KEYSTROKE DYNAMICS AUTHENTICATION USING A SMALL NUMBER OF SAMPLES

Jan Čapek[1], Miloslav Hub[2]

[1] *University of Pardubice, Faculty of Economics and Administration, Institute of System Engineering and Informatics, Czech Republic, ORCID: 0000-0002-2643-4355, capek@upce.cz;*
[2] *University of Pardubice, Faculty of Economics and Administration, Institute of System Engineering and Informatics, Czech Republic, ORCID: 0000-0002-3167-0918, miloslav.hub@upce.cz.*

Abstract: *The verification of a person's identity is very important in today's information society, especially in e-commerce systems and directly affects user account management and administration. Although present e-commerce systems use many modern sophisticated methods of authentication, large numbers of e-commerce systems use passwords for this purpose incessantly. However, passwords are not considered be too secure because users usually do not adhere to security policies for creating and managing theirs passwords. This problem can be solved by security policies that require the user to change the password frequently, select a completely new password, and structure the password, which places additional demands on the user. The solution is a two-factor authentication where a user needs to know the right password and at the same time, he must write this password in the correct way. Indeed, many different methods for keystroke dynamics authentication exist nowadays, but unfortunately, many of them need a large number of samples to create a stable template and therefore it is impossible use them in systems whose security policy requires frequent password change. The authors suggest a completely new method for these purposes that is enough stable even with a small number of measurements to create a template. This proposed method of keystroke dynamics authentication is validated and results are compared with existing methods both over the own dataset and the existing reference datasets. The authors believe that the proposed method will simplify the management and administration of user accounts as well as their security.*

Keywords: *Account management, account administration, authentication, biometric, keystroke dynamics, password.*

JEL Classification: *C38, C60, C88.*

APA Style Citation: Čapek, J., & Hub, M. (2020). Keystroke Dynamics Authentication Using a Small Number of Samples. *E&M Economics and Management, 23*(4), 215–226. https://doi.org/10.15240/tul/001/2020-4-014

Introduction

The ubiquitous Internet connectivity has led to the introduction of an ever-increasing list of diverse online services ranging from financial transactions to online gaming and the other e-commerce purposes. For example, with cloud computing on the rise, geographically distant employees of organizations are able to access and share sensitive organizational resources online. The mentioned trend has increased the amount of user authentication processes.

The aim of authentication is to decide whether a subject in question is in fact the subject that he claims to be. As an example can be mentioned traditional authentication, when end users authenticate themselves on computers by using the pair of username and password. In the past, many sophisticated authentication methods were developed. Generally, they can by divided to the three basic types of authentication depending on what kind of identification feature is used: authentication by knowledge, authentication by ownership of something, and authentication by biometrics. Each of these ways has its advantages and disadvantages. For example authentication by passwords ("something to know") is easy to implement and it is widely accepted by end users but it is not considered be too safe (Hub, 2003; Stallings, 2012). Many client/server applications use a user's ID and password for authentication, for example, when remotely logging onto a supplier's web database and/or bank systems. In all these applications, it is often possible for an attacker to intercept the password and then replay it to the server. Of course, this replay problem can be overcome by using a system called a "onetime password system" (OTP) when a password is generated by a separate device or distributed by another communication channel (Haller et al., 1998; Hoque, 2014; Soh & Joy, 2003). An OTP system generates a different password for each time of authentication. However, in this contribution, the authors do not use the OTP method and show that there exist an option to use the old password system with an acceptable level of security that does not need for example a mobile phone to receive an OTP password.

It is well known that different authentication methods can be combined together to strengthen the strengths and eliminate the shortcomings of each authentication methods and thus increase the security level of the authentication. In this context, we talk about two, respectively three-factor authentication. An example is an ATM where you need to have the appropriate bankcard and know the appropriate PIN.

To solve the problem of not very secure passwords we focused on the combination of passwords and keystroke dynamics authentication (KDA) based on the principle that every person has a different method of keyboard typing (Legget et al., 1990; Liu et al., 2015). This two-factor authentication process involves two steps. Firstly, the character string of the typed password is compared with that of the valid user's recorded password. If they match, the system evaluates the similarity between the given typing sample and the stored typing patterns (a template) of the valid user. If this similarity is large enough, user's identity is accepted and access to the system is granted to the user. Otherwise, the user's identity is rejected. This idea is not entirely new, but at present, the application of this two-factor authentication is limited by the limitations of existing KDA methods, which require a large number of samples to reliably identity verification.

The aim of this paper is to present a new method of KDA, which gives reliable results even in the case of a small number of measurements for creating a template. Our proposed method is especially suitable for systems whose security policy requires frequent change of password and end users cannot be asked for multiple passwords entering when creating a KDA template.

