# ENISA Briefing: Behavioural Biometrics

ENISA Briefings are short descriptions of emerging issues in security aimed at policy and decision makers. They give a brief introduction to the topic, areas of debate and propose a reasoned opinion on controversial points.

The purpose of this briefing is to give an introduction to the possibilities offered by behavioural biometrics, as well as their limitations and the main issues of disagreement between experts in the field. Suggestions for further reading can be found in [Sources and further reading].

**Contact details:**
This report has been edited by: Giles Hogben, email: Giles.hogben@enisa.europa.eu

**Acknowledgements:**
*We would like to thank the following experts for their input and advice:*

- Roman Yampolskiy, University of Louisville
- Yannis Damousis, Center for Research and Technology Hellas

## Key points

- Behavioural biometrics offer a tool which may enhance the security of user authentication and intrusion detection applications, in some cases with very low impact on the system users.
- They are most useful in multimodal systems (those using more than one type of biometric at the same time) as a complement to more robust methods largely because most behavioural biometrics are highly sensitive to the means of implementation. E.g. keystroke dynamics depend on the keyboard hardware used, blinking behavior depends on illumination etc…
- Some behavioural biometrics, require specialised and sometimes highly obtrusive equipment which may be off-putting to users.
- Other behavioural biometrics on the other hand offer a completely unobtrusive technique to identify or classify individuals. Such unobtrusiveness may be challenging from the point of view of collecting user consent, as required by law in many jurisdictions.
- Data collected by behavioural biometrics may be used for secondary purposes which can involve the processing of highly sensitive data which may be inferred from the data collected.
- Behavioural biometrics are vulnerable to several spoofing attacks specific to the technique (see [Areas of controversy and open problems]).

## Introduction

Behavioural biometrics are used in an information security context to identify individuals by using unique features of activities they perform either consciously or unconsciously. There is a very large number of possible techniques. For a more complete taxonomy of behavioural biometrics see (1). Some interesting examples include:

- **Blinking pattern:** Time between blinks, how long the eye is held closed at each blink, physical characteristics the eye undergoes while blinking
- **ECG:** features of electromagnetic signals generated by the heart
- **EEG:** features of electromagnetic signals generated by the brain
- **Gait:** the way a person walks.
- **Game strategy:** a statistical model of player's strategy in various games including online role playing games can be used to detect imposters. This is increasingly important in massively mutiplayer games involving real money trading – see (2)
- **Keystroke dynamics**: the way a person types. This can cover the timing of keystrokes, or with an adapted keyboard, the pressure used.
- **Text style:** many linguistic features can be profiled such as: lexical patterns, syntax, semantics, pragmatics, information content or item distribution through a text (3).

- **Voice:** Speaker identification is one of the best researched biometric technologies (4) (5). Speaker identification systems can be classified based on the freedom of what is spoken (6):
    - **Fixed text:** The speaker says a particular word selected at enrollment.
    - **Text dependent:** The speaker is prompted by the system to say a particular phrase.
    - **Text independent:** The speaker is free to say anything he/she wants.

