Andreas Pfitzmann

Biometrie

Neue Sicherheitsprobleme

Überwachbarkeit und Datenschutz müssen nicht nur innerhalb einzelner Anwendungen (wie Reise- und Zahlungsverkehr, E-Mail, Überwachungskameras, ...) ausbalanciert werden, sondern über Anwendungen hinweg. Die geplanten Pässe schaffen ernste Sicherheitsprobleme. Fingerabdrücke in Pässen fördern Kriminalität mehr, als sie sie bekämpfen, und erschweren polizeiliche Ermittlungen – also keine Fingerabdrücke in Pässen!

In der Biometrie werden Körper- oder Verhaltensmerkmale gemessen, um durch Vergleich mit Referenzwerten Menschen zu authentifizieren oder zu identifizieren. Die Fehlerrate beim Erkennen (und Zulassen) hängt reziprok mit der beim Nicht-Erkennen (Abweisen) zusammen. Heute und zumindest auch in der überschaubaren Zukunft können nicht beide Fehlerraten so weit gesenkt werden, wie wir dies von Systemen kennen, die auf Wissen (z.B. Passwort/PIN) oder Besitz (z.B. Chipkarte) der Menschen beruhen.

Sicherheitsprobleme für klassische forensische Techniken

1. Verbreitete und umfangreiche Datenbanken mit Fingerabdrücken oder generelles „Abgeben" des Fingerabdrucks erleichtern den Nachbau von „Fingern" und damit das Hinterlassen falscher Fingerabdrücke. Je mehr Fingerabdrücke mit Kontextdaten zur Auswahl stehen, desto hilfreicher für Kriminelle und fremde Geheimdienste.

2. Werden mittels Fingerabdruck-Biometrie große Werte gesichert, wird eine Finger-Nachbau-„Industrie" entstehen.

3. Da Infrastrukturen beispielsweise für Grenzkontrollen weniger schnell zu aktualisieren sind als einzelne Maschinen zum Fingernachbau, ist insgesamt ein Sicherheitsverlust zu erwarten.

Diebstahl von Körperteilen

4. Die (vermeintliche) Verbesserung der Sicherheit durch Biometrie kann die körperliche Unversehrtheit der Betroffenen gefährden. Es wurden schon Finger abgeschnitten, um ein Auto zu stehlen.

5. Sollte biometrische Lebenderkennung funktionieren, dürften Entführung oder Erpressung den Diebstahl von Körperteilen ersetzen.

Datenschutzprobleme

Datenschutz durch Löschung funktioniert im Internet nicht, da man alle Kopien entdecken müsste: Bereits die Erhebung der Daten muss vermieden werden.

Es ist ein wesentlicher Unterschied, ob der zu vermessende Mensch explizit mitwirken muss (aktive Biometrie), sodass er sich der Messung bewusst ist, oder ob seine Mitwirkung unnötig ist (passive Biometrie), sodass eine Messung ohne sein Wissen erfolgen kann.

6. Daten lassen sich ohne Information der Betroffenen erheben und auswerten, z.B. bei der Gesichts- oder Spracherkennung.

7. Ein Netzhaut-Scan liefert Daten über den Alkoholkonsum der letzten beiden Tage, der Fingerabdruck möglicherweise über Homosexualität. Das kann Menschen erpressbar machen.

8. RFIDs in Pässen sind unsicher. Das RFID kann auslesen, wer immer Zugriff auf den Papierteil hatte (ausstellendes Land, Grenzposten bei Ein- oder Ausreise, Händler, die z.B. Mobilfunkverträge verkaufen und dabei eine Papierkopie des Passes erhalten) oder die Kooperation einer solchen Person. RFIDs in Pässen müssen deshalb entweder vermieden oder beispielsweise durch eine metallische Hülle des Passes vor unbemerktem Auslesen geschützt werden.

9. Werden mehrere biometrische Merkmale erfasst, um die Unsicherheit einzelner Merkmale zu kompensieren, vervielfacht dies das Datenschutzproblem.

Über den Autor
Prof. Dr. Andreas Pfitzmann leitet seit 1993 die Forschungsgruppe „Datenschutz und Datensicherheit" an der Fak. Informatik der TU Dresden. Er war Sachverständiger für das Bundesverfassungsgericht, unterschiedliche Bundesregierungen, mehrere Parteien, die EU-Kommission und die OECD.

Enttarnung gewünschter Mehrfachidentitäten

Staaten werden nicht nur Terroristen und Kriminelle, sondern auch fremde Geheimdienstagenten enttarnen wollen und dazu personenbezogene Biometriedatenbanken anlegen. Die organisierte Kriminalität wird Biometriedatenbanken zur Enttarnung verdeckter Ermittler oder von Personen in Zeugenschutzprogrammen anlegen.

Biometrie – wie einsetzen und wie keinesfalls?

Zwischen Menschen und ihren Geräten ist die Authentifizierung durch Besitz und/oder Wissen *und* Biometrie unproblematisch. Forensische Techniken werden nicht entwertet, es entstehen keine Datenschutzprobleme.

Es bleibt das Problem des Diebstahls von Körperteilen. Eine Abschaltmöglichkeit der Biometrie nach der Authentifizierung kann Entführungsopfern die Chance geben, durch Kooperation mit ihren Entführern unversehrt zu bleiben. Auch Kompromisse zwischen keinerlei Abschaltbarkeit und vollständiger, dauerhafter Abschaltbarkeit können sinnvoll sein, natürlich nur, wenn allgemein bekannt.

Wir sollten anderen Staaten das Anlegen von Biometrie-Datenbanken über ihre Besucher weder durch ein „Abrichten“ auf brave Mitwirkung an jedem beliebigen Lesegerät erleichtern noch durch Maschinenlesbarkeit unserer Reisepässe verbilligen. In Demokratien ist vor dem breiten Einsatz von Biometrie in Infrastrukturen, etwa in Ausweisen, eine qualifizierte, plurale Debatte nötig. Sie wird bisher von den Innen- und Sicherheitspolitikern der westlichen Industriestaaten verweigert oder – wo dies nicht möglich ist – durch unhaltbare Versprechungen oder grob einseitige Problemdarstellungen manipuliert.

Passive Biometrie durch fremde Geräte ist vom Betroffenen nicht erkennbar und darum kaum zu verhindern. Verdeckt angewandte technisch unterstützte Biometrie sollte unter Strafe gestellt werden.

erschienen in der FIfF-Kommunikation,
herausgegeben von FIfF e.V. - ISSN 0938-3476
www.fiff.de