This article is structured as follows. The first chapter provides an overview of the current state of all of the areas that are important for the purpose of this article. The second chapter deal with proposed method based on a rectangular system, using Pythagoras' formula contains the formal definition of the proposed approach. The third chapter provides verification of the proposed methods. We choose for verifications six possible passwords (dA7upR0k, eagle512, ext25ra8, eXt25rA8, facebook, standard), the verification procedure in detail is contained in this chapter. The next chapter deal with comparison our method with Killoury and Maxion datasets. The fifth chapter discusses the proposed approach including a summary of its advantages and disadvantages in the context of the current state of this issue. The final chapter summarizes this article and outlines the possible future research in this area.

1. Background and Related Work

Keystroke dynamics authentication (KDA) is a behavioral biometric authentication method that verify identity of a keyboard user via his keyboard typing habits, when a string of characters is typed. It is similar to one's signature. During keyboard typing, different measures can be measured. Nowadays, durations of a key press and the intervals between two key presses usually constitute a keystroke dynamic because measuring of these features do not need a special keyboard such as placing your finger on the key or the intensity of a keystroke.

KDA has been proposed and developed in many papers and patents for decades. Although it has a long history dating back to the use of telegraph in the 19th century and Morse code in the Second World War, new methods are still emerging. Most of the prior work still focuses on static text; i.e., all users type the same text. Only a few efforts have addressed the issue of free text (when a user can type an arbitrary text) which is necessary for continuous authentication (Gunetti & Picardi, 2005; Kang & Cho, 2015; Tappert et al., 2009).

The keyboard dependency of personal identification by keystroke dynamics was studied by Matsubara et al. (2015). Chang (2012) suggests using keystroke dynamics for cryptographic purposes. An exhaustive review of KDA studies were published, such as Banerjee and Woodard (2012), Bhatt (2013), Kanimozhi and Kanimozhi (2015) and Pin et al. (2013), where authors compare methods, reference databases and errors within the authentication processes. All biometric authentication methods are based on the calculation of similarity between a template created by the proper user and an authenticated user's sample in KDA usually the keystrokes (durations) and the times between keystrokes (latencies) are evaluated. Relatively different methods were suggested by Roth et al. (2013), when authors suggested KDA that authenticated a user by keystroke sounds. Especially in the last decade, various authors suggested using of soft computing methods, such as Ant Colony Optimization (ACO), Particle Swarm Optimization (PSO). The Genetic Algorithm (GA) is used together with Extreme Learning Machine (ELM) for feature subset selection as used by Karnan and Akila (2009) and Karnan and Akila (2010) respectively. These methods to learn by themselves require a big amount of data and therefore all these methods use a relatively large datasets for the teaching process which is their disadvantage.

2. Proposed Method

All previous methods are based on linear systems; i.e. the vector is composed of serial digraphs of the passwords and user's ID respectively. However, it have to be noted that while the duration times are always positive, latency times may be both positive and negative, as is shown in Fig. 1.

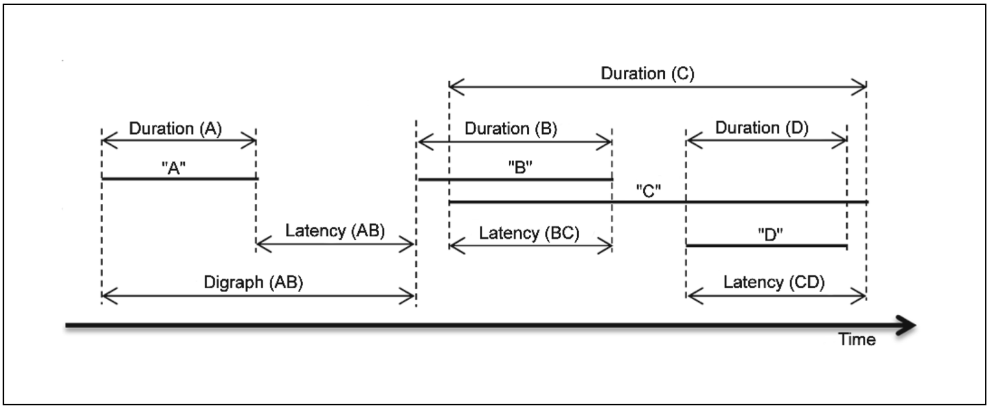
Unlike existing approaches, our new approach is based on a rectangular system, using Pythagoras' formula (see Fig. 2).

Registration phase of two-factor authentication proposed by us contains except ID and a password choice also biometrics enrolment processes when several samples of the user's keystroke dynamics are obtained and processed (completeness control, quality control, features extraction…) to create a template in the form:

$$\mathbf{T} = \begin{vmatrix} \mathbf{T}^D \\ \mathbf{T}^L \end{vmatrix} \qquad (1)$$

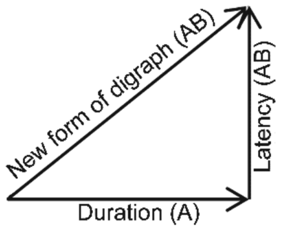
where $\mathbf{T}$ is the keystroke dynamics template of a user, $\mathbf{T}^D$ is the durations template of a user and $\mathbf{T}^L$ is the latencies template of a user. The durations template $\mathbf{T}^D$ and the latencies template $\mathbf{T}^L$ of a user are expressed by (2) and (3) respectively.

