Investigate the impact of user’s state on the quality of authentication by keystroke dynamic

I E Panfilova, N E Karpova

Department of Electronic Systems and Information Security, Samara State Technical University, Samara, Russia
panfilova_2015@bk.ru

Abstract. One of the most important issues in the field of information security has been and remains the issue a reliable user’s authentication. A special place among the possible authentication methods today is occupied by behavioural biometrics, which have a high degree of reliability. A keystroke dynamic, as a type of behavioural biometrics, is also capable of providing a high level of protection of information systems in the case of correctly selected characteristics. This article shows that external factors, including the psychophysiological state of a person, can also influence the authentication process by keystroke dynamics. In the paper, the state of the user was assessed in the process of collecting a sample of keystroke dynamics and a conclusion was made about the presence of such an influence.

1. Introduction

Nowadays, it becomes obvious that the use of a password (or a combination of "login-password") as a means of users’ authentication is at least insufficient in view of the impossibility of achieving an adequate balance between security and convenience for the users. Attempts to improve this approach (for example, "strong passwords" or two-factor authentication), only partially solve the problems of insecurity and high probability of unauthorized access.

Along with hardware authentication tools (smart cards, USB tokens, readers, etc.), which have an increased level of reliability, but still remain inconvenient in everyday use, biometric authentication methods are increasingly penetrating into the life of a modern person, which have repeatedly proved their reliability and efficiency. At the same time, the means of biometric authentication are quite diverse and, in general, are divided into two categories: static and dynamic. Static methods are based on a human physiology, and as means of authentication they use such unique characteristics of a person that remain unchanged throughout all life: face geometry, hand geometry, iris, retina, vein pattern, fingerprint, etc. Static methods are the most widespread type of biometrics, and it is not surprising that more and more reports appear that static biometrics is also quite easy to hack [1], and attackers are expanding their range of approaches to the implement of such operations.

That is why modern governmental programs and major commercial structures are paying more and more attention to the second category of biometrics - dynamic, or behavioral. Dynamic methods use human behavioral features as a means of authentication, which are also unique and exhibit automatic (unconscious) movements. Dynamic authentication methods include handwriting, voice, gesture dynamics, gait, keystroke dynamics, mouse dynamics, etc.

The process of both static and behavioral biometric authentication can be divided into two phases: the registration phase and the authentication (verification) phase [10]. During the registration phase, the user's biometric data is collected, processed and stored as a sample, i.e. a template is formed for subsequent use by the system. During the authentication phase, newly acquired biometric data is
collected, and the authentication decision is based on the result of the process of matching them with previously saved reference templates.

According to the above indicators, at the moment methods for analysing the dynamics of working with the keyboard are the most effective and one of the most reliable methods of behavioural biometrics. The question of determining the characteristics that describe the keystroke dynamic [4] [18], their processing [2] [17] and the authentication process [10] are devoted to a lot of both domestic and foreign works. However, much less attention while working with this type of behavioral biometrics is paid to the question of the impact of external factors, including the user's state, on the collection of keystroke dynamics’ characteristics and the further authentication process.

In order to provide a comprehensive overview of the special collection and recognition of keystroke dynamic, as well as to explain the relevance of the above tasks, this work is organized as follows: Section 2 provides an overview of the most common characteristics of keystroke dynamics, as well as methods of authentication by CP. Section 3 is devoted to the consideration of the issue of CP variability depending on external factors. Section 4 provides an example of assessing the impact of a person's fatigue a typing speed. Finally, section 5 is a conclusion on the work done and an indication of the prospects for further research.

2. Keystroke dynamics. Characteristics and processing methods
Among all the methods of authentication using behavioral patterns, a special place is occupied by the dynamics of working with the keyboard, or the so-called keystroke dynamic. The obvious advantages of the method most often include secrecy and efficiency [2], because to implement it, the user already has a keyboard and software running in the background. Since users usually use a keyboard while using a computer, this method is well suited for authenticating to computer systems. In addition, it can provide a high level of security [15], since it is almost impossible to reproduce unconscious human behavioral patterns.

In general, keystroke dynamic is a set of characteristics that describe the dynamics of a user's keyboard experience. Dynamics, in this case, refers to the process of capturing the rhythm of typing and the manner in which the user works with the keyboard.

