Internationale Arbeitsgruppe
zum Datenschutz in der
Telekommunikation

675.53.18

Arbeitspapier zu Biometrie in der Online-Authentifizierung

60. Sitzung am 22. und 23. November 2016 in Berlin

- Übersetzung -

Einleitung

1. Das Management der Benutzeridentifizierung und des Zugangs zu Computersystemen ist von außerordentlicher Bedeutung, um die Sicherheit und die Funktionalität dieser Systeme sicherzustellen. Um Datenschutz und Datensicherheit zu gewährleisten, ist eine Zugangskontrolle erforderlich, damit sichergestellt wird, dass die richtigen Nutzer den richtigen Zugriff auf IT-Systeme und die dort gespeicherten persönlichen Daten erhalten. Eine kluge Abwägung der verschiedenen Facetten der Zugangskontrolle, d.h. der Identifikation, Authentifizierung und Autorisierung muss erfolgen, damit ein angemessenes Niveau von Sicherheit und Privatsphäre gewährleistet werden kann. Bei der Authentifizierung wird etwas, das mit der Person in Verbindung gebracht und durch sie kontrolliert wird (z. B. ein Passwort oder ein Token) eingesetzt, um eine behauptete Identität nachzuweisen. Im Vergleich hierzu wird bei der Identifizierung versucht, eine spezifische Person innerhalb einer Population anhand ihrer Eigenschaften herauszugreifen (z. B. bei einer Suche nach einer bestimmten Person in einer Menge).

2. Ein Beispiel für Authentifizierung: Wenn eine Person ein Gepäckstück bei einer Theatergarderobe abgibt, gibt sie sich als Eigentümer des Gepäckstückes zu erkennen. Keine weiteren Überprüfungen, etwa ob der anfängliche Eigentumsanspruch zutrifft, sind für das zuverlässige Funktionieren der Garderobe erforderlich. Um sicherzustellen, dass die rechtmäßigen Eigentümer ihre Gepäckstücke zurückerhalten, muss das Personal vor der Rückgabe den Anspruch einer Person auf ihr Eigentum verifizieren. Häufig wird in diesem Zusammenhang **etwas, das die Person hat**, überprüft und zwar ein nummerierter Token, der ausgegeben worden ist, als das Gepäckstück abgegeben wurde. Als häufigste Methode der Authentifizierung für Online-Dienste wird etwas genutzt, **das der Person bekannt ist,** wie z. B. ein Passwort, um die Identität (hier die Angabe des Benutzernamens) zu authentifizieren. Eine weitere Authentifizierungsmethode, die häufig als Biometrie bezeichnet wird, besteht darin, **etwas** zu überprüfen**, das die Person ist** (ein physikalisches oder physiologisches

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

E-Mail:
IWGDPT@datenschutz-berlin.de

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

Die Arbeitsgruppe wurde durch Datenschutzbeauftragte verschiedener Länder initiiert, um den Datenschutz in der Telekommunikation und den Telemedien zu verbessern.

Charakteristikum, z. B. ihr Gesicht) oder tut (ein verhaltensbezogenes Charakteristikum, z. B. ihre Unterschrift).

3. Verschiedene Authentifizierungsmethoden können kombiniert werden, um ein höheres Maß an Vertrauen in die Authentifizierung zu bieten oder um bekannten Bedrohungen und Schwachstellen zu begegnen. Ein typisches Beispiel ist die Verwendung einer PIN (etwas, das der Benutzer kennt) mit einer Kredit- oder Kundenkarte (etwas, das der Benutzer hat), um die Person als Besitzer des Bankkontos, das für den Kauf genutzt wird, zu authentifizieren. Die Auswahl der Authentifizierungsmethode, die für eine bestimmte Aufgabe erforderlich ist, oder der Verzicht darauf haben eine direkte Auswirkung auf das System, aber auch auf die Privatsphäre. Bei der Nutzung eines nummerierten Tokens in der Gepäckabgabe kann die Person anonym bleiben, aber es besteht ein Restrisiko, dass ein Betrüger die Tasche abholt. Durch die Nutzung eines Ticketdesigns, das extra für den Veranstaltungsort ausgegeben wird und den Vergleich des abgerissenen nummerierten Tickets mit der Nummer auf der Gepäckmarke der Tasche kann dieses Risiko als ausreichend gering angesehen werden, so dass die Benutzer kein Fingerabdrucksystem nutzen oder ein von einer Behörde ausgestelltes Ausweisdokument aushändigen müssen.

