

Biometrie: Standardisierung kontra Datenschutz

Genormte Systeme bergen auch Risiken

Die Entscheidung, Biometrie im betrieblichen Umfeld einzusetzen, ist keine triviale Angelegenheit. Neben Kosten-Überlegungen, technischen Einzelheiten und Sicherheitsabwägungen ist auch der Datenschutz zu berücksichtigen. Bei der Investitionsentscheidung klingen „standardisierte Systeme“ meist besonders verlockend. Sie versprechen eine „glatte“, sichere und zugleich unbedenkliche Zukunftsinvestition. Doch leider: Normung ist nicht gleich Normung.



Von Manfred Bromba,
München

Die besonders schützenswerte Natur biometrischer Daten ergibt sich im Wesentlichen aus zwei Gegebenheiten: Biometrische Daten lassen sich wie eindeutige, aber nicht änderbare Personenkennziffern nutzen und sie können zusätzliche Informationen über den Betroffenen enthalten, etwa über seine Gesundheit.

Missbrauchspotenzial

Eine bei manchen Herstellern beliebte „Nebelkerze“ ist die Aussage „Aus den gespeicherten biometrischen Referenz-

daten (Templates) lassen sich die Originaldaten nicht zurückrechnen“. Nebelkerze deshalb, weil die Aussage zwar rein formal richtig ist, von Laien aber gerne so aufgefasst wird, dass Datenschutz kein Problem ist.

Genau das Gegenteil lässt sich am Beispiel „Fingerprint“ zeigen. Zur Erstellung eines Referenzdatensatzes berechnen die meisten biometrischen Systeme aus dem Fingerabdruck-Rohbild eine Minuzienliste (Minuzien repräsentieren als Träger der Einmaligkeitsinformation die für jeden Finger unterschiedlichen Orte der Fingerlinienverzweigungen und -endungen). Allerdings lässt sich mit Hilfe spezieller mathematischer Methoden – und notfalls sogar von Hand – aus diesen Minuzien ein Fingerbild rekonstruieren, das das Erkennungssystem nicht vom ursprünglichen Fingerabdruckbild unter-

scheiden kann. Daraus ergibt sich ein hohes Missbrauchspotenzial (s. „2.“).

Bei der Frage, inwiefern die Standardisierung der Datenformate einen Einfluss auf Datenschutz und Sicherheit haben kann, stehen zwei Problemfälle besonders im Mittelpunkt:

1. Standardisierte Referenzdaten ermöglichen einen besonders einfachen Austausch. Das wissen auch Kriminelle, die versuchen könnten, eigene biometrische Daten in eine Datenbank zu schmuggeln, um so die Berechtigungen eines registrierten Nutzers zu übernehmen. Dieser Fall ist zumindest für die Zielanwendung durch das Signieren der Daten zu beheben, ohne die Standardisierung aufzugeben. Das verhindert allerdings nicht das Sammeln und Nutzen für andere, unbekanntere Zwecke durch eine wie auch immer geartete An-

Biometriebezogene Standardisierung

Bei der Standardisierung und insbesondere der Normung geht es darum, Vorteile durch die Austauschbarkeit von Hardware-, Software und Daten zu gewinnen und dem Beschaffer vergleichbare Messwerte für Investitionsentscheidungen zu liefern. Im Bereich der Biometrie gibt es inzwischen allein in der „ISO-Arbeitsgruppe SC 37“ insgesamt 30 publizierte ISO/IEC-Normen – und mindestens genauso viele sind zusätzlich in Arbeit. Dabei ist „BioAPI“, einer der ältesten biometrischen Standards, datenschutztechnisch eher weniger kritisch.

Die in Bezug auf Datenschutz größte Relevanz haben ISO/IEC-Normen zum Austausch von biometrischen Daten. Die erste große Anwendung fanden die Normen für Gesichts- und Fingerabdruckdaten bei der Einführung biometrischer Pässe, und zwar in Form von Bilddaten. Hier kommt es darauf an, mit der Hard- und Software unterschiedlichster Hersteller arbeiten zu können und gleichzeitig einen Datenaustausch über Ländergrenzen hinweg zu ermöglichen. Während bei den Pässen noch Rohbilddaten gespeichert werden,

sind inzwischen einige biometrische Systemkomponenten erhältlich, die auch Minuzien in einem der Normformate von ISO/IEC 19794-2 austauschen können. Generell hat die Austauschbarkeit biometrischer Daten innerhalb eines Systems im Idealfall verschiedene Vorteile:

- 1) Die bei der Erstregistrierung (Enrolment) gespeicherten biometrischen Referenzdaten lassen sich beispielsweise gleichzeitig zur PC-basierten Zugriffskontrolle und bei der Zutrittskontrolle durch vernetzte autonome Türöffnersysteme nutzen – insbesondere auch dann, wenn die Komponenten von unterschiedlichen Herstellern stammen.
- 2) Es lassen sich theoretisch sowohl Erkennungsalgorithmen als auch Sensorkomponenten mit zugehöriger Software austauschen, ohne die Referenzdaten neu aufnehmen zu müssen – was unabhängig macht, wenn etwa eine Hardware-Komponente ausfällt.

wendung, die in diesem Fall die angehängten Signaturen einfach ignorieren könnte.

2. Das zweite, sehr konkrete Problem ist die erwähnte Rekonstruierbarkeit eines Fingerabdrucks, was einen „Angriff“ auf das System zur Folge haben könnte. Gelingt es einem Angreifer, Referenzdaten in Minuzienform aus einer Datenbank zu stehlen, kann er ein Fingerabdruckbild zurückrechnen, um daraus etwa ein Plagiat in Form eines mechanisch nachgemachten Fingers zu erstellen.

Dieses Bild wird in der Regel wenig Ähnlichkeiten mit dem Originalbild haben, zeichnet sich aber durch eine fatale Eigenschaft aus: Präsentiert man dem Sensor des betroffenen biometrischen Systems das geschilderte Plagiat, wird es bei unzureichender Fälschungserkennung daraus wieder exakt die gleichen Minuzien extrahieren, die bereits als Fälschungsvorlage dienten. Damit kann das biometrische System das nachgemachte Bild nicht vom echten unterscheiden, denn die Minuzien-

ten von gestohlener Referenz und Plagiat sind die gleichen.

Standardisierung „hilft“

Zwar ist dieser Angriff kein einfacher, doch die Gefahr liegt in der teilweisen Automatisierbarkeit. Er setzt nach einem erfolgreichen Datendiebstahl voraus, dass das Referenzdatenformat bekannt ist. An dieser Stelle kommt die Standardisierung ins Spiel. Von IT-Angriffen ist bekannt, dass oft die schiere Menge den Erfolg für den Angreifer ausmacht. Wäre das Referenzdatenformat nicht standardisiert, müsste der Angreifer zunächst das proprietäre Format verstehen lernen und in seine Rekonstruktionssoftware einbauen – was sich nur in Ausnahmefällen „rechnet“. Dieser Angriff ließe sich mit einer gut funktionierenden Fälschungserkennung übrigens vollständig abwehren – leider ist die Wirklichkeit von diesem Ideal weit entfernt, zumindest für Fingerprint. Bisherige Methoden mögen zwar zur Abwehr von speziellen Plagiaten recht erfolgreich sein, allerdings ist kaum jemals zu erwarten, dass sämtliche – auch

bisher nicht bekannte – Methoden abwehrbar sind, ohne dass die Erkennung berechtigter Nutzer darunter erheblich leiden würde.

Was tun?

Ein wirkungsvoller und unerlässlicher Schutz vor Missbrauch ist eine starke Verschlüsselung. Dies gilt sowohl für die Speicherung als auch für die Übertragung. Besonders über LAN ist eine Verschlüsselung biometrischer Daten unentbehrlich, da im Prinzip jeder angeschlossene PC die Kommunikation mitschneiden kann. Empfohlen wird sogar eine Mehrfachverschlüsselung durch Algorithmenanbieter, Applikationsentwickler und Anwender. In diesem Fall kann keine der drei Parteien ohne die zwei anderen erfolgreich die erforderliche Komplet-Entschlüsselung eines gestohlenen Datensatzes durchführen. Mit der Verschlüsselung im Fall unterschiedlicher Schlüssel für unterschiedliche Anwendungen und Datenbanken ist damit die Standardisierung und Austauschbarkeit wirkungsvoll aufgehoben, und zwar besser ▶

als es proprietäre Formate jemals vermögen. Dabei ist zu berücksichtigen, dass auch der Schlüssel korrumpiert werden kann. Dagegen hilft selbst die stärkste Verschlüsselung nicht.

Allerdings sind mit einer Verschlüsselung auch die sonstigen Vorteile der Standardisierung der Referenzdaten „dahin“: Im Fall der empfohlenen Dreifachverschlüsselung ist immer dann eine Neuregistrierung erforderlich, wenn der Algorithmushersteller oder die Applikation gewechselt wird. Aber ist das wirklich so schlimm?

Für die meisten Anwendungen ist es durchaus möglich, den Registrierungsprozess einfach und gleichzeitig sicher zu gestalten, so dass er nur wenige Minuten in Anspruch nimmt und quasi jederzeit durchführbar ist. Wem etwa als Betreiber eine Neuregistrierung pro Jahr zu teuer ist, der sollte auf Biometrie ganz verzichten. Denn dann wird entweder „mit Kanonen auf Spatzen geschossen“ oder die Vorteile des Biometrieinsatzes reichen in diesem Fall offenbar nicht aus, diese Zusatzkosten wieder wett zu machen.

Grundsätzlich ist die Möglichkeit einer unkomplizierten Neuregistrierung auch für den Normalbetrieb vorzusehen. Wenn der Betroffene bei der Erstregistrierung noch nicht mit dem Umgang mit dem biometrischen System vertraut ist, wird üblicherweise auch die Referenzdatenqualität noch nicht optimal sein. Die erneute Registrierung bietet dann die Möglichkeit, die Erkennungsraten individuell deutlich zu verbessern. Unabhängig davon wird die Definition eines festen Verfallsdatums die Akzeptanz beim Anwender deutlich erhöhen.

Grenzen der Normung

Die Standardisierung biometrischer Referenzdaten ist darüber hinaus keine Gewähr für bestmögliche Erkennungsraten. Maximale Performanz ist nur dann zu erwarten, wenn die gleiche Hardware und die gleichen Erkennungsalgorithmen, die die Referenz erzeugt haben, auch die Erkennung durchführen. Andernfalls liegt die Leistung regelmäßig unter den für diesen Algorithmus üblichen Werten. Wird in

einer Anwendung der Algorithmus gewechselt, sollte man auch bei standardisierten Referenzdaten eine Neuregistrierung durchführen. Allerdings, und das ist der verbleibende Vorteil der Standardisierung, muss die Neuregistrierung nicht unmittelbar zusammen mit dem Wechsel stattfinden.

Bereits der Wechsel der Erfassungshardware kann zu deutlichen Performanzeinbußen führen, selbst wenn der integrierte Sensor der gleiche ist. Dies gilt insbesondere für kleinere Sensoren, die aus Kostengründen nur einen Teil des Fingerabdrucks abbilden. Wenn sich in diesem Fall die mechanische Fingerführung geändert hat, so dass sich Abdrücke mit alter und neuer Hardware nicht mehr zu 100% überlappen, ist auf jeden Fall mit einer Erhöhung der Erkennungsfehlerraten zu rechnen. Soll alte und neue Hardware parallel betrieben werden, ist eine Neuregistrierung keine Lösung. Hier helfen eher Algorithmen weiter, die schon bei der Erstregistrierung auf eine ausreichende Variation der Fingerlage auf dem Sensor achten und auf diese Weise einen größeren Referenzfingerabdruck erzeugen, als der Sensorfläche entsprechen würde.

Ist die Entscheidung für einen Referenzdaten-Standard gefallen, lässt sich ohne Neuregistrierung (oder Formatkonverter) nur noch zu Algorithmen wechseln, die den gleichen Standard unverschlüsselt nutzen. Allein für Fingerprint gibt es derzeit vier unterschiedliche biometrische Datenaustauschformate, die untereinander inkompatibel sind:

- ISO/IEC 19794-2: Fingerminuziendaten
- ISO/IEC 19794-3: Spektrale(s) Muster der Finger-Daten
- ISO/IEC 19794-4: Fingerbilddaten
- ISO/IEC 19794-8: Daten skelettierter Fingerabdrücke

Selbst bei Beschränkung auf einen der genannten Standards gibt es immer noch unterschiedliche, inkompatible Subformate. Teilweise lassen sich die einzelnen Formate ineinander umrechnen, und zwar mittels geeigneter Formatkonverter. Dies kann allerdings mit Konvertierungsverlusten einhergehen, wobei das Fingerbilddatenformat nach ISO/IEC 19794-4 noch die beste Möglich-

keit darstellt, Referenzdaten systemunabhängig dauerhaft zu speichern, abgesehen vom originären Bitmap-Format. Da es sich hier mehr oder weniger um ein Rohdatenformat handelt, ist es auch das Format mit der meisten Information. Es lässt sich deshalb mit den geringsten Verlusten in fast beliebige weitere, ebenfalls standardisierte Formate umwandeln. Die Speicherung ist im Sinne des Datenschutzes dann natürlich mit den höchsten Schutzvorkehrungen vorzunehmen.

Es zeigt sich also auch hier, dass die Entscheidung für einen Standard nicht automatisch eine beliebige Austauschbarkeit mit gegenwärtigen, geschweige denn zukünftigen Formaten bedeutet – zumal sich schon heute nicht alle Referenzdaten derzeit am Markt erhältlicher Systeme ohne deutliche Leistungseinbußen in ein verfügbares Standardformat zwingen lassen. Andererseits gibt es Referenzdatennormen, die am Markt nur von wenigen, wenn nicht gar nur von einem einzigen Algorithmushersteller unterstützt werden (ISO/IEC 19794-3). Die Verwendung eines selten genutzten Standards hat deshalb für die Austauschbarkeit keine wirklichen Vorteile gegenüber einem proprietären Format. Aber seine Software als „standardkonform“ bezeichnen zu können, klingt allemal gut und wird so manchen technisch weniger bewanderten Einkäufer geschickt am eigentlichen Ziel vorbeilenken: Das Beste für sein Geld zu erwerben.

So sind Standardformate nur dort zu empfehlen, wo eine Austauschbarkeit unabdingbar ist und angemessene besondere Schutzmaßnahmen kostengünstig kein Problem darstellen. Das gilt insbesondere für Systeme, die mit den Komponenten mehrerer Hersteller gleichzeitig arbeiten müssen.

Über unseren Autor:

Manfred Bromba ist Geschäftsführer der Bromba GmbH Biometrics und für die Themen Sicherheit und wissenschaftlich-technische Kundenberatung verantwortlich. Als Mitarbeiter unter anderem in der Arbeitsgruppe NI-37 des DIN e.V. wirkte er bei der Förderung und Normung biometrischer Systeme mit.
Kontakt: www.bromba.com/contactd.htm