The extraction of characteristics used to form a unique keystroke dynamic of a user is almost independent of the type of authentication [14], which can be static (password) or dynamic (continuous) [2]. Static authentication consists in comparing keystroke dynamics obtained by typing a predetermined text sequence, usually of short length (password, passphrase, login). Continuous authentication allows for continuous analysis of the dynamics of the keyboard for a particular user. Moreover, the text that the user enters to train the system can be either pre-generated or arbitrary [3].

Often, as characteristics of the dynamics of keystrokes, that is, as a sample of keystroke dynamic, there is a sequence of durations of holding a word’s individual keys and time intervals between releasing a key and pressing the next one [18]. In addition to these parameters, the duration between pressing a key and pressing the next key, as well as the length of time the key is released and the next key is released, are sometimes additionally considered. These four main parameters can be attributed to the group of timing features that are used in both static and dynamic authentication.

Also, the group of timing features of keystroke dynamic includes digraphs and trigraphs (n-graphs in general), which represent a time delay between two or three consecutive keystrokes, respectively [15].

In [4] this paper, researchers, studying authentication on a text of arbitrary length, in addition to generally accepted timing features, distinguish two more groups: semi-timing features and editing patterns.

The article’s authors refer to the group of semi-timing features such as characteristics of keystroke dynamic, in which, as well as in timing features, time calculation is used, however, this calculation requires longer periods and is mathematically expressed differently from time vectors, for example, by intervals. Such characteristics of keystroke dynamic include, in particular, the number of words per minute (WPM), which, as the name suggests, measures the average typing speed by the user. This parameter is widely used in the study of the dynamics of working with the keyboard [17], however, as
the researchers themselves note, it is not sufficient to unambiguously distinguish between users with similar typing speeds.

The group of semi-timing features also includes such parameters as a negative time interval between releasing the first key and pressing the next [12] (this behavior occurs when entering text in users who tend to press the second key before releasing the first), as well as a negative time interval. the interval between the release of the first and second keys (occurs when the user releases the second key before releasing the first).

The group of editing patterns, in turn, does not pay any attention to the time that the user spends on entering text; rather, it takes into account how the user performs the input process. Conventionally, such a process can be divided into how often the user makes mistakes and how he edits errors. The error rate parameter [9] reflects the percentage of cases when the user makes an input error and corrects it. In this case, the operation of the Backspace or Del key is taken as an error (in this case, a separate but less significant authentication task can distinguish users by the habit of using either Backspace or Del).

The manners in which the user corrects the errors that have already turned out or simply edits complex multi-register text are also a characteristic pattern of behavior while working with the keyboard. These parameters include the percentage of usage of the Shift key, the specificity of the usage of left and right Shift [11], as well as the percentage of usage of CapsLock (also a separate authentication task in this case can serve to distinguish users by the habit of using either Shift or CapsLock).

A separate group, which is not identified in the study, but of interest from a research point of view, is a group of characteristics that require additional equipment. This group includes studies devoted to the force of pressing keys [13] and the definition of keystroke dynamic by sound [20].

3. Variability of the keystroke dynamic
In contrast to the definition of the characteristics used to describe the keystroke dynamic, the question of the variability of the keystroke dynamic depending on external conditions remains open. Often, a reference template, obtained during the registration phase and under the predefined conditions, tends to be less representative of the user's behavior when entering the same text over time. Researchers [7] call the intraclass variability the main reason for the “obsolescence” of the KP template. As noted in [14], the latter can be associated with:

1. Gained experience in entering a password: a person gets used to entering a set of characters (for example, he does it faster each time), which results in a change in the keystroke dynamic;
2. Emotional state and user’s activity: the behavior of users can be strongly influenced by their mood (stress, anger, happiness, etc.) or physical well-being (fatigue, illness, etc.);
3. Different keyboards: user interaction with the keyboard changes depending on its layout, type (virtual or real) and even depending on the device used (computer, laptop, smartphone).

Nowadays, there are already mechanisms for taking into account most of the factors considered, and as a result, methods for adapting keystroke dynamic. For example, the account of the gained experience of entering a password can be observed mathematically and corrected by preliminary training on an independent passphrase [8] or by reducing the number of input attempts during the registration phase, and accounting for the keyboard type can be done by creating a standard based on a combination of the dynamics of typing on different keyboards [6].

At the same time, the psychophysiological states of a person, both at the stage of handwriting registration and during direct authentication, remain the least studied and difficult to account for factors. One of such conditions, which can have a significant impact on a person's performance, and, as a consequence, on the quality of keystroke dynamic, is the state of fatigue. The assessment of the impact of the fatigue state on the BC is given in the next section.

