Die geplanten Pässe haben und schaffen ernste Sicherheitsprobleme:

A. Fingerabdrücke in Pässen fördern Kriminalität mehr, als sie zu bekämpfen

B. Grundsatzüberlegungen zu Biometrie

C. Sicherheitsprobleme von und durch RFIDs

Prof. Dr. Andreas Pfitzmann

TU Dresden, Fakultät Informatik, D-01062 Dresden
Tel.: 0351/ 463-38277, e-mail: pfitza@inf.tu-dresden.de, http://dud.inf.tu-dresden.de/

23. April 2007

A. Fingerabdrücke in Pässen helfen Kriminellen ...

... und erschweren polizeiliche Ermittlungen – also keine Fingerabdrücke in Pässe!

- Die Aufnahme des biometrischen Merkmals „Fingerabdruck“ in Pässe und seine **Prüfung** werden Menschen daran gewöhnen, ihre **Fingerabdrücke an** von ihnen **nicht kontrollierbaren Geräten in hoher Qualität abzugeben**.
- Damit werden **Fingerabdrücke** (selbst bei perfektem Schutz innerhalb der Pässe, den es niemals geben wird) **vielen Akteuren zugänglich** – insbesondere auch fremden Geheimdiensten und Kriminellen.
- Digitale Fingerabdrücke können dazu verwendet werden, **Fingeroberflächen nachzubilden** und so **an Tatorten falsche Spuren zu hinterlassen** – sei es um die Ermittlungen durch falsche Fährten zu erschweren (ein lohnendes Ziel für Kriminelle) oder als Agent Anzuwerbende in eine Notsituation zu bringen (ein lohnendes Ziel für fremde Geheimdienste).

Biometrie – wie einsetzen und wie keinesfalls?

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

Grundsatzüberlegungen zu Biometrie (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
   - Sensible persönliche Daten, z.B. Netzhaut-Scan oder Fingerabdruck
   - 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 ?

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

- Gesicht(sform)
- Temperaturverteilung Gesicht
- Fingerabdruck
- Handgeometrie
- Venen-Muster der Netzhaut
- Muster der Iris
- DNS
- ...
- Dynamik des eigenhändigen Schreibens (u.a. bei Unterschrift)
- Sprechweise
- Gangbewegung
- ...

2. Wozu Biometrie ?

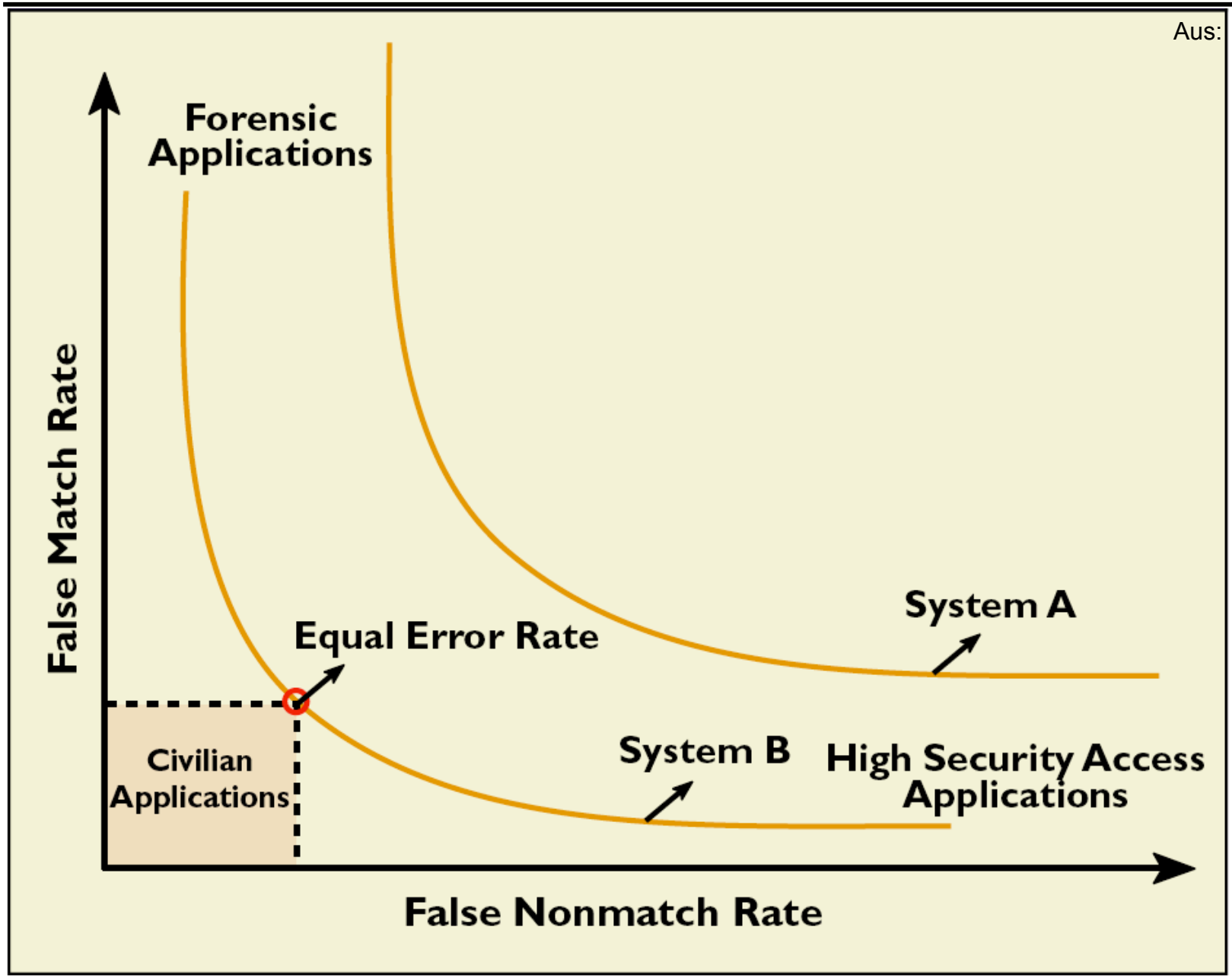
Körper- oder Verhaltensmerkmale werden gemessen, um durch Vergleich mit Referenzwerten Menschen zu

