Neural Networks in Keystroke Dynamics for Multi-Factor Authentication in Biomedicine

[1,2]A. Schlenker, [3]M. Sarek

[1]Institute of Computer Science, Academy of Sciences of the Czech Republic, 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
Email: schlenker.anna@gmail.com

Abstract. *This paper presents an improved authentication method for biomedicine based on behavioural biometrics. A brief definition of keystroke dynamics and neural networks is provided. The main part of the work focuses on evaluation of typing dynamics which is then proposed as an interesting behavioural biometric characteristic for use in computer security not being widely used so far. The result of the work will be a new application, which allows optimal multi-factor authentication method regarding its comfort, cost and reliability.*

Keywords: Neural Network, Keystroke Dynamics, User Authentication

1. Introduction

With still growing extension of computer systems the need for their appropriate security increases [1]. After the user has successfully logged into the system, he/she has the opportunity to not only see, but also modify and copy sensitive data.

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. These are so called biometrics. Firstly, there are anatomical-physiological characteristics such as fingerprints, palm prints, hand geometry, blood vessel in the hand, patterns in the face, and patterns in the iris or retina. Secondly, there are behavioural characteristics such as signature, voice, and keystroke or mouse dynamics [2].

On the other hand, we can use some external attributes, whether it is a knowledge factor like password, or a possession factor like a magnetic strip card [2].

Based on the shortcomings of single-factor authentication methods, only multi-factor authentication seems adequately reliable to eliminate unauthorized access securely. It can be for example combination of anatomical or behavioural features with an external attribute or a password [2].

2. Subject and Methods

Keystroke dynamics is a type of behavioural biometrics that authenticates users based on habitual typing rhythm patterns [2]. It has been shown already [3, 4, 5] that the keystroke rhythm, during typing user's account name or password, is a good sign of identity.

Unlike other biometric systems, programs using keystroke dynamics do not require any hardware modifications and can be easily integrated with most computer systems [5, 6, 7].

During typing the username or password we can measure so called timing vector [8] which consists of the keystroke duration times and keystroke latencies [2]. The keystroke duration is a period time during which a key is held for (see Fig. 1) and keystroke latency is the time between individual keystrokes (see Fig. 1). During fast typing when the next key is pressed before a previous key is released [8], the negative time can be measured (see Fig. 2). Figure 2 shows the timing vector when a password of eight characters is typed. This timing vector consists of eight keystroke duration times and seven keystroke interval times (two of them are negative).

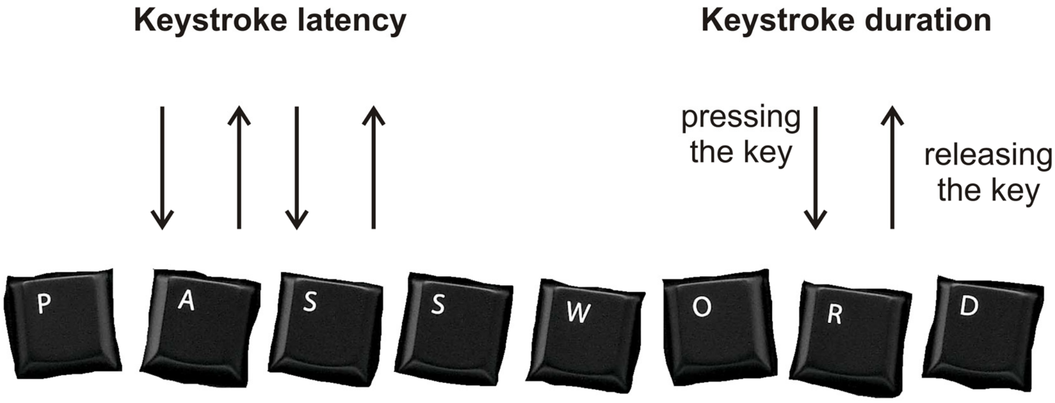

Fig. 1. Keystroke duration and keystroke latency (adapted from [2]).

Basis for Comparison
Samples for evaluation are obtained from users who type their name or username. These samples are then compared with samples obtained from other users (imposters), who try to imitate real users by typing the same name or username [3].

A basis for comparison is provided by two simple metrics: rejection of an authorized user and acceptance of an unauthorized user.

For the rate of rejection authorized users several metrics are used. The False Alarm Rate (FAR) represents a number of authentic user samples rejected by the authentication method and is used by Brown and Rogers [3] or Lin [5]. The False Rejection Rate (FRR) is the measure of the likelihood that the biometric security system will incorrectly reject an access attempt by an authorized user and it is used by Loy et al. [4] or Cho et al. [8].

