International Working Group
on Data Protection
in Telecommunications

675.53.16

Working Paper on Biometrics in Online Authentication

60th meeting, 22-23 November 2016, Berlin (Germany)

Introduction

1. The management of user identity and access to computer systems is of critical importance in ensuring the security and functionality of those systems. In order to protect privacy and data security, access control is required to ensure that the right users gain the right access to IT systems and the personal data stored therein. However, the correct consideration of the different facets of access control, namely identification, authentication and authorisation, is required to ensure that an appropriate level of both security and privacy can be maintained. Authentication will test for a match between something that is known to be associated with and controlled by the individual (i.e., a password or numbered token) and the proof that the individual is offering to support their claim. This is in contrast to the problem of identification which seeks to identify a specific individual within a population (e.g., looking for someone specific within a crowd).

2. As an example of authentication, to store an item of luggage in a cloakroom the item is deposited at the counter (subject to any security checks) by the individual identifying themselves as the owner of that item. No additional checks are required to determine if that initial claim of ownership is correct. To ensure that items are reunited with their rightful owners, the cloakroom staff must authenticate all claims of ownership when items are being collected. The most common method in this scenario would be to check for **something the individual has**, namely the numbered token which was issued when the item was dropped off. The most common type of authentication factor for online services is to check for **something that is known to the individual** such as a password, in order to authenticate the statement of identity (the provision of the username). Another type of authentication factor, commonly referred to as biometrics, is to check for **something that the individual is** (a physical or physiological characteristic, e.g., their face) **or does** (a behavioural characteristic, e.g., their signature).

Secretariat
Berliner Beauftragte für
Datenschutz und Informationsfreiheit
Friedrichstr. 219
D-10969 Berlin
Phone +49 / 30 / 13889 0
Fax +49 / 30 / 215 5050

Email:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.berlin-privacy-group.org

The Working Group has been initiated
by Data Protection Commissioners
from different countries in order
to improve privacy and data protection
in telecommunications and media

3. Multiple authentication factors can be combined in order to provide a higher degree of confidence in the authentication or to address known threats and vulnerabilities. A common example is the use of a PIN (something the user knows) with a credit or debit card (something the user has) in order to authenticate the individual as the owner of the bank account being used to make a purchase. Selecting which authentication factors (if any) are required for a particular task has a direct impact on the security of the system but also on the privacy implications. For example, when using a numbered token in a cloakroom, the individual may remain anonymous but there is a residual risk of an impostor claiming a bag. By using a ticket design specific to the venue and matching the numbered ticket stub with the number on the bag label this risk can be considered sufficiently low that users need not enrol in a fingerprint recognition system or surrender a government issued identity document.

4. Passwords have a long history in authentication protocols in computing as a way of authenticating users as the owner of an account. They are relatively convenient for users, since they can be used across a wide range of devices, and are easy to integrate into online services.

5. However, the proliferation of online services means that an individual may have many tens or hundreds of user accounts. In consequence, maintaining the secrecy of passwords presents a number of challenges, including:

   - Users re-use the same password at multiple sites.

   - Users may intentionally share their passwords with third-parties to permit them access to the account on their behalf.

   - Passwords are frequently forgotten requiring time and resource intensive reset mechanisms which can be insecure and vulnerable to attack.

   - A user can encounter a variety of policies which may require passwords of different length and composition or which force regular changes[1].

   - Passwords are frequently stored in an insecure manner.

   - Passwords can be compromised in other ways, (e.g., through phishing).

6. As a result, it is increasingly common for online services to replace or augment password-based authentication with so-called multi-factor authentication. Common technologies used for multi-factor authentication include:

[1] Recent guidance suggests regular password changes can lead to a reduction in the security of passwords as users choose those which are more easily remembered, see https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach, https://www.cs.unc.edu/~reiter/papers/2010/CCS.pdf, and http://arstechnica.com/security/2016/08/frequent-password-changes-are-the-enemy-of-security-ftc-technologist-says/

- One time password token or apps,

- Trusted devices (like smartcards), and

- Biometrics.

7. The use of biometrics in online authentication offers one possibility to address some of the shortcomings of current password-based authentication. However, as this Working Paper shall demonstrate, careful consideration must be given to the data protection and privacy risks that result from their use.

8. The purpose of this Working Paper is not to specify when biometrics could be used as a factor in online authentication. This is a decision which should be documented in a Privacy Impact Assessment (PIA) carried out during the design phase of a project and updated throughout the lifetime of the IT system. This Working Paper will highlight the privacy risks when biometrics are introduced and used in authentication and how these risks can be managed in an appropriate manner.

