14 MISUNDERSTANDINGS WITH REGARD TO BIOMETRIC IDENTIFICATION AND AUTHENTICATION

June 2020

www.aepd.es/es
www.edps.europa.eu

Identification is the process of identifying an individual among a group. This process compares the data of the individual to identify to those of the each individual in the group. Authentication is the process of proving the identity claimed by an individual. This process compares the data of the individual only with the data of the claimed identity.

The increased use of biometric data (e.g. fingerprints or facial measurements) for identification and authentication purposes recently attracted public interest and coincided with the spread of related misunderstandings. This paper lists and explains fourteen of them, and provides further scientific references for clarification.

1. "Biometric information is stored in an algorithm"

An algorithm is a method, an ordered set of operations or a recipe and not a means to store biometric data.

The collected biometric information (e.g. the image of a fingerprint) is processed following standard-defined procedures[1] and the result of that process is stored in data records called signatures, patterns or templates. These patterns numerically record the physical characteristics making it possible to differentiate people.

However, there are machine learning techniques which leak parts of their training datasets to the models they create[2]. Some of these techniques are used in biometric identification and authentication.

2. "The use of biometric data is as intrusive as any other identification/ authentication system"

Unlike a password or certificate, biometric data collected during an authentication or identification procedure reveals more information about the subject. Depending on the biometric data collected, data can be derived from the subject such as race or gender (even from fingerprints[3]), emotional

1 See the ISO 19794-2 fingerprint data format: https://www.ekds.gov.tr/bio/FM3_README.pdf (page 2); see for a much more extensive example for a handwritten signature in: R.Pizarro Santos, Análisis de las normas internacionales de firmas manuscritas ISO/IEC 19794-7 y 19794-11, Universidad de Carlos III, Madrid 2010,:https://e-archivo.uc3m.es/bitstream/handle/10016/10990/PFC_Roberto_Pizarro_Santos.pdf?sequence=1&isAllowed=y

2 Congzheng Song, Thomas Ristenpart, and Vitaly Shmatikov. 2017. Machine Learning Models that Remember Too Much. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS '17). Association for Computing Machinery, New York, NY, USA, 587–601. DOI: https://doi.org/10.1145/3133956.3134077

3 More information on the data that can be extracted from a fingerprint in: The Hidden Data in Your Fingerprints. Scientific American (27/04/2018) https://www.scientificamerican.com/article/the-hidden-data-in-your-fingerprints

aepd agencia española protección datos

EDPS

state, diseases, genetic characteristics and tares, substance consumption, etc[4]. Since this information is "built-in", the user cannot prevent the collection of such additional information.

3. "Biometric identification / authentication is accurate"

Unlike password-based or certified processes, which are 100% accurate (e.g. a password is right or is not), biometric identification/authentication relies on probability (e.g. the captured fingerprint is 96% similar to the one of X). There is a certain rate of false positives (accepting an impersonator) and false negatives (rejecting an authorised individual). These rates are higher, the less accurate the data capture equipment is and also depend on the capture conditions (e.g. room luminosity or sensor cleanliness).[5] The accuracy of some biometric data, like fingerprints, is dependent on the age of the individual and affected by the ageing of individuals[6].

4. "Biometric identification/ authentication is precise enough to always differentiate between two people"

It is demonstrated that the biometric resemblance between siblings or relatives has confused biometric systems[7]. In particular, the identity of biometric patterns for the identification of twin siblings beyond facial recognition is a field of study[8]. Moreover, environmental conditions in uncontrolled environments (i.e. facial recognition in public spaces or the use of facial paint or antiviral masks) lead to an increase in the error rate and therefore confusion is more likely.

5. "Biometric identification/ authentication is suitable for all people"

Some people cannot use certain types of biometrics because their physical characteristics are not recognised by the system. In case of injuries, accidents, health conditions (such as paralysis) and others, this incompatibility might be temporary. Permanent biometric incompatibility could be one factor leading to social

4 Biometrics-Soft is the field of study of non-unique characteristics of the individual based on his biometric information, such as mental state, health, etc. Fairhurst, Michael; Li, Cheng; Da Costa-Abreu, Márjory: 'Predictive biometrics: a review and analysis of predicting personal characteristics from biometric data', IET Biometrics, 2017, 6, (6), p. 369-378, DOI: 10.1049/iet-bmt.2016.0169 IET Digital Library, https://digital-library.theiet.org/content/journals/10.1049/iet-bmt.2016.0169

5 More information on the poor performance of the British police facial recognition system in: UK police use of facial recognition technology a failure, says report. The Guardian (15/05/2018) https://www.theguardian.com/uk-news/2018/may/15/uk-police-use-of-facial-recognition-technology-failure

