TeleTrusT Deutschland e.V.

Der IT-Sicherheitsverband.

Biometrische Authentisierung

Christoph Busch
Hanns-Wilhelm Heibey
Gisela Quiring-Kock
Thomas T. Kniess
Hildegard Herzog

Impressum

Herausgeber:

TeleTrusT Deutschland e.V.
Chausseestraße 17
10115 Berlin
Tel.: +49 30 400 54 306
Fax: +49 30 400 54 311
E-Mail: info@ TeleTrusT.de
http://www.TeleTrusT.de

Herstellung:

DATEV eG, Nürnberg

2. Auflage

© 2010 TeleTrusT

In der modernen Gesellschaft steigt der Bedarf an zuverlässiger Personenidentifizierungstechnologie. In diesem Zusammenhang gewinnt die Biometrie an Bedeutung, da sie Personenidentifikation mit eindeutigen und teilweise unveränderbaren bzw. über einen langen Zeitraum stabilen Merkmalen eines Menschen verknüpft. Die "Biometrische Authentisierung" folgt dabei anderen Maßgaben als klassische Identifizierungsverfahren. In der vorliegenden Publikation widmen sich die Autoren der Abwägung von Vor- und Nachteilen biometrischer Authentisierung, z.B. im Verhältnis zu Passwörtern und mit Blick auf Datenschutzimplikationen.

ANMERKUNG: Unbeschadet der in dieser Veröffentlichung verwendeten, teilweise abweichenden Definitionen sei auf das aktuelle ISO/JTC1/SC37 "Harmonized Biometric Vocabulary" hingewiesen. Diese ISO-Definitionen sind einsehbar unter: http://www.3dface.org/media/vocabulary.html.

Dr. Holger Mühlbauer
TeleTrusT Deutschland e.V.

PROF. DR. CHRISTOPH BUSCH[1]

Biometrische Erkennung

Einführung

Seit dem Herbst 2005 werden biometrische Daten in Reisepässen integriert. Das digitale Passbild erlaubt in Zukunft dem Grenzbeamten den visuellen Vergleich mit dem Passbesitzer und dient auch zur automatischen biometrischen Erkennung. In Portugal wurde im Jahr 2007 ein erstes Gesichtserkennungssystem in Europa an einer Schengen-Außengrenze in Betrieb genommen [rapid2008]. Eine vergleichbare Installation ist seit dem letzten Herbst am Frankfurter Flughafen in Betrieb. Schon seit 2004 konnten vorab registrierte Viel-Flieger mit einem Iris-Erkennungssystem in Frankfurt die Grenze in einer biometrischen Kontrollspur passieren. Nun wird die Nutzung von Biometrie jedem EU-Bürger ermöglicht, der einen biometrischen Reisepass besitzt. Dieser Beitrag beleuchtet die Methoden zur biometrischen Erkennung und führt in die Nutzungsmöglichkeiten und Herausforderungen ein.

Funktionsweise der biometrischen Erkennung

Unter Biometrie versteht man ein Messverfahren zur Wiedererkennung von Personen. Die Internationale Standardisierung definiert den Begriff *biometrics* wie folgt: "*automated recognition of individuals based on their behavioural and biological characteristics*" [iso-sc37]. Biometrische Verfahren analysieren demnach das Verhalten des Menschen und/oder eine Eigenschaft der biologischen Charakteristika. Die biologischen Charakteristika gliedern sich einerseits in anatomische Charakteristika, die geprägt werden durch Strukturen des Körpers, und andererseits in physiologische Charakteristika, die geprägt werden durch Funktionen des Körpers, wie beispielsweise die Stimme.

Der Vorgang der biometrischen Authentisierung liefert eine eindeutige Verknüpfung einer Person mit ihrer Identität unabhängig davon, wo diese Identität gespeichert ist. Der Vorgang der biometrischen Wiedererkennung lässt sich in die folgenden Schritte untergliedern:

- Erfassung der biologischen Charakteristika mit geeigneten Sensoren (Kamera, Mikrofon etc.) und Speicherung als digitale Repräsentation
- Vorverarbeitung zur Datenverbesserung oder -bereinigung
- Merkmalsextraktion zur signifikanten Beschreibung der Muster
- Vergleich der Merkmale mit den Referenzdaten.

Der Vorgang bedingt, dass grundsätzlich eine Person vorab eingelernt wurde (Enrolment), um die notwendigen Referenzdaten zu bilden. Biometrische Systeme können als Verifikationssysteme oder als Identifikationssysteme ausgelegt sein. Bei einem Verifikationssystem gibt der Nutzer eine Identität vor, zu der im System eine Referenz vorliegt. Sofern biometrische Systeme mit einem authentischen

[1] Fraunhofer IGD / Hochschule Darmstadt; Leiter der TeleTrusT-Arbeitsgruppe "Biometrie"

Dokument kombiniert werden, kann die biometrische Referenz (z.B. Passfoto) auf diesem Dokument abgelegt sein. Zum Zeitpunkt der Verifikation wird ein Vergleich mit genau diesem einen Referenzbild durchgeführt (1:1 Vergleich). Bei einem Identifikationssystem hingegen wird das erfasste Bild mit vielen eingelernten Bildern verglichen und aus dieser Menge das am besten passende Muster ermittelt (1:n Vergleich). Die Ähnlichkeit zwischen beiden Bildern muss jedoch ein definiertes Mindestmass erreichen, damit eine zuverlässige Zuordnung der mit dem Referenzbild verbundenen Identität vorgenommen werden kann.

Die Gesichtserkennung ist das biometrische Verfahren, das der Mensch selbst am häufigsten zur Erkennung verwendet. Während dabei jedoch intuitiv Kontextinformationen wie Körperform und -größe zusätzlich analysiert werden, stehen diese Parameter einem computergestützten Erkennungsverfahren zunächst nicht zur Verfügung. Die in der biometrischen Gesichtserkennung bislang eingesetzten Systeme verwenden im Normalfall eine Fotokamera, um zweidimensionale Frontalbilder zu erfassen. Systeme, die auf diesen Sensoren aufbauen, verarbeiten das 2D-Bild und müssen zunächst das eigentliche Gesicht im Kamerabild lokalisieren und herausfiltern. Ein Frisurwechsel, aber auch Bärte und Brillen können die Aufgabe für den Gesichtsfindungsalgorithmus erschweren. Bei der zweidimensionalen Gesichtserkennung ist es unerlässlich, dass das Bildmaterial in sehr guter Bildqualität vorliegt. Werden Bildqualitätskriterien nicht erfüllt, muss mit einer schwachen Erkennungsleistung des biometrischen Systems gerechnet werden.

