

1

# Biometrie – wie einsetzen und wie keinesfalls?

**Wie umgehen mit Sicherheitsproblemen von Biometrie und  
Sicherheits- und Datenschutzproblemen durch Biometrie?**

Andreas Pfitzmann

TU Dresden, Fakultät Informatik, D-01062 Dresden  
Hans-Grundig-Str. 25, Raum 120  
Tel.: 0351/ 463-38277, e-mail: [pfitza@inf.tu-dresden.de](mailto:pfitza@inf.tu-dresden.de), <http://dud.inf.tu-dresden.de/>

2

## Gliederung

1. Was ist Biometrie?
2. Wozu Biometrie?
  - Authentifizieren vs. Identifizieren
3. Sicherheitsprobleme von Biometrie
  - FMR vs. FNR
4. Sicherheitsprobleme durch Biometrie
  - Entwertung klassischer forensischer Techniken
  - Safety-Problem: Fingerdiebstahl, um Auto stehlen zu können
  - Enttarnbarkeit gewünschter Mehrfachidentitäten
5. Datenschutzprobleme durch Biometrie
  - Medizinisch relevante Daten, z.B. Netzhaut-Scan
  - Auswertung ohne Information des Betroffenen, z.B. Gesichtserkennung
6. Wie einsetzen und wie keinesfalls?
  - Nur zwischen Mensch und seinen Geräten!
7. Ausblick

## 1. Was ist Biometrie ?

3

**Körper- oder Verhaltensmerkmale werden gemessen,**  
z.B.:

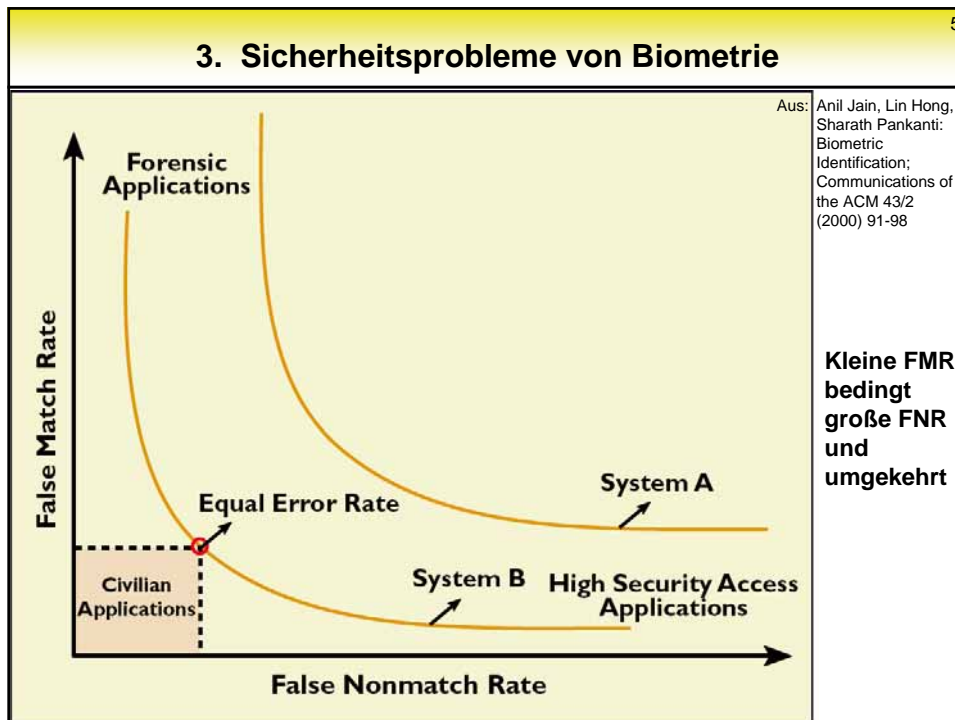
- Gesicht(sform)
- Temperaturverteilung Gesicht
- Fingerabdruck
- Handgeometrie
- Muster der Netzhaut
- ...
- Eigenhändige Unterschrift
- Stimme
- ...