Fig. 1: Duration and latency times



Source: own

Fig. 2: Duration and latency times



Source: own

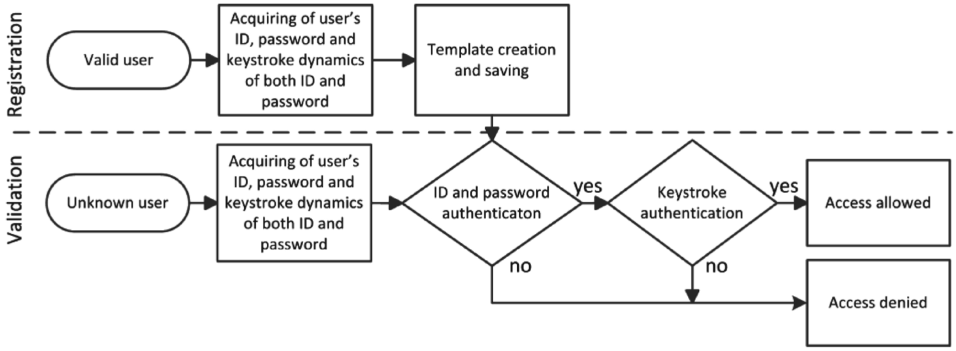
$$\mathbf{T}^{D} = \begin{vmatrix} t_{1,1}^{D} & t_{1,2}^{D} & \cdots & t_{1,n}^{D} \\ t_{2,1}^{D} & t_{2,^{..}2}^{D} & \cdots & t_{2,n}^{D} \\ \vdots & \vdots & \ddots & \vdots \\ t_{m,1}^{D} & t_{m,2}^{D} & \cdots & t_{m,n}^{D} \end{vmatrix} \qquad (2)$$

$$\mathbf{T}^{L} = \begin{vmatrix} t_{1,1}^{L} & t_{1,2}^{L} & \cdots & t_{1,n}^{L} \\ t_{2,1}^{L} & t_{2,^{..}2}^{L} & \cdots & t_{2,n}^{L} \\ \vdots & \vdots & \ddots & \vdots \\ t_{m,1}^{L} & t_{m,2}^{L} & \cdots & t_{m,n}^{L} \end{vmatrix} \qquad (3)$$

where $t^{D}_{j,i}$ is the i-th duration time obtained from j-th sample, $t^{L}_{j,i}$ is the i-th latency time obtained from the j-th sample, m is the number of samples and n is the number of duration/latency times.

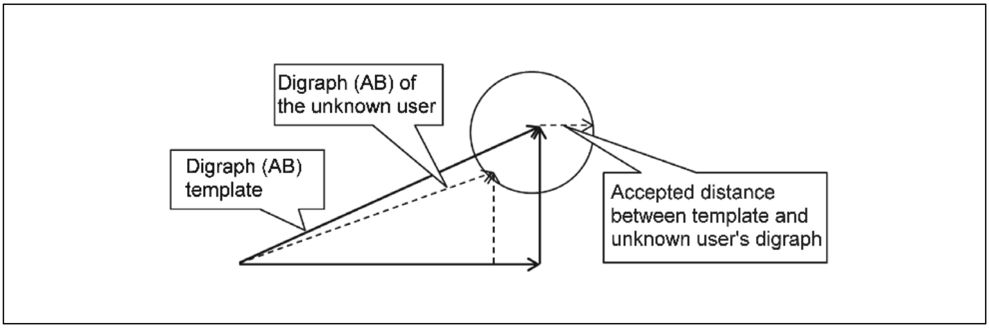
During the verification phase of authentication proposed of us, the user enters his or her ID and password and in the background, besides the password text the keystroke dynamics of the typing is measured. Principle of proposed two-factor authentication shows Fig. 3.

Fig. 3: Enrolment and login process


Registration
Valid user
Acquiring of user's ID, password and keystroke dynamics of both ID and password
Template creation and saving
Validation
Unknown user
Acquiring of user's ID, password and keystroke dynamics of both ID and password
ID and password authenticaton
yes
no
Keystroke authentication
yes
no
Access allowed
Access denied

Source: own

Fig. 4: Comparison of template digraph with unknown user



Source: own

Generally, knowledge-based authentication through passwords is deterministic in its nature – the user both knows the password and enters it correctly or he does not. KDA, however, like most biometric authentication is stochastic in its nature. Both duration and latency times are stochastic variables whose values are influenced by random events. Therefore, they are not be the same for a given user every time. That is why it is necessary to set an appropriate tolerance level of dissimilarity between the keystroke dynamics obtained during the verification phase with the template stored in the system (see Fig. 4).

In our approach, we consider that certain characteristics are more significant for authentication purposes than others are. By other words, characteristics with a lower variance are more stable and therefore have a more significant role in a verification process than characteristics whose variance is high.

Consider that we obtain the following characteristics (4) during the verification phase:

$$\mathbf{V} = \begin{vmatrix} v_1 \\ v_2 \\ \vdots \\ v_3 \end{vmatrix} \tag{4}$$

where $\mathbf{V}$ is the keystroke dynamics obtained during verification and v_i is the i-th digraph obtained during verification.