Biometrics

9. The term *biometric* is defined in ISO/IEC 2382:2015[2] as:

   "pertaining to the use of specific attributes that reflect unique personal characteristics, such as a fingerprint, an eye blood-vessel print, or a voice print, to validate the identity of a person."[3]

10. It is the attribute of uniqueness (within the population of users) and relative ease of use that makes biometrics an attractive candidate for authentication. The use of biometrics in authentication is not a new trend but rather a continuation of techniques such as fingerprint analysis which has long been used in law enforcement for the purposes of identification. There is, however, a shift to include biometric sensors in consumer devices, most commonly fingerprint sensors in smartphones, tablets and laptops, or to utilise the camera and microphone of these devices to perform facial or voice recognition.

11. To authenticate a user with a password-based system, it is a simple computational task to verify that the user has provided the correct password which results in an irrefutable yes or no response – a password is either correct or not. Biometric authentication on the other

[2] ISO/IEC 2382:2015(en) Information technology — Vocabulary, https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:ed-1:v1:en

[3] The General Data Protection Regulation 2016/679 of the European Union defines biometric data to be "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data".

hand generally follows a probabilistic methodology where two templates are compared and a percentage match or confidence score generated. Scoring above a certain threshold determines whether or not a comparison is considered a positive match.

12. To further improve the accuracy and reduce the likelihood of spoofing, an authentication system can use a mix of more than one biometric characteristic or combine biometric and non-biometric data from the same individual. Depending on the scenario, it may or may not be necessary to obtain a positive match across all provided data (biometric and non-biometric) for successful authentication.

13. Capture of an individual's biometric data will often require the use of a dedicated device or component built into a PC, laptop or smartphone, for example a smartphone fingerprint scanner or an ATM vein pattern reader. Other types of biometric data, such as face and speech, can be captured using more generic capture devices such as a cameras and microphones and may then be processed further either locally or by a third party.

14. In addition to increasing adoption by consumers as a convenient means of authentication, governments and organisations are also looking towards biometrics in authentication. For example, the European Union's eIDAS Regulation (Electronic identification and trust services for digital transactions in the internal market)[4] calls for the optional use of biometrics to support eSignature applications across the EU.

15. Highly advanced privacy-enhancing technologies include biometric encryption[5] and cancellable biometrics[6]. Both techniques provide several advantages over traditional biometric systems, in particular, the revocability of the stored biometric data. Also, a remote biometric authentication protocol has been recently proposed[7] that is resilient against advanced security threats. This protocol provides security if either the user's device or the server is compromised (but not both).

16. Activity in the field of standardisation within the FIDO Alliance[8] and ISO[9] as well as codes of conducts such as The Biometrics Institute's Privacy Trust Mark[10] aim to address security and privacy issues whilst promoting robust authentication mechanisms.

[4] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

[5] Colin Soutar, Danny Roberge, Alex Stoianov, Rene Gilroy, and B.V.K. Vijaya Kumar. Biometric Encryption. McGraw-Hill, 1999

[6] Cancellable biometrics add a repeatable distortion to the stored template, e.g. see Ruud M. Bolle, Jonathan H. Connell, and Nalini K. Ratha. Biometric perils and patches, volume 35, pages 2727-2738. Elsevier, 2002.

[7] Syta et al., Private Eyes: Secure Remote Biometric Authentication, 2015, http://dedis.cs.yale.edu/dissent/papers/secrypt15-biometric.pdf

[8] https://fidoalliance.org/

[9] JTC 1/SC 37, http://www.iso.org/iso/home/standards_development/list_of_iso_technical_committees/jtc1_home/jtc1_sc37_home.htm

[10] http://www.biometricsinstitute.org/pages/trust-mark.html

Privacy and data protection risks

17. The privacy and data protection risks in this area have been previously documented by various data protection and privacy regulators including those in the EU (in 2003[11] and 2012[12,13]), Canada[14] and the US[15].

18. It is important to note that, in general, different biometric systems will impact on data protection and privacy differently and may therefore require a different approach to addressing these risks. Face recognition, for example, may work with data subjects not knowing they are being subjected to such a system, while fingerprint systems will usually require the individual's active participation (although this may not be the same as the individual's consent). The former may therefore require greater efforts devoted to informing users that the system is in operation.

19. Certain biometrics can be obtained by other parties without the knowledge of the individual - we leave our fingerprints on many surfaces, and our faces may be detected, and images of them stored and processed with ease. Unlike passwords biometrics are not secrets, or simple to change or revoke. Individuals are generally aware of the dangers associated with disclosing a password but attempting to prevent the sharing of a face or voice can be impractical.

20. The fact that biometric authentication is based on probability (i.e., how likely is it that the sample matches the enrolled template?) means that there is a possibility of error. A false negative will result in the individual being unable to be correctly authenticated and likely denied access to the system. Conversely, a false positive leads to an individual being incorrectly authenticated or an impostor successfully fooling the system and thus gaining unauthorised access to the system. Error rates need to strike a balance between usability and security. Setting thresholds too high may result in greater accuracy but with an associated increase of legitimate users not being accepted and vice versa. There may be a temptation to lower accuracy rates in the trade-off between usability and performance in order to reduce false rejection rates, or to fail to test the system in a real-world situation to identify negative impacts on security and privacy .