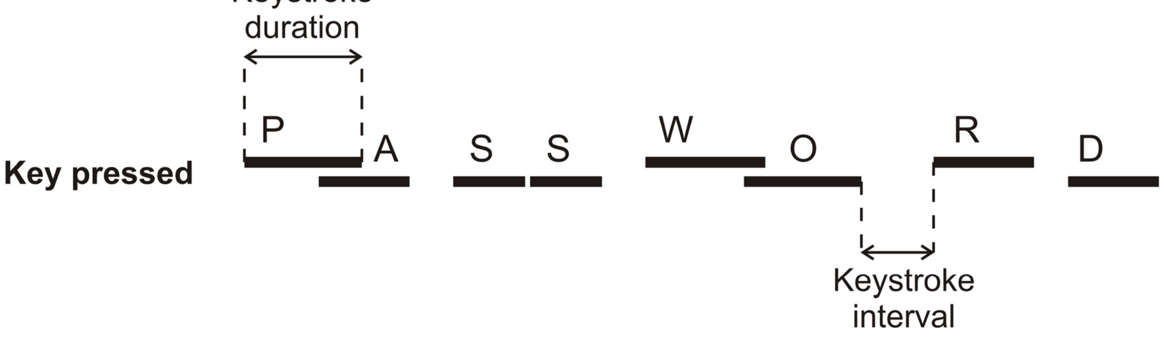

Fig. 2. Timing vector corresponding to “PASSWORD” (adapted from [8]).

For the rate of acceptance of unauthorized users several metrics are used, too. The Imposter Pass Rate (IPR) represents a number of imposter samples incorrectly authenticated and it is used by Brown and Rogers [3] or Lin [5]. Another metric is called the False Acceptance Rate (FAR) and it is used by Loy et al. [4] or Cho et al. [8]. The False Acceptance Rate is the measure of the likelihood that the biometric security system will incorrectly accept an access attempt by an unauthorized user.

Different biometric security systems determine different values for threshold for the False Acceptance Rate and False Rejection Rate. Therefore another metric called the Equal Error Rate (EER) is introduced [4]. The Equal Error Rate determines the point at which the proportion of false acceptances is equal to the proportion of false rejections. The lower is value of this variable, the higher is accuracy of the biometric system.

3. Experimental Approach

In previous studies, different types of neural networks are used for solving the problem of identifying users through the typing characteristics.

The Backpropagation Neural Network (BPNN) used by Akila and Suresh Kumar [1] is a typical multilayer neural network. This neural network uses the back propagation learning rule. The network consists of one input layer, one output layer and at least one hidden layer [1, 3, 9].

The Kohonen Neural Network used by Brown and Rogers [3] is a relatively simple self-organizing map. This neural network consists of two layers, an input layer and a Kohonen layer.

The Counterpropagation Neural Network (CPNN) is a hybrid network developed by Robert Hecht-Nielsen and used by Obaidat [9]. The simplest version of this network consists of two layers. The first layer is the Kohonen layer trained in the unsupervised mode. The second layer is an outstar array, called the Grossberg layer.

The Dynamic Backpropagation Neural Network used by Lin [5] has a changeable number of input nodes.

4. Discussion and Future Work

Based on previous research, there is a fairly surprising result that for the identification of a user only a short text is needed. In most cases it is a string of 6-8 characters which corresponds to user’s name. We believe that the selection of a suitable neural network technique will help us to reach high accuracy of our application and to create a highly reliable biometric system for multi-factor authentication in biomedicine.

The proposal to further increase safety involves also the use of keystroke dynamics while typing a password.

Our work is now in the stage of selecting an appropriate method. The future work will focus on creating a pilot application and its testing on a group of volunteers. This method will be suitable also for on-line applications, due to the fact that it does not require any hardware modification on the side of a user.

5. Conclusion

For centuries the handwritten signature is maintained as an important identification sign. Nowadays, we have to accept replacing handwriting by typing on a keyboard. This paper summarizes the available information about this phenomenon. Combination of keystroke dynamics with neural network techniques offers better possibilities to use it for computer security. Using keystroke dynamics and neural networks during typing a username and a password can improve a multifactorial authentication system in biomedicine rapidly.

References

[1] Akila M, Suresh Kumar S. Improving feature extraction in keystroke dynamics using optimization techniques and neural network. In proceedings of International Conference on Sustainable Energy and Intelligent Systems, 2011, 891-898.

[2] Schlenker A, Sarek M. Behavioural biometrics for multi-factor authentication in biomedicine. *European Journal for Biomedical Informatics,* 8 (5): 19-24, 2012.

[3] Brown M, Rogers SJ. User identification via keystroke characteristics of typed names using neural networks. *International Journal of Man-Machine Studies*, 39:999-1014, 1993.

[4] Loy CC, Lai WK, Lim CP. Keystroke patterns classification using the ARTMAP-FD Neural Network. In proceedings of International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2007, 61-64.

[5] Lin DT. Computer-access authentication with neural network based keystroke identity verification. In proceedings of International Conference on Neural Networks, 1997, 174-178.

[6] Ilonen J. Keystroke Dynamics. In Advanced Topics in Information Processing – Lecture, 2003.

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

[8] Cho S, Han CH, Han DH, Kim H. Web based keystroke dynamics identity verification using neural network. *Journal of Organizational Computing and Electronic Commerce*, 10(4):295-307, 2000.

[9] Obaidat MS, Sadoun B. Verification of computer users using keystroke dynamics. *IEEE Transactions on Systems, Man, and Cybernetics – Part B: Cybernetics*, 27(2):261-269, 1997.