4. Passwörter haben als Methode, Nutzer als die Eigentümer eines Accounts zu authentifizieren, eine lange Geschichte in der IT. Sie sind für die Nutzer relativ bequem, da sie auf vielen verschiedenen Geräten genutzt werden können und einfach in die Online-Dienste zu integrieren sind.

5. Die weite Verbreitung von Online-Dienstleistungen bedeutet jedoch auch, dass eine Person Dutzende oder Hunderte von Nutzeraccounts haben kann. Folglich bringt die Geheimhaltung der Passwörter einige Herausforderungen mit sich, die dadurch entstehen, dass

    - Nutzer das gleiche Passwort auf verschiedenen Seiten benutzen;

    - Nutzer sich möglicherweise das Passwort mit Dritten teilen, um ihnen Zugang zu dem Account in ihrem Namen zu gestatten;

    - Passwörter häufig vergessen werden, was Zeit und ressourcenintensive Wiederherstellungsmechanismen erfordert, die unsicher und anfällig für Angriffe sein können;

    - ein Nutzer mit einer Vielzahl von Richtlinien konfrontiert werden kann, die Passwörter mit unterschiedlicher Länge und Zusammensetzung erfordern oder regelmäßige Änderungen erzwingen[1];

    - Passwörter häufig unsicher gespeichert werden und

    - Passwörter auf andere Art und Weise kompromittiert werden können (z. B. durch Phishing).

---

1 Empfehlungen der letzten Zeit legen nahe, dass regelmäßige Passwortänderungen zu einer Verminderung der Sicherheit der Passwörter führen können, da die Nutzer Passwörter wählen, an die sie sich leichter erinnern können, vgl. https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach, https://www.cs.unc.edu/~reiter/papers/2010/CCS.pdf, und http://arstechnica.com/security/2016/08/frequent-password-changes-are-the-enemy-of-security-ftc-technologist-says/

6. Als Folge ersetzen mehr und mehr Online-Dienste passwortbasierte Authentifizierung oder sie ergänzen sie mit einer sogenannten mehrstufigen Authentifizierung. Gängige Technologien, die eine mehrstufige Authentifizierung nutzen, bedienen sich

   - eines Tokens oder einer App für Einmal-Passwörter,
   - vertrauenswürdiger Geräte (wie z. B. Chipcards) oder
   - der Biometrie.

7. Die Nutzung von Biometrie bei der Online-Authentifizierung bietet die Möglichkeit, etwas gegen einige der Mängel der jetzigen passwortbasierten Authentifizierung zu tun. Wie dieses Arbeitspapier jedoch im Weiteren beschreibt, muss dieser Vorteil sorgfältig gegen die Datenschutzrisiken, die als Folge entstehen können, abgewogen werden.

8. Der Zweck dieses Arbeitspapieres besteht nicht darin aufzuzeigen, wann Biometrie als ein Faktor in der Online-Authentifizierung genutzt werden kann. Dies ist eine Entscheidung, die in einer Datenschutz-Folgenabschätzung dokumentiert werden sollte, die in der Planungsphase eines Projektes durchgeführt wird und während der gesamten Lebensdauer des IT-Systems aktualisiert werden muss. Dieses Arbeitspapier will auf die Risiken für die Privatsphäre, die bei der Einführung von Biometrie und ihrer Nutzung für die Authentifizierung entstehen, und auf Methoden hinweisen, wie diese Risiken angemessen gemanagt werden können.