Die Einhaltung aller Kriterien sowohl beim Enrolment als auch beim Versuch der Wiedererkennung ist schwer herzustellen: Nur selten werden die Gesichtsausrichtung (Pose), der Gesichtsausdruck (Mimik) und die Beleuchtungssituation identisch sein.

Der Vergleichsalgorithmus in einem Gesichtserkennungssystem, der letztlich die Authentisierungsprobe mit dem Referenzbild vergleicht, hat keine Kenntnis darüber wie die Probe (*biometric probe sample*) entstanden ist. Woher soll der Algorithmus wissen, ob eine lebende Person vor der Kamera steht, ein gedrucktes Foto vor die Kamera gehalten wird oder gar ein Mobiltelefon, auf dessen Display das Bild einer Person dargestellt wird? Es ist keine große Überraschung, wenn ich den Algorithmus in einem Zugangskontrollsystem mit einem Foto von meinem Gesicht davon überzeugen kann, dass dieses Foto und die in der Datenbank hinterlegte biometrische Referenz von ein und derselben Person stammen. Das ist die Aufgabe des Algorithmus. Viele Systeme können keine Lebenderkennung durchführen oder beschränken sich auf die Auswertung einer Bildfolge. Viele Gesichtserkennungssysteme verfügen nicht über hinreichende Mechanismen, um eine Lebenderkennung zu gewährleisten und sind daher in nicht-überwachten Umgebungen nur bedingt einsetzbar. Grundsätzlich kann man der 3D-Gesichtserkennung eine verbesserte Robustheit hinsichtlich der Überwindungsangriffe attestieren, da ein Replikat deutlich schwieriger zu erstellen ist. Schon die Beschaffung der 3D-Geometrie ist ohne Kooperation der zu replizierenden "Zielperson" mit erheblichem Aufwand verbunden. Die Produktion eines 3D-Printouts ist zwar technisch beispielsweise mit einem Stereo-Lithographieverfahren möglich – ein derart hergestellter künstlicher Kopf könnte jedoch mit einfachen Lebender-

kennungsmechanismen automatisch detektiert werden, was die Wahrscheinlichkeit eines erfolgreichen Angriffs reduziert.

Forschung und Entwicklung

Ein Hauptziel der aktuellen Forschung und Entwicklung ist es, die Leistungsfähigkeit der biometrischen Verfahren zu verbessern. Ein Forschungsbestreben ist es, multibiometrische Systeme zu entwickeln, die verschiedene biometrische Charakteristika in einer Aufnahme erfassen - beispielsweise das Gesichtsbild und die Geschichtsgeometrie (3D-Scan) mit einem kombinierten Aufnahme-System [3dface2006]. Ein Entscheidungssystem verbindet die Ähnlichkeitswerte und führt zu einer stabileren Aussage. Zudem wird durch gleichzeitige 3D-Gesichtserkennung eine verbesserte Robustheit hinsichtlich eines etwaigen Überwindungsangriffs erreicht.

Eine weitere relevante Frage bei der Nutzung eines biometrischen Systems ist die sichere und datenschutzfreundliche Speicherung der biometrischen Daten. Biometrische Daten sind im Sinne der geltenden Datenschutzregelungen personenbezogene Daten und daher einem besonderen Schutz zu unterwerfen. Als Schutzmaßnahmen bieten sich dabei grundsätzlich zwei Möglichkeiten an: Oft wird zur Speicherung der biometrischen Referenzdaten ein Token (z.B. RFID-Chip) eingesetzt, wie dies beim ePass der Fall ist. Wünschenswert wäre es, wenn bei der Wiedererkennung der Vergleich zwischen der biometrischen Probe und den Referenzdaten gleich direkt in dieser Karte unter Kontrolle der betroffenen Person durchgeführt werden könnte. Die Karte liefert in diesem Fall ein positives oder negatives Ergebnis an die Anwendung zurück, ohne dass die Anwendung Zugriff auf die Referenzdaten erhält.

Alternativ werden die Referenzdaten in einer zentralen Datenbank gespeichert. Dies wird in nichthoheitlichen Anwendungen mitunter umgesetzt, um eine kartenlose Authentisierung zu ermöglichen. Mit der Speicherung von Samples in einer Datenbank werden einige potenzielle Probleme assoziiert: Diese reichen vom Identitätsdiebstahl bis zu dem Bedürfnis, gespeicherte Referenzdaten „zurückrufen“ zu können. Lösungsmöglichkeiten für die Probleme wurden und werden entwickelt und sind in einem von TeleTrusT herausgegebenen White-Paper *Datenschutz in der Biometrie* publiziert [ttt2008].

Weitere Informationen

Die interdisziplinäre Diskussion über technische Machbarkeit und datenschutzfreundliche Gestaltung von biometrischen Systemen wird in Deutschland im Wesentlichen in drei Fachverbänden geführt. Die TeleTrusT-Arbeitsgruppe "Biometrie" diskutiert mögliche Anwendungen und Datenschutz-Aspekte [ttt2009]. Die Fachgruppe BIOSIG der Gesellschaft für Informatik bietet eine Plattform für wissenschaftlichen Austausch [biosig2009]. Hier werden mögliche Lösungen für die Herausforderungen für biometrische Systeme gesucht und vorgestellt. Diese sind beispielsweise Unterschiede in der Ausrichtung des Gesichts (*Pose*), Lichtveränderungen und andere Störfaktoren die Bildqualität beeinträchtigen können. Biometrische Standards werden im Normenausschuss NIA des DIN entwickelt [din2009]. Auch wenn biometrische Systeme derzeit noch kaum verbreitet sind, mittelfristig wird jeder Bundes-

bürger mit der Biometrie in Berührung geraten. In den kommenden Jahren werden die Grenzkontrollpunkte Schritt für Schritt mit einem biometrischen Verifikationssystem ausgestattet.