4. Evaluating the effect of fatigue on a user's typing speed
The typing speed a keyword (the number of letters per second), consisting of 12 lowercase Cyrillic characters, was chosen as a characteristic describing the CP. The choice of the speed characteristic is
largely due to the simplicity of its extraction and further processing, as well as the prevalence of this parameter when authenticating a user using keystroke dynamic.

The study involved 30 subjects, who were asked to make 25 attempts to enter a predetermined password in the morning (before the start of the working day) and in the evening (after the end of the working day) for five days. Attempts were recorded using special software that allows you to save and export a dataset for each of the attempts of each individual user to the processing environment. Attempts, in which the user entered a keyword incorrectly or tried to correct it, spending extra time, were not counted.

To assess the fatigue impact on the speed (or lack of it) of typing a password, two criteria were chosen:

1. Reduction of the average print speed by the end of the working day in case of the effect of fatigue on the print dynamics or its stability in case of no such influence
2. Changing the type of frequency distribution of the printing speed in the morning and in the evening.

The last criterion is also explained by the assumption that if the speed authentication process is reduced to the task of testing the hypothesis that a new observation (a new anonymous attempt to enter a keyword) belongs to the general population of the template, then the fact that the distribution of observations is normal also becomes significant for the possibility of using the t-test of the following form:

$$ t = \frac{x_{new} - \bar{x}}{s\sqrt{n+1}} $$

where $n$ is the sample size, $x_{new}$ is the value of the speed of a new anonymous input attempt,

$$ \bar{x} = \frac{1}{n} \sum_{i=1}^{n} x_i \quad \text{– sample average,} $$

$$ s = \sqrt{\frac{\sum_{i=1}^{n} (x_i - \bar{x})^2}{n-1}} \quad \text{– sample standard deviation.} $$

Checking the normal distribution of the typing speed depending on the fatigue of the subjects can be assessed using the Shapiro-Wilk test, since it is convenient for small samples and it is well applicable in the absence of a priori information about the type of possible deviation from normalcy:

$$ W = \frac{b^2}{s^2} $$

where:

$$ b = \sum_{i=1}^{n} a_{n-i+1} (x_{n-i+1} - x_i) $$

$$ s^2 = \sum_{i=1}^{n} (x_i - \bar{x})^2 $$

Based on the first criterion for assessing the effect of fatigue on the speed of typing a password, the results presented in table 1 were obtained (the table illustrates the indicators of three randomly selected subjects).

The table shows that in the evening (E) the average speed values are lower than the morning (M) ones, that is, the subjects write the same password as if in the evening more slowly than in the morning. For the first two subjects, this tendency is traced in 60% of cases, for the third in 100% of
cases. This observation does not allow us to reject the hypothesis of the effect of fatigue on typing speed.

Additionally, we can trace how the characteristics of the frequency distribution of velocities change. These changes are presented in figure 1.

**Table 1.** Changing the average print speed during the day.

|        | Day 1          | Day 2          | Day 3          | Day 4          | Day 5          |
|--------|----------------|----------------|----------------|----------------|----------------|
| №1    | M: 3.177       | E: 3.475       | M: 3.704       | M: 4.488       | M: 3.680       |
|        | E: 4.104       | E: 4.030       | E: 4.281       | E: 4.191       |                |
| №2    | M: 4.310       | E: 4.373       | M: 4.394       | M: 4.454       | M: 4.196       |
|        | E: 4.368       | E: 4.325       | E: 4.378       | E: 4.282       |                |
| №3    | M: 2.692       | E: 2.521       | M: 2.961       | M: 2.930       | M: 2.738       |
|        | E: 2.830       | E: 2.552       | E: 2.826       | E: 2.649       |                |

(a) change in frequency distributions for test subject № 1

(b) change in frequency distributions for test subject № 2

(c) change in frequency distributions for test subject № 3

**Figure 1.** Graphs of frequency distributions of printing speed at the beginning and at the end of the working day.
In addition to the characteristics of the frequency distribution, one can also observe determine the p-values using the Shapiro-Wilk test in the morning and in the evening, at a significance level of $\alpha = 0.05$ (table 2).