Biometrie

9. Der Begriff *Biometrie* ist in der ISO/IEC 2382:2015[2] definiert als

   “die Nutzung verschiedener Attribute, die einzigartige persönliche Merkmale wiedergeben, wie z. B. ein Fingerabdruck, ein Scan der Adernstruktur der Augennetzhaut oder Voiceprinting, um die Identität einer Person zu validieren.“”[3]

10. Die Einzigartigkeit der genutzten Merkmale (innerhalb der Nutzergruppe) und die relative Einfachheit der Anwendung führen dazu, dass Biometrie zu einem attraktiven Kandidaten für die Authentifizierung geworden ist. Bei der Anwendung von Biometrie bei der Authentifizierung handelt es sich nicht um einen neuen Trend, sondern eher um eine Weiterentwicklung der Technik wie der Analyse von Fingerabdrücken, die bereits lange in der Strafverfolgung für die Identifizierung eingesetzt wird. Heute werden biometrische Sensoren allerdings auch in Verbrauchergeräte eingebaut. Am häufigsten kommen Fingerabdrucksensoren in Smartphones, Tablets und Laptops zum Einsatz. Zur Gesichts- und Stimmerkennung können ferner die in diese Geräte eingebauten Kameras und Mikorphone genutzt werden.

11. Um einen Nutzer mit einem passwortbasierten System zu authentifizieren, wird durch eine einfache Rechenoperation verifiziert, ob der Nutzer das richtige Passwort verwendet hat. Dies führt zu einer unwiderlegbaren Ja- oder Nein-Antwort – ein Passwort ist entweder korrekt oder

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

3 Die Verordnung (EU) des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr definiert biometrische Daten als „mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten“.

nicht. Biometrische Authentifizierung auf der anderen Seite folgt im Allgemeinen einer wahrscheinlichkeitstheoretischen Methode, bei der zwei Templates miteinander verglichen werden und eine prozentuale Übereinstimmung oder eine Vertrauenspunktzahl generiert wird. Ein Ergebnis oberhalb einer bestimmten Schwelle bestimmt, ob der Vergleich als eine positive Übereinstimmung gewertet werden kann oder nicht.

12. Um die Genauigkeit zu verbessern und die Möglichkeit für Spoofing zu verringern, kann das Authentifizierungssystem eine Mischung von mehr als einem biometrischen Charakteristikum benutzen oder biometrische und nicht-biometrische Daten der gleichen Person kombinieren. Abhängig vom Szenario kann es für eine erfolgreiche Authentifizierung notwendig sein, einen positiven Vergleich über alle zur Verfügung gestellten Daten (biometrische und nicht-biometrische) zu erhalten, dies trifft aber nicht immer zu.

13. Die Erfassung der biometrischen Merkmale eines Nutzers setzt oft den Einsatz dedizierter Geräte oder Komponenten voraus, die in einen PC, Laptop oder Smartphone eingebaut sind, z. B. einen Fingerabdruckleser am Smartphone, oder auch spezialisierte Geräte wie Venenscanner, wie sie gelegentlich bereits in Bankautomaten zum Einsatz kommen. Andere Typen von biometrischen Daten können mit generischeren Aufnahmegeräten wie Kameras oder Mikrophonen gewonnen und lokal oder durch einen Dritten weiterverarbeitet werden.

14. Nicht nur die Verbraucher interessieren sich mehr und mehr für die Verwendung von Biometrie als einer bequemen Authentifizierungsmethode, sondern auch Regierungen und Organisationen. So sieht z. B. die eIDAS-Verordnung der Europäischen Union (Verordnung über elektronische Identifizierung und Vertrauensdienste im internen Markt)[4] die optionale Nutzung von Biometrie vor, um die Anwendung elektronischer Signaturen in ganz Europa zu unterstützen.

15. Fortgeschrittene Technologien zum Schutz der Privatsphäre schließen biometrische Verschlüsselung[5] und widerrufbare Biometrie[6] ein. Beide Techniken bieten verschiedene Vorteile gegenüber traditionellen biometrischen Systemen, im Besonderen die Widerrufbarkeit der gespeicherten biometrischen Daten. Außerdem wurde vor kurzem ein aus der Ferne einsetzbares biometrisches Authentifizierungsprotokoll vorgestellt[7], das gegenüber fortgeschrittenen Sicherheitsbedrohungen Widerstand zu leisten vermag. Dieses Protokoll bietet solange Sicherheit, wie höchstens entweder das Gerät des Nutzers oder der Server kompromittiert wurde (aber nicht, wenn dies bei beiden geschieht).

---

4 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG, http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32014R0910&from=EN

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

6 Widerrufbare Biometrie fügt dem gespeicherten Template eine wiederholbare Distorsion zu, vgl. z. B. Ruud M. Bolle, Jonathan H. Connell, und 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

16. Aktivitäten auf dem Feld der Standardisierung innerhalb der FIDO Alliance[8] und der ISO[9] sowie Verhaltensregeln wie die Privacy Trust Mark[10] des Biometrics Institute zielen auf Themen wie Sicherheit und Privatsphäre ab, indem sie robuste Authentifizierungsmechanismen fördern.

Datenschutzrisiken

17. Die Datenschutzrisiken in diesem Bereich wurden bereits durch verschiedene Datenschutzbeauftragte dokumentiert, einschließlich derer in der EU (2003 [11] und 2012[12],[13]), Kanada[14] und den USA[15].

18. Es ist darauf hinzuweisen, dass im Allgemeinen verschiedene biometrische Systeme sich sehr unterschiedlich auf Datenschutz und Schutz der Privatsphäre auswirken und daher einen unterschiedlichen Ansatz im Umgang mit diesen Risiken erforderlich machen. So kann Gesichtserkennung bei Personen eingesetzt werden, die nicht wissen, dass sie von diesem System betroffen sind, während Fingerabdrucksysteme normalerweise die aktive Beteiligung der Person erforderlich machen (wobei diese Beteiligung nicht mit ihrer Zustimmung gleichzusetzen ist). Ersteres kann daher größere Anstrengungen erforderlich machen, um die Nutzer über den Betrieb des Systems zu informieren.

19. Bestimmte biometrische Daten können von anderen ohne das Wissen des Einzelnen erworben werden – wir hinterlassen unsere Fingerabdrücke auf vielen Oberflächen, unsere Gesichter können erkannt werden, die entsprechenden Fotos können gespeichert und leicht weiterverarbeitet werden. Im Gegensatz zu Passwörtern sind biometrische Daten keine Geheimnisse und nicht einfach zu ändern oder zu widerrufen. Die Personen sind sich im Allgemeinen der Gefahren bewusst, die mit der Offenlegung eines Passwortes verbunden sind, aber man kann nur schwer verhindern, dass das Gesicht oder die Stimme aufgenommen wird.

20. Die Tatsache, dass biometrische Authentifizierung auf Wahrscheinlichkeitsaussagen beruht (da bei dem Abgleich zwischen ermitteltem biometrsichem Merkmal und gespeichertem Template zufällige Störungen beeinflussen, ob es ein Match gibt), bedeutet, dass die Möglichkeit eines Irrtums besteht. Ein falsches negatives Match wird dazu führen, dass die Identiät der Person nicht bestätigt und ihr möglicherweise der Zugang zum System verweigert wird. Umgekehrt führt ein falsches positives Match dazu, dass eine Person fälschlicherweise authentifiziert wird oder ein Betrüger das System erfolgreich täuscht und dadurch unautorisierten Zugang zu dem System erhält. Die Fehlerraten müssen ein Gleichgewicht zwischen Benutzerfreundlichkeit und

---

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

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

Sicherheit schaffen. Wenn die Schwelle zu hoch angesetzt ist, kann dies zu einer höheren Genauigkeit führen, aber mit einem damit verbundenen Anstieg an legitimen Nutzern, die nicht akzeptiert werden und umgekehrt. Dadurch kann die Versuchung entstehen, in einem unbedachten Kompromiss zwischen Benutzerfreundlichkeit und Performanz die Genauigkeitsrate zu senken, um so falsche Ablehnungsraten zu reduzieren, oder zu versäumen, das System unter realen Arbeitsbedingungen auf negative Auswirkungen auf die Sicherheit und Privatsphäre zu testen.

21. Bestimmte Geräte oder Komponenten, die in einem PC, Laptop oder Smartphone eingebaut sind, haben möglicherweise aufgrund des Drucks, die Produktionskosten zu senken, keine hohe Qualität. Diese Low-End-Sensoren können eine höhere Fehlerquote produzieren mit größeren Auswirkungen auf die Sicherheit und Privatsphäre für den Endverbraucher. Einige Systeme können durch gestohlene oder gefälschte biometrische Merkmale[16] getäuscht werden, falls mangelhafte Tests diese Fälschungen nicht zurückweisen.

22. Falls eine Person nicht in der Lage ist, eine verlässliches biometrisches Datum zu hinterlegen (z. B. durch abgenutzte oder beschädigte Fingerspitzen) oder weil sie aus einem anderen Grund nicht in der Lage oder nicht gewillt ist, das Aufnahmegerät zu nutzen (z. B. wenn das Gesicht durch einen Schleier, einen Schal oder Ähnliches bedeckt ist), kann dies zu einer regelmäßigen Zugangsverweigerung führen.

23. Biometrische Merkmale sind ebenso wie Passwörter nicht immun gegenüber unberechtigten Offenlegungen personenbezogener Daten. Das Hacken von mehr als 5,6 Millionen Fingerabdrücken aus dem Office of Personnel Management (OPM)[17] im Juni 2015 zeigt die potentielle Gefahr von zentral gespeicherten Anmeldeinformationen. Dieser Angriff war besonders ernst, da das OPM die Originalfingerabdrücke gespeichert hatte, statt Templates oder die digitale Darstellung der biometrischen Daten.

24. Biometrische Daten sind dauerhaft und können nicht leicht geändert oder erneut genutzt werden, wie dies der Fall bei einem unautorisierten Zugriff oder der Offenlegung von Passwörtern, Keycards oder Tokens ist. Während die Liste aller möglichen Passwörter, aus der eine Person wählen kann, unglaublich lang ist, gibt es eine niedrige und begrenzte Anzahl von Quellen, die für biometrische Daten eines Einzelnen genutzt werden können (d. h. zwei Retinas, 10 Fingerabdrücke und ein Gesicht). Daher gibt es ein reales Risiko, dass Nutzeraccounts bei verschiedenen Diensten verlinkt werden können (wenn bei ihnen derselbe Fingerabdruck hinterlegt worden ist). Dies spiegelt die gegenwärtigen Probleme der erneuten Verwendung von Passwörtern wider.

25. Die Verwendung von biometrischen Daten für die Authentifizierung kann die Möglichkeit der Nutzer, ein pseudonymes Konto zu nutzen, verringern. Dies reduziert die Verfügbarkeit von Dienstleistungen für Nutzer, die ihre wahre Identität dem Dienstleister nicht offenbaren möchten, oder Nutzer, die unterschiedliche Accounts für verschiedene Zusammenhänge (z. B. verschiedene Accounts für berufliche und private Zwecke) beibehalten möchten.

26. Die Verhinderung großflächiger Angriffe wie z.B. des unautorisierten Zugriffs auf Datenbanken, die biometrische Templates speichern, stand ebenso wie die Erleichterung der Anwendung biometrischer Systeme im Mittelpunkt der jüngsten Standardisierungsbemühungen.