Literatur

[3dface2006] EU Integrated Project *3D Face*, http://www.3dface.org

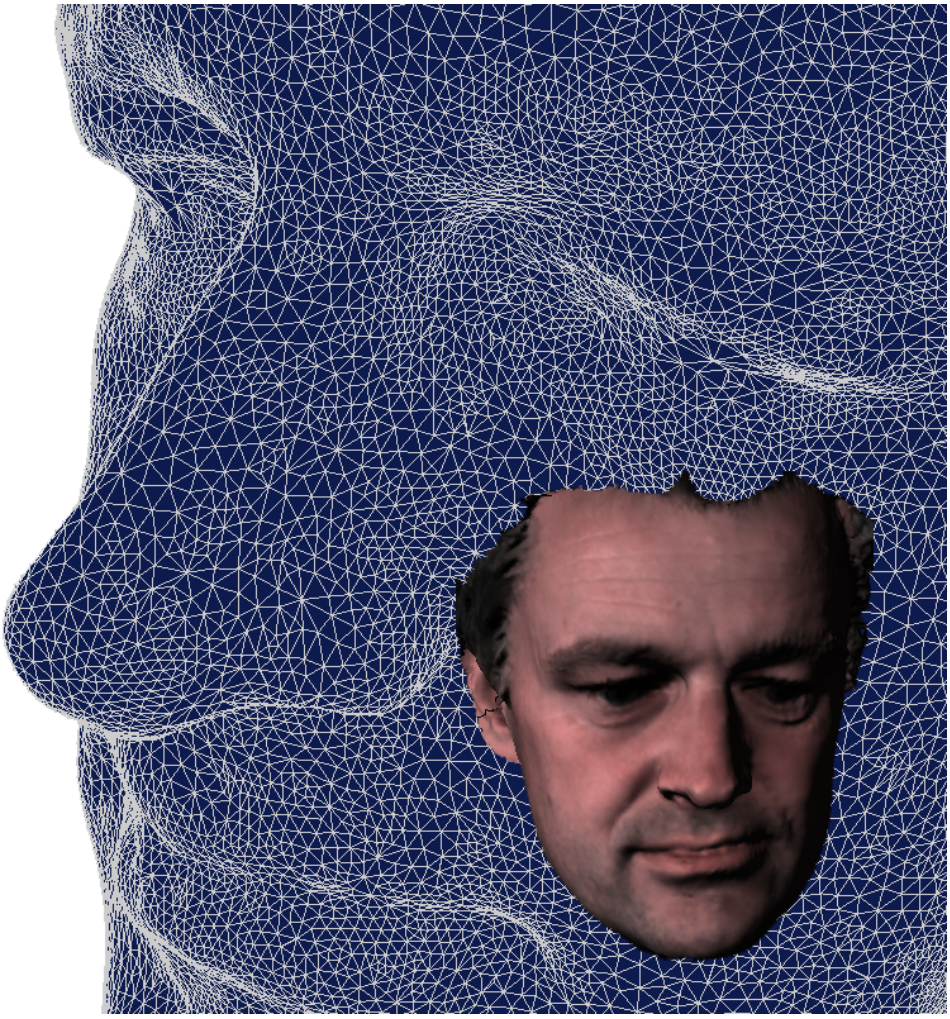
[biosig2009] BIOSIG, http://www.biosig.org

[din2009] DIN-Normenausschuss NIA, Arbeitsausschuss NIA-37, http://www.nia.din.de

[rapid2008] RAPID, http://www.rapid.sef.pt/

[ttt2008] TeleTrusT e.V. – Arbeitsgruppe Biometrie, White-Paper zum Datenschutz in der Biometrie

[ttt2009] TeleTrusT e.V., http://www.teletrust.de/fachgruppen/biometrie/



HANNS-WILHELM HEIBEY[1], DR. GISELA QUIRING-KOCK[2]

Biometrische Authentisierung – Möglichkeiten und Grenzen[3]

Die Authentisierung von Personen mit bestimmten körperlichen Merkmalen wie z. B. Fingerabdrücken, Gesichtsgeometrie oder Irismuster wird gelegentlich als Alternative zu den Authentisierungsverfahren durch Besitz und/oder Wissen angesehen. In diesem Beitrag geht es nicht um die spezifischen Datenschutzfragen beim Einsatz biometrischer Verfahren, sondern um die Möglichkeiten und Grenzen dieser Verfahren bei der Authentisierung.

Die biometrische Authentisierung setzt zunächst die Erfassung eines biometrischen Merkmals einer Person mittels optischer, thermischer, chemosensorischer, akustischer oder drucksensitiver Verfahren für spätere Vergleichszwecke voraus. Aus den erfassten Rohdaten wird mittels geeigneter Algorithmen ein sog. Template (Muster) berechnet und zentral oder dezentral für spätere Vergleiche (z. B. auf einer Chipkarte) abgespeichert. Dabei ist sicher zu stellen, dass eine Rekonstruktion des biometrischen Merkmals durch Rückrechnung aus dem Template ausgeschlossen ist. Beim eigentlichen Authentisierungsvorgang wird mit den gleichen Erfassungssystemen das biometrische Merkmal erfasst und ebenfalls mit den gleichen geeigneten Algorithmen aus dem aktuellen Merkmal die sog. biometrische Signatur berechnet. Die biometrische Signatur wird mit dem hinterlegten Template computergestützt verglichen. Das Ergebnis dieses Vergleichs führt dann zur automatisierten Entscheidung, ob die Authentisierung zum Erfolg führt oder nicht.

Die wichtigsten Erkennungsarten bei der Überprüfung sind die biometrische Verifikation (1:1-Vergleich) und die biometrische Identifikation (1:n-Vergleich). Bei der Verifikation wird die Identität durch den Vergleich der biometrischen Signatur mit genau einem Template geprüft, das dezentral, zum Beispiel auf einem bei der zu verifizierenden Person befindlichen Chip gespeichert werden kann. Bei der Identifikation wird die biometrische Signatur mit einer Vielzahl von Templates verglichen, die zentral in einer Datenbank gespeichert sind. Aus datenschutzrechtlicher Sicht ist wegen der Datensparsamkeit und -vermeidung der biometrischen Verifikation eindeutig der Vorzug vor der biometrischen Identifikation zu geben. Dies gilt insbesondere bei einer dezentralen Speicherung der Referenzdaten.

