystroke dynamics is ideal also for remote users.

4.2 Disadvantages of Keystroke Dynamics

1. Keystroke dynamics is a non-static biometrics like for example voice. This can change quite fast during time, also one-hand typing (due to injury), etc. can influence typing rhythm [13].
2. Low accuracy – keystroke dynamics one of the less unique biometric characteristics [21].
3. Small commercial widespread of technology [21].
4. Dependency on keyboard characteristics, for example layout of keys. Some users may be used to a full-sized keyboard, while the others may prefer to use a laptop, where the typing behaviour will probably be very different [20].
5. Typing style usually differs depending on the language (native vs. foreign) [2].

5 Mouse Dynamics

While authentication with keystroke dynamics has been studied extensively over the past three decades, mouse dynamics has just recently begun to gain interest over the last decade [9]. The idea behind this biometric is to monitor all mouse actions generated as a result of user interaction with a graphical user interface, and then process the data obtained from these actions in order to analyse the behaviour of the user [1].

Mouse dynamics describes an individual's behaviour with a pointing device, such as a mouse or a touch-pad [9]. Similar to keystroke dynamics, mouse dynamics does not require a special device for data collection [16].

Mouse actions can be classified under the following four different categories [14]:

- mouse movement – corresponds to general movement,
- drag and drop – the action starts with mouse button down, movement, then mouse button up,
- point and click – mouse movement followed by a click or double click, and
- silence – no movement.

Same as in other fields of behavioural analysis, mouse dynamics utilizes neural networks and statistical approaches to generate a number of factors from the captured set of actions; these factors are used to construct what is called a Mouse Dynamics Signature or MDS, a unique set of values characterizing user's behaviour over the monitoring period. Some of the factors consist of the calculated average speed against the travelled distance, or the average speed against the movement direction. In [1] up to seven factors that exhibit strong stability and uniqueness capability are reported.

When collecting the actions, several factors have to be taken into account because they can affect the accuracy of the analysis of the mouse biometric samples. These factors are listed below [14]:

1. Desktop Resolution: If the samples are collected with a different screen resolution than assumed, it will affect the results by changing the range of the collected data.
2. Mouse Cursor Speed Setting: This is the speed and acceleration setting of the cursor set by the operating system. Any changes done to those settings can affect the calculated figures, and also affect the user behaviour itself in dealing with the mouse input device.
3. Mouse Button Configuration: In order to achieve reproducible results, the mouse button configuration should be fixed for each user on a specific workstation.
4. Hardware Characteristics: Factors such as the workstation speed, and the pointing device type and properties can also impact the data collection process.

6 Applications in Biomedicine

Keystroke dynamics can be used very well in cooperation with other authentication methods, especially with login and password (structured text), which gain good security results [21]. Now only one company, Net Nanny, works on commercial release of their product BioPassword [7].

There are many potential areas of application for this technology, especially for its low cost and feature of continuous checking. Limitations are mainly non-consistent typists [21].

Monrose [13] also believes that keystroke dynamics can be theoretically used as possible attack to PGP[2], because random seed collected during key generation is calculated from user's typing. This can be weakness, if users typing characteristics are known [21].

Monrose [13] also reports, that there can be some differences between left-handed and right-handed users, but he does not have enough left-handed users to give some useful results [21].

Alternatively, dynamic or continuous monitoring of the interaction of users while accessing highly restricted documents or executing tasks in environments where the user must be alert at all times (for example air traffic control), is an ideal scenario for the application of a keystroke dynamics authentication system. In such case, keystroke dynamics may be used to detect uncharacteristic typing rhythm (brought on by drowsiness, fatigue etc.) and notify third parties [13].

7 Conclusion

For centuries handwritten signature is maintained as an important identification datum. This is a unique expression of human brain. The signature is formed already at school and influenced further by personality and health of individual. We have to accept that a new generation of students is gradually replacing handwriting by typing on a keyboard. So it is appropriate to deal with this new way of human signing. This paper summarizes the available information about this new phenomenon. We can assume that typing has its own specifics, which can be used similarly to the case of handwritten text.

Acknowledgements

This work has been supported by "Projects of Large Infrastructure for Research, Development, and Innovations (LM2010005)" and by the specific research project no. SVV-2012-264513 "Semantic Interoperability in Biomedicine and Health Care", Charles University in Prague.

References

[1] Ahmed AAE, Traore I. A New Biometrics Technology based on Mouse Dynamics. IEEE Transactions on Dependable and Secure Computing. 2007;4(3):165-179.

[2] Barghouthi H. Keystroke Dynamics. How typing characteristics differ from one application to another. [Master's thesis]. Gjovik, Norway: Gjovik University College; 2009.

[3] Bergadano F, Gunetti D, Picardi C. User authentication through Keystroke Dynamics. ACM Transactions on Information and System Security. 2002;5(4):367-397.

[4] Boechat GC, Ferreira JC, Carvalho ECB. Using the Keystrokes Dynamic for Systems of Personal Security. Proceedings Of World Academy Of Science, Engineering And Technology. 2006;24(18):61-66.

[5] Coventry L. Usable Biometrics. In: Cranor LF, Garfinkel S, editors. Security and Usability. Sebastopol, CA. O'Reilly Media, Inc.; 2005.

[6] Gunetti D, Pikardi C. Keystroke analysis of free text. ACM Transactions on Information and System Security. 2005;8(3):312-347.

[7] Identity Assurance as a Service: AdmitOne Security [Internet] 2010 [cited 2012 Aug 4] Available from: http://www.biopassword.com/

[8] Ilonen J. Keystroke Dynamics. Advanced Topics in Information Processing. Lappeenranta University of Technology. [Internet] 2003 [cited 2011 Aug 22]. Available from: http://www2.it.lut.fi/kurssit/03-04/010970000/seminars/Ilonen.pdf

[9] Jorgensen Z, Yu T. On Mouse Dynamics as a Behavioral Biometric for Authentication. Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security. 2011;476-482.

[10] Joyce R, Gupta G. Identity authorization based on keystroke latencies. Communications of the ACM. 1990 Feb;33(2):168-176.

[11] Matyas SM, Stapleton J. A Biometric Standard for Information Management and Security. Computers & Security. 2000;19(2):428-441.

[12] Miller B. Vital sings of identity. IEEE Spectrum. 1994;31(2):20-30.

[13] Monrose F, Rubin D. Keystroke dynamics as a biometric for authentication. Future Generation Computer Systems. 2002:16(4):351-359.

[14] Nazar A, Traore I, Ahmed AAE. Inverse Biometrics for Mouse Dynamics. International Journal of Pattern Recognition and Artificial Intelligence. 2008;22(3):461-495.

[15] Olzak T. Reduce multi-factor authentication costs with behavioral biometrics. TechRepublic. [Internet]. 2007 [cited 2012 Aug 5] Available from: http://www.techrepublic.com /article/reduce-multi-factor-authentication-costs-with-behavioral-biometrics/6150761

[16] Raj SBE, Santhosh AT. A Behavioral Biometric Approach Based on Standardized Resolution in Mouse Dynamics. International Journal of Computer Science and Network Security. 2009;9(4):370-377.

[2] Pretty Good Privacy (PGP) is a computer program that provides cryptographic privacy and authentication. PGP is often used for signing, encrypting and decrypting electronic mails (e-mails) to increase the security of e-mail communications (see [22]).

[17] Rouse M. Multifactor authentication (MFA) [Internet] 2007 [cited 2012 Aug 10] Available from: http://searchsecurity.techtarget.com/definition/multifactor-authentication-MFA

[18] RSA SecurID [Internet] 2012 [cited 2012 Sep 15]. Available from: http://www.rsa.com/node.aspx?id=1159

[19] Schlenker A, Sarek M. Biometric Methods for Applications in Biomedicine. EJBI. 2011;7(1):37–43.

[20] Senathipathi K, Batri K. Keystroke Dynamics Based Human Authentication System using Genetic Algorithm. European Journal of Scientific Research. 2012;28(3):446-459.

[21] Svenda P. Keystroke Dynamics. [Internet] 2001. [cited 2012 Jul 28] Available from: http://www.svenda.com/petr/docs/KeystrokeDynamics2001.pdf

[22] Zimmermann P. PGP Source Code and Internals. MIT Press; 1995.