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/ - Verwaltung des Öffentlichen Dienstes

Datenschutzfreundlichere biometrische Systeme speichern biometrische Templates lokal auf den Geräten der Endnutzer wie z. B. einem Smartphone oder Tablet. Während diese Lösung es erforderlich macht, dass der Angreifer eine große Anzahl von Geräten eines nach dem anderen angreifen muss, muss auch bei der Implementierung dieser Lösung mit Bedacht vorgegangen werden, wie ein Sicherheitszwischenfall zeigte, bei dem es um Mobiltelefone ging, in denen biometrische Templates (Fingerabdruck) unverschlüsselt auf dem Filesystem[18] gespeichert wurden. Durch die lokale Speicherung von Templates auf den Geräten der Endnutzer werden sie darüber hinaus den Vorgehensweisen der Endnutzer selbst ausgesetzt[19], die ebenso wenig sicher sind.

27. Einige Hersteller biometrischer Systeme verlassen sich immer noch auf die Geheimhaltung der Algorithmen, die sie einsetzen, um Sicherheit und Vertrauen zu gewährleisten. Proprietäre Algorithmen und Technologien, die auf Geheimhaltung basieren, sind jedoch im Allgemeinen weniger vertrauenswürdig als diejenigen, die von Seiten Dritter überprüft wurden oder auf weithin akzeptierten Standards basieren[20].

Empfehlungen

28. Mit Blick auf das oben Gesagte gibt die Arbeitsgruppe den Interessenvertretern folgende Empfehlungen:

Regulierungsbehörden, Gesetzgeber und Aufsichtsbehörden

29. Regulierungsbehörden auf regionaler, nationaler und internationaler Ebene sollten die Entwicklung von datenschutzfreundlichen Authentifizierungstechnologien, die die Defizite der existierenden passwortbasierten Authentifizierungstechnologien beheben, unterstützen. Bei regulatorischen Vorgaben und der Formulierung von Standards sollte darauf geachtet werden, dass die in diesem Papier identifizierten Datenschutzrisiken adressiert und auch alle anderen Risiken, die aus der Anwendung neuer Authentifizierungstechnologien entstehen, berücksichtigt werden, besonders, soweit es um sich um biometrische Technologien handelt.

30. Proaktive Vorgehensweisen des Datenschutzes wie z. B. die Durchführung von Datenschutz-Folgeabschätzungen, sowie der Datenschutz durch Technikgestaltung und Voreinstellung sollten gefördert und durch Material zur Bewusstseinsbildung unterstützt werden. Diese Vorgehnsweisen könnten durch Gesetze in bestimmten Rechtsbereichen vorgeschrieben werden.

Dienstleister für biometrische Authentifizierung, Software-Entwickler und Hardwarehersteller

31. Die Arbeitsgruppe fordert Dienstleister, Software-Entwickler und Hardwarehersteller nachdrücklich auf, sich über datenschutzfördernde Technologien im Bereich Biometrie zu informieren, sie zu implementieren und anzuwenden. Datenschutzbeauftragte und Daten-

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 Das "moralische Risiko" anzunehmen, dass wir die volle Kontrolle über unsere Daten haben, kann zu unvorsichtigem Verhalten führen. Vgl. "Misplaced Confidences: Privacy and the Control Paradox" von 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.

schutzexperten sollten zu einem frühen Zeitpunkt bei Überlegungen zu biometrischen Lösungen eingebunden werden und Datenschutz-Folgeabschätzungen sollten an geeigneten Meilensteinen während der gesamten Lebensdauer des Projekts durchgeführt werden.

32. Falls biometrische Daten als Authentifizierungsfaktor genutzt werden, sollte dies nicht isoliert passieren, um ein angemessenes Niveau des Identitätsnachweises zur Verfügung zu stellen und die Risiken zu mindern, dass nicht autorisierte Dritte sich Zugang verschaffen.

33. Bei der Konzeption des biometrischen Authentifizierungssystems sollten die Anwender Lösungen in Betracht ziehen, die die Speicherung der biometrischen Templates in zentralen Datenbanken und anderen Datenspeichern verhindern. Idealerweise sollte bei den Lösungen versucht werden, die biometrischen Templates lokal in einer sicheren Art und Weise zu speichern[21] (z. B. in einem gekapselten Speichergerät). Darüber hinaus ist es auch wichtig, dass die Authentifizierung lokal erfolgt, so dass keine biometrischen Daten (weder Sensor-Rohdaten noch Templates) das Computergerät verlassen.

34. Biometrische Systeme sollten so konzipiert sein, dass die biometrischen Rohdaten nach Generierung des biometrischen Template gesichert gelöscht werden können, es sei denn, dass sie wegen spezifischer und angemessener Gründe nicht gelöscht werden dürfen. Biometrische Templates (und die biometrischen Daten) müssen sicher gelöscht werden, wenn sie nicht länger benötigt werden (z. B. wenn der Nutzeraccount deaktiviert oder gelöscht wird). Hardwarehersteller sollten Möglichkeiten für eine sichere Löschung von biometrischen Templates zur Verfügung stellen und das biometrische Material in Endverbrauchergeräten verschlüsseln.

35. Es sollten möglichst Systeme zum Einsatz kommen, die auf anerkannten Standards basieren. Standards werden typischerweise vielen Überprüfungen unterzogen und bieten zudem eine verbesserte Interoperabilität.

36. Die Dokumentation aller relevanten Hardware- und Softwarekomponenten sollte möglichst zur Verfügung gestellt werden. Dies gestattet es den Interessenvertretern in der Lieferkette, informierte Entscheidungen zu treffen und schneller zu reagieren, wenn Sicherheits- oder Datenschutzfehler entdeckt werden. Endverbraucher sollten in die Lage versetzt werden, informierte Datenschutz- und Sicherheitsrisikobewertungen zu treffen.

37. Geeignete physikalische, technische und organisatorische Sicherheitsmaßnahmen, die auf dem neuesten Stand der Technik sind, müssen implementiert werden, um Schutz gegen Angriffe auf das System zu bieten. Bei der Speicherung biometrischer Templates sollten Organisationen die Nutzung spezialisierter Sicherheitsmodule[22] in Erwägung ziehen. Das reduziert die negativen Auswirkungen in dem Fall, dass das Hauptbetriebssystem erfolgreich angegriffen wurde. Effektiver Schutz gegen Spoofing und Fälschung der biometrischen Samples müssen ebenfalls vorhanden sein.

---

21 Zum Beispiel als Hilfsdaten im Kontext der biometrischen Verschlüsselung oder als transformierte Daten im Kontext der widerrufbaren Biometrie.

22 Zum Beispiel die iOS Secure Enclave (https://support.apple.com/en-us/HT204587) oder das Android Trusted Execution Environment (https://source.android.com/security/authentication/fingerprint-hal.html)

38. Dienstleister müssen standardmäßig die Menge der persönlichen Daten begrenzen, die gespeichert und während der Anmeldung und der Verifizierung der biometrischen Daten bearbeitet werden.

39. Dienstleister sollten ihre Kunden (d. h. die Organisationen, die das Authentifizierungssystem beschaffen) über die Datenschutzeigenschaften und die Sicherheitscharakteristika des biometrischen Authentifizierungsservices informieren, den sie nutzen. Diese Information sollte Einzelheiten über die Soft- und Hardwarehersteller, die vorhandenen Sicherheitsmaßnahmen, die Speichermodalitäten der biometrischen Daten, die Falschakzeptanzrate bzw. Falschrückweisungsrate sowie Angaben über die Aufbewahrungszeit biometrischer Daten enthalten.

40. Das biometrische System sollte so beschaffen sein, dass die Handlungen der Nutzer nicht durch die Anwendung verschiedener Implementationen eines biometrischen Authentifizierungssystems nachverfolgt werden können. Mit anderen Worten, das biometrische System muss die Unverkettbarkeit der gespeicherten Daten sicherstellen. Das bedeutet z. B., dass zwei Dienstleister, die biometrische Authentifizierungslösungen anbieten, nicht in der Lage sein dürfen, verschiedene Aktionen eines Anwenders durch die Anwendung der Authentifizierungstechnologie selbst zu korrelieren. Dies ist besonders wichtig, wenn ein Provider das gleiche System zwei oder mehreren unterschiedlichen Kunden anbietet.

41. Das biometrische System muss mit realistischen Testdaten in der Situation getestet werden, die für den Einsatz geplant ist. Organisationen müssen sicherstellen, dass die Performanz und die Genauigkeitsgrade während der gesamten Lebensdauer des Systems angemessen bleiben.

Nutzerbeteiligung

42. Es müssen Systeme entwickelt werden, die dem Nutzer eine aktive Wahl bei der Authentifizierung mit Hilfe von Biometrie lassen und ihn nicht dazu zwingen, sie anzuwenden. Die Aufnahme in ein biometrisches Authentifizierungssystem muss stets ein bewusster Akt sein. Die Arbeitsgruppe fordert Dienstleister nachdrücklich dazu auf, ein alternatives (nichtbiometrisches) Authentifikationssystem für Anwender bereitzustellen, das ein angemessenes Sicherheitsniveau bietet. Man sollte außerdem beachten, dass es schwierig sein dürfte, eine rechtlich wirksame Einwilligung zu erhalten, falls keine praktikable Alternative zur Verfügung steht. Dies ist noch wichtiger, wenn die Einwilligung im Beschäftigungszusammenhang eingeholt werden soll.

43. Es sollte den Nutzern gestattet sein, den Dienstleister für ihre Authentifizierungstechnologie, wann immer dies möglich ist, auszuwählen. Dies gestattet es sicherheitsbewussten Nutzern, eine standardbasierte Technologie auszuwählen und sie in kompatiblen Onlineservices wiederzuverwenden, ohne weitere finanzielle Ausgaben zu haben und ohne zusätzliche Hardware-Token mit sich herumzutragen.

Überlegungen für den Betrieb

44. Alle Teilnehmer der Lieferkette müssen schnell auf Sicherheits- oder Datenschutzmängel in den Protokollen und der angewendeten Hardware oder Software reagieren.

45. Dienstleister müssen sicherstellen, dass Sicherheits- und Datenschutzfeatures ihrer Produkte standardmäßig aktiviert und Sicherheits- und Datenschutzmechanismen ohne überhöhte Kosten für den Kunden angeboten werden.

46. Dienstleister sollten föderierten Zugriff auf ihre Dienste anbieten, da individuelle Registrierungsprozesse zeitaufwändiger sein könnten, wenn biometrische Profile generiert werden müssen. Dies gestattet es den Anwendern, ihren existierenden Identitätsprovider weiterzunutzen, ohne sich bei jeder Site registrieren zu müssen. Föderierte Identitätsprovider müssen jedoch die Notwendigkeit respektieren, den Umfang und die Verkettbarkeit der Daten, die sie speichern, zu begrenzen.

Anwender

47. Nutzer von biometrischen Dienstleistungen sollten die mögliche Gefährdung des Datenschutzes und den Schutz der Privatsphäre bei der Verwendung biometrischer Authentifizierung ernst nehmen, die ihnen von Seiten des Dienstleisters übermittelt wurden. Sie sollten sich auch über die Sicherheits- und Datenschutzeigenschaften der verschiedenen Dienstleister informieren und die Dienstleistungen und Dienstleister, die sie nutzen, entsprechend auswählen. Schließlich sollten sie sich vergewissern, dass die existierenden Sicherheits- und Datenschutzfeatures einer Dienstleistung aktiviert sind, bevor sie den Service nutzen, und sich einen alternativen Mechanismus statt einer biometrischen Authentifizierung zunutze machen, falls sie dies wünschen.