Die Treffsicherheit biometrischer Verfahren folgt im Gegensatz zu den kausalen Verfahren der Authentisierung durch Besitz und/oder Wissen Gesetzen der Wahrscheinlichkeit. Es ist stets davon auszugehen, dass die biometrische Signatur und das Template nie ganz gleich sein werden. Der Vergleich zwischen Signatur und Template kann daher nur einen Grad von Ähnlichkeit ermitteln.

---

[1] Bereichsleiter Informatik beim Berliner Beauftragten für Datenschutz und Informationsfreiheit
[2] Referatsleiterin Informatik beim Hessischen Datenschutzbeauftragten. Mitglied der TeleTrusT-Arbeitsgruppe "Biometrie"
[3] Vom Arbeitskreis "Technische und organisatorischen Datenschutzfragen“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder als Orientierungshilfe verabschiedet.

Je nach den Anforderungen an die Treffsicherheit des biometrischen Erkennungssystems muss ein Schwellenwert für die Ähnlichkeit festgelegt werden, über dem die Berechtigung vergeben (Acceptance) und unter dem sie verweigert (Rejection) wird. Je höher (*oder geringer*) der Schwellenwert gewählt wird, desto geringer (*oder höher*) ist die Wahrscheinlichkeit, dass eine Berechtigung unzutreffend erteilt wird. Andererseits steigt (*sinkt*) mit dem Schwellenwert die Wahrscheinlichkeit, dass jemand unberechtigt abgewiesen wird.

Die Wahrscheinlichkeit, dass jemand unrichtigerweise zurückgewiesen wird, wird als "False Rejection Rate" (FRR) bezeichnet; die Wahrscheinlichkeit, dass jemand unberechtigterweise eine Berechtigung erteilt bekommt, wird als "False Acceptance Rate" (FAR) bezeichnet. Unter Kalibrierung versteht man die für eine konkrete Anwendung sinnvolle Vergabe von FRR bzw. FAR. Wenn eine der beiden Größen festgelegt bzw. beschränkt wird, ergibt sich die Festlegung bzw. Beschränkung für die andere wegen der wechselseitigen Abhängigkeit aus dem jeweiligen konkreten biometrischen Verfahren.

Die "Equal Error Rate" ist der Wert, für den FRR=FAR gilt. Sie kann ein sinnvoller Kompromiss hinsichtlich der Sicherheitskalibrierung sein. Es gibt jedoch Anwendungs-Szenarien, bei denen die FAR im Vergleich zur FRR sehr niedrig sein muss, z. B. beim Zutritt/Zugang zum Hochsicherheitsbereich eines Kernkraftwerkes. Und es gibt Anwendungen, bei denen die FRR beispielsweise aus Performancegründen sehr niedrig sein muss und man eine höhere FAR gerne in Kauf nimmt. Das wäre bei der Zugangskontrolle für Besucher eines großen Fußballspiels der Fall, wenn wenige unberechtigt eingelassene Besucher akzeptiert werden.

Von den vielen übrigen "Rates", die etwas über das biometrische System aussagen, sei noch die "Failure to Enroll Rate" (FTE) erwähnt, die die Wahrscheinlichkeit benennt, dass von einer Person aus medizinischen Gründen kein brauchbares Template zu späteren Vergleichszwecken gewonnen werden kann. Dies gilt vor allem für Fingerabdrücke, bei denen FTEs von ca. 2 % der Gesamtbevölkerung ermittelt worden sind.

FRR und FAR sind abhängig von der Qualität des biometrischen Systems hinsichtlich der Genauigkeit der Erfassung, der Qualität der Template- und Signatur-Berechnung und der Genauigkeit des Vergleichs, von der Kalibrierung des biometrischen Systems, also der Wahl der Schwellenwerte und der Kooperation der Betroffenen.

Bei allzu kleiner FAR wird die FRR zu groß, d. h. z. B. bei einem Zutrittskontrollsystem bleiben zu viele Berechtigte vor der Tür. Dagegen führt eine allzu kleine FRR zu einer großen FAR, d. h. zu viele Unberechtigte können die Tür durchschreiten.

Kausale Verfahren der Authentisierung mit Besitz und/oder Wissen

Beim kausalen Authentifizierungsvorgang, d. h. der Prüfung, ob der Besitz vorhanden und das Wissen korrekt wiedergegeben wurde, ist eine Ja-Nein Entscheidung möglich. Diese Verfahren treffen aber keine 100-prozentige, eindeutige und zutreffende Entscheidung, ob die zu authentifizierende Person wirklich anwesend ist oder nicht. Vielmehr wird unterstellt bzw. angenommen, dass wenn Besitz und Wissen im Authentisierungsverfahren mit dem der zu authentifizierenden Person übereinstimmen, [nur] diese Person anwesend ist. Es kann keine Wahrscheinlichkeit dafür berechnet, hergeleitet oder angegeben werden, dass diese Annahme oder Unterstellung zutrifft. Auch eine Lebenderkennung ist damit nicht verbunden.

Es gibt eine Fülle von Beispielen, die belegen, dass ein korrekter Ablauf des Authentisierungsverfahrens nicht sicherstellt, dass auch die richtige Person das System nutzt. So können die Authentisierungsmittel beispielsweise

- weitergegeben sein,
- gestohlen (Besitz) oder erpresst (Wissen) sein.
- Der Besitz kann technisch dupliziert und das Wissen durch technische Manipulation ganz oder teilweise in falsche Hände gekommen sein (vgl. hierzu u. a. die vielfältigen Manipulationen an Geldausgabeautomaten).
- So kann der richtige Benutzer zwar anwesend sein und das Authentisierungsverfahren bedienen, die anschließende Nutzung des Systems aber mit oder ohne Anwendung von Gewalt ausschließlich durch Dritte erfolgen etc.

Biometrische Authentisierung

Bei der biometrischen Authentisierung kann immerhin mit einer berechenbaren bzw. hohen Wahrscheinlichkeit davon ausgegangen werden, dass die richtige Person anwesend ist, wenn das biometrische Merkmal dauerhaft und direkt mit ihr verbunden ist. Dies gilt insbesondere für biometrische Merkmale, die nicht wie der Fingerabdruck an vielen Orten ständig hinterlassen werden. Hierbei ist natürlich auch zu berücksichtigen, ob das Verfahren eine Lebenderkennung beinhaltet.
Die tatsächliche Bindung des biometrischen Merkmals an die Person ist als echter Vorteil gegenüber personenbezogenen Merkmalen wie Besitz und Wissen zu werten, bei denen die Anwesenheit der Person nur angenommen werden kann.