- **Authentifizieren** (Ist dies der, der er behauptet zu sein?)

oder gar zu

- **Identifizieren** (Wer ist das?).

3. Sicherheitsprobleme von Biometrie



Aus: Anil Jain, Lin Hong, Sharath Pankanti: Biometric Identification; Communications of the ACM 43/2 (2000) 91-98

Kleine FMR bedingt große FNR und umgekehrt !

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)

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

5. Datenschutzprobleme durch Biometrie

- **Sensible persönliche Daten**, z.B.
  Netzhaut-Scan liefert u.a. Daten über Alkoholkonsum,
  Fingerabdruck möglicherweise über Homosexualität

- 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 ? (1)

- 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.

6. Wie einsetzen und wie keinesfalls ? (2)

- **Visa mit Biometrie** sind bzgl. Datenschutz deutlich weniger gefährlich als **Reisepässe mit Biometrie**.
  - **Fremde Länder** werden versuchen, über Besucher personenbezogene **Biometriedatenbanken** aufzubauen – wir sollten es ihnen weder erleichtern noch durch Maschinenlesbarkeit unserer Reisepässe verbilligen.
  - Die **organisierte Kriminalität** wird versuchen, personenbezogene **Biometriedatenbanken** aufzubauen – wir sollten es ihr nicht erleichtern, indem wir das Abgeben biometrischer Merkmale an „fremden“ Geräten zur Normalität erklären oder gar noch durch unkontrollierte Maschinenlesbarkeit unserer Reisepässe unterstützen (vgl. Unsicherheit der RFID-Chips gegen unautorisiertes Auslesen).
  - **Unterschiedliche Messungen** und damit **unterschiedliche Werte** biometrischer Merkmale eignen sich – da biometrisches Identifizieren bei weitem nicht perfekt klappt – **weniger** als **Personenkennzeichen** als ein über 10 Jahre konstanter digitaler Referenzwert im Reisepass. Dies gilt natürlich nur, wenn die unterschiedlichen Messergebnisse zumindest nicht immer von einem konstanten Personenkennzeichen wie der Passnummer „begleitet“ werden.

