Physiological signals: The next generation authentication and identification methods!?

Egon L. van den Broek[1,2,3] and Martijn Spitters[1]
[1] Media and Network Services, TNO Technical Sciences, Delft, The Netherlands
[2] Human-Media Interaction, Faculty of EEMCS, University of Twente, Enschede, The Netherlands
[3] Karakter University Center, Radboud University Medical Center, Nijmegen, The Netherlands
Email: vandenbroek@acm.org, martijn.spitters@tno.nl

***Abstract*—Throughout the last 40 years, the security breach caused by human error is often disregarded. To relief the latter problem, this article introduces a new class of biometrics that is founded on processing physiological personal features, as opposed to physical and behavioral features. After an introduction on authentication, physiological signals are discussed, including their advantages, disadvantages, and initial directives for obtaining them. This new class of authentication methods can increase biometrics' robustness and enables cross validation. I close this article with a brief discussion in which a recap of the article is provided, law, privacy, and ethical issues are discussed, some suggestions for the processing pipeline of this new class of authentication methods are done, and conclusions are drawn.**

I. Introduction

Authentication and identification are (traditionally) approached from various angles. For example, encryption algorithms for communication in computer networks [1], [2], smart cards and their remote authentication schemes [2], [3], CAPTCHA [4], but also questions concerning trust, beliefs and implicit assumptions of users [5], [6]. All these authentication methods have in common that the user (or human) is (somewhere) in the loop and, hence, human errors can occur [7]. As such, the user (or human) can be considered as a security breach in many systems [8], [9]. However, as Wood and Banks already denoted 20 years ago with their article:

"Human error: An overlooked but significant information security problem" [10]

(e.g., see also [7], [8]). Moreover, it has been noted that

"...we demonstrate the feasibility of security conditions attached to our definitions, but which are impractical for use by humans." [1, p. 52]

To relief this burden, this article proposes a new method for authentication and identification of people. As such, I hope to provide ground to tackle the problem, at least, in a part of the current security frameworks (cf. [8], [9]).

Almost half a century ago, IBM already envisioned the authentication and identification of persons by machines [11]. IBM posed that this could be realized via:

1) something the user knows or memorizes;
2) something the user carries; and
3) a personal physical characteristic.

From this point on, a new branch of research emerged: biometrics[1] (i.e., using a physical or behavioral personal feature [12]). This article proposes a new class of biometrics for authentication and identification purposes using physiological personal features instead of physical or behavioral ones.

Essentially, biometrics is a pattern recognition challenge [13]. It can be applied to either verify the authenticity of a person or identify a person. In this article, I provide concise definitions for both of them, adopted from [12, p. 2]:

- *authentication*[2]: the process of checking the validity of an identity claim by matching a credential against a set of reference values; and
- *identification*: the process of searching the entire set of possible identities in order to find the right one matching the measured feature.

In the former case, biometric data of a person is recorded and compared with that person's biometric data available (e.g., in a database (DB)); that is, 1:1 matching. In the latter case, the biometric data recorded is compared with all biometric data available, with the aim to identify the person who's biometric data was captured [13]; that is, 1:n matching, with n being the size of the data (e.g., DB). The following definition of authentication and identification illustrates this:

$$I_x = \begin{cases} I_n \text{ if } \max_n\{D(I_x, I_n)\} < T \\ I_x \text{ otherwise} \end{cases} \quad (1)$$

where I_x is the biometric data of an unidentified person. I_n is the n^{th} sample from the DB. D is a distance metric and T is a threshold. Note that if Eq. 1 results in $I_x = I_x$, the person remains unidentified.

In case of authentication of persons, 1:1 matching is applied. So, the DB, as depicted in Eq. 1, contains a single profile. Hence,

$$\max_n\{D(I_x, I_n)\} < T \quad (2)$$

holds but can be reduced to

$$D(I_x, I_n) < T. \quad (3)$$

[1] Biometrics is derived from the Greek language, meaning: life measuring.
[2] Often called *verification* in biometric literature.

978-0-7695-5062-6/13 $26.00 © 2013 IEEE
DOI 10.1109/EISIC.2013.35

In practice, a way in between 1:1 and 1:n matching is often employed. Then, (some) knowledge on the identity of an unknown person (I_x) is used to enable a query on a subset (s) of the DB (i.e., $s \subset n$) instead of the complete DB.