Every digraph consists of both duration and latency time (5):

$$v_i = \begin{vmatrix} v_i^D \\ v_i^L \end{vmatrix} \tag{5}$$

where v_i^D is the duration time of the i-th digraph obtained during verification and v_i^L is the latency time of the i-th digraph obtained during verification.

Then we can define the proposed measure of dissimilarity (hypotenuse) as (6):

$$d_H(\mathbf{V}, \mathbf{T}) = \max_i{}^{2nd} \frac{d(v_i, t_i)}{s(\mathbf{T_i})} \tag{6}$$

where $d_H(\mathbf{V}, \mathbf{T})$ is the hypotenuse measure of dissimilarity between verification $\mathbf{V}$ and template $\mathbf{T}$, $d(v_i, t_i)$ is the distance between the i-th verification digraph and the i-th average template digraph and $s(\mathbf{T}_i)$ is the variance of the i-th digraph of the template. The superscript $2nd$ above $\max_i{}^{2nd}$ in formula (6) shows that we want the second maximum value. It serves to eliminate the influence of exceptional random adverse effects on the authentication results.

Distance $d(v_i, t_i)$ between the i-th verification digraph v_i and the i-th average template digraph t_i is that expressed as (7):

$$d(v_i, t_i) = \sqrt{(v_i^D - \bar{t}_i^D)^2 + (v_i^L - \bar{t}_i^L)^2} \tag{7}$$

where v_i^D is the duration time of the i-th digraph of verification, v_i^L is the latency time of the i-th digraph of verification, $\bar{t}_i^D$ is the average duration time of the i-th digraph of template and $\bar{t}_i^L$ is the average latency time of the i-th digraph of the template.

In the previous formula (7), the i-th average template digraph t_i may be expressed as (8) and its constituent average duration time of the i-th digraph of template $\bar{t}_i^D$ and average latency time of the i-th digraph of template $\bar{t}_i^L$ can be calculated by formulas (9) and (10) respectively.

$$t_i = \left|\frac{\bar{t}_i^D}{\bar{t}_i^L}\right| \tag{8}$$

$$\bar{t}_i^D = \frac{1}{m}\sum_{j=1}^{m} t_{j,i}^D \tag{9}$$

$$\bar{t}_i^L = \frac{1}{m}\sum_{j=1}^{m} t_{j,i}^L \tag{10}$$

where m is the number of samples for template creation, $t_{j,i}^D$ is the duration time of the i-th digraph of template from the j-th sample and $t_{j,i}^L$ is the latency time of the i-th digraph of template from the j-th sample.

Variance $s(\mathbf{T}_i)$ of the i-th digraph at template $\mathbf{T}$ is expressed as:

$$s(\mathbf{T}_i) = \sqrt{\frac{1}{m-1}\cdot\sum_{j=1}^{m}\sqrt{\left(t_{j,i}^D - \bar{t}_i^D\right)^2 + \left(t_{j,i}^L - \bar{t}_i^L\right)^2}} \tag{11}$$

3. Proposed Method Verification

To verify the proposed method it is necessary to obtain appropriate biometric data. We conducted a search of existing datasets and we hoped that we would find a dataset that would be suitable for verification of our method and for comparison of the results with existing methods.

The most frequently mentioned dataset was created by Killourhy and Maxion (2009) with the help of 51 subjects (typists) when all these subjects typed the same password (.tie5Roanl), and each subject typed the password 400 times over 8 sessions (50 repetitions per session). Firstly, we assume a certain influence of learning during repeated password entries and thus we believe that the dynamics of writing passwords for the fiftieth time will be quite different from when a user enters the password for the first time. Secondly, it is possible to assume that an experienced typist has his writing style more stabilized than a regular user who does not use the keyboard so often. Thirdly, we believe that users not choose for their passwords randomly generated strings that but they choose passwords that are easy to remember and easy to type. Fourthly, the results of the individual methods are presented here simplified only as Average Equal-Error Rate and its deviation. We think that a much more convenient tool for comparing different methods is the Detection Error Tradeoff (DET) graph than only one point on this graph. For these reasons, we do not consider this database as suitable for keystroke dynamics authentication methods validation in a real environment.

Another frequently mentioned dataset (Allen, 2010) was obtained with help of a pressure sensitive keyboard when three different passwords were typed: “pr7q1z”, “jeffrey allen” and “drizzle”. Overall 104 users were present on the database, but only seven of them provided a significant amount of data (between 89 and 504), whereas the other 97 only provided between 3 and 15 samples. We consider that he number of participants who provided sufficient data is inadequate. Moreover, our goal is to propose a method of authentication that requires no special hardware, so this dataset is not suitable for our purposes as well.

The last dataset that is worth mentioning is the dataset by Bello et al. (2010) that was released in 2010. This dataset stores data from an experiment when 58 volunteers typed 14 phrases extracted from books and 15 common UNIX commands. Unfortunately, it seems that almost all the users did only one session and therefore this dataset is not useable for us.