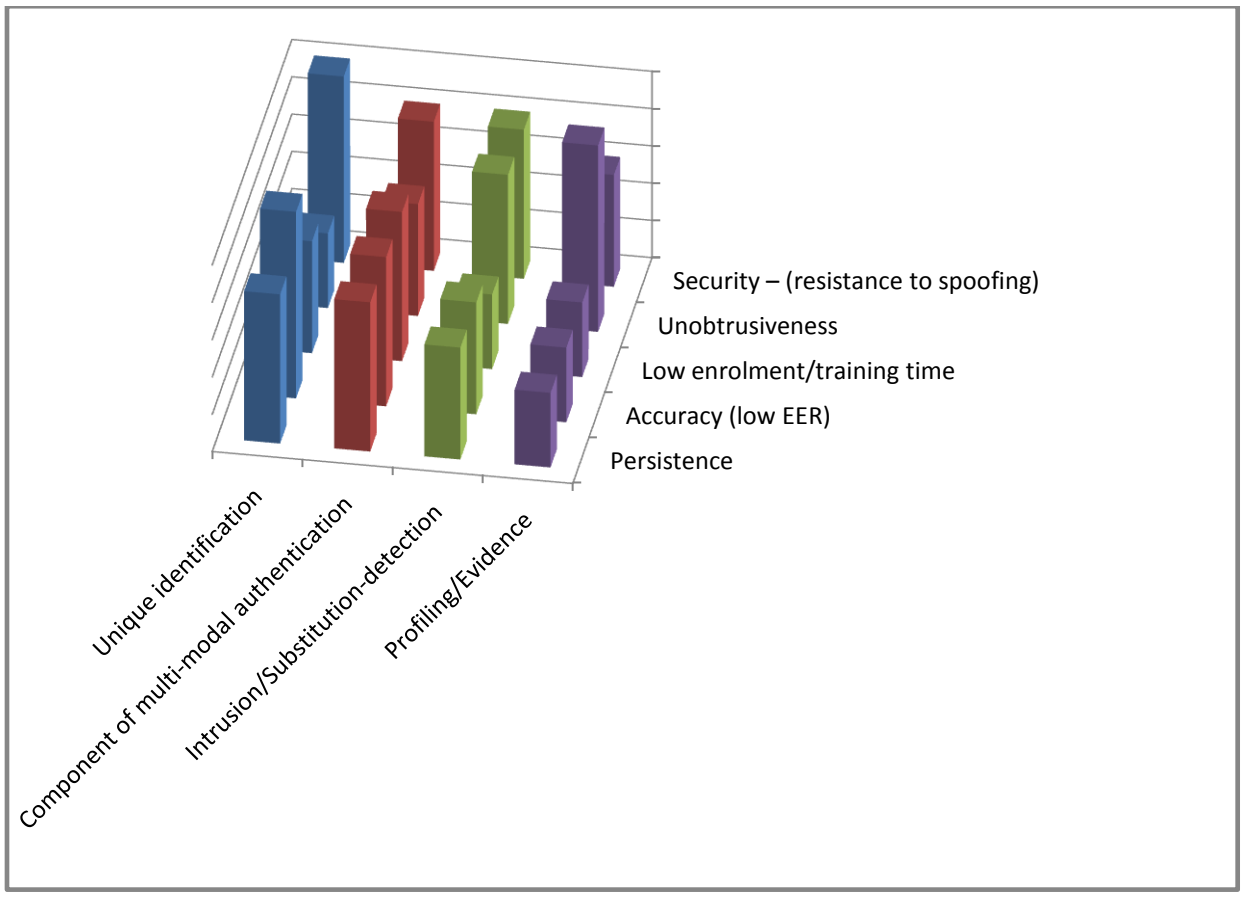
A number of techniques are limited to specific use-cases – for example, car driving style (to identify drivers), handgrip pressure patterns (for authentication to handheld devices including weapons) and credit card usage patterns (credit card fraud detection).
Important factors in the successful implementation behavioural biometrics include:

- **Equipment required:** this can vary from none at all (e.g. in the case of simple keystroke dynamics) to multiple cameras, EEG sensors etc...
- **Enrollment time:** the time required to train the system to recognise a given individual.
- **Persistence**: The time before an identifying feature changes in an individual after an initial training period of the system.
- **Obtrusiveness**: How much the system alters the normal experience of the identification subject. For example, EEG sensors which must be attached to the scalp are obviously obtrusive.
- **Error rates:** As with all biometrics, error rates are analysed according to:
    - **False rejection rate (FRR):** the percentage of individuals wrongly denied access to a system.
    - **False acceptance rate (FAR):** the percentage of individuals wrongly authorised by a system
    - **Equal error rate:** a measure often used to evaluate the accuracy of a biometric technology. It is the value of the FRR and FAR when a system is tuned to have an equal FAR and FRR.

## Suitability by application area

These factors vary dramatically between different types of behavioural biometrics. For example ECG biometrics can give EER values of less than 3% but highly obtrusive equipment is still used (7). Keystroke dynamics on the other hand when applied to timing only, requires no special equipment. The confidence in the identity of the subject however depends strongly on the length of the sample and the system training period (the time taken for the application to build up a reliable model of a given user) . This makes it most suitable for use as a way of detecting if a user is substituted after an initial login, or to add an extra level of confidence to another factor (8).

It is important, therefore, to understand how the limitations of a given technique affect the use-cases for which it is suited. The following table shows the requirements of different application areas – higher bars mean this requirement is more important.




## Areas of controversy and open problems

**Collection of sensitive information:** some of the techniques used collect data which may be used to derive highly sensitive information. Perhaps the clearest example of this is the collection and analysis of EEG patterns. EEG patterns may be used simply for identification, but it is now possible to extract significant information about the thoughts of the subject from records of brain activity (fMRI): see (9) (10). Even less obviously, sensitive types of behavioural biometrics may incidentally gather highly sensitive information however. For example, gait features may reveal emotional features such as depression (11) (12).