In nowadays practice, authentication and identification are mainly approached as follows [13]:

1) Manual authentication or identification: either through an object (e.g., ID card, its reader, or a USB stick) or via knowledge (e.g., personal identification number, password, and secret questions).
2) Biometrics that distinguishes: i) behavioral attributes (e.g., signature, keystroke dynamics, mouse gestures, and gait) [14]; ii) physical attributes such as fingerprint, iris and retina (e.g., see [15]), facial image and facial thermogram [16], geometrical features of the face (e.g., ear and nose), and geometrical features of the hand (incl. vein pattern) and feet; and iii) miscellaneous, such as audio-based (e.g., voice), chemical attributes (e.g., odor), and DNA.

The particular combination of methods chosen is, in practice, founded on a combination of trade-offs. These can include level of accuracy, ease of use (or intrusiveness), security (i.e., barrier to attack), (public) acceptability, long-term stability, size, and (of course) costs. Moreover, aspects such as connectivity, compatibility (e.g., ports, operating systems, and CPU), and speed play are of influence.

Taking manual authentication or identification and biometric-based authentication or identification as two types of methods, one can extract a nomological framework on biometrics. Such a framework can be characterized using the following dimensions [13]: universality (i.e., all persons should possess the trait); uniqueness (i.e., the level of discrimination it provides between persons); permanence (i.e., invariance or stability of the trait); measurability (i.e., effort related to acquisition and processing in practice; e.g., to what extent a person needs to cooperate in obtaining the biometric and in how far the environment needs to be controlled?); performance (i.e., the reliability of the biometric); acceptability for the people; and circumvention (i.e., sensitivity to fraud). These dimensions can help in making a structured analysis of the authentication and identification methods needed for a certain application.

Next, a new class of authentication and identification methods will be introduced, which rely on physiological characteristics of persons. First, a concise introduction is provided on this new class of methods. It is explained how this new class can be used to validate traditional methods and how it can enhance their robustness. Additionally, advantages, disadvantages, and initial directives are provided for this new class of authentication and identification methods. This article ends with a discussion in Section III.

II. Processing physiological signals

Physiological signals (or biosignals) are electrochemical changes in nerve cells (or neurons), muscles, and gland cells. These physiological signals spread from their source through the body to the surface of the skin. Via surface electrodes attached (or close) to the body surface, signals from a broad range of sources can be recorded [17]. For example, from the heart, the electrocardiogram (ECG) can be recorded [18], [17], [19]; the muscles' activity can be recorded through the electromyogram (EMG) [20], [21]; the sweat glands determine the electrodermal activity (EDA) [20], [21]; and also brain activity can be recorded, for example, using EEG [17], [6] and fNIRS [6].

Physiological signal processing is expected to be of significant value for authentication and identification purposes. It can relief problems that can occur with traditional biometrics [13], [18], [22], [23], [19], [24]; for example,

1) facial image: recording, processing, and matching remains problematic;
2) movement analysis (e.g., gait): often not possible in practice; and
3) voice: often, either speech is absent or suffering from severe distortions.

However, it is not only these problems that illustrate the need for a new class of biometrics. The steep progress in sensor engineering throughout the last decade brought the progress that was needed to use physiological sensors for various applications (e.g., [25]). Sensors that enable physiological signal recording have declined in price, have become more reliable, and can be applied wireless [25]. Next, I will discuss the advantages and disadvantages of physiological signals as biometrics. Subsequently, I will provide an initial set of initial directives for the application of the new class of physiological signal-based authentication and identification.

A. Advantages

Traditional biometrics can be (conveniently) manipulated; in contrast, physiological signals are much harder to manipulate. As mentioned, the rapid development of non-invasive wireless sensors [25] have made them suitable for a wide range of applications [21], [23], [26]. As such, physiological signals can act a new class of interfaces (e.g., authentication and identification) between man and machine.

Physiological signals are known to discriminate among people, like traditional biometrics do. Moreover, physiological signals can conveniently be combined with traditional biometrics. So, adding physiological signals into the process of authentication and identification will increase the chance on reliable profile and its adequate matching. More precise, this can provide the following advantages:

1) Increasing robustness: Data gathered via physiological signals can be used to verify data gathered via traditional authentication and identification methods. Also, corrections can be made on missing or corrupt data using data extracted from physiological signals. Last, integration of these sources can be used for noise canceling.
2) Cross validation: Traditional biometrics can be validated against physiological signals; that is, constructs can be mapped to both biometric features and features extracted from physiological signals in parallel. This concerns the expression of the relation between physiological signals on the representation of a person's characteristic (e.g., their voice and handwriting).