7. Ausblick

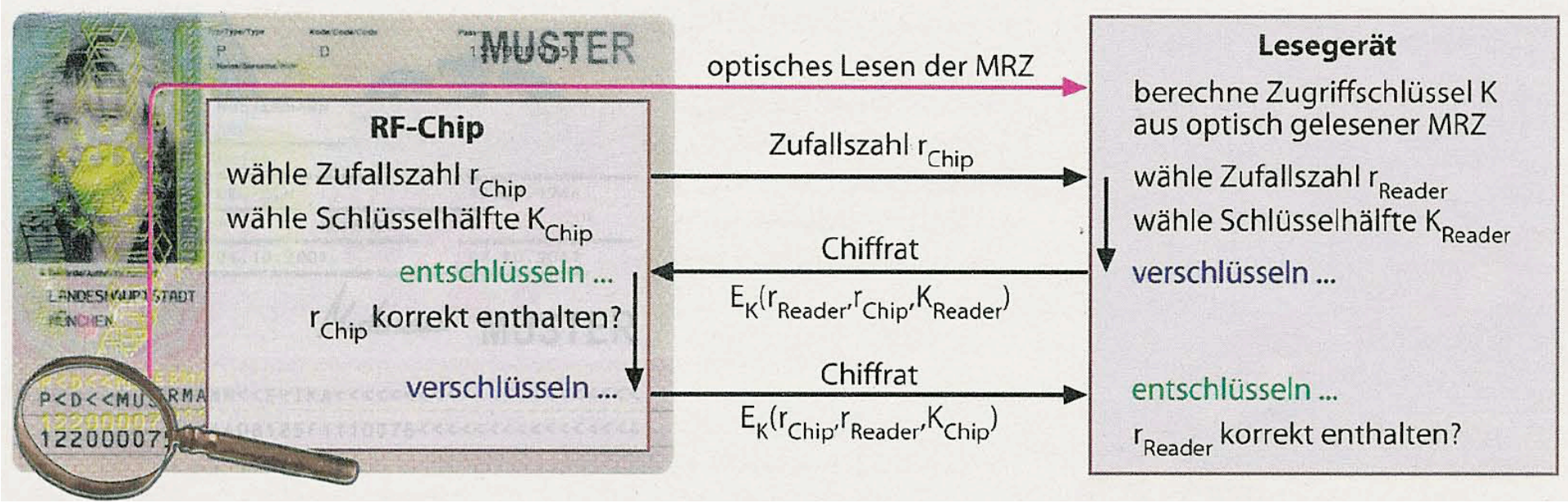
- **Balancierung** sollte nicht nur innerhalb einzelner Anwendungen, sondern **über Anwendungen hinweg** erfolgen.
- **Genomdatenbanken** werden möglicherweise die **Sicherheit von Biometrie**, die **ererbte Körpermerkmale** misst, **untergraben**.
- **Genomdatenbanken** und **Ubiquitous Computing** (= 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.

C. Sicherheitsprobleme von und durch RFIDs

- **RFIDs in Reisepässen** (ab Herbst 2005 in Deutschland) **und Personalausweisen** (ab 2008) **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.

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 Dater im RF-Chip; ct 5/2005, Seite 88

Was bringt PKI für Lesegeräte ?

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.

- Wenn PKI nur für Zugriff auf **manche Passdatenfelder** benutzt, bringt PKI bzgl. der Verhinderung von Bewegungsprofilen und personenspezifischen Bomben **wenig bzw. nichts** (extended access control).
- Wenn *PKI* ***für jeden Zugriff*** und ***kein Klonen von Lesegeräten*** *möglich* und ***kein Schurkenstaat*** *beteiligt* (was wegen der universellen Gültigkeit des Passes praktisch bedeutet: kein Schurkenstaat auf Erden), dann **RFID-Zugriffsproblem gelöst**.
- Sehr wünschenswert: **Anzeige durch Pass** oder (unfälschbar!) durch Lesegerät, ob Biometriemerkmal dem Lesegerät vom Menschen gegeben werden soll.

Resultierende politische Forderungen

- **Biometrie** sollte nicht gepushed, sondern **allenfalls sehr behutsam und umsichtig eingeführt** werden.
- Die Erfassung und Speicherung biometrischer Merkmale **außerhalb des Verfügungsbereichs des Betroffenen** stellt ein **hohes Sicherheits- und Datenschutzrisiko** dar und sollte deshalb möglichst vermieden werden.
- Vor der Aufnahme von maschinenlesbaren biometrischen Merkmalen in **Reisepässe und Personalausweise** ist eine nachvollziehbare **Kosten-/Nutzenanalyse** vorzulegen. Ggf. sind die Biometriepläne zu revidieren.
- **RFIDs in Reisepässen und Personalausweisen gefährden** selbst in den bzgl. Sicherheit vom BSI et al. verbesserten Fassungen (basic/extended access control) **Leib und Leben ihrer Träger**. 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.