6 Galbally, Javier & Haraksim, Rudolf & Beslay, Laurent. (2018). A Study of Age and Ageing in Fingerprint Biometrics. IEEE Transactions on Information Forensics and Security. PP. 1-1. 10.1109/TIFS.2018.2878160. https://www.researchgate.net/publication/328526153_A_Study_of_Age_and_Ageing_in_Fingerprint_Biometrics

7 See for an example on how users could trick iPhone's facial recognition technology: The iPhone X's Face ID thinks these two brothers are the same person. MSPoweruser (5/11/2017) https://mspoweruser.com/iphone-xs-face-id-thinks-two-brothers-person

8 K. W. Bowyer and P. J. Flynn, "Biometric identification of identical twins: A survey," 2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS), Niagara Falls, NY, 2016, pp. 1-8, doi: 10.1109/BTAS.2016.7791176. https://www3.nd.edu/~kwb/Bowyer_Flynn_BTAS_2016.pdf

exclusion[9].

6. "The biometric identification/ authentication process cannot be circumvented"

There are procedures and techniques that allow to circumvent biometric authentication systems and assume the identity of another person. Some of these procedures and techniques, such as the use of masks[10] or footprint reproductions[11], do not require extensive technical knowledge or economic resources. The so-called "adversary systems" are specifically designed to deceive image recognition systems and can be used to circumvent biometric identification[12].

7. "Biometric information is not exposed"

Unlike password or certificate based processes, most of a person's biometric characteristics are exposed and can be captured at a distance, as the face, footprints, way of moving, thermal footprints, etc. are not usually hidden.

On the other hand, those individuals who want to actively circumvent biometric tracking or identification systems have resources available to do so[13] while for a large majority of the population this will not be the case.

If no measures are taken to reduce the risk of unauthorised use of biometric data, their use would be equivalent to writing our access codes in our forehead[14].

8. "Any biometric processing involves identification/ authentication"

Not necessarily. For example, the biometric data processing of mouse movement used to determine whether a robot is accessing a website involves treating biometric information to differentiate human from machine. Biometric data processing may also be performed to determine whether a human or animal intruder exists in a restricted space, or in digital signage[15] systems to differentiate between men, women and children. Still, there is a risk of processing such information beyond the original purpose in case of e.g. of a security failure, regulatory change or unlawful processing.

9 More information on the risks of social exclusion from UK ID card biometric systems in: UK Identity Cards and Social Exclusion. Privacy International (May 2005)https://privacyinternational.org/sites/default/files/2017-12/UK%20Identity%20Cards.pdf

10 Hackers just broke the iPhone X's Face ID using a 3D-printed mask. Wired UK (13/11/2017) https://www.wired.co.uk/article/hackers-trick-apple-iphone-x-face-id-3d-mask-securit

11 You will be glued to this: Mumbai college's students trick biometric system. Hindustan Times (15/05/2017) https://www.hindustantimes.com/mumbai-news/you-will-be-glued-to-this-mumbai-college-s-students-trick-biometric-system/story-W64f1jdMtecxKDmI2DakeI.html

12 Pautov, Mikhail et al. "On Adversarial Patches: Real-World Attack on ArcFace-100 Face Recognition System." 2019 International Multi-Conference on Engineering, Computer and Information Sciences (SIBIRCON) (2019): n. pag. Crossref. Web. https://arxiv.org/pdf/1910.07067.pdf

13 These clothes use outlandish designs to trick facial recognition software into thinking you're not human. Business Insider (5/6/2020) https://www.businessinsider.com/clothes-accessories-that-outsmart-facial-recognition-tech-2019-10?IR=T#images-from-echizens-lab-shows-how-the-visor-blocks-ais-ability-to-detect-a-face-6

14 Scientists Extract Fingerprints from Photos Taken From up to Three Meters Away. Bleeping Computer (12/01/2017) https://www.bleepingcomputer.com/news/security/scientists-extract-fingerprints-from-photos-taken-from-up-to-three-meters-away/

15 Spanish CaixaBank offers an appointment to capture facial recognition: https://www.caixabank.es/particular/banca-digital/face-id_en.html

9. "Biometric identification/ authentication systems are safer for users"

Any of the multiple systems in which our biometric data are processed can suffer a security breach. Unauthorised access to our biometric data in a system would allow or facilitate (in the case of multiple authentication factors) access in the rest of the systems using such biometric data. It could have the same effect as using the same password on many different systems, so the scale in biometric deployment is a problem in itself. Moreover, unlike password-based systems, once biometric information has been compromised it cannot be modified or cancelled.