The added value of robustness and cross validation are expressed on respectively signal processing and pattern recognition level and on a conceptual level.

B. Disadvantages

As with all processing techniques, also physiological signal processing has its downside. Several crucial concerns that limit both their acceptation and application in practice have to be acknowledged; see also Section I and [21], [18], [22], [23], [19]. Some of the most important concerns are:

1) Obtrusiveness of physiological sensors [25];
2) Unreliability of physiological sensors; for example, due to movement artifacts, bodily position, air temperature, and humidity [25];
3) Many-to-many relationships; that is, multiple physiological signals can (partially) serve as indicators for multiple traditional biometric features;
4) Varying time windows of physiological signals; and
5) Physiological processes and, hence, their residues (i.e., the physiological signals are linear time invariant (e.g., they habituate).

Regrettably, these issues still have not been solved completely. Hence, a significant additional progress in physiological signal processing needs to be realized to unveil the true potential of physiological signals.

C. Initial directives

Physiological signals have been posed to be a promising new class of authentication and identification methods. However, as denoted in the closing sentence of the previous section, significant progress is needed before physiological signals can truly be exploited as a reliable authentication and identification class of methods. Undoubtedly, the recording of physiological signals lies at the core of making them a success. Therefore, I will present in this section some directives for physiological signal recording.

So far, there is a lack of a coherent and concise set of initial directives for obtaining physiological signals outside of controlled (e.g., laboratory) settings. This can be considered as one of, if not, the main problem(s) with physiological signal processing. Both academic and industrial knowledge on physiological signal processing is scattered and, consequently, also are its initial directives. Hereby, I introduce a concise set of initial directives that can help to improve the quality of physiological signals recordings:

1) The concept validity, specifically:
   a) Content validity (i.e., either the agreement among experts and/or the degree of representation of a construct through the signals);
   b) Concurrent validity (i.e., determine the reliability of the signal in relation to its ground truth); and
   c) Ecological validity (i.e., operationalize the context of measurements).
2) Integration of data streams and, subsequently, apply triangulation.
3) Physical characteristics; for example, type of electrodes (i.e., dry and wet), gel, location of electrodes, and environmental characteristics.
4) Temporal aspects that need to be acknowledged because:
   a) people habituate and physiological activity tends to move to a neutral state;
   b) physiological processes develop over different time windows; and
   c) physiological responses are likely to be layered.
5) Normalization in its broadest sense; that is, applying suitable corrections to the physiological signals.

These initial directives do not solve all disadvantages mentioned in the previous section. However, they can help in bringing physiological signals to authentication and identification practice.

In addition to the five initial directives mentioned above, the importance of respecting the rich history on physiological signal processing needs to be stressed. Please note that physiological signals are already processed since the 17^{th} century. Regrettably, this rich history is ignored to a large extent; hence, a vast amount of knowledge remains unused [27].

III. Discussion

This article started with an introduction on the topic of *"authentication based on biometric systems ..."*, which *"...has gained momentum, pushed by smart marketing slogans: authentication based on a personal feature that can never be lost, stolen or forgotten."* [12, p. 2]. For this purpose, a new class of biometrics was introduced (see Section II): physiological signals, as opposed to more traditional approaches to achieving progress in biometrics. Both advantages and disadvantages of physiological signal-based biometrics were denoted as well as initial directives for their application.

One of the advantages of embracing a new class of authentication and identification methods is that such a class can add data to a person's profile (see also Section II). However, this implies that a new class of data that is gathered on the same objects (i.e., people) increases data traffic, data storage, and the required investments data mining. This is in particular the case, as physiological signals are generally recorded at sample frequencies of 100Hz–1000Hz and, hence, can quickly generate a relatively large amount of raw data. Moreover, the current trend is to collect biometrics of more and more people and, hence, the size of biometric data streams increases rapidly. Consequently, data reduction becomes even more important than it already was. This can be realized via the choice of the physiological signals dimension (as there are many, each with their own characteristics [21]) reduction, optimal sample rates, and efficient distance metrics, combined with tailored data mining schemes.