Biometrie – wie einsetzen und wie keinesfalls? *

Andreas Pfitzmann

Biometrie wird als Lösung vieler Authentifizierungs- und Identifizierungsprobleme angepriesen. Sie weist jedoch ein grundlegendes Sicherheitsproblem auf und verursacht zusätzlich Sicherheits- und Datenschutzprobleme. Was genau kann Biometrie, was nicht, und welche Gestaltungsaufgaben stellen sich?

Was ist Biometrie?

Als Biometrie wird das Messen von Körper- oder Verhaltensmerkmalen bezeichnet. Gemessen werden können beispielsweise die *Körpermerkmale*

- Gesicht(sform)
- Temperaturverteilung des Gesichts
- Fingerabdruck
- Handgeometrie
- Venen-Muster der Netzhaut
- Muster der Iris
- DNS

oder beispielsweise die *Verhaltensmerkmale*

- Dynamik des eigenhändigen Schreibens (u.a. bei Unterschriften)
- Sprechweise
- Gangbewegung

Unterschieden werden kann danach, ob der Mensch, dessen Körper- oder Verhaltensmerkmale gemessen werden, hierbei explizit mitwirken muss (*aktive* Biometrie), so dass er sich der Messung bewusst ist, oder ob seine explizite Mitwirkung nicht nötig ist (*passive* Biometrie), so dass solch eine Messung ohne seine Kenntnis erfolgen kann.

Wozu Biometrie?

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

- *authentifizieren* (Ist dies derjenige, der er behauptet zu sein?)

oder gar zu

- *identifizieren* (Wer ist das?).

Beides wird umso schwieriger, je größer die Menge ist, aus der Menschen authentifiziert oder gar identifiziert werden sollen. Besonders im Fall der Identifizierung nimmt die Genauigkeit biometrischer Verfahren mit der Anzahl möglicher Personen stark ab.

Sicherheitsprobleme von Biometrie

Wie bei allen Entscheidungsproblemen kann man auch bei biometrischen Authentifizierungs-/Identifizierungsverfahren zwei Arten von Fehlern beobachten:

- Menschen werden fälschlicherweise abgewiesen bzw. nicht erkannt.
- Menschen werden fälschlicherweise authentifiziert oder falsch identifiziert.

* Überarbeitung und Erweiterung eines in digma, Zeitschrift für Datenrecht und Informationssicherheit, Schulthess 5/4 (Dez. 2005) 154–157 erschienenen Artikels.

DOI 10.1007/s00287-006-0098-4

Prof. Dr. Andreas Pfitzmann
Fakultät Informatik,
Institut für Systemarchitektur,
TU Dresden,
01062 Dresden
E-mail: Andreas.Pfitzmann@tu-dresden.de

Das Dilemma der (biometrischen) Mustererkennung ist folgendes [3]: Macht man den Vergleich auf Ähnlichkeit strenger, dann werden zwar Menschen seltener fälschlicherweise authentifiziert oder falsch identifiziert – es kommt aber auch häufiger zu falschen Abweisungen bzw. Nichterkennen. Macht man den Vergleich lässiger, dann werden Menschen zwar seltener fälschlicherweise abgewiesen bzw. nicht erkannt – es kommt aber auch häufiger zu einer falschen Authentifizierung oder falschen Identifizierung. Die Praxis hat gezeigt: Man kann die Häufigkeit höchstens einer Fehlerart minimieren – und dies nur um den Preis, dass die Häufigkeit der anderen steigt. Kurzum: Ein biometrisches Verfahren ist für eine bestimmte Einsatzumgebung sicherer als ein anderes, wenn dort *beide* Fehlerarten seltener auftreten.