Besondere Vorkehrungen bei biometrischer Authentisierung

Die biometrischen Daten sind - im Gegensatz zu UserID und Passwort und zu Verfahren von Besitz und Wissen - eindeutig und potenziell lebenslang mit der Betroffenen verbunden. Deshalb sind für biometrische Authentisierungsverfahren - unabhängig vom verwendeten biometrischen Verfahren - besondere Vorkehrungen zu treffen:

a. Die Verbindung zwischen biometrischen und anderen Identitätsdaten muss sicher geschützt werden.

b. Der Schutz des Speichersystems der biometrischen Referenzdaten ist für Datensicherheit und Datenschutz des Verfahrens von grundlegender Bedeutung. Dabei sollte keine zentrale, sondern eine dezentrale Speicherung der Referenzdaten, z. B. auf einer Chipkarte, realisiert werden.
c. Speicherung und Übertragung der biometrischen Daten müssen gegen Abhören, unbefugte Offenbarung und Modifikation geschützt werden. Dies erfordert den Einsatz kryptografischer Verfahren. Die biometrischen Daten sind nicht geheim und sie können nach Bekanntwerden oder Missbrauch nicht verändert oder gesperrt werden. Deshalb ist folgendes wichtig:
d. Die biometrischen Daten dürfen nicht allein zur Authentisierung herangezogen werden, sondern sie sind mit sperr- und veränderbaren Daten wie Besitz und Wissen wirksam zu koppeln.

Die Stärke biometrischer Verfahren kann sich bei der biometrischen Authentisierung wegen der Nicht-Änderbarkeit und Nicht-Sperrbarkeit biometrischer Merkmale nur entfalten, wenn die genannten Anforderungen erfüllt sind und die mit der Verarbeitung der biometrischen Daten verbundenen Risiken insgesamt wirksam beherrscht werden. Wenn eine Methode mit Besitz und Wissen durch die biometrische Authentisierung ergänzt wird, verleiht dies damit dem kausalen Verfahren höhere Sicherheit vor Kompromittierung.

Literatur

1. Astrid Schumacher und Kristina Unverricht: Rechtliche und gesellschaftliche Empfehlungen zur Gestaltung biometrischer Systeme, DuD 5/2009, S. 308ff
2. Jeroen Breebaart, Bian Yang, Ileana Buhan-Dulman, Christoph Busch: Biometric Template Protection, DuD 5/2009, S. 299 ff.
3. Ulrike Korte, Johannes Merkle, Matthias Niesing: Datenschutzfreundliche Authentisierung mit Fingerabdrücken, DuD 5/2009, S. 289 ff
4. Heinz Biermann, Manfred Bromba, Christoph Busch, Gerrit Hornung, Martin Meints, Gisela Quiring-Kock: Whitepaper "Datenschutz in der Biometrie", TeleTrusT 2008.
5. Arslan Brömme: Leistungsfähigkeit biometrischer Personenidentifikation – Mehrerlei Maß, iX 10/2007, S. 42 ff
6. Thomas Petermann, Arnold Sauter: Biometrische Identifikationssysteme – Sachstandsbericht, Arbeitbericht Nr.76 des Büros für Technikfolgenabschätzung beim Deutschen Bundestag, 2002
7. Christoph Busch: Biometrische Verfahren – Chancen, Stolpersteine und Perspektiven, in: Peter Schaar (Hrsg.): Biometrie und Datenschutz – Der vermessene Mensch, tagungsband zum Symposium des Bundesbeauftragten für den Datenschutz und Informationsfreiheit am 27. Juni 2006 in Berlin
8. Privatim – die schweizerischen Datenschutzbeauftragten (Hrsg.): Leitfaden zur datenschutzrechtlichen Beurteilung von biometrischen Verfahren, Version 1.0, Oktober 2006

THOMAS T. KNIESS*

Biometrie – Alternative zum Passwort?

Eine eindeutige Aussage für pro Passwort oder pro Biometrie zu treffen, ist schwer möglich. Jedes der beiden Verfahren hat seine Vor- oder Nachteile, auch im Hinblick auf die Szenarien in denen die Authentifizierungsverfahren eingesetzt werden, kann sich das Sicherheitsniveau durch den Einsatz von Biometrie verbessern oder nicht.

Die Sicherheit von Passwörtern hängt davon ab, wie lang und kryptisch sie sind. Hier kann der Administrator eines Sicherheitssystems viel Einfluss durch Policies nehmen, um den geforderten Sicherheitsstand zu erreichen. Jedoch hat die Unlesbarkeit und die Fülle Folgen. Viele Benutzer fangen an, ihre Passwörter auf Zettel zu schreiben und diese z.B. unter der Tastatur aufzubewahren, ebenso kann man häufig beobachten, dass PINs im Handy als Telefonnummer gespeichert sind. Wird dieses Benutzerverhalten und die Benutzerfreundlichkeit bei der Verwendung von Passwörtern bei einem Vergleich mit betrachtet, punktet klar die Biometrie.

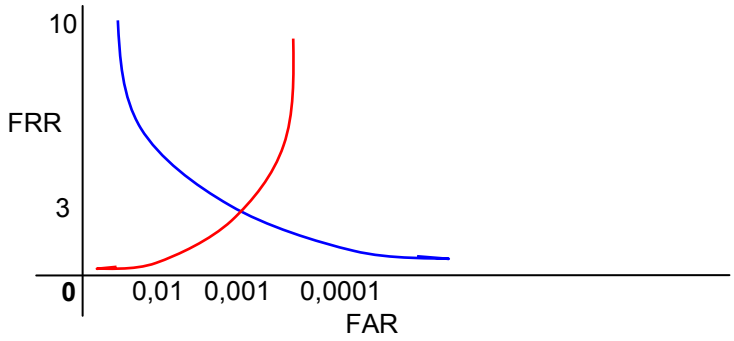
Biometrische Systeme hingegen können keinen Vergleich auf exakte Übereinstimmung wie bei der Passwortabfrage vornehmen, da sich die Biometrie von Aufnahme zu Aufnahme unterscheidet, zum Beispiel durch die Flexibilität der Haut beim Fingerprintverfahren. Aus diesem Grund müssen Toleranzen bei einem Vergleich berücksichtigt werden. Dadurch kommt es zu zwei Fehlerraten, die Aufschluss über die Leistungsfähigkeit von Biometrieverfahren geben können:

- Die Falsch-Akzeptanz Rate (FAR) beschreibt, wie viele Nutzer fälschlicherweise Zugang bekamen.
- Die Falsch-Rückweisungs Rate (FRR) beschreibt die Rate der berechtigten Personen die fälschlicherweise zurückgewiesen wurden.

Da diese beiden Raten konkurrierend zueinander stehen, muss entschieden werden, wie das System eingestellt wird: komfortabel, mit einer sehr niedrigen FRR, oder sicher, mit einer niedrigen FAR.

Hilfestellung beim Einstellen des Systems kann die Equal-Error-Rate (EER) geben. Diese beschreibt den Schnittpunkt der beiden Fehlerraten und somit den Punkt, bei dem beide Raten am niedrigsten sind.

* Wissenschaftlicher Mitarbeiter im Fraunhofer Institut für Sichere Informationstechnologie (SIT)
Das Fraunhofer Institut SIT ist TeleTrusT-Mitglied.



Anhand dieser Grafik werden die Zusammenhänge zwischen FAR/FRR und EER deutlich.
Der EER liegt bei einer FAR von 0,001 und einer FAR von 3.

Eine weitere Rolle in Bezug auf die Sicherheit spielt die Auswahl der Merkmale, die bei einem Biometrieverfahren herangezogen werden. Hierzu einen Überblick über die Charakteristiken einzelner Merkmale:

- Verhaltensmerkmale, darunter fallen Merkmale die durch bestimmte Bewegungen oder durch die Stimme, einer Person zuzuordnen sind (Stimmerkennung / Gangerkennung / Unterschriftenerkennung)
- Feststehende physikalische Merkmale sind Merkmale die Körpereigenschaften vermessen (Fingerabdruck / Gesicht / Unterschriftenbild)
- Öffentliche Merkmale sind Körpereigenschaften, die hinterlassen oder einfach zu sehen sind, z.B. auf einem Foto (Gesichterkennung / Fingerprint)
- Nicht-öffentliche Merkmale sind Merkmale, die wir nicht offen mit uns tragen (DNA / Handvenenmuster / Retina). Hierzu zählen auch die Verhaltensmerkmale.

Bei Lösungen mit Verhaltensmerkmalen oder nicht-öffentlichen Merkmalen wird es einem Angreifer schwerer, bei der Beschaffung der nötigen Informationen gemacht. Auch das Nachbauen oder Nachahmen solcher Merkmale gestaltet sich deutlich schwieriger als das von öffentlichen Merkmalen. Dies hat der Chaos Computer Club anhand von Fingerabdruckverfahren schon mehrfach gezeigt.

Ein Sicherheitsaspekt, den die Biometrie mit sich bringt, ist, dass sie Ad-hoc-/Kleinkriminalität verhindert. In der Zeiterfassung werben Hersteller mit 5% bis 10% Einsparung bei Lohnarbeit durch Biometrielösungen, da die Möglichkeit, für Kollegen mitzustempeln, "gegen Null" geht. Ebenso wird die Weitergabe verhindert, wie sie oftmals bei Karten oder Schlüsseln der Fall ist.

Ein grundlegender Nachteil der Biometrieverfahren erweist sich dann, wenn man angegriffen wird und genügend kriminelle Energie vorhanden ist, um forensisch vorzugehen, um z.B. den Fingerabdruck von einem Wasserglas zu entnehmen, diesen grafisch aufzuarbeiten um daraus eine Attrappe zu er-

stellen. Dabei ist weniger die Überwindung als solche das Problem, denn wenn ein Angreifer diesen Weg beschreitet, gelangt er auch an Passwörter oder PINs. Kritischer ist die Tatsache, dass die biometrischen Merkmale, die ein Mensch besitzt, begrenzt sind.

Eine ähnliche Problematik besteht bei der Speicherung der Biometriedatensätze, den Templates. Die sichere Verwahrung dieser ist eine besondere Herausforderung, da bei einer Identifizierung eine verschlüsselte Ablage schwer realisierbar ist, es müsste für alle Datensätze derselbe Schlüssel verwenden werden. Dies hätte zur Folge, dass der Betreiber auf die Daten zugreifen könnte. Daraus könnte sich folgendes Szenario ergeben: Betreiber A hat Zugriff auf optimale Biometriedaten. Mit diesen Daten und einem Arbeitnehmerwechsel zu einem Mitbewerber mit ebenfalls Biometrie als Zutrittskontrolle, könnte sich der Betreiber A Zugang zu fremden Ressourcen verschaffen.

Wird die Biometrie zur Verifikation genutzt, besteht die Möglichkeit, jeden Biometriedatensatz mit einem anwenderspezifischen Schlüssel zu verschlüsseln. Beim Abgleich gegen eine Datenbank im Verifikationsmodus müsste sich dann jeder Benutzer zunächst gegenüber seinem ausgewählten Datensatz entsprechend authentisieren. Die Möglichkeit für den Betreiber, an diese Daten zu gelangen, ist praktisch nahe Null.

Fazit

Biometrie ist definitv eine sichere Alternative zur PIN oder zum Passwort als Mittel zur Benutzerauthentisierung, d.h. zum Beweis einer vorgegebenen Identität mit bestimmten Rechten. Durch Biometrie lassen sich zahlreiche Probleme lösen, die bei Passwortverfahren durch unsachgemäßen Umgang (z.B. Vergessen oder nach außen sichtbares Aufschreiben) entstehen.

In vielen Anwendungsbereichen bietet Biometrie einen höheren Sicherheits- und Benutzer-Komfort, z.B. bei Bezahlvorgängen, wo das Leisten einer Unterschrift unter Aufsicht der Verkäufer durch das Auflegen des Fingers auf einen Sensor ersetzt werden könnte.

Für einen reinen Identifikationsbetrieb (Ermittlung der Identität ohne Abfrage weiterer Daten) ist die Biometrie, speziell der Fingerprint, nur bedingt geeignet. Empfehlenswert aus unserer Sicht ist hier eine Kombination von Biometrie und PIN, bei der die Biometrie die Identifikation und die PIN die anschließende Authentifizierung übernimmt. Dadurch kann auf Benutzernamen oder Karten verzichtet werden und es wird eine deutliche Anhebung des Sicherheitsniveaus und des Bedienkomforts erreicht. Zusätzlich sinken die administrativen Kosten.

HILDEGARD HERZOG*

Biometrie oder Passwörter - was ist sicherer?

Stellt man biometrische Verfahren dem Passwort gegenüber, ist von vornherein eines sicher: Hundertprozentigen Schutz gewährt kein Verfahren. Aber es gibt doch erhebliche Unterschiede. Und der Ruf nach biometrischer Absicherung steigt mit jedem neu bekannt werdenden Fall von Datendiebstahl.

Passwörter sind am weitesten verbreitet: Praktisch und einfach anzuwenden, bedürfen sie keiner speziellen Hardware und sind weitgehend unabhängig nutzbar. Die Sicherheit eines Passwortes bemisst sich an dessen Komplexität: Je länger und je mehr mit Sonderzeichen und Ziffern kombiniert, desto sicherer ist es.

Das Problem hier stellt eindeutig in erster Linie der Benutzer dar: Er kreiert sein Passwort meist eigenständig und verwendet – auch nach neuesten Untersuchungen – immer noch ein standardisiertes ("123abc" etc. oder Familiendaten) für alle seine Anwendungen, ob geschäftlich oder privat. Die Durchsetzung von Unternehmensanweisungen zur regelmäßigen Passwortänderung scheitert häufig. Angesichts der Fülle von Passwörtern, die man bräuchte, ein nachvollziehbares Phänomen. Hier kommen Betrüger ins Spiel: Für ausreichend motivierte kriminelle Angreifer ist es so ein Leichtes, Passwörter auszuspähen und in Firmennetze und Onlineportale einzudringen, was Schäden in Milliardenhöhe verursacht. Eine weitere Sicherheitslücke entsteht durch die bewusste oder unbewusste Weitergabe von Passwörtern: Der Kollege soll schnell etwas nachsehen - oder das Passwort klebt gleich unter dem Keyboard…

Grundlage der Biometrie ist die Erfassung eines personenspezifischen Merkmals ("Enrolment" - z. B. optisch, thermisch, akustisch oder drucksensitiv) zu späteren Vergleichszwecken. Aus den erfassten Rohdaten wird mittels festgelegter Algorithmen ein Profil ("Template") berechnet und für spätere Vergleiche abgespeichert. Dies dient der Authentifizierung beim Zugang. Dafür gibt der Benutzer zuerst seinen Usernamen oder seinen Code an, um dann statt oder in Ergänzung eines Passwortes zur Sicherheitshärtung die biometrische Authentisierung durchzuführen: Also den Vergleich seines aktuell erzeugten persönlichen Merkmals, z. B. Fingerabdruck, Stimme oder Tippverhalten, mit dem hinterlegten Template. Ist dies im Rahmen der Toleranzgrenzen authentisch, so wird der Zugang freigegeben; weicht sie vom vordefinierten Vergleichsmuster zu stark ab, wird der Nutzer abgewiesen.

* Psylock GmbH, Marketing. Die Psylock GmbH arbeitet in der TeleTrusT-Arbeitsgruppe "Biometrie" mit.

Biometrie hat den unschätzbaren Vorteil der Personenbindung, d. h. der Benutzer muss persönlich vor Ort sein, um seine Berechtigung durch ein biometrisches Merkmal wie Fingerabdruck, Iris, Handvenenstruktur, Tippverhalten oder Stimme nachzuweisen. Dies gewährt ein hohes Maß an Sicherheit. Andererseits ist die Sicherheitsverantwortung bei Biometrien eher systemimmanent, wogegen die Umsetzung der Passwort-Policy nicht abschätzbar ist.

Eine praktikable biometrische Methode ist besonders im IT-Bereich die Voraussetzung zur Authentisierung anstelle des Passwortes. Hohe Sicherheit, komfortable Anwendung und große Akzeptanz beim Nutzer sowie unkomplizierte Installation sind wesentliche Faktoren. Weitgehende zeitliche und räumliche Unabhängigkeit sowie überschaubare Kosten sind aufgrund der Anforderungen hinsichtlich mobiler Arbeitsplätze und zunehmenden Kostendrucks wünschenswert.

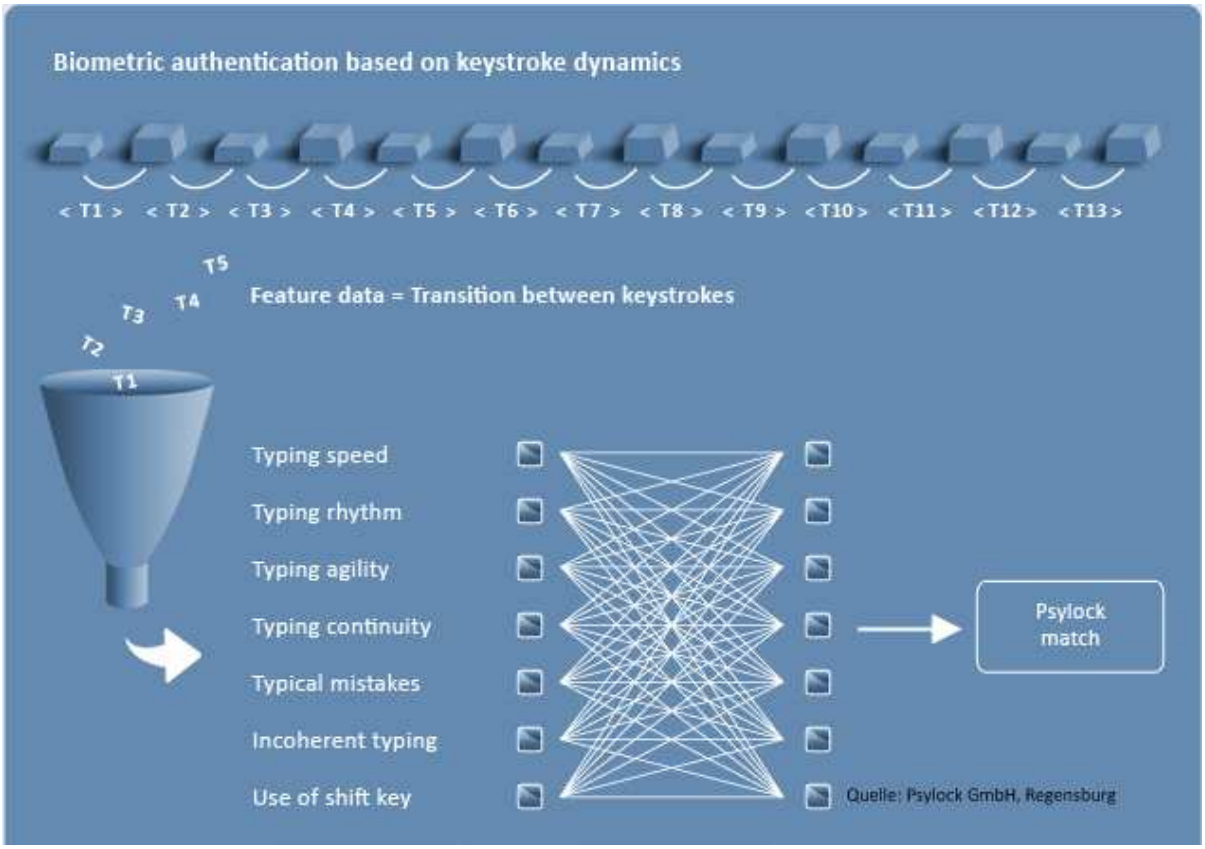
Die Wahrscheinlichkeit eines identischen biometrischen Merkmals bei zwei unterschiedlichen Personen ist zwar selbst bei eineiigen Zwillingen ausgesprochen gering, aber es gibt sie. Zufällig kann jemand mit ähnlichem Merkmal eine "identische" Probe abgeben, da bei Biometrien eine gewisse Varietät berücksichtigt werden muss.

Nachteil der meisten biometrischen Verfahren ist der Bedarf zusätzlicher Hardware (z. B. Fingerprint-Reader, Irisscan, Webcam etc.). Sie stellt ein logistisches Hemmnis dar. Einzig bei der Tippverhaltens-Biometrie trifft das nicht zu: Hier ist die vorhandene Tastatur der Sensor.

Bequemlichkeit contra Sicherheit?

Es gibt zwei Kriterien: Zum einen die Falschakzeptanz-Rate (FAR), die darüber Auskunft gibt, wie viele nicht autorisierte Nutzer akzeptiert werden; andererseits die Falschrückweisungs-Rate (FRR). Sie stellt dar, wie oft autorisierte Benutzer ungewollt zurückgewiesen werden. Über die Balance dieser Parameter lässt sich das Sicherheitsniveau einer Methode definieren. Je sicherer, desto mehr evtl. ungewollte Rückweisungen muss man unter Umständen in Kauf nehmen.

Anhand der folgenden Grafik kann man erkennen, dass bei der Template-Erstellung und beim Login zahlreiche Parameter in einem mathematischen Verfahren ausgewertet werden, um eine sichere Authentifizierung zu gewährleisten.



Eine gewisse Bandbreite gewährleistet die Akzeptanz geringfügiger Unterschiede. Zudem gibt es "lernende" Software, die bei jedem erfolgreichen Login das Profil entsprechend modifiziert. Wichtig ist häufig auch die Skalierbarkeit einer Biometrie. Bei wenigen Verfahren ist sie gewährleistet.

Ersetzbares Profil bei Biometrie?

Der Ausschluss "veralteter" Profile, die lange Zeit nicht benutzt wurden, bietet zusätzliche Sicherheit. Für den Fall, dass ein biometrisches Merkmal ausgespäht wurde, lohnt es sich, darüber nachzudenken, ob man nicht eine Biometrie wählt, bei der das Profil problemlos ersetzt werden kann, da man Fingerabdrücke oder Stimmen ja nicht beliebig vervielfältigen kann. Es gibt eine Methode, bei der dies funktioniert: Sollte trotz Replayschutz der Verdacht bestehen, dass ein Keylogger am Werk war, wird einfach der Login-Satz geändert und dafür ein neues Template erstellt, dann kann das Verfahren auch umstandslos weiter genutzt werden.

Biometrien können Passwörter durchaus ersetzen oder ergänzen. Sie stellen in jedem Fall eine zusätzliche, personengebundene Sicherheit dar. Um sich für die im einzelnen Fall angemessene Biometrie zu entscheiden, ist es jedoch wichtig, individuell erforderliche Bedürnisse zu klären wie: Sicherheit, Bedienungskomfort, Anpassung bei Personalveränderung, Anschaffungs- und Folgekosten, Installationsaufwand, Logistik, Ersatz bei Betrugsverdacht etc.

TeleTrusT Deutschland e.V.

Der IT-Sicherheitsverband TeleTrusT Deutschland wurde 1989 gegründet, um verlässliche Rahmenbedingungen für den vertrauenswürdigen Einsatz von Informations- und Kommunikationstechnik zu schaffen. TeleTrusT entwickelte sich zu einem bekannten Kompetenznetzwerk für IT-Sicherheit, dessen Stimme in Deutschland und Europa gehört wird. Heute vertritt TeleTrusT rund 100 Mitglieder aus Industrie, Wissenschaft und Forschung sowie öffentlichen Institutionen. In Projektgruppen zu aktuellen Themen der IT-Sicherheit und des Sicherheitsmanagements tauschen die Mitglieder ihr Know-how aus. TeleTrusT äußert sich zu politischen und rechtlichen Fragen, organisiert Messen und Messebeteiligungen und ist Träger der "European Bridge CA" (Bereitstellung von Public-Key-Zertifikaten für sichere E-Mailkommunikation) sowie des Zertifikates "TeleTrusT Information Security Professional" (T.I.S.P.). Hauptsitz des Verbandes ist Berlin.

Kontakt:
Dr. Holger Mühlbauer
TeleTrusT Deutschland e.V.
Chausseestraße 17
10115 Berlin
Tel.: + 49 30 400 54 310
holger.muehlbauer@TeleTrusT.de
www.TeleTrusT.de


TeleTrusT
Pioneers in IT security.