So far, this article presented physiological signal-based authentication as some sort of holy grail for security. However, introducing this new class of authentication methods brings in its own problems as well. As [28] already denoted: *"A couple of new items of interest are biometric issues and acquisition trends. The trend toward biometrics is going to lead to new*

threats as their use grows. First there are no governing statutes protecting our biometric data today. Second, biometrics is not a silver bullet – the threat will eventually find ways to compromise it. Finally as we field these systems we will need to build analytics and security integrated into the design. If we use biometrics (be it to avoid someone voting multiple times or registering for government aid under multiple names) we need to ensure it has been reviewed by folks who think like malicious hackers not engineers who think about how to make things work." (see also [6, p. 266]).

Introducing physiological signal-based authentication also introduces a new dimension in law, privacy, and ethical issues (cf. [29]). Law considerations include: i) rules of privacy, ii) the constitutional background, and iii) privacy under law (including physical, decisional, and information privacy) [13, Ch. 18]. Physiological signal-based biometrics differ in multiple ways from traditional authentication and identification methods; for example, they need other registration and processing schemes. Moreover, it should be noted that physiological signals are a very rich data source and can reveal much more than a person's identity. In general, I would like to stress, that it is of the utmost importance that lessons learned in traditional biometrics (e.g., face recognition [16]), in wireless technology in general (e.g., RFID [30]), but also, for example, in (wireless) healthcare applications [31] should be taken into account.

This article introduced a new class of authentication and identification methods; nothing more, nothing less. So, the undeniable conclusion is that there is still a long way to go. The validity of the position taken in this article should be assessed experimentally. The stakes, gains, and costs in the landscape of security are all high and it is hard to forecast what direction the future will go in. However, given the speed physiological sensors are broad to daily practice, it seems inevitable that the new class of physiological signal-based biometrics will settle among the traditional classes of biometrics.

REFERENCES

[1] N. J. Hopper and M. Blum, *Secure human identification protocols*, ser. Lecture Notes in Computer Science. Berlin/Heidelberg, Germany: Springer-Verlag, 2001, vol. 2248, pp. 52–66.

[2] W. Ren, L. Yu, L. Ma, and Y. Ren, "How to authenticate a device? formal authentication models for M2M communications defending against ghost compromising attack," *International Journal of Distributed Sensor Networks*, vol. 2013, p. Article ID 679450, 2013.

[3] H. M. Sun, "An efficient remote use authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 46, no. 4, pp. 958–961, 2000.

[4] L. von Ahn, M. Blum, and J. Langford, "Telling humans and computers apart automatically," *Communications of the ACM*, vol. 47, no. 2, pp. 56–60, 2004.

[5] M. Burrows, M. Abadi, and R. M. Needham, "A logic of authentication," *Philosophical Transactions of the Royal Society A: Mathematical, Physical & Engineering Sciences*, vol. 426, no. 1871, pp. 233–271, 1989.

[6] D. Trček, "An integrative architecture for a sensor-supported trust management system," *Sensors*, vol. 12, no. 8, pp. 10 774–10 787, 2012.

[7] S. Dekker, *The field guide to understanding human error*. Aldershot, Hampshire, England: Ashgate Publishing Limited, 2006.

[8] G. P. Im and R. L. Baskerville, "A longitudinal study of information system threat categories: The enduring problem of human error," *ACM SIGMIS Database*, vol. 36, no. 4, pp. 68–79, 2005.

[9] M. E. Whitman, "Enemy at the gate: Threats to information security," *Communications of the ACM*, vol. 46, no. 8, pp. 91–95, 2003.

[10] C. C. Wood and W. W. Banks, "Human error: An overlooked but significant information security problem," *Computers & Security*, vol. 12, no. 1, pp. 51–60, 1993.

[11] K. de Leeuw and J. Bergstra, *The History of Information Security: A Comprehensive Handbook*. Amsterdam, The Netherlands: Elsevier B.V., 2007.

[12] A. Esposito, "Debunking some myths about biometric authentication," *arXiv, CoRR*, vol. arXiv:1203.0333 [cs.CR], 2012.

[13] A. K. Jain, P. Flynn, and A. A. Ross, *Handbook on Biometrics*. New York, NY, USA: Springer Science+Business Media, LLC, 2008.