Zwar kann Biometrie über die Strenge des Vergleichs auf Ähnlichkeit an unterschiedliche Einsatzbereiche in gewissen Grenzen angepasst werden. Aber möchte man auch nur eine der beiden Fehlerraten soweit senken, wie wir dies von gut gemanagten Authentisierungs- bzw. Identifikationssystemen anderer Art kennen, die auf Wissen der Menschen (z.B. Passphrase) oder ihrem Besitz (z.B. Chipkarte) beruhen, haben die heutigen biometrischen Verfahren als andere Fehlerrate jeweils eine unakzeptabel hohe Fehlerrate.

Seit mehr als 20 Jahren wird angekündigt, die biometrische Forschung würde dies in zwei, spätestens vier Jahren ändern. Langsam zweifle ich daran, ob es solch ein biometrisches Verfahren überhaupt gibt, sofern man die von den Verfechtern der Biometrie versprochene Benutzungsfreundlichkeit (welche die Qualität der der Mustererkennung zugrunde liegenden Daten begrenzt) sowie akzeptable Kosten (trotz der vom technischen Fortschritt ebenfalls profitierenden Angreifer, s.u.) als zusätzliche Bedingungen sieht.

Zusätzlich zum beschriebenen Entscheidungsproblem, das ein inhärentes Sicherheitsproblem der Biometrie ist, muss die Implementierung biometrischer Authentifizierungs-/Identifizierungsverfahren sicherstellen, dass die biometrischen Messdaten aktuell von der zu messenden Person kommen, d.h. weder von einer Messung in der Vergangenheit noch von einer Messung an einem anderen Ort [5]. Dies sicherzustellen kann schwieriger sein, als es klingt. Es ist aber ein allgemeines Problem aller Authentifizierungs-/Identifizierungsverfahren.

Sicherheitsprobleme durch Biometrie

Biometrie *hat* nicht nur die gerade skizzierten Sicherheitsprobleme, sondern der Einsatz biometrischer Verfahren *verursacht* auch gravierende Sicherheitsprobleme. Beispiele hierfür werde ich im Folgenden darstellen.

Entwertung klassischer forensischer Techniken

Ein verbreiteter Einsatz von Biometrie kann klassische forensische Techniken entwerten, wie dies am Beispiel von Fingerabdrücken als Fahndungs- und Beweismittel skizziert wird:

- Datenbanken mit Fingerabdrücken oder weit verbreitetes qualitativ hochwertiges „Abgeben" des eigenen Fingerabdrucks erleichtern den Nachbau von „Fingern" und damit das Hinterlassen falscher Fingerabdrücke am Tatort erheblich.
- Wenn mittels Fingerabdruck-Biometrie große Werte gesichert werden, wird vermutlich eine Fingernachbau-„Industrie" entstehen.
- Da Infrastrukturen z.B. für Grenzkontrollen weniger schnell auf den neuesten Stand gebracht werden können als einzelne Maschinen zum Fingernachbau in den Händen der Angreifer, ist insgesamt ein Sicherheitsverlust zu erwarten.

Diebstahl von Körperteilen (Safety-Problem der Biometrie)

Es ging bereits eine Meldung durch die Presse, nach der dem Fahrer eines S-Klasse Mercedes ein Finger abgeschnitten worden sei, um sein Auto zu stehlen. Unabhängig vom Wahrheitsgehalt der Meldung verdeutlicht sie ein Problem, das ich das Safety-Problem der Biometrie nenne:

- Selbst eine temporäre (oder auch nur vermeintliche) Verbesserung der „Sicherheit" durch Biometrie ist nicht unbedingt ein Fortschritt, sondern gefährdet die körperliche Unversehrtheit ihrer Nutzer.
- Sollte biometrische Lebenderkennung jemals funktionieren, dürfte Entführung oder Erpressung an die Stelle des Diebstahls von Körperteilen treten.

Auch gewünschte Mehrfachidentitäten könnten leichter enttarnbar werden

Der naive Traum mancher Sicherheitspolitiker, Menschen biometrisch eindeutig (wieder)erkennen zu können, wird zum Alptraum, wenn wir nicht verdrängen, dass es in unseren Gesellschaften auch und gerade im Umfeld von Geheimdienst und Polizei

akzeptierte und vielfältig nützliche Mehrfachidentitäten für Geheimdienstagenten, verdeckte Ermittler sowie Personen in Zeugenschutzprogrammen gibt und weiterhin geben muss. Die Auswirkungen eines weit verbreiteten Einsatzes von Biometrie wären:

- Um Geheimdienstagenten leichter enttarnen zu können, wird jeder Staat personenbezogene Biometrie-Datenbanken zumindest für alle „fremden" Staatsbürger anlegen.
- Um verdeckte Ermittler und Personen in Zeugenschutzprogrammen leichter enttarnen zu können, wird insbesondere die organisierte Kriminalität personenbezogene Biometrie-Datenbanken anlegen.