## 2. Wozu Biometrie ?

4

Körper- oder Verhaltensmerkmale werden gemessen, um  
durch Vergleich mit Referenzwerten Menschen zu

- **Authentifizieren** (Ist dies der, der er behauptet zu sein?)  
oder gar zu
- **Identifizieren** (Wer ist das?).



- 6
- ### 4. Sicherheitsprobleme durch Biometrie (1)
- **Entwertung klassischer forensischer Techniken**
    - Beispielsweise erleichtern Datenbanken mit Fingerabdrücken oder weit verbreitetes „Abgeben“ des eigenen Fingerabdrucks den Nachbau von „Fingern“ und damit das Hinterlassen falscher Fingerabdrücke am Tatort erheblich.
    - Werden mittels Fingerabdruck-Biometrie große Werte gesichert, wird eine **Finger-Nachbau-Industrie** entstehen.
    - Da Infrastrukturen z.B. für Grenzkontrollen weniger schnell upgradebar sind als einzelne Maschinen zum Fingernachbau, ist **insgesamt ein Sicherheitsverlust** zu erwarten.
  - **Diebstahl von Körperteilen (Safety-Problem der Biometrie)**
    - Bsp.: **Finger abgeschnitten**, um S-Klasse Mercedes zu stehlen.
    - Selbst eine **temporäre** (oder auch nur **vermeintliche**) **Verbesserung** der „Sicherheit“ durch Biometrie ist nicht unbedingt ein Fortschritt, sondern gefährdet die körperliche Unversehrtheit der Betroffenen.
    - Sollte biometrische **Lebenderkennung** funktionieren, dürfte **Entführung oder Erpressung** an die Stelle von Diebstahl von Körperteilen treten.

#### 4. Sicherheitsprobleme durch Biometrie (2)

7

- **Auch gewünschte Mehrfachidentitäten könnten leichter enttarnbar werden**
  - **Geheimdienstagenten** – jeder Staat wird biometrische Datenbanken zumindest für alle „fremden“ Staatsbürger anlegen
  - **Verdeckte Ermittler und Personen in Zeugenschutzprogrammen** – insbesondere die organisierte Kriminalität wird biometrische Datenbanken anlegen

#### 5. Datenschutzprobleme durch Biometrie

8

- **Medizinisch relevante Daten**, z.B. Netzhaut-Scan liefert u.a. Daten über Alkoholkonsum
- Auswertung **ohne Information des Betroffenen**, z.B. Gesichtserkennung
- **Erfassung mehrerer biometrischer Merkmale**, um die Unsicherheit einzelner Merkmale zu kompensieren, vervielfacht das Datenschutzproblem (vgl. Mosaiktheorie des Datenschutzes).

Datenschutz durch Löschen von Daten funktioniert im Internet nicht, da man *alle* Kopien erwischen müsste. Also muss bereits die Erfassungsmöglichkeit der Daten vermieden werden.

## 6. Wie einsetzen und wie keinesfalls ?

9

- Zwischen **Mensch** und **seinen Geräten**
  - Authentifizierung durch Besitz und/oder Wissen *und* Biometrie
  - Keine Entwertung klassischer forensischer Techniken
  - Keine Datenschutzprobleme durch Biometrie
  - Aber: Safety-Problem bleibt bestehen  
⇒ ggf. Abschaltmöglichkeit der Biometrie nach erfolgreicher biometrischer Authentifizierung vorsehen
- Aktive Biometrie (d.h. Mensch tut etwas explizit) in Pässen und/oder gegenüber „fremden“ Geräten kann und sollte vermieden werden!
- Passive Biometrie durch fremde Geräte ist leider kaum zu verhindern.

## 7. Ausblick

10

- **Balancierung** sollte nicht nur innerhalb einzelner Anwendungen, sondern **über Anwendungen hinweg** erfolgen.
- **Genomdatenbanken** werden möglicherweise die **Sicherheit von Biometrie**, die **ererbte Körpermerkmale** misst, **untergraben**.
- **Genomdatenbanken** und **Ubiquitous Computing** (= pervasive Computing = Rechner in allen Dingen und deren Vernetzung) werden **Datenschutz in der physischen Welt weitgehend untergraben**.
- **Freiräume in der digitalen Welt sind möglich** (und wohl auch notwendig, Bsp. Jugendgruppe Kirchengemeinde) **und sollten geschaffen werden** – anstatt mit hohen Kosten unsinnige (im Sinne einer Balancierung über Anwendungen hinweg) Vorratsdatenspeicherung anzustreben.


11

**Ein weiteres aktuelles Thema im Umfeld Pässe: RFIDs**

- **RFIDs in Reisepässen** (ab Herbst 2005 in Deutschland) **und Personalausweisen** (ab 2007) **unterstützen** nicht nur das Erstellen von Bewegungsprofilen, sondern auch **den Bau von personenspezifischen Bomben**, die genau dann explodieren, wenn ein bestimmter Pass(inhaber) ganz in der Nähe ist.
- Die **Verbesserung von BSI et al. bzgl. der Sicherheit der RFIDs in europäischen Pässen (basic access control) ändert daran nichts:**  
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 von so jemand, kann das RFID auslesen, wenn immer es in der Nähe ist.

12

**Sicherheit von RFIDs vom BSI et al. ungenügend verbessert**



**Das Lesegerät muss sich gegenüber dem RF-Chip auf den neuen Ausweisen authentisieren. Dafür benötigt das Lesegerät einen geheimen Zugriffsschlüssel, der sich aus der maschinenlesbaren Zone des Reisepasses berechnet.**

Aus:  
 Dr. Dennis Kügler:  
 Risiko Reisepass?  
 Schutz der  
 biometrischen Daten  
 im RF-Chip; ct  
 5/2005, Seite 88

Was bringt PKI für Lesegeräte ? <span style="float: right;">13</span>
<p>Lesegerät identifiziert sich gegenüber RFID-Chip (z.B. signiert Challenge und sendet PKI-Zertifikat für seinen Public Key), bevor RFID-Chip irgendetwas Chip-Spezifisches überträgt.</p> <ul style="list-style-type: none"> <li>• Wenn PKI nur für Zugriff auf <b>manche Passdatenfelder</b> benutzt, bringt PKI bzgl. der Verhinderung von Bewegungsprofilen und personenspezifischen Bomben <b>wenig bzw. nichts</b> (<a href="#">extended access control</a>).</li> <li>• Wenn <b>PKI für jeden Zugriff</b> und <b>kein Klonen von Lesegeräten</b> möglich und <b>kein Schurkenstaat</b> beteiligt (was wegen der universellen Gültigkeit des Passes praktisch bedeutet: kein Schurkenstaat auf Erden), dann <b>RFID-Zugriffsproblem gelöst</b>.</li> <li>• Sehr wünschenswert: <b>Anzeige durch Pass</b> oder (unfälschbar!) durch Lesegerät, ob Biometriemerkmale dem Lesegerät vom Menschen gegeben werden soll.</li> </ul>

Resultierende politische Forderungen <span style="float: right;">14</span>
<ul style="list-style-type: none"> <li>• <b>Biometrie</b> sollte nicht gepushed, sondern <b>allenfalls sehr behutsam und umsichtig eingeführt</b> werden.</li> <li>• Die Erfassung und Speicherung biometrischer Merkmale <b>außerhalb des Verfügungsbereichs des Betroffenen</b> stellt ein <b>hohes Sicherheits- und Datenschutzrisiko</b> dar und sollte deshalb möglichst vermieden werden.</li> <li>• Vor der Aufnahme von maschinenlesbaren biometrischen Merkmalen in <b>Reisepässe und Personalausweise</b> ist eine nachvollziehbare <b>Kosten-/Nutzenanalyse</b> vorzulegen. Ggf. sind die Biometriepläne zu revidieren.</li> <li>• <b>RFIDs in Reisepässen und Personalausweisen gefährden</b> selbst in den bzgl. Sicherheit vom BSI et al. verbesserten Fassungen (<a href="#">basic/extended access control</a>) <b>Leib und Leben ihrer Träger</b>. RFIDs in Pässen müssen deshalb entweder komplett vermieden oder z.B. durch physische Schirmung des Passes mittels einer entsprechenden Schutzhülle gegen unbemerktes Auslesen geschützt werden.</li> </ul>

