Keystroke Dynamics for Authentication in Biomedicine

Schlenker, Anna
2012

Keystroke Dynamics for Authentication in Biomedicine

Post-Graduate Student:
ING. ANNA SCHLENKER
Institute of Computer Science of the ASCR, v. v. i.
Pod Vodárenskou věží 2
182 07 Prague 8, CZ
schlenker.anna@gmail.com

Supervisor:
ING. MILAN ŠÁREK, CSC.
CESNET
Zikova 4
160 00 Prague 6, CZ
ms@cesnet.cz

Field of Study:
Biomedical Informatics

This work has been supported by "Projects of Large Infrastructure for Research, Development, and Innovations (LM2010005)".

Abstract

This paper analyzes current state of use of behavioral biometrics in authentication. It provides a brief definition of identification and authentication and biometric characteristics. The main part of the work deals with keystroke dynamics, its advantages and disadvantages and applications in biomedicine. Keystroke dynamics could be an interesting behavioral biometric characteristic for use in computer security not being widely used so far. The result of the work will be a new set of methods, which allows multi-factor authentication in the most comfortable and cheaper way.

1. Introduction

When choosing a security strategy, it is interesting to realize the principles of methods, which accompanies us for the whole existence of human society.

On the one hand, we can think of methods that are 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 the detection of people in a relatively narrow group, where everyone knows each other. This method obviously has its weaknesses, for example fake wigs and beards or double. When compared only one physiological character, the mistake may occur in simple characters such as face shape. In the case of scanning more than one character or complex characters (iris or retina), the processing may be slow and bothering users.

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

Only with multi-factor authentication we can eliminate unauthorized access. It can be for example combination of anatomical or behavioral features with external attribute or password.

2. Identification and Authentication

In biomedicine there is a need to protect informations and data. There are two necessary conditions to assure that only authorised person can access or modify the data [2]:

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 the same proof of identity to obtain the certainty that the person is really who is affirming to be [2].

Basically, there are three ways in which person can be authenticated to the system [7, 9]:

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 that the person is, such as a measurable biological or behavioural characteristic, that reliably distinguishes one person from another and that can be used to verify or recognize the claimed identity of the person, called a *biometric factor*.

Security measures which fall under first two categories are inadequate because possession or knowledge may be compromised without discovery – the information or article may be extorted from its rightful owner. Increasingly, attention is shifting to positive 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. Rather, the use of biometric technologies will provide a significantly higher level of identification and accountability than passwords and cards alone, especially in situations where security is paramount [9].

3. Biometric Characteristics

Biometrics, the physical traits and behavioral characteristics that make each of us unique, are a natural choice for identity verification. Biometrics are excellent candidates for identity verification because unlike keys or passwords, biometrics cannot be lost, stolen, or overheard, and in the absence of physical damage they offer a potentially foolproof way of determining someone's identity. Physiological (i.e., static) characteristics, such as fingerprints, are good candidates for verification because they are unique across a large section of the population [9].

Indispensable to all biometric systems is that they recognize a living person (see [10]) and encompass both physiological and behavioral characteristics. Physiological characteristics such as fingerprints are relatively stable physical features that are unalterable without causing trauma to the individual (see [10]). Behavioral traits, on the other hand, have some physiological basis, but also reflect a person's psychological makeup. Unique behavioral characteristics such as the pitch and amplitude in our voice, the way we sign our names, and even the way we type, form the basis of non-static biometric systems [9].

Biometric technologies are defined as "automated methods of verifying or recognizing the identity of a living person based on a physiological or behavioral characteristic"[8]. Biometric technologies are gaining popularity because when used in conjunction with traditional methods for authentication they provide an extra level of security.

3.1. Anatomical-Physiological Biometric Characteristics

Some examples of identifying biometric features being used for identification based systems include fingerprints, palm prints, hand geometry, blood vessel patterns in the hand, thermal patterns in the face, patterns in the iris or retina (see [10]). Today, a few devices based on these biometric techniques are commercially available. However, some of the techniques being deployed are easy to fool, while others like iris pattern recognition, are too expensive and invasive [10].

3.2. Behavioral Biometric Characteristics

In contrast, behavioral biometrics can be cheaper and easier to use. This group can include signature dynamics, voice verification and mouse or keystroke dynamics.

Mouse dynamics is a measurement of distance, speed and angle during the work with it.

Keystroke dynamics is the duration of each key-press and the time between keystrokes.

4. Keystroke Dynamics

Keystroke dynamics is the process of analyzing the way a user types at a terminal by monitoring the keyboard inputs thousands of times per second in an attempt to identify users based on habitual typing rhythm patterns [9]. It has already been shown that keystroke rhythm is a good sign of identity [6].

Moreover, unlike other biometric systems which may be expensive to implement, keystroke dynamics is almost free – the only hardware required is the keyboard [9, 5].

The application of keystroke rhythm to computer access security is relatively new. There has been some sporadic work done in this area. Joyce and Gupta [6] present a comprehensive literature review of work related to keystroke dynamics prior to 1990. The brief summary of these efforts and examination of the research, that has been undertaken since then, can be found in [9].

Keystroke verification techniques can be classified as either *static* or *continuous* [9].

- *Static verification* approaches analyze 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 can not detect a substitution of the user after the initial verification.

- *Continuous verification*, on the contrary, monitors the user's typing behavior throughout the course of the 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 [1]. This offers a possibility of continuous control 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 while [3].

Some features can be extracted of the keystroke rhythm as [2, 10]:

- the time that a key is pressed (keystroke duration),
- the time of pressing individual keys (keystroke latency),
- speed of the keystroke,
- frequency of errors,
- style of writing capital letters,
- placement of the fingers and
- pressure that the person applies when pressing a key (pressure keystroke).

This latter type 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 [9, 5].

The history of keystroke dynamics can be found in [9, 6] or in [2].

4.1. Advantages and Disadvantages of this Method

Advantages of technology [11]:

1. The ultimate goal is ability to continually checking the identity of a person as they type at a keyboard [9, 1].
2. Neither enrolment nor verification affect the regular work flow because the user would be typing needed text anyway. Easy to use for example with login and password during logon process.
3. Unlike other biometrics system, keystroke dynamics is almost free. The only hardware required is the keyboard [9, 5].
4. Time to training of users is minimal and ease of use is very high.
5. Public acceptability is very high. There are no prejudices such in case of criminal pattern in fingerprint verification or discomfort such as retina pattern scanning [10].
6. Keystroke dynamics is ideal also for network users.

Disadvantages of technology [11]:

1. Keystroke dynamics are non-static biometrics same as for example voice. This can change quite fast during time, also one-hand typing (due to injury), etc. can influent typing rhythm [9].
2. Low accuracy – keystroke dynamics is one less unique biometrics.
3. Small commercial widespread of technology.

5. 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 [11]. Now only one company, Net Nanny, works on commercial release of their product BioPassword [4].

There are many potential areas for this technology, especially for its low cost and feature of continuous checking. Limitations are mainly non-consist typists [11].

Monrose [9] also believes that keystroke dynamics can be theoretical used as possible attack to PGP[1], because random seed collected during key generation is calculated from user's typing. This can be weakness, if users typing characteristics are known [11].

Monrose [9] also reports, that there can be some differences between left-handed and right-handed users, but he has only small part of left-handed users in testing group to give some useful results [11].

[1] 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 [12]).

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 a ideal scenario for the application of a keystroke authentication system. Keystroke dynamics may be used to detect uncharacteristic typing rhythm (brought on by drowsiness, fatigue etc.) in the user and notify third parties [9].

6. Conclusion

For centuries the handwritten signature is maintained as one of the important identification data. This is a unique expression of human brain. The signature is formed already in 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 keyboard. So it is appropriate to deal with this new way of human signing.

The purpose of this paper is to concentrate the available information about this new phenomenon. We can assume that typing has its own specifics, which can be in use similar to written text.

References

[1] F. Bergadano, D. Gunett, and C. Picardi, “ User authentication through Keystroke Dynamics:”ACM Transactions on Information and System Security. 5(4):367–397, 2002.

[2] G.C. Boechat, J.C. Ferreira, and E.C.B. Carvalho, “Using the Keystrokes Dynamic for Systems of Personal Security”. Proceedings Of World Academy Of Science, Engineering And Technology. 24(18):61–66, 2006.

[3] D. Gunett and C. Pikardi, “Keystroke analysis of free text”. ACM Transactions on Information and System Security. 8(3):312–347, 2005.

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

[5] J. Ilonen, “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

[6] R. Joyce and G. Gupta, “Identity authorization based on keystroke latencies”. Communications of the ACM. 33(2):168–176, 1990.

[7] S.M. Matyas and J. Stapleton, “A Biometric Standard for Information Management and Security”. Computers & Security.19(2):428–441, 2000.

[8] B. Miller, “Vital sings of identity”. IEEE Spectrum. 31(2):20–30, 1994.

[9] F. Monrose and D. Rubin, “Keystroke dynamics as a biometric for authentication”. Future Generation Computer Systems. 16(4):351–359, 2002.

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

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

[12] P. Zimmermann, “PGP Source Code and Internals”. MIT Press; 1995.