**Table 2.** The values of the Shapiro-Wilk criterion in the morning and in the evening.

| № | Morning        | Evening       |
|---|----------------|---------------|
| №1| 2.074e-07      | 5.723e-05     |
| №2| 0.0006333      | 3.075e-06     |
| №3| 8.037e-05      | 0.001069      |

Depending on the time of day (morning and evening), the nature of the private distribution changes, which confirms the hypothesis that the state of a person, in this case fatigue, at the time of collecting keystroke dynamic affects the typing speed, and, consequently, the quality of authentication by CP.

5. Conclusion
In this paper, an assessment of the influence of one of the factors, namely fatigue, on such a CP characteristic as the speed of typing a password was proposed. As a result of the assessment, it was concluded that there is an influence of the state of fatigue on the users’ typing speed, which cannot but affect the quality of the authentication process, if such a factor is not taken into account.

In further studies of the influence of human states on the CP and determining the reliable area of user’s authentication, the problem of developing a universal algorithm for assessing the influence of the above factors on the CP, as well as the implementation of an adaptation mechanism that allows at least to take into account, and as a maximum to neutralize such factors in order to improve the quality is of particular interest, the authentication process and the degree of protection of the system.

6. References
[1] Dogval V A and Dogval D V 2017 Analysis of promising methods of behavioral biometrics for user authentication *Bulletin of ASU* pp 139–142
[2] Krutokhvestov D S and Khitsenko V E 2017 Password and continuous authentication by keystroke dynamic by means of mathematical statistics *Cybersecurity issues* pp 91–98
[3] Alsultan A and Warwick K 2013 Keystroke dynamics authentication: a survey of free–text methods *Int. J. Comput. Sci. Issues* 10 pp 1–10
[4] Alsultan A, Warwick K, Wei H 2017 Non-conventional keystroke dynamics for user authentication *Pattern Recognition Letters*, 89 pp 53–59
[5] Araujo L C F, Sucupira L H R, Lizarraga M G 2005 User authentication through typing biometrics features *IEEE Trans. Signal Process* 53 pp 851–855
[6] Bours P and Ellingsen J 2018 Cross Keyboard Keystroke Dynamics 2018 1st International Conference on Computer Applications & Information Security
[7] Epp C, Lippold M, Mandryk R L 2011 Identifying emotional states using keystroke dynamics *Proceedings of the SIGCHI conference on human factors in computing systems* (New York, NY, USA) pp 715–24
[8] Grabham N and White N 2008 Use of a novel keypad biometric for enhanced user identity verification *Proceedings of the instrumentation and measurement technology conference proceedings* pp 12–16
[9] Guven A and Sogukpinar I 2003 Understanding users’ keystroke patterns for computer access security *Computers & Security* (22) pp 695–706
[10] Karnan M, Akila M, Krishnaraj N 2011 Biometric personal authentication using keystroke dynamics: A review *Applied Soft Computing, 11*(2) pp 1565–1573
[11] Lau E, Liu X, Xiao C, Yu X. 2004 Enhanced user authentication through keystroke biometrics Computer and Network Security
[12] Lin D T 1997 Computer-access authentication with neural network based keystroke identity verification Proceedings of the International Conference on Neural Networks (Houston, TX, USA) pp 174–178
[13] Martono W, Ali H, Salami M J E 2007 Keystroke Pressure-Based Typing Biometrics Authentication System Using Support Vector Machines Computational Science and Its Applications pp 85–93
[14] Mhenni A, Cherrier E, Rosenberger C, Najoura E B A 2019 Double serial adaptation mechanism for keystroke dynamics authentication based on a single password Computers & Security, 83 pp 151–166
[15] Princy A T, Lakshmi P A, Dr. Suvanam S B A 2016 Review of Behaviometric Techniques for User Authentication IOSR Journal of Computer Engineering pp 11–14
[16] Roth J, Liu X, Ross A, Metaxas D 2015 Investigating the Discriminative Power of Keystroke Sound Information Forensics and Security, IEEE Transactions on Biometrics Compendium, Vol:10 No. 2 pp 333–345
[17] Villani M, Tappert C, Ngo G, Simone J, Fort H S, Cha S H 2006 Keystroke biometric recognition studies on long-text input under ideal and application oriented conditions Proceedings of IEEE Conference on Computer Vision and Pattern Recognition Workshop pp 39–46
[18] Zhong Y, Deng Y, Jain A K 2012 Keystroke dynamics for user authentication Computer Society Conference on Computer Vision and Pattern Recognition Workshops