[11] "Working Document on Biometrics", August 2003, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2003/wp80_en.pdf

[12] "Opinion 3/2012 on developments in biometric technologies", March 2012, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf

[13] Opinion 02/2012 on facial recognition in online and mobile services, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf

[14] Data at your fingertips, https://www.priv.gc.ca/information/pub/gd_bio_201102_e.pdf

[15] FTC Recommends Best Practices for Companies That Use Facial Recognition Technologies, https://www.ftc.gov/news-events/press-releases/2012/10/ftc-recommends-best-practices-companies-use-facial-recognition

21. Dedicated devices or components built into a PC, laptop or smartphones may not be of high quality due to pressures to lower production costs. Such low-end sensors may produce more error rates with higher security and privacy implications for end-users. Some systems can be fooled by stolen or fabricated biometrics[16] if insufficient tests are conducted on the biometrics sample.

22. If an individual is unable to provide a reliable biometric sample (e.g., because of worn or damaged fingertips) or they are otherwise unable or unwilling to use the capture device (e.g., face covered by a veil, scarf or similar), this can lead to a regular denial of access.

23. Biometrics are, like passwords, not immune to being the subject of a personal data breach. The compromise of more than 5.6 million fingerprint records from the Office of Personnel Management (OPM)[17] in June 2015 illustrates the potential danger of centrally stored credentials. This attack was particularly serious as the OPM had retained the original fingerprint images rather than only retaining a template or digital representation of the biometric data.

24. Biometrics are permanent and cannot be easily changed or re-issued like passwords, keycards or tokens in the event of unauthorised access or disclosure. Whilst a list of all possible passwords an individual could choose from is incredibly large, there is a low and finite number of sources which can be used for biometrics for any one individual (i.e., two irises/retinas, 10 fingerprints and one face). There is, therefore, a real risk that user accounts can be linked between services (i.e., where the same fingerprint has been enrolled) which mirrors the current problems of password re-use.

25. The use of biometrics for authentication purposes may reduce the opportunity for users to use a pseudonymous account. This reduces the availability of services for users who don't want to reveal their true identity to the service, or users who want to maintain separate accounts for different contexts (e.g., separate accounts for professional and personal use).

26. Preventing large scale attacks, such as unauthorised access to databases storing biometric templates, as well as making biometrics systems easier to use, has been the subject of recent standardisation efforts. More privacy friendly biometric systems store biometric templates locally on the end users' devices, such as smart phone or tablet. While such a solution requires an adversary to attack a large number of devices one-by-one, care has to be taken with regards to the implementation of such a solution as well, as a security incident involving mobile phones demonstrated that the biometric (fingerprint) template was stored

[16] Chaos Computer Club breaks Apple TouchID, https://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid

[17] https://www.opm.gov/cybersecurity/cybersecurity-incidents/

unencrypted on the file system.[18] Storing templates locally on end user devices, on the other hand, also exposes them to less secure practices by end-users themselves.[19]

27. Some manufacturers of biometric systems still rely on secrecy of their algorithms for security and trust. Proprietary algorithms and technologies which rely on secrecy for their strength are generally considered less trustworthy than those which have been subject to independent third party review or rely on widely accepted standards[20].

Recommendations

28. In light of the above, the Working Group makes the following recommendations to stakeholders:

Regulators, legislators and oversight bodies

29. Regulators at the regional, national and international levels should encourage the development of privacy friendly authentication technologies that address the shortfalls of existing password-based authentication technologies. From a regulatory and standards point of view, while addressing the privacy risks identified in this paper, this should be balanced with consideration of all risks that may arise from the adoption of new authentication technologies, particularly where they make use of biometrics.

30. Proactive privacy tools, such as privacy impact assessments, privacy by design and privacy by default should be promoted and supported by awareness materials, such as guidelines, and may be legally required in certain jurisdictions.

Biometric authentication service providers, software developers and hardware manufacturers

31. The Working Group strongly encourages service providers, software developers and hardware manufacturers to keep informed about, implement, and use, privacy enhancing technologies in the field of biometric authentication. Data protection officers and privacy specialists should be involved at the early stages of considering biometric solutions and privacy impact assessments should be conducted at appropriate milestones throughout the project lifecycle.

[18] Y. Zhang, et al. „Fingerprints On Mobile Devices: Abusing and Leaking", Black Hat, August 2015, available at https://www.blackhat.com/docs/us-15/materials/us-15-Zhang-Fingerprints-On-Mobile-Devices-Abusing-And-Leaking-wp.pdf

[19] The "moral hazard" of assuming to be in full control of our own data, which may lead to incautious behaviors. See "Misplaced Confidences: Privacy and the Control Paradox" Laura Brandimarte, Alessandro Acquisti, George Loewenstein, In: Ninth Annual Workshop on the Economics of Information Security (WEIS), June 7-8 2010, Harvard University, Cambridge, MA

[20] Cf. https://www.enisa.europa.eu/publications/recommended-cryptographic-measures-securing-personal-data.

32. When biometric data are to be used as an authentication factor, it should not be in isolation in order to provide an appropriate level of identity assurance, and mitigate the risks of their acquisition by unauthorized parties.

33. In the design of a biometric authentication system, organisations should consider solutions that avoid storage of biometric templates in central databases and other repositories. Ideally, solutions should attempt to store biometric templates locally in a secure manner[21] (e.g., in an encapsulated storage device). Furthermore, it is important that authentication should also happen locally so that the biometric data (raw sensor data or the template) never leave the computing device.

34. Biometric systems should be designed such that the raw biometric data should be securely deleted once a biometrics template is generated unless there is a specific and proportionate requirement for ongoing retention. Biometric templates (and the biometric data) must be securely deleted when no longer necessary (e.g., when the user account is disabled or deleted). Hardware providers should offer ways to securely delete biometric templates and keying material from end consumer devices.

35. Use systems based on recognized standards, when possible. Standards typically undergo a fair amount of review and are often of higher quality and offer improved interoperability.

36. Documentation on relevant hardware and software components should be made available, when possible. This allows stakeholders in the supply chain to make informed decisions and react more quickly when security or privacy flaws are discovered. End users should be empowered to make informed privacy and security risk assessments.

37. Appropriate state-of-the-art physical, technical and organisational security measures must be implemented to protect against attacks on the system. When storing biometric templates, organisations should consider using specialized security modules[22]. This reduces the impact when the main operating system gets compromised. Effective protection against spoofing and falsification of biometrics samples must also be in place.

38. Service providers must, by default, restrict the amount of personal data stored and processed during enrolment and verification of the biometric data.

39. Service providers should inform their clients (i.e., the organisations procuring the authentication system) about the privacy and security characteristics of the biometric authentication service they utilise. This information should include details about the software and hardware manufacturer, the security measures in place, the storage modalities of the

[21] For example, as auxiliary data in the context of biometric encryption or as transformed data in the context of cancellable biometrics.

[22] For example the iOS Secure Enclave (https://support.apple.com/en-us/HT204587) or the Android Trusted Execution Environment (https://source.android.com/security/authentication/fingerprint-hal.html)

biometric data, the false acceptance rate and the false rejection rate, and the retention period of the biometric data.

40. The biometric system should be designed in such a way that it does not allow for users to be tracked through the use of different implementations of the system. In other words, the biometrics system must guarantee unlinkability of the stored data. This means that, for example, two providers offering a biometric authentication solution must not be able to correlate the actions of a user through the use of the authentication technology itself. This is especially important when one provider offers the same system to two or more different clients.

41. The biometrics system must be tested with realistic test data applicable to the situation where it will be deployed. Organisations must ensure that the performance and accuracy levels are appropriate throughout the lifetime of the system.

User Participation

42. Systems should be developed such that authentication with biometrics remains an active choice by the user and not a condition of use and that the user is fully aware when enrolment takes place. The Working Group strongly encourages service providers to provide users the possibility of using an alternative (non-biometric) authentication system that provides an appropriate level of security. It is also noteworthy that gaining legally valid consent for the processing of biometric data is hard to obtain in the absence of a workable alternative. This is even more important when consent is being sought in an employment context.

43. Individuals should be allowed to choose the provider of their authentication technology, whenever possible. This may allow security conscious individuals to select the standards-based technology of their choice and to re-use it across compatible online services without having to make additional financial investments and without carrying additional hardware tokens with them.

Operational Considerations

44. All stakeholders in the supply chain must react quickly to security or privacy flaws in the protocols and the hardware or software in use.

45. Service providers must make sure that security and privacy features of their products are activated by default and security and privacy mechanisms should be offered without prohibitive costs for the customer.

46. Service providers should offer federated access to their services as individual registration processes may be more time consuming when biometric profiles have to be generated. This

also allows users to re-use their existing identity provider without having to re-register at each site. Federated identity providers however must respect the need to limit the volume and linkability of data they store.

Users

47. Users of biometric services should take heed of the possible risks for security and privacy of the use of biometric authentication which are communicated to them by the service provider. They should also educate themselves about the security and privacy properties of the different services, and choose the services and service providers they use accordingly. Finally, they should make sure that existing security and privacy features of a service are activated before using the service and take advantage of an alternative mechanism to biometric authentication if they so choose.