[14] B. Sayed, I. Traore, I. Woungang, and M. S. Obaidat, "Biometric authentication using mouse gesture dynamics," *IEEE Systems Journal*, vol. 7, no. 2, pp. 262–274, 2013.

[15] M. S. Hosseini, B. N. Araabi, and H. Soltanian-Zadeh, "Pigment melanin: Pattern for iris recognition," *IEEE Transactions on Instrumentation and Measurement*, vol. 59, no. 4, p. 792, 2010.

[16] K. W. Bowyer, "Face recognition technology: Security versus privacy," *IEEE Technology and Society Magazine*, vol. 23, no. 1, pp. 9–19, 2004.

[17] Y. N. Singh, S. K. Singh, and A. K. Ray, "Bioelectrical signals as emerging biometrics: Issues and challenges," *ISRN Signal Processing*, vol. 2012, p. Article ID 712032, 2012.

[18] E. L. van den Broek, M. H. Schut, J. H. D. M. Westerink, and K. Tuinenbreijer, "Unobtrusive Sensing of Emotions (USE)," *Journal of Ambient Intelligence and Smart Environments*, vol. 1, no. 3, pp. 287–299, 2009.

[19] E. L. van den Broek, "Ubiquitous emotion-aware computing," *Personal and Ubiquitous Computing*, vol. 17, no. 1, pp. 53–67, 2013.

[20] E. L. van den Broek and J. H. D. M. Westerink, "Considerations for emotion-aware consumer products," *Applied Ergonomics*, vol. 40, no. 6, pp. 1055–1064, 2009.

[21] J. H. Janssen, P. Tacken, J. de Vries, E. L. van den Broek, J. H. D. M. Westerink, P. Haselager, and W. A. IJselstein, "Machines outperform lay persons in recognizing emotions elicited by autobiographical recollection," *Human-Computer Interaction*, vol. [DOI: 10.1080/07370024.2012.755421], [preprint online available].

[22] E. L. van den Broek, V. Lisý, J. H. Janssen, J. H. D. M. Westerink, M. H. Schut, and K. Tuinenbreijer, *Affective Man-Machine Interface: Unveiling human emotions through biosignals*, ser. Communications in Computer and Information Science. Berlin/Heidelberg, Germany: Springer-Verlag, 2010, vol. 52, pp. 21–47.

[23] E. L. van den Broek, "Robot nannies: Future or fiction?" *Interaction Studies*, vol. 11, no. 2, pp. 274–282, 2010.

[24] E. L. van den Broek, F. van der Sluis, and T. Dijkstra, "Cross-validation of bi-modal health-related stress assessment," *Personal and Ubiquitous Computing*, vol. 17, no. 2, pp. 215–227, 2013.

[25] B. H. Calhoun, J. Lach, J. Stankovic, D. D. Wentzloff, K. Whitehouse, A. T. Barth, J. K. Brown, Q. Li, S. Oh, N. E. Roberts, and Y. Zhang, "Body sensor networks: A holistic approach from silicon to users," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 91–106, 2012.

[26] C. Jorgensen and S. Dusan, "Speech interfaces based upon surface electromyography," *Speech Communication*, vol. 52, no. 4, pp. 354–366, 2010.

[27] E. L. van den Broek, *Affective computing: A reverence for a century of research*, ser. Lecture Notes in Computer Science. Berlin/Heidelberg, Germany: Springer-Verlag, 2012, vol. 7403, pp. 434–448.

[28] J. Andress and S. Winterfeld, *Cyber warfare: Techniques, tactics and tools for security practitioners*. Waltham, MA, USA: Syngress / Elsevier, Inc., 2011.

[29] E. Mordini and D. Tzovaras, *Second generation biometrics: The ethical, legal and social context*, ser. The International Library of Ethics, Law and Technology. Dordrecht, The Netherlands: Springer Science+Business Media B.V., 2012, vol. 11.

[30] S. L. Garfinkel, A. Juels, and R. Pappu, "RFID privacy: An overview of problems and proposed solutions," *IEEE Security & Privacy*, vol. 3, no. 3, pp. 34–43, 2005.

[31] P. Kumar and K. J. Lee, "Security issues in healthcare applications using wireless medical sensor networks: A survey," *Sensors*, vol. 12, no. 1, pp. 55–91, 2012.