If biometric information was previously stored in a few databases (mainly for public security or border control purposes), it is now stored in an increasing number of devices. This greatly increases the probability of a security breach leaking biometric data (during its collection, transmission, storage or processing), something that is already happening[16].

10. "Biometric authentication is strong"

By definition, a strong authentication system is one requiring to provide at least two of the following: something you know, something you have or something you are (biometrics). By definition, using only biometric data is a weak authentication process, while using an access card and a password is strong. Although biometric authentication often requires a previous process of enrolment or identification in which, for example, in facial recognition, it is necessary to compare with the photo in the ID, if, after the identification process, the authentication process is only biometric, it remains a weak system.

11. "Biometric identification/ authentication is more user-friendly"

It depends on the technology used and the circumstances, perception and culture of each user. Apart from the suitability problems described in the fifth misunderstanding, there may be other problems that negatively affect the user's perception: Feeling of invasion of privacy, failures in biometric systems that prevent access to services, non-biometric alternatives lacking completely or not being suited to provide the same service, as well as the need to perform enrolment processes in each entity[17].

12. "Biometric information converted to a hash is not recoverable"

To add security to the processing of biometric information, it is recommended to remove the biometric pattern from

16 An example of a security breach exposing millions of biometric data: New Data Breach Has Exposed Millions Of Fingerprint And Facial Recognition Records: Report. Forbes (14/08/2019) https://www.forbes.com/sites/zakdoffman/2019/08/14/new-data-breach-has-exposed-millions-of-fingerprint-and-facial-recognition-records-report

17 Spanish CaixaBank offers an appointment to capture facial recognition: https://www.caixabank.es/particular/banca-digital/face-id_en.html

which the hash[18] or biohash[19] has been obtained. However, there are studies showing that the hash could be reversible, that is, it could be possible to obtain the original biometric pattern, especially if the secret of the key used to generate the hash is violated[20].

13. "Stored biometric information does not allow the original biometric information to be reconstructed from which it has been extracted"

Stored biometric information (i.e. pattern) allows the original biometric data (e.g. a face) to be partially reconstructed. Such partial reconstruction sometimes has sufficient accuracy for another biometric system to recognise it as the original one. For example, in facial biometric information there are studies that show that it is possible to get from a robot portrait a faithful representation[21]. The accuracy of the reconstruction depends on the amount of biometric information collected.

14. "Biometric information is not interoperable"

On the contrary, biometric information processing systems are developed according to standards to ensure their interoperability[22]. Systems that work by comparing the result of applying a hash function on biometric patterns can also be made interoperable by the simple method of sharing keys used during the hashing process.

18 A hash function is a process, which transforms any random dataset (e.g. a fingerprint pattern) in a fixed length character series, regardless of the size of input data. More information on hash functions and their use as pseudonymisation technique in: https://edps.europa.eu/data-protection/our-work/publications/papers/introduction-hash-function-personal-data_en

19 Biohashing is a technique used to combine tokenized random number and biometric data. More information in: https://www.researchgate.net/publication/234809846_Remarks_on_BioHash_and_its_mathematical_foundation

20 More information on biohash inversion attacks in: Topcu, B., Karabat, C., Azadmanesh, M. et al. Practical security and privacy attacks against biometric hashing using sparse recovery. EURASIP J. Adv. Signal Process. 2016, 100 (2016) https://link.springer.com/article/10.1186/s13634-016-0396-1#Sec5More information on how the pattern can be obtained from a biohash: Davide Maltoni, Dario Maio, Anil K. Jain, Salil Prabhakar. Handbook of Fingerprint Recognition. Springer Science & Business Media (2009) https://books.google.es/books?id=1Wpx25D8qOwC&pg=PA407&lpg=PA407&dq=BIOHASHING&source=bl&ots=9yS_1Spp9-&sig=ACfU3U3Vk-dF7ybO2p8jfhOhslMnAEhL8A&hl=es&sa=X&ved=2ahUKEwiUqMfNpPznAhWLxYUKHSkiDmk4ChDoATAFegQIChAB#v=onepage&q=BIOHASHING&f=false

21 A comparison of original faces and faces reconstructed from patterns on page 3 in: Michelle Chibba and Alex Stoianov. On Uniqueness of Facial Recognition Templates. Information and Privacy Commissioner's Office of Ontario, Canada March 2014https://www.ntia.doc.gov/files/ntia/publications/uniqueness_of_face_recognition_templates_-_ipc_march-2014.pdf

22 Examples of conversion between biometric formats in: Convert fingerprints to ISO and ANSI fingerprint template data format https://jomutech.com/convertfingerprintimagestoisooransifingerprinttemplateformats A description of biometric interoperability standards can be found in: http://biometria611.blogspot.com/p/estandares.html