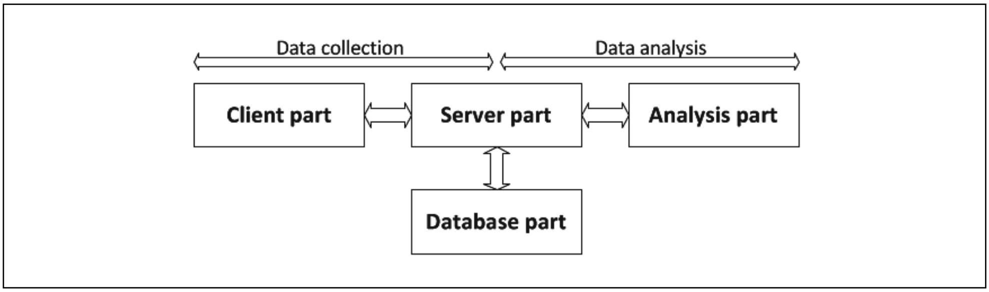
Because we consider these three mentioned datasets are not suitable for our purposes, we decided to create our own dataset for the model validation and comparison with current models of keystroke dynamics authentication. We developed experimental software that consists of four parts and serves for data collection and data analysis:

1. Client part – a graphic user interface that instructs a participant what to do; it contains an electronic form for entering a password and an algorithm for duration and latency times measured when the password is written.
2. Server part – an application that instructs the client part and communicates with it.
3. Database part – the place where the collected data are stored.
4. Analysis part – software that reads and selects data from the database and exports this data for analysis tools (Matlab, Statistica, SPSS).

The experiment where biometric data were collected can be divided to the two phases:

1. During the first phase, one of six possible passwords (dA7upR0k, eagle512, ext25ra8, eXt25rA8, facebook, standard) was randomly assigned by a system to every

Fig. 5: **Experimental software**



Source: own

participant (a college student). Afterwards, the participants were asked to register on the experimental software. During registration, the participants typed their passwords 20 times. On the background, duration and latency times were automatically measured and saved to a database. This phase imitated the registration of the users.

2. During the second phase, the participants were asked to type the assigned password one time. This phase takes for three weeks and participants wrote their passwords usually one time per a week. Duration and latency times were automatically measured on the background and saved to a database. This phase imitated attempts of valid users' verification.

During the verification phase of the authentication process, two types of end user can occur:

1. Valid users are those users who identify as themselves during the verification phase of the authentication process. Verifications of authorized users were simulated so that the individual measurements obtained in the second stage of data collection were compared with the data of the given participant obtained in the first stage of data collection.
2. Impostors are those users who identify through the identity of other users during the verification phase of the authentication process. Verifications of impostors were simulated so that the individual measurements obtained in the second stage of data collection were compared with the data of other participants (who had been assigned the same password) obtained in the first phase of data collection.

The result of the verification phase of the authentication process is the decision whether to accept the identification features presented by an authenticated person as a proof of his identity, or whether to refuse these features as proof of identity claiming. Of course, ideally,

Tab. 1: **Number of participants**

Password	Participants	Valid user attempts	Impostor attempts
dA7upR0k	16	21	555
eagle512	25	69	2,256
eXt25rA8	26	57	2,075
ext25ra8	18	42	1,020
facebook	23	54	1,694
standard	26	43	1,725

Source: own

these features presented by valid users are always accepted and features presented by impostors are always rejected. Unfortunately, the result of this verification will be wrong decision when a valid user is rejected (false rejection) or an impostor is accepted (false acceptance). This is the reason why we choose, as a criterion for comparison of our model to contemporary models, a false acceptance ratio FAR and false rejection ratio FRR, which can be defined as:

$$FAR = \lim_{NIA \to \infty} \frac{NFA}{NIA} \tag{12}$$

$$FRR = \lim_{NVA \to \infty} \frac{NFR}{NVA} \tag{13}$$

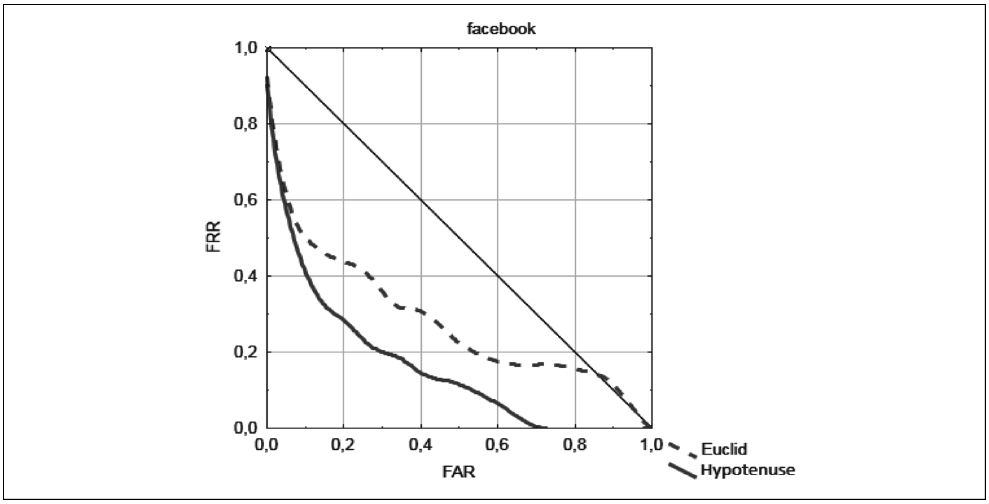
where NFA is the number of false acceptances, NIA is the number of impostor accesses, NFR is the number of false rejections and NVA is the number of valid accesses.

Of course, both FAR and FRR are theoretical values that are not known but can be estimated on the basis of the experiment, within which we find how many impostors are mistakenly accepted and how many valid users are mistakenly rejected.

It is necessary to note that the specific values of the FAR and FRR depends on the “tolerance” which is required when comparing the values obtained during verification and the values obtained during registration and stored in the system. With increasing tolerance, the FRR decreases while the FAR increases and vice versa. A convenient way to view the relationship of FAR and FRR at different tolerances is a Detection Error Tradeoff graph (DET graph) with one axis as the variable FAR and the second axis as the variable FRR. This graph can be also used for comparing multiple biometric authentication methods, which plots curves of these methods. A biometric authentication method where the curve lies under the curves of other methods is advantageous in terms of recognition accuracy. At the same, for the FAR value, it always has a lower FRR value than other methods of biometric authentication, and for the same FRR value it always has a lower FAR value.

Fig. 6 shows the result of the proposed method in comparison with the traditional Euclid method for the password “facebook”. It can be seen that the result of our proposed method is better, because the curve lies below the curve of the Euclid method. The results for other passwords are similar and always better than the Euclid method.

Fig. 6: **Result of the Hypotenuse method**



Source: own

4. Comparison with Killourhy and Maxion Dataset

Although we have justified why the use of the reference database of Killourhy and Maxion (2009) is not appropriate for comparing individual methods of keystroke dynamics biometric authentication, we decided to compare the outputs of our method with others within this dataset. The result of our Hypotenuse method is compared with the most discussed methods in Tab. 2.

It has to be noted again that Average equal error rate is an only one point of a Detection error tradeoff curve and that is why this comparison is too simplified. Interesting results are seen when comparing these methods with different number of measurements (template size) for the template creation (see Fig. 7).

It can be seen for the small amount of template creation samples our hypotenuse method is more stable and it results in smaller Average equal error rate then other methods (see Tab. 3).

Fig. 8 shows comparison of different methods when only 5-size sample is used. This comparison proves the stability of our method.

5. Discussion and Future Work

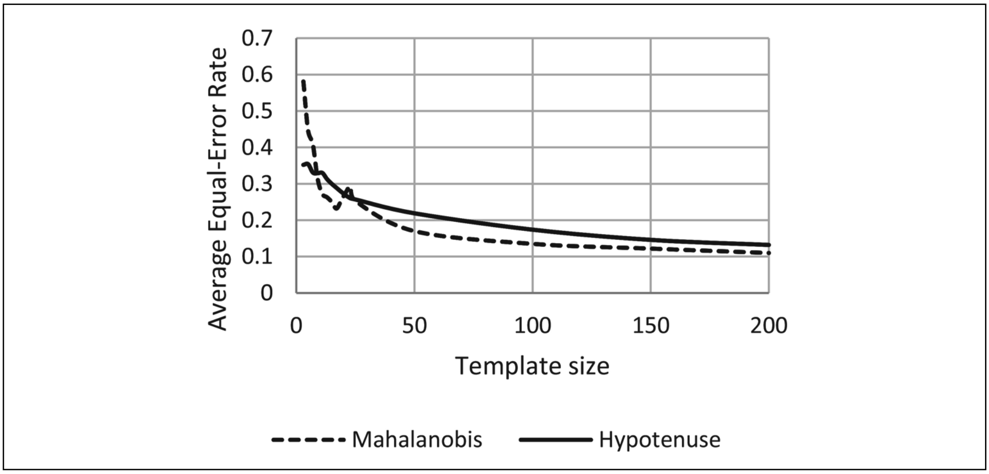
Keystroke biometrics has an advantage over most other biometric authentication schemes, namely, user acceptance. Since users are already accustomed to authenticating themselves through usernames and passwords, most proposed keystroke biometric methods are completely transparent. By comparing Karnan et al. (2011), Killourhy and Maxion

Tab. 2: Comparison with Killourhy and Maxion dataset

Detector	Average equal error rate	Standard deviation
Euclidean	0.171	0.095
Manhattan	0.153	0.092
Mahalanobis	0.110	0.065
Hypotenuse	0.132	0.085

Source: own

Fig. 7: Result of the Hypotenuse method with different template size



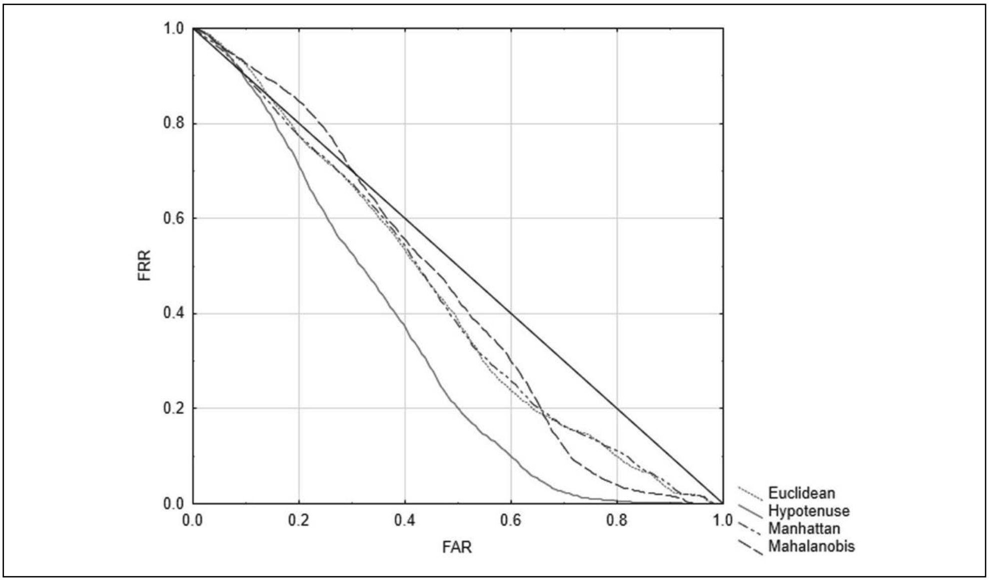
Source: own

Tab. 3: Different template size

Template size	Mahalanobis	Hypotenuse
3	0.581	0.352
5	0.446	0.354
7	0.409	0.331
9	0.315	0.329
11	0.272	0.330
13	0.263	0.313
15	0.250	0.300

Source: own

Fig. 8: Different methods with using 5-size sample



Source: own

(2009) and our work it seems that the proposed methods are depend on a password, collecting methods and evaluation methodology.

Some may criticize this method of authentication as not very reliable. Certainly keystroke dynamics in comparison with something like iris scanning is not so stable and therefore has a higher probability of and errors. However, a method has no higher demands on equipment and end users.

The proposed method of authentication provides approximately 30% of identification of impostors without rejecting a legitimate user (without taking into account the knowledge part of this two-factor authentication). The great weakness of knowledge authentication via passwords is the risk of a successful dictionary or brute force attack. In the first case, the attacker checks if the password is not some commonly used words, in the latter case, the attacker sequentially checks whether the password is not an alphanumeric string. These attacks have a higher probability of success when the set of candidate passwords that must be tried is small. By incorporating authentication via keystroke dynamics, the set of candidate passwords significantly increases. The attacker would have to test not only the individual strings, but also the method of writing these text strings on the keyboard. The proposed method of two-factor authentication therefore does not require such high demands on strong password creation (random length, special characters, the use of uppercase/lowercase letters...) by the end users while maintaining a “reasonable” level of safety.

Conclusions

Password authentication in combination with keystroke dynamics authentication have a great potential. The user does not have to change their habits, nor even know when entering the password that its dynamics are measured. An attacker who wants to trick this authentication must guess not only the correct password, but must also type it correctly on the keyboard. This does not make it easier to use automated password attack tools; it is no longer possible to use a dictionary attack or brute force attack. Keyboard typing dynamics cannot be easily seen and recorded with a hidden camera (attack over shoulder).

However, the current methods of verifying the identity of the user through keyboard typing dynamics had a relatively large drawback that prevented their massive spread. They required a large number of measurements to create a relatively stable template against which subsequent accesses are verified. However, our proposed method returns relatively accurate results even with a small number of samples, which is especially important when the security policy requires the user to change the password frequently.

Of course, compared to other biometric systems, the and values are higher, but it is important to note that there is another authentication factor – the password. We believe that filtering out 30% of intruders without mistakenly rejecting a single valid user is a significant contribution to improving authentication security, especially when there is no need to incur additional high costs. Moreover, although this method of authentication is less reliable especially in comparison with physiological biometric methods, it requires no special equipment and is inexpensive. By incorporating keystroke dynamics into a knowledge-based authentication through passwords, these passwords significantly increase resistance against brute force and dictionary attack. Users will be allowed to choose more easily memorised passwords that cannot be noted.

References

Allen, J. D. (2010). *An analysis of pressure-based keystroke dynamics algorithms* (Master Thesis). Dallas, TX: Southern Methodist University.

Banerjee, S. P., & Woodard, D. L. (2012). Biometric Authentication and Identification Using Keystroke Dynamics: A Survey. *Journal of Pattern Recognition Research, 7*(1), 116–139. https://doi.org/10.13176/11.427

Bello, L., Bertacchini, M., Benitez, C., Pizzoni, J. C., & Cipriano, M. (2010). Collection and publication of a fixed text keystroke dynamics dataset. In *XVI Congreso Argentino de Ciencias de la Computacion (CACIC 2010)* (pp. 822–831). https://doi.org/10.13140/2.1.4572.4960

Bhatt, S., & Santhanam, T. (2013). Keystroke Dynamics for Biometric Authentication – A Survey. In *Proceedings of the 2013 International Conference on Pattern Recognition, Informatics and Mobile Engineering (PRIME),* February 21–22, 2013, Salem, India (pp. 17–23). https://doi.org/10.1109/ICPRIME.2013.6496441

Chang, T. Y. (2012). Dynamically generate a long-lived private key based on password keystroke features and neural network. *Information Sciences, 211,* 36–47. https://doi.org/10.1016/j.ins.2012.04.009

Gunetti, D., & Picardi, C. (2005). Keystroke Analysis of Free Text. *ACM Transactions of Information and System Security, 8*(3), 312–347. https://doi.org/10.1145/1085126.1085129

Haller, N., Metz, C., Nesser, P., & Straw, M. (1998). *A One-Time Password System*. RFC 2289.

Hoque, N., Bhuyana, M. H., Baishyaa, R. C., Bhattacharyyaa, D. K., & Kalitab, J. K. (2014). Network attacks: Taxonomy, tools and systems. *Journal of Network and Computer Applications, 40,* 307–324. https://doi.org/10.1016/j.jnca.2013.08.001

Hub, M. (2003). Strategie výběru identifikačních znaků ve vícefaktorové autentizace. *E&M Economics and Management, 6*(4), 147–150.

Kang, P., & Cho, S. (2015). Keystroke dynamics-based user authentication using long and free text strings from various input devices. *Information Sciences, 308,* 72–93. https://doi.org/10.1016/j.ins.2014.08.070

Kanimozhi, M., & Kanimozhi, A. (2015). Implementing Neural Network in Keystroke Dynamics for a Better Biometric Authentication System. *International Journal on Applications in Information and Communication Engineering, 1*(3), 44–49.

Karnan, M., & Akila, M. (2009). Personal Authentication Based on Keystroke Dynamics Using Ant Colony Optimization and Back Propagation Neural Network. *International Journal of Communications, Network and System Sciences, 1*(2).

Karnan, M., & Akila, M. (2010). Personal Authentication based on Keystroke Dynamics using Soft Computing Techniques. In *Second International Conference on Communication Software and Networks.* Singapore, Singapore. https://doi.org/10.1109/ICCSN.2010.50

Karnan, M., Akila, M., & Krishnaraj, N. (2011). Biometric personal authentication using keystroke dynamics: A review. *Applied Soft Computing, 11*(2)*,* 1565–1573. https://doi.org/10.1016/j.asoc.2010.08.003

Killourhy, K. S., & Maxion, R. A. (2009). Comparing Anomaly Detectors for Keystroke Dynamics. In *Proceedings of the 39th Annual International Conference on Dependable Systems and Networks (DSN-2009)* (pp. 125–134). Lisbon, Portugal. https://doi.org/10.1109/DSN.2009.5270346

Legget, J., Williams, G., Usnick, M., & Longnecker, M. (1990). Dynamic identity verification via keystroke characteristics. *International Journal of Man-Machine Studies, 35*(6), 859–870. https://doi.org/10.1016/S0020-7373(05)80165-8

Liu, C.-L., Tsai, C.-J., Chang, T.-Y., Tsa, W.-J., & Zhong, P.-K. (2015). Implementing multiple biometric features for a recall-based graphical keystroke dynamics authentication system on a smart phone. *Journal of Network and Computer Applications, 53,* 128–139. https://doi.org/10.1016/j.jnca.2015.03.006

Matsubara, Y., Samura, T., & Nishimura, H. (2015). Keyboard Dependency of Personal Identification Performance by Keystroke Dynamics in Free Text Typing. *Journal of Information Security, 6*(3), 229–240. https://doi.org/10.4236/jis.2015.63023

Roth, J., Liu, X., Ross, A., & Metaxas, D. (2013). Biometric Authentication via Keystroke Sound. In *2013 International Conference on Biometrics (ICB)*. Madrid, Spain. https://doi.org/10.1109/ICB.2013.6613015

Soh, B., & Joy, A. (2003). A Novel Web Security Evaluation Model for a One-Time-Password System. In *Proceedings of the IEEE/WIC International Conference on Web Intelligence (WI'03)* (pp. 413–416).

Stallings, W. (2012). *Network security essentials: Applications and standards*. Upper Saddle River, NJ: Prentice Hall.

Tappert, C. C., Cha, S. H., Villani, M., & Zack, R. S. (2009). Keystroke Biometric System for Long-Text Input. *International Journal of Information Security and Privacy, 4*(1), 32–60. https://doi.org/10.4018/jisp.2010010103

Teh, P. S., Beng Jin Teoh, A., & Yue, S. (2013). A Survey of Keystroke Dynamics Biometrics. *The Scientific World Journal, 4,* 408280. https://doi.org/10.1155/2013/408280