Wer also an den Erfolg biometrischer Authentifikation und Identifikation glaubt, sollte sie gerade nicht in den Masseneinsatz im Passwesen führen.

Datenschutzprobleme durch Biometrie

Biometrie verursacht nicht nur Sicherheitsprobleme, sondern auch Datenschutzprobleme:

- Jede biometrische Messung liefert potentiell sensitive persönliche Daten, z.B. offenbart ein Netzhaut-Scan Daten über den Alkoholkonsum der vergangenen zwei Tage, und es wird diskutiert, ob Fingerabdrücke Informationen über die sexuelle Orientierung von Männern liefern [1, 2].
- Bei manchen biometrischen Verfahren (passive Biometrie) ist eine Messung und Auswertung möglich, ohne dass der Betroffene darüber informiert wird, z.B. bei Gesichts(form)erkennung.

In der Praxis werden die Sicherheitsprobleme von Biometrie ihre Datenschutzprobleme verschärfen:

- Die gleichzeitige Erfassung mehrerer biometrischer Merkmale, um die Unsicherheit einzelner Merkmale zu kompensieren, vervielfacht das Datenschutzproblem (vgl. Mosaiktheorie des Datenschutzes).

Zudem sei daran erinnert, dass Datenschutz durch Löschen von Daten in Rechnernetzen normalerweise nicht durchsetzbar ist, da man *alle* Kopien erwischen müsste. Also muss bereits die Erfassungsmöglichkeit der Daten vermieden werden, sprich die biometrische Messung unterbleiben.

Wie einsetzen und wie keinesfalls?

Gerade weil Biometrie selbst Sicherheitsprobleme besitzt sowie zusätzliche Sicherheits- und Datenschutzprobleme verursachen kann, stellt sich die Frage, wie Biometrie eingesetzt werden sollte – und wie sie keinesfalls eingesetzt werden darf.

Zwischen Menschen und ihren Geräten

Selbst biometrische Verfahren, die Menschen häufiger fälschlicherweise authentifizieren, dafür aber selten fälschlicherweise abweisen, haben zwischen dem Menschen und seinen persönlichen Geräten ihren Anwendungsplatz – auch dann, wenn sie in anderen Konstellationen viel zu unsicher wären oder dort völlig unakzeptable Datenschutzprobleme verursachen würden:

- Authentifizierung durch Besitz und/oder Wissen und zusätzlich Biometrie erreicht eine Steigerung der Sicherheit der Authentifizierung.
- Klassische forensische Techniken werden nicht entwertet, da die biometrischen Merkmale nicht die persönlichen Geräte verlassen und Menschen nicht daran gewöhnt werden, ihre biometrischen Merkmale „fremden" Geräten zu geben.
- Es gibt keine Datenschutzprobleme durch Biometrie, da jeder Mensch (hoffentlich) die Kontrolle über seine persönlichen Geräte hat (und behält).
- Zwar bleibt das Safety-Problem der Biometrie bestehen. Wird aber eine Möglichkeit zur vollständigen und dauerhaften Abschaltung der Biometrie (natürlich nur direkt nach erfolgreicher biometrischer Authentifizierung) vorgesehen und ist dies allgemein bekannt, dann gefährdet die Biometrie die körperliche Unversehrtheit kaum, sofern ihre Nutzer zur Kooperation mit entschlossenen Angreifern bereit sind. Je nach Anwendungskontext der Biometrie können auch Kompromisse zwischen keinerlei Abschaltbarkeit der Biometrie und vollständiger dauerhafter Abschaltbarkeit sinnvoll sein.

Wie keinesfalls?

Leider ist zu erwarten, dass auch in anderen Konstellationen versucht wird, Biometrie einzusetzen:

- Aktive Biometrie beim Vorlegen von Pässen und/oder gegenüber „fremden" Geräten kann vom Betroffenen erkannt werden. Dies sollte ihm helfen, sie zu vermeiden!
- Passive Biometrie durch fremde Geräte ist leider vom Betroffenen nicht erkennbar und darum kaum zu verