DIE ZEIT

Wissen 46/2001

Das gestohlene Gesicht

Die biometrische Identifizierung gilt als besonders sicher. Aber auch sie ist vor Hackern nicht gefeit

von Thomas Vacek; Sven Scheffler

Angenommen, jemand würde Ihr Gesicht stehlen. Ein böswilliger Computerhacker könnte zum Beispiel ein Kabel in einem Gesichtserkennungssystem anzapfen, Ihr digitalisiertes Bild entwenden und bei nächster Gelegenheit wieder einspielen. Wenn Sie zu einem Kreis von Leuten gehören, die Zugang zu einem Hochsicherheitstrakt haben, könnte der Bösewicht zum Beispiel ein Terrorist sein, der Ihre Identität missbraucht. Als Normalsterblicher müssten Sie Angst haben vor Gaunern, die auf Ihre Rechnung im Internet einkaufen oder in Ihrem Namen Geld von der Bank abheben.

Einen solchen Hacker-Angriff auf ein biometrisches System nennt man eine Replay-Attacke. Gleichgültig, ob die Technik auf der Erkennung von Gesichtern, von Fingerabdrücken oder von Mustern der Iris im menschlichen Auge basiert - mit einem solchen Angriff lassen sich biometrische Methoden bisweilen überlisten.

Seit dem 11. September werden die Biometriehersteller nicht müde, ihre Technik als Wunderwaffe gegen den Terrorismus anzupreisen: Gesichtserkennungssysteme könnten Terroristen in einer Menschenmenge aufspüren; per Fingerabdruck ließe sich verhindern, dass "Schläfer" verschiedene Identitäten annehmen. In Deutschland hat sich die Koalition im Rahmen des Sicherheitspakets darauf geeinigt, die gesetzliche Grundlage für biometrische Merkmale im Pass zu schaffen, entscheiden wird letztlich der Bundestag.

Gestohlene Körpermerkmale

Biometrische Methoden erlauben es, eine Person anhand bestimmter Körpermerkmale zu identifizieren. Die Natur selbst liefert die Sicherheit: Viele Körpermerkmale sind einzigartig und verändern sich im Verlauf des Lebens nicht. Die Vorteile liegen auf der Hand: Einen Personalausweis kann man fälschen, ein Passwort kann verloren gehen oder in unbefugte Hände geraten. Den eigenen Körper hingegen trägt jeder ständig mit sich herum, man kann ihn weder verlieren noch an andere weitergeben. Im Kern funktionieren alle biometrischen Methoden nach demselben Prinzip: Ein Sensor, etwa eine Videokamera oder ein Fingerabdruck-Scanner, liest ein Körpermerkmal ein. Aus dem digitalisierten Bild, zum Beispiel von einem eingescannten Fingerabdruck, gewinnt ein Computerprogramm bestimmte Charakteristika und reduziert das Körpermerkmal letztlich auf einen Zahlenwert. Nur dieser Wert und nicht der Fingerabdruck oder das Foto selbst wird dann mit einem gespeicherten Datensatz abgeglichen. Aus diesem so genannten Template, gewissermassen dem mathematischen Skelett, lässt sich das Originalbild nicht mehr rekonstruieren. Beispielsweise erlauben die so genannten Minutien eines Fingerabdrucks - Charakteristika der Papillarlinien - keinen Rückschluss auf das eingescannte Bild.

Das klingt nach hoher Sicherheit und effizientem Datenschutz: Aus den Biometriedaten allein könnte niemand Ihr Gesicht nachbilden.

"Absolute Identifizierung ist eine verlockende Idee", schreibt der US-Datenschutzexperte Simson Garfinkel in seinem Buch *Database Nation.* "Unglücklicherweise hat sie einen fundamentalen Fehler: Diese Methoden identifizieren nicht Menschen, sondern Körper."

Biometrische Merkmale zu fälschen ist extrem schwierig, aber im Prinzip machbar. Dazu muss man auch gar nicht das Auge des Opfers stehlen wie im James-Bond-Film. Es gab bereits Fälle, in denen ein Fingerabdruck aus Silikon modelliert wurde, um ein Erkennungssystem auszutricksen. Allerdings sind moderne Fingerabdrucksysteme durchaus in den Lage, einen toten Finger von einem lebenden zu unterscheiden, etwa

mit Infrarotlicht im Sensor, das von totem Gewebe nicht genügend reflektiert wird.

Das nützt allerdings wenig, wenn das Gesamtsystem unsicher ist. Statt das Merkmal selbst zu fälschen, was sehr aufwändig ist, könnten Hacker die übermittelten biometrischen Daten stehlen. Im Rahmen einer Studie des Bundesamts für Sicherheit in der Informationstechnik (BSI) aus dem Frühjahr 2000 konnten Experten des Fraunhofer-Instituts für Grafische Datenverarbeitung eine Reihe von kommerziellen Biometriesystemen knacken. Verwundbar sind viele Systeme nicht bloß für die bereits erwähnten Replay-Attacken, bei denen das Bild eines Merkmals einfach nochmals vorgespielt wird. Angreifer könnten auch versuchen, den Schwellwert eines Systems zu manipulieren. Kein biometrisches Template stimmt nämlich mit dem anderen überein - selbst dann nicht, wenn es sich um ein und dieselbe Person handelt. Der Grund sind Abweichungen, für die die Natur selbst verantwortlich ist. Bei Fingerabdrucksystemen kann sich eine Abweichung selbst dann ergeben, wenn die biometrischen Daten einer Person bloß ein paar Momente später gemessen werden. Deshalb muss der mathematische Algorithmus in der biometrischen Software gewissermaßen entscheiden, ob die "Ähnlichkeit" zwischen den Datensätzen ausreichend ist für die Identifizierung. Ein Hacker könnte nun versuchen, diesen Toleranzwert zu manipulieren, um vom System akzeptiert zu werden.

"Biometrie ist nur dann toll, wenn das System zwei Dinge prüfen kann: erstens, dass die biometrischen Daten von der Person zum Zeitpunkt der Überprüfung stammen. Zweitens, dass diese Daten mit den als Muster abgespeicherten Daten übereinstimmen", sagt der US-Kryptografie- und Sicherheitsexperte Bruce Schneier. "Wenn das System nicht beides kann, ist es unsicher."

Wie verwundbar die Methoden sein können, demonstrierte auch ein Forscherteam von IBM. Die Wissenschaftler fanden insgesamt acht mögliche Attacken gegen ein biometrisches System. Eine besonders raffinierte Methode besteht darin, ein so genanntes Trojanisches Pferd, eine Art von Computervirus, einzuschleusen. Der Virus versorgt einfach jenes Programm, das die biometrischen Merkmale aus dem eingescannten Bild extrahiert, mit falschen Daten. Möglich ist schließlich auch, das Endresultat des biometrischen Vorgangs zu manipulieren - man veranlasst das System einfach dazu, trotz korrekter Eingabe und Analyse der Daten das falsche Ergebnis auszuspucken. Die Schlussfolgerung der Forscher ist ernüchternd: "Auch biometrische Systeme sind verwundbar, wenn sie von wirklich entschlossenen Hackern attackiert werden."

Ein Grund dafür liegt auch darin, dass die Technik selbst bislang noch keine großen Bewährungsproben in der Praxis zu bestehen hatte. Zudem gibt es bis heute keine weltweit einheitlichen Richtlinien für die Bewertung der Sicherheit biometrischer Systeme: Die Hersteller neigen aus nahe liegenden Gründen dazu, ihre Methoden unter optimalen, aber idealisierten Laborbedingungen zu testen.

Man hat nur zwei Daumen

"Biometrie ist eine noch junge Technik", sagt Axel Munde, Biometrieexperte beim BSI. Die Herstellerfirmen seien häufig Kleinunternehmen mit universitärem Hintergrund und wenig praktischer Erfahrung. "Wir haben festgestellt, dass viele Hersteller wenig über Computersicherheit wissen."

Biometrische Daten sind an sich nicht geheim. Permanent hinterlassen wir beispielsweise Fingerabdrücke an vielen Orten. Damit sie nicht in falsche Hände geraten, bedarf es vor allem starker Verschlüsselung. Die Hamburger Biometriefirma Dermalog etwa hat für das fernöstliche Sultanat Brunei eine Vielzweckkarte entwickelt, die nicht bloß als Personalausweis, sondern auch als Sozialversicherungskarte sowie zur Identifizierung für eine Reihe weiterer Anwendungen fungiert. Auf der Karte sind zwei Fingerabdruck-Templates sowie das komprimierte Foto der Person gespeichert. Starke Verschlüsselung soll den Chip vor einem Zugriff schützen. "Wird nur ein Bit geändert, sind die Daten unbrauchbar", sagt Geschäftsführer Gunther Mull.

Nach der Erfassung der Daten muss das System nicht nur prüfen, ob die Biometrie stimmt, sondern auch erkennen können, ob die übermittelten Daten mit den tatsächlich erfassten übereinstimmen. So genannte *challenge and response*-Methoden sorgen dafür, dass Systeme reagieren, wenn jemand etwa ein Kabel anzuzapfen versucht. Bei einigen Systemen muss sich die Videokamera gegenüber dem Computer mit einer Nummer identifizieren, um sicherzustellen, dass die Daten auch von der richtigen Stelle kommen. Digitale Wasserzeichen können garantieren, dass ein Datensatz nicht unterwegs verfälscht wurde.

Bei Hacker-Attacken erweist sich die große Stärke biometrischer Methoden, dass sich nämlich biometrische Merkmale während eines Menschenlebens nicht verändern, als gravierende Schwäche. Verliert jemand sein Passwort oder sein digitales Zertifikat, braucht er bloß ein neues zu beantragen - kein Problem. Aber was, wenn zum Beispiel die biometrischen Daten des rechten Daumens gestohlen werden? Dann ist das entsprechende Merkmal auf Dauer kompromittiert und lässt sich nicht mehr gebrauchen. Eines der zentralen Probleme biometrischer Systeme besteht deshalb darin, ein Merkmal zu widerrufen, damit es nicht missbraucht werden

kann.

Das Ausweichen auf ein nicht kompromittiertes Merkmal ist bloß eine vorübergehende Lösung. Denn die Anzahl der Finger ist begrenzt. US-Sicherheitsexperte Schneier kommentiert das lakonisch: "Man hat eben nur zwei Daumen. Wenn jemand Ihre Biometriedaten gestohlen hat, bleiben sie für immer gestohlen. Nichts kann sie zurückholen."

Und stiehlt jemand Ihr Gesicht, haben Sie nicht einmal ein zweites.

Mitarbeit: Sven Scheffler