It should be emphasised however that the in some cases, such as keystroke dynamics, this issue is less important since there is less likely to be a correlation between the biometric measurement and more

sensitive features of a person's profile (such as mood, health state etc...). The use-case of the technique also affects the importance of this issue. For example, when used to detect intrusion into a home computer (which is assumed to be trusted), such sensitive data may be kept private to the user, while when used to authenticate to a corporate web application, this may not be the case.

Furthermore, techniques exist to limit the exposure from collected behavioral profiles, provided that the data collector is trusted (e.g. hashable profiles, etc.). Currently this area of research is in its infancy and will undoubtedly grow as does the adaptation of behavioral biometrics.

**Negative reaction to obtrusive equipment:** Due to the above possibilities, as well as the obtrusiveness of the equipment used, there is a strong negative reaction on the part of end-users to certain kinds of biometrics, including behavioural biometrics such as EEG scanning. Whether or not fears are well-founded, this is a significant problem for deployment. For a more in depth discussion of this issue see: (13) (14)

**Consent and secondary use for data collected with unobtrusive equipment:** Some behavioural biometrics are at the other end of the obtrustiveness spectrum. For example, gait recognition and keystroke dynamics are possible without any impact on the subject whatsoever. This has its own drawbacks, because it means that a subject may be identified without their awareness. This raises the issue of consent: according to the European directive (15), personal data (which are collected in every identification event involving behavioural biometrics), should always be processed with the informed consent of the data subject.

Highly unobtrusive techniques offer the possibility of identifying people outside the scope of the original application, without any special equipment. For example, if a person's keystroke signature is known to ,they could be recognized on other systems with keystroke analysis software. A key question is therefore, how to limit behavioural profiles to a specific context and what happens if the information is leaked outside the system.

**Higher error rates:** Many behavioural biometrics have error rates which are high enough to make them unsuitable for use as an authentication technology in isolation. For example, haptic (touch-based) authentication has an EER of 22.3%. This does not mean that such techniques should not be used. However, they may only be useful in their current form when combined with other authentication techniques. For example, keystroke dynamics, which has a minimum FRR of 4%, may only be useful in combination with an initial static biometric technique such as fingerprint machine. An excellent summary of error rates can be found in (1).

**Sensitivity to change of application configuration:** most behavioural biometrics are sensitive to the implementation context. For example, gait recognition using video analysis is quite sensitive to

illumination changes, keystroke dynamics depend on the keyboard hardware used, blinking behavior also depends on illumination etc… For this reason they are mainly used in multimodal systems as complements to more robust and methods.

**Spoofing attacks[1]:** A number of different types of spoofing attacks are described in the literature (15):

- **Coercive Impersonation**- is a type of attack in which the attacker physically forces a genuine user to identify himself to an authentication system or removes the biometric (for example, a finger) from the person to use as a key to gain access to the resources.
- **Replay Attack**- is based on recording a previously produced biometric such as taking a picture of a face or recording a person's voice and submitting it to the biometric data collection unit.
- **Impersonation Attack**- involves an attacker who can change his appearance to match a legitimate user for example use makeup to copy somebody's face or impersonate voice or forge a signature.

Approaches to spoofing behavioral biometrics are similar to those for physical biometrics but with some domain specific features. Replay attacks are very popular since it is easy to record an individual's voice or copy a signature. Human mimicking or forgery is also a very powerful technique with experts consistently breaching security of signature-based or voice-based authentication systems. On the other hand, the removal of body parts such as fingers or DNA, is  less likely to be a useful attack.

Just as software can be trained to recognize samples based on feature recognition, it can also be trained to generate samples containing a given set of features. Such techniques produce models of behavior parameterized with observed target user data which steadily improve in their performance. It may also be possible to perform a brute force attack on a biometric system by going through a large number of possible behavioral parameters. For example, experiments demonstrate that with respect to game-strategy biometrics it is possible to secretly and automatically monitor the target user during play, generate an accurate statistical profile of his actions and train an artificially intelligent program to mimic target player's behavior.

Spoofing approaches for voice-based behavioral biometrics are very numerous and creative in nature including impersonation (16) (17) (18) (19), cut-and-paste (20) (16), text-to-speech (20) (16) (21) and voice morphing (22) (16) (23) (24).

A promising solution proposed in the literature for preventing spoofing of behavioral biometric systems is to use automatic computerized methods aimed at telling humans and computers apart

[1] *(text in this section taken from Mimicry Attack on Strategy-Based Behavioral Biometric. Yampolskiy, Roman V. (32))*

automatically. Commonly known as CAPTCHAs, these take advantage of the differences in abilities between human beings and intelligent machines to identify to which group an agent being tested belongs. The risk of spoofing or theft of biometric data should also be reduced by appropriate encryption of profiles and templates.

**Cross over with behavioural marketing**

Behavioural marketing uses data which is not classified as personally identifiable according to the European Directive 95/46 to target narrow classes of individuals. It is interesting to note that behavioural biometrics provide data and techniques which could be used for the same purpose. The same data which might allow the detection of anomalous behaviour for intrusion detection purposes – e.g. keystroke dynamics, haptic feedback etc..., could also be used to classify individuals for marketing purposes. This means that the same issues (25) which have sparked fierce debate on behavioural marketing in Europe, should also be considered in respect of behavioural biometrics.

## Future trends and research

The following are areas where significant developments can be expected in behavioural marketing:

- **Standardisation:** Some standardization initiatives are pursued under Joint Technical Committee 1 (JTC 1) of ISO/IEC subcommittee SC37 "Biometrics". There are also some large scale projects attempting to develop standards for behavioral biometrics (26). In particular within HUMABIO project, biometric data interchange formats were defined for the new biometric modalities (EEG, ECG, anthropometric profile), as a contribution to the work of ISO SC 27, WG 3..

  Specifically in the area of Cognitive biometrics such efforts are undertaken by the journal of the field (27) to establish an international standard(s) for cognitive biometrics which would provide a means for integrating this branch of biometrics within government frameworks, engendering widespread integration into a common global biometric framework.

- **Multi-modal biometrics:** One approach to prevent spoofing attacks is to use multi-modal biometric systems (28). Multi-modal biometrics are more difficult to spoof since they require simultaneous spoofing of multiple different biometric modalities for example fingerprint and face. A very interesting approach is combining of physical and behavioral biometrics into a single authentication system. Probably the most popular such methodology combines the audio (voice) and video (face) signal obtained from the user. Such systems can still be spoofed by concurrent presentation of a recorded or mimicked voice together with a photograph or a video clip of the user's face but a lot of successful techniques have been developed to check for liveness in such multi-modal biometric systems (29) (30)

- **Unobtrusiveness:** various techniques which currently require highly obtrusive devices will evolve towards more unobtrusive techniques. For example, currently some techniques for gait recognition require the subject to wear special trousers. This may be released by video based techniques.
- **Privacy enhancing techniques:** to limit the exposure from collected behavioral profiles.
- **Efficiency:** error rates and training periods will be reduced.

## Sources and further reading

1. *Behavioral Biometrics: a Survey and Classification.* **R Yampolskiy, V Govindaraju.** Issue 1, s.l. : International Journal of Biometrics (IJBM), 2008, Vol. Volume 1, pp. 81-113.

2. **Giles Hogben, ENISA.** Security and Privacy in Virtual Worlds and Gaming. [Online] http://www.enisa.europa.eu/act/it/oar/massively-multiplayer-online-games-and-social-and-corporate-virtual-worlds/security-and-privacy-in-virtual-worlds-and-gaming/at_download/fullReport.

3. *Linguistic profiling for author recognition and verification.* **Halteren, H.** 2004. Proceedings of ACL.

4. *Speaker verification for multimedia applications.* **Ciota, Z.** 2004. IEEE International Conference on Systems. pp. 2752-2756.

5. *Information Fusion for Robust Speaker Verification.* **C. Sanderson, K. K. Paliwal.** Aalborg : s.n., 2001. 7th European Conference on Speech Communication and Technology (EUROSPEECH'01).

6. *Automated Biometrics.* **N. K. Ratha, A. Senior, R. M. Bolle.** Rio de Janeiro : s.n., 2001. International Conference on Advances in Pattern Recognition.

7. *Verification of humans using the electrocardiogram.* **G Wubbeler, M Stavridis, D Kreiseler, R Bousseljot, C Elster.** s.l. : Elsevier Pattern Recognition Letters, 2007, Vol. 28.

8. *Keystroke dynamics as a biometric for authentication.* **F Monrose, D Aviel, B Rubin.** s.l. : Future Generation Computer Systems, 2000, Vol. 16.

9. **Naselaris T, Prenger RJ, Kay KN, Oliver M, Gallant JL.** Bayesian reconstruction of natural images from human brain activity. Neuron. 2009 Sep 24;63(6):902-15.

10. *Signatures of Depression in Non-Stationary Biometric Time Series.* **M Culic, B Gjoneska, H Hinrikus, M Jändel, W Klonowski, H Liljenström, N Pop-Jordanova, D Psatta,D von Rosen, B Wahlund.** 2009, 2009, Vol. Computational Intelligence and Neuroscience.

11. **Troje, N. F.** Retrieving information from human movement patterns. In: Shipley, T. F. and Zacks, J. M. (eds.) Understanding Events: How Humans See, Represent, and Act on Events. s.l. : Oxford University Press, 2008, pp. pp. 308-334.

12. *Spatiotemporal gait patterns during over ground locomotion in major depression compared with healthy controls.* **Lemke MR, Wendorff T, Mieth B, Buhl K, Linnemann M.** 2000, Vols. J Psychiatr Res. 2000 Jul-Oct;34(4-5):277-83.

13. *Body, Biometrics and Identity.* **S Massari, E Mordini.** 9, s.l. : Bioethics, 2008, Vol. 22.

14. **Bioethics, Irish Council for.** *Biometrics, Enhancing Security or Invading Privacy.* Dublin : s.n., 2009.

15. *The state of the art in abuse of biometrics.* **Hartel, I. Buhan and P.** s.l. : Technical Report TR-CTIT-05-41 Centre for Telematics and Information Technology, University of Twente, 2005.

16. *Vulnerability of speaker verification to voice mimicking, Video and Speech Processing.* **Y. W. Lau, M. Wagner and D. Tran.** s.l. : Proceedings of 2004 International Symposium on Intelligent Multimedia, 20-22 Oct. 2004. pp. pp. 145- 148.

17. *Vulnerability in speaker verification- A study of technical impostor techniques.* **Blomberg, J. Lindberg and M.** 1999. Proceedings of Eurospeech. pp. 1211-1214.

18. *Speaker verification scores and acoustic analysis of a professional impersonator.* **M. Blomberg, D. Elenius and E. Zetterholm.** 2004. Fonetik. pp. 84-87.

19. *A comparison between human perception and a speaker verification system score of a voice imitation.* **E. Zetterholm, M. Blomberg and D. Elenius.** Tenth Australian International Conference on Speech Science & Technology.

20. *Towards Speech-Generated Cryptographic Keys on Resource-Constrained Devices.* **F. Monrose, M. Reiter, Q. Li, D. P. Lopresti and C. Shih.** San Francisco : s.n., 2002. Eleventh USENIX Security Symposium. pp. 283-296.

21. *Imposture Using Synthetic Speech against Speaker Verification Based on Spectrum and Pitch.* **T. Masuko, K. Tokuda and T. Kobayashi.** Beijing : s.n., 2000. 6th International Conference on Spoken Language Processing. pp. 302-305.

22. *Quality-enhanced Voice Morphing using Maximum Likelihood Transformations.* **Young, H. Ye and S.** s.l. : IEEE Audio, Speech and Language Processing, 2006.

23. *Voice Forgery Using ALISP: Indexation in a Client Memory.* **P. Perrot, G. Aversano, R. Blouet, M. Charbit and G. Chollet.** 2005. IEEE International Conference on Acoustics, Speech, and Signal Processing. pp. 17- 20.

24. *Wavelet-based voice morphing.* **C. Orphanidou, I. M. Moroz and S. J. Roberts.** s.l. : WSEAS Journal on Systems, 2004, pp. 3297-3302.

25. **ENISA.** How to strengthen EU legislation, improve international cooperation and secure the growing market of internet services. [Online] 2007. http://www.enisa.europa.eu/act/it/library/pp/eu-leg/at_download/fullReportb3oFliP21RN.

26. Actibio project. [Online] http://www.actibio.eu.

27. International Journal of Cognitive Biometrics. [Online] http://www.inderscience.com/browse/index.php?journalCODE=ijcb.

28. *Spoofing and Anti-Spoofing Measures, Information Security Technical Report.* **Schuckers, S. A. C.** 2002, pp. 56-62.

29. *Detecting Replay Attacks in Audiovisual Identity Verification.* **H. Bredin, A. Miguel, I. H. Witten, G. Chollet.** Paris : s.n., 2006. Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP 2006). pp. 1-6.

30. *Audio-Video Biometric system with liveness checks.* **G. Chetty, M. Wagner.** s.l. : Image and Vision Computing, 2005.

31. [Online] http://www.inderscience.com/storage/f861114357101292.pdf.

32. *Mimicry Attack on Strategy-Based Behavioral Biometric.* **Yampolskiy, Roman V.** Las Vegas : IEEE Computer Society, 2008. 5th International Conference on Information Technology: New Generations (ITNG2008). pp. 916-921.