BIOMETRIC MULTI-FACTOR AUTHENTICATION

Prof. Ing. Smejkal V. CSc. LL.M.[1], Ing. et Ing. Hortai F. [2]
Department of Informatics - Faculty of Business and Management – Brno University of Technology, the Czech Republic [1, 2]

smejkal@znalci.cz [1], hortai.frantisek@gmail.com [2]

Abstract: *This paper focuses on multi-factor authentication methods. It primarily addresses biometric methods, in particular authentication through written expression. It summarises the results of many years of research activities by the authors in the field of the dynamic biometric signature[1] (DBS), including new experiments. It concludes by comparing this type of signature with a signature based on cryptographic methods with a view to the current eIDAS Regulation.*

Keywords: AUTHENTICATION TECHNOLOGIES, BIOMETRICS, DYNAMIC BIOMETRIC SIGNATURE; BIOMETRIC DATA OF THE SIGNATURE; STABILITY OF THE DYNAMIC BIOMETRIC SIGNATURE

1. Introduction

Cybercrime and cyberterrorism are problems becoming increasingly urgent given the increasing dependence of civilization on information and communication technologies. Today's popular phenomena such as the Internet of Things, Industry 4.0, BYOD (Bring Your Own Device), the increasing prevalence of control systems (SCADA), and the almost precipitous rush towards robotization are increasing the potential risks arising from possible attacks on these technologies. As the numbers of connected things (thus becoming part of cyberspace) increases, we must face the fact that the risk of their abuse also increases. Yet the prevention of cybercrime is more important than the subsequent rectification of damage. A key assumption for constructing secure information systems is ensuring the proper identification and authentication of people, assets and events in the system. [1] Only after a high quality authentication we can move to the next essential step which is authorisation. For these reasons it is important to focus on the issue of multifactor authentication, in particular where biometric methods play an important role.

2. Preconditions and means for resolving the problem

The secondary research uses resources which were collected for specified purposes and its main objective is to clarify the benefits and pitfalls of authentication technologies. Based on many years of research further experiments were made which focuses on the dynamic biometric signature (further abbreviated as DBS).

The so called on-line dynamic biometric signature [2] was examined to show the possible change of the stability of the DBS of a signer depending on the scanning device. The used hardware was produced by the company Signotec GmbH. The used pads (biometric signature scanning devices) differ from each other in terms of their design, the size of the signature field, resolution, sampling rate, and even the scanning method used – a regular pen or a special pen using the ERT (Electromagnetic Resonance Technology).

The experiment was attended by 40 people in one session. As the sample represented people of both sexes aged 20 to 65, the size of the heterogeneous sample used was statistically representative enough. 8 scanning devices were used. The sampling frequency of the used devices can be set up to 150 Hz, 250 Hz or 500 Hz. The scan rate (sampling) was set up to recommended 250 points/sec. The x, y, time and pressure coordinates were scanned. The testing was carried out on the dynamic biometric signature devices with the various technical parameters produced by the company Signotec GmbH in the last five years (see listed in Table 1).

DBS were recorded on the devices using the program signoSign2 (version 10.4.5) produced by Signotec. Each participant made 10 signatures on each device to separately named *.pdf files. From the 10 times signed pdf file the biometric data were exported, so the final matrix of signatures of each participant and all devices was formed: $P_{ij} = [x_1, \dots ,x_{10}]_{ij}$; where *i* is a serial number of the device, *j* is a serial number of the participant, x_k (k = 1, … , 10) are the particular signatures.

2.1 From single-factor authentication to multi-factor authentication

We will build on the classic split of authentication methods (authentication based on knowledge, ownership, and the personal characteristics of the user), which are sometimes supplemented with authentication based on physical location (geographical authentication as an additional factor). There are many examples of failure of single-factor authentication when performed based on all the above methods, and so it is superfluous to explicitly state them.

At present, two-factor authentication is dominant – this ever-increasingly uses a combination of the factor of ownership (token) and knowledge (ID, password, PIN etc.) Yet even two-factor authentication may not be sufficient, in particular in cases where the human factor fails (typically a PIN written on a credit card) or when in reality it is not genuine two-factor authentication, but actually the repeated use of a single authentication method on the same channel (the entry of two text strings of the type ID + password or several passwords), and so if the channel is compromised, all the authentication data will be compromised. [3]

Failure of the human factor is also the greatest weakness in the ever-more-popular cryptographic tools used today – see the so-called Level 4, requiring authentication based on evidence that keys are held through a cryptographic protocol and the use of tokens in the form of FIPS 140-2 level 3 or higher hardware cryptographic modules with FIPS 140-2 level 3 minimum physical security. [4] Yet from practice we know how commonly these tokens for signing are entrusted to other people, typically assistants.

Also, other proposals that have appeared – such as authentication via other people in the case of remote access – have not proven sufficiently secure or have proven complicated to apply and are thus appropriate rather for emergencies than for normal activities. [5]

The opinion that multi-factor authentication is essential to ensure sufficient security of information systems now practically dominates. [6] We can select practically any combination of authentication factors, for example according to the following diagram Fig.1 [7]:

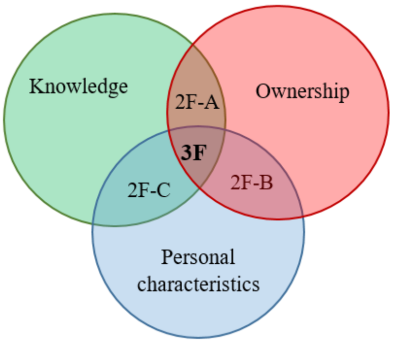

Fig. 1 *Combinations of authentication factors. [7]*

Nevertheless, without a risk analysis and a formal verification of the correctness of the authentication method, we cannot be sure that a proposal is genuinely secure. [8] The authentication methods must provide a high level of protection against their breaking or exploitation, while at the same time remaining user friendly, secure, easy to use and unobtrusive, and have reasonable implementation costs. The addition of an extra factor for authentication also brings with it an increase in the technological, organisational, and primarily financial demands of such a solution, including an impact on the user. The analysis must therefore include economic (costs for acquisition and operation of the security mechanism) and ergonomic (meaning the ease of administration and, in particular, use) assessments. For example, a system based on a secret key stored in a token, password and biometric data has a high level of protection against attack, yet its acquisition and operation costs may prove too high, in particular compared to the value of the protected assets.

The risk analysis may also be an appropriate starting point for the creation of a system for a multi-step authentication process when differing authentication scenarios are launched depending on the importance of the protected item (information, thing), or in the event of doubt as to identity.

2.2 Biometric authentication methods

Risk may arise not only from the person being authenticated and his/her behaviour, but also from an inadequately secured product. In addition, with remote access, an attack may take place anywhere along the path from the authenticated person to the authentication site. Biometric authentication methods appear to be a reasonable compromise between demands on the user and/or on the authentication tool, while not reducing the level of security. However, we must make a fundamental distinction between static and dynamic methods, where static methods are basically a continuation of the authentication principle that the user “has something”, even if this means something that is part of their physiology. Here, the risk of the falsification of biometric information (faking fingerprints, an iris image, etc.) [9] or their use through coercion remains.

Hence dynamic authentication methods are increasingly of interest, where we can assume a higher level of protection from abuse, as we are moving from the variant that the user “has something” to the variant in which the user “knows something” – and, what is more, they “do not know what they know”. In addition, these methods implicitly include a “test of life”. This is particularly true when scanning blood flow in the palm, the back of the hand or finger [10] and in the dynamic recording of written expression. (For the sake of completeness, we must add that other dynamic methods, such as walking dynamics, typing on a keyboard, facial expressions or gestures, show relatively high instability and error rates). Hence, authentication through the recording and analysis of a person’s written expression appears promising.

2.3 Authentication through written expression

The static recording of a person’s writing – typically their signature – is one of the oldest authentication tools but, nevertheless, also one of the riskiest. The signature image can be imitated or forged, while comparison (e.g. of markers) is a subjective process, in particular in the case of short records such as signatures. This is especially true for experienced counterfeiters. [11]

Writing is a natural human activity and, as such, these are processes where the primary impulse arises in the central nervous system – in the human brain – with a predefined intensity and duration. The nervous system then activates the relevant muscles in a defined order so that the user can perform a certain activity – a signature, a certain gait, a gesture, and so on. [1]

Generally speaking, the dynamic recording of writing can be used to authenticate the person producing the written record. [12] The dynamic biometric signature (“DBS”) is then a special variant, where by creating a signature, the person certifies a certain fact – presence at a specific location (when entering a protected space, when logging in to an IS), or a legal act, etc. In the first case, it is possible to create a comparison benchmark by entering a specific phrase or drawing which, to improve security, may be individual for each person. In the second case, the handwritten signature of the person is used.

When authenticating a person, we generally employ the 1:N model, meaning that we compare the scanned record with all the records in a database of people. Some disadvantages of this are the higher risk of mistaken identification and high demands on computing power in the system. We remove this problem by using a prior identification step (entering identification data such as name, number, ID etc.), which can be done both in the case of authentication using a general record and also for authentication using a signature. This gives us a 1:1 variant with higher accuracy and lower processing demands.

On-line verification is used in both cases, when the record is made using a special “pen” and a digitising tablet that records the data, enabling analysis of the static and, in particular, the dynamic characteristics of the record in the form of the data string (text, image or signature) connected with the typical behaviour of the person in question, which is assessed by the verification device. These include the basic features of the record: the duration, including the periods between strokes, typical points and curves in different parts of the signature, the pressure exerted by the pen on the pad during different parts of the signature, the overall size of the signature, the length and angle of lines, arcs and curves, the number of loops, the speed of individual stokes, acceleration and deceleration, etc. [13] This is all usually established by scanning the x and y coordinates (horizontal and vertical pen position), or z (the height of the pen above the writing surface). The output data must also include T (time) or DT (time difference) or uniform sampling must be indicated. The inclusion of additional parameters is optional – here, it is important to emphasise that the number of analysed channels has a significant impact on the uniqueness and reliability of the authentication of the signing person. [14]

The dynamic biometric signature contains information about how the signature was created, and thus reflects characteristics of the signing person, their habits and behaviour. These characteristics represent a biometric footprint that is unique for each individual and cannot be reproduced by a forger (unlike the actual image of the signature itself, which only makes up one of the parameters of the biometric footprint). One important attribute of a DBS is that it contains not only the element that the writer is alive, but also the fact that the signature was created by the writer consciously, and so there is no need to develop additional mechanisms to test whether the subject is present and alive or not – unlike with static biometric methods (checking the print of a finger, palm, iris etc.) It is also legally beneficial, in that we can rely on the (theoretically rebuttable) assumption that the person knew what they were signing. [15]

3. Results

As we previously showed [16] each individual has an individual set of component movements. This enables verification of the signature to be based on the stability of the set of component movements during its implementation. A decisive indicator for a DBS is that this unique set significantly eliminates the possibility of its reconstruction by a counterfeiter. Regarding alleged changes in a signature due to aging and other influences, it is important to realise that two identical signatures do not exist – or rather, if they are identical, we can be sure that they are a so-called technical forgery, produced by copying from a specimen. Hence it is crucial to know how the level of agreement between the signature and its specimen should be set for automatic evaluation to ensure that handwriting experts only receive signatures in exceptional cases.

The presented results are a summary of our original research in the field of DBS performed between 2011 and 2016, when we focused on its properties, security, resistance to counterfeiting and its stability. We addressed issues relating to an unquestionable connection between a created DBS and the text of the signed electronic document in our previous ICCST papers [15], [16].

Experiments demonstrating the uniqueness of the DBS as well as its resistance to counterfeiting have been extremely helpful [17]. These experiments examined the signatures of a sample of 102 people of varying ages, who created real and intentionally altered signatures. Subsequently they tried, using submitted specimens, to copy the signature of somebody else. It was shown that 1. the stability of the real signatures is high and the degree of conformity hovered over around 85%, with only some exceptions, 2. conformity was still found with 25% of the intentionally altered signatures, 3. not even a single forged signature was accepted. The experiments showed that the biometric data acquired during the creation of a signature provide such a set of information that enables the preparation of a clear opinion during subsequent authentication in the event of a dispute over the authenticity of a signature. It will only be appropriate to have an analysis prepared by a handwriting expert in exceptional cases for the authentication of a signature for the purpose of increasing probative value in court proceedings, while usually it is sufficient to use a validation server. In such a case, the biometric data are an ideal source of information for the handwriting expert compared to a situation in which they can only use two short texts, namely signatures on paper, for a comparison.

Another decisive aspect of DBS is its stability. Hence, in 2015, we addressed the influence of alcohol on DBS stability. [18] Before and after consuming alcohol, our test subjects 1. took the Brickemkamp-Zillmer variant of the d2 Test of Attention [19], 2. underwent an alcohol-level breath test, 3. created a set of signatures. While the results of the d2 test changed, no influence of alcohol on signature performance was proven.

It is common for the person providing a signature to be exposed to stress, one reason for this being the importance of the situation in which they are appending the signature. After all, stress, and very often negative stress, is one of the most common emotions in human life. Hence, in a different experiment, we examined whether and in what way stress influences the quality and constancy of DBS. [19] In our experiments, we used the extreme situations in which test subjects in survival courses (X-tream course) at the University of Defence of the Czech Republic found themselves, while once again we used the d2 Test of Attention and signature stability at the start, in the middle, and at the end of the course. The results of the experiments showed that irrespective of the stress levels of the participants, the stability of their DBS was high, respectively actually improved. The results are in accordance with phases I. and II. of the Selye model. [21]

These experiments also showed a high level of signature instability with so-called short signatures –initials. Hence, we performed another experiment focusing on the stability of short signatures (initials), which showed that signature recognition quality increased together with the length of the recorded information. This corresponds with the information from the manufacturer of the equipment (Signotec), namely that the method they use for evaluating signature concurrence using their own algorithm requires a specific minimum number of points (determined by the x, y and z coordinates), which leads to greater fluctuations (variability of the observed match between signatures) during comparisons of short signatures.

Based on the series of experiments we have performed [15], [16], [17], [18], [20], we consider DBS stability sufficiently demonstrated for this method to be used to identify and authenticate people or the documents they have signed with a high degree of reliability and verifiability. The use of short signatures (initials) can be something of a problem, as they show a high level of variability when evaluating conformity or non-conformity.

It was also confirmed once again that the use of the 1st signature as "practice", not included in the results reduces the variability of signatures among all test subjects [18] [20]. In accordance with these findings, the first signatures made by each person on the devices were not included in the evaluation. For the signature match rate automatic evaluation a special algorithm was created which uses the original analytical software of the device manufacturer (Signotec - eSig-Analyze). The end result was a data matrix where the signature matches were evaluated among themselves in percent for every person each. Every person (40 people) had 8 times (number of the devices) 10 signatures. From every these 10 signatures minus the first signature (so 9) which in one case (1 person and 1 device) had 36 signature alikeness comparisons. The overall 11520 signature alikeness comparison data were then used for calculations. The following values of selective means and unbiased estimates for variances of the degree of compliance of signatures were detected on the stated devices (Table 1):

Table 1: *Overview of the tested devices and the selective means and unbiased estimates for variances of the degree of compliance of signatures.*

Method of the signature capture	Scanning device of the dynamic biometric signature	x [%]	S^2
The active pen, display, and pen are mutually synchronized	Signotec Alpha Pad, ST-A4E-2-UFTE100: Color LCD Signature Pad Alpha ERT (Electromagnetic Resonance Technology)	80.342	113.019
The display is electromagnetic, the pressure is captured on the basis of the outward pressure of the passive pen on the display	Signotec Delta Pad, Touch display ST-DERT-3-U100 ERT	76.749	238.268
The display is electromagnetic, the pressure is captured on the basis of the outward pressure of the passive pen on the display	Signotec Gamma Pad, Touch display ST-GERT-3-U100: 5" Color LCD Signature Pad Gamma ERT	78.971	232.027
The display is a touch-screen, the pressure is captured on the basis of the outward pressure of the passive pen	Signotec Omega Pad revision B, Touch display ST-CE1075-2-U100 (old version)	76.02	228.052
	Signotec Omega Pad revision E, Touch display ST-CE1075-2-U100 (current version)	83.002	125.844
	Signotec Sigma Pad revision B, Touch display ST-ME105-2-U100-B (old version)	77.097	148.574
	Signotec Sigma Pad revision E, Touch display ST-ME105-2-U100-B (current version)	85.233	139.194
There is no display, only the touch area	Signotec Sigma Lite, Touch area without a display function STLT105-2-U100	77.195	120.338

The result characterizing the technology as a whole, i.e. without differentiation of types of devices and signers (i.e. for all people on all devices) is the average percentage 79.33 % with the standard deviation of σ = 13.16 %. The selective mean of the degree of compliance of signatures came under an accepted level of compliance of biometric signatures > 60% only in case of two people.

4. Conclusion

The dynamic biometric signature is in accordance with the eIDAS Regulation (Regulation (EU) No 910/2014 of the European Parliament and of the Council), which became valid on 17 September 2014 and focuses on the secure identification of people in electronic communication, respectively the provision of remote services. DBS is not a replacement for a cryptographic electronic signature, but an important alternative that can be used in cases when the use of certificates, the secure storage and "policing" of private keys, etc. would significantly impact routine and stable processes, and potentially form a barrier discouraging normal users and also bringing significant organisational and technical problems during the deployment of a guaranteed or qualified electronic signature (Advanced Electronic Signature, Qualified Electronic Signature) under the eIDAS Regulation. Its advantage over a cryptographic electronic signature is the existence of this "handwritten" quality.

There was no statistically significant difference in the means and variances of the degree of compliance of signatures of a particular person on individual devices. The different scanning technology does not affect the degree of compliance and variability of signatures (see Table 1). In the opinion of the authors, the "user-friendliness" is a key factor in creating the signature. Another factor is then the individual characteristics of the signer. The variability of the signature, and hence the low degree of compliance among individual signatures, which is exceptionally manifested among the signers, is closely related to the stability of the signature. The greater the intra-personal variability is, the less stable the signer is.

5. Reference

[1] Smejkal, V. aj. J. Kodl. Authentication and Encryption in Ensuring the Security of Information Systems. In: Lisník, A., Pavlíček, A. (ed.) Current Trends and Challenges in Economics and Management. Conference proceedings of the international conference "The message of John Paul II", 21.-22. 4. 2016, Poprad: VERBUM – vydavateľstvo Katolíckej univerzity v Ružomberku, 2017, p. 251-262. ISBN 978-80-561-0440-8.

[2] Galbally, J. Diaz-Cabrera, M., Ferrer, M. A., Gomez-Barrero, M., Morales, A., & Fierrez, J. On-line signature recognition through the combination of real dynamic data and synthetically generated static data. *Pattern Recognition*, Volume 48, Issue 9, 1 September 2015, Pages 2921-2934. ISSN: 00313203

[3] Al-Faiinz, M. and K. Renaud. Multi-channel, Multi-level Authentication for More Secure eBanking. In: Venter, H., Coetzee M. and M. Loock (eds.). Proceedings of the 2010 Information Security for South Africa Conference. Pretoria, South Africa, 2010. ISBN 978-1-4244-5494-5.

[4] Burr, W. E. et al. Electronic Authentication Guideline. NIST Special Publication 800-63-2. August 2013. DOI: 10.6028/NIST.SP.800-63-2.

[5] Brainard, J. et al. Fourth-Factor Authentication: Somebody You Know. In: Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06). ACM, New York, NY, USA, 168-178. ISBN: 1-59593-518-5.

[6] Smejkal, V., Kodl., J. Development Trends of Electronic Authentication. In: Sanson, L. D. (ed.) *Proceedings of the 42nd Annual Conference 2008 IEEE International Carnahan Conference on Security Technology*, pp. 1–6. DOI: 10.1109/CCST.2008.4751267. ISBN 978-1-4244-1816-9.

[7] Hortai, F. Options and Benefits of Authentication System via Dynamic Biometric Signature. In: *Proceedings of the international conference International Day of Science 2017.* Olomouc: Moravian University College Olomouc, 2017, p. 75-83. ISBN 978-80-7455-060-7.

[8] Pointcheval, D. and p. Zimmer. Multi-factor Authenticated Key Exchange. In: Bellovin, p. M. et al. (eds.). *Proceedings of the 6th International Conference on Applied Cryptography and Network Security* (ACNS'08), Springer-Verlag, Berlin, Heidelberg, 2008, LNCS 5037, pp. 277-295. ISBN:3-540-68913-3 978-3-540-68913-3

[9] DRAHANSKÝ, M.; KANICH, O. Vulnerabilities of Biometric Systems. In *Security and Protection of* Information 2015. Brno: Brno University of Defence, 2015. p. 53-60. ISBN: 978-80-7231-997-8.

[10] DRAHANSKÝ, M. et al. Biometrie. Brno: Computer Press, s.r. o, 2011. pp. 141-152. ISBN: 978-80-254-8979-6.

[11] Dewhurst T., Found B., Rogers D. Are Expert Penmen Better Than Lay People at Producing Simulations of a Model Signature? Forensic Science International, 180 (2008) , pp. 50-53. DOI 10.1016/j.forsciint.2008.06.009.

[12] Fischer, A. and R. Plamondon. Signature Verification Based on the Kinematic Theory of Rapid Human Movements. IEEE Transactions on Human-Machine Systems, Vol. 47, No. 2, April 2017, pp. 169-180. DOI 10.1109/THMS.2016.2634922.

[13] ISO/IEC 19794-7: 2014. *Information technology -- Biometric data interchange formats -- Part 7: Signature/sign time series data.*

[14] Mates, P., Smejkal, V. *E-government v České republice. Právní a technologické aspekty.* 2. podstatně přepracované a rozšířené vydání. Praha: Leges, 2012, pp. 335-336. ISBN 978-80-87576-36-6.

[15] Smejkal, V. and J. Kodl. Strong Authentication Using Dynamic Biometric Signature. In: *Proceedings of 45th Annual 2011 IEEE International Carnahan Conference on Security Technology (ICCST)*, 18-21 October 2011, Tecnocampus Mataró Maresme, Barcelona, Spain, pp. 340–344, ISBN 978-145-7709-02.

[16] V. Smejkal, J. Kodl and J. Kodl Jr. Implementing Trustworthy Dynamic Biometric Signature according to the Electronic Signature Regulations. Proceedings of 47th Annual 2010 IEEE International Carnahan Conference on Security Technology (ICCST), 9-11 October 2013, Medellín, Colombia, pp. 165–170. ISBN: 978-958-8790-65-7.

[17] Smejkal, V. and J. Kodl. Assessment of the Authenticity of Dynamic Biometric Signature. The Results of Experiments. In: *Proceedings of 48th Annual 2014 IEEE International Carnahan Conference on Security Technology (ICCST)*, 13-16 October 2014, Roma, Italia, p. 45 – 49, ISBN: 978-1-4799-3530-7.

[18] Smejkal, V., Kodl, J., Sieger, L., Novák, D. and J. Schneider. The Dynamic Biometric Signature. Is the Biometric Data in the Created Signature Constant? In *Proceedings of 49th Annual 2015 IEEE International Carnahan Conference on Security Technology (ICCST)*, 21-24 September 2015, Taipei, Taiwan, R.O.C., pp. 385 – 390, ISBN 978-9-860-46303-3.

[19] Brickenkamp, R., Zillmer, E. *D2 – Test of Attention.* Seattle: Hogrefe & Huber, 1998.

[20] Smejkal, Vladimír, Kodl, Jindřich and Ladislav Sieger. The Influence of Stress on Biometric Signature Stability. In: *Proceedings of 50th Annual 2016 IEEE International Carnahan Conference on Security Technology (ICCST), 24-27 October 2016, Orlando, Florida, USA,* New York: Institute of Electrical and Electronics Engineers, Inc., p. 37 – 41, ISBN 978-1-5090-1070-7. DOI: 10.1109/CCST.2016.7815680.

[21] Selye, H. *Stress without Distress.* Philadelphia: J.B. Lippincott Co., 1974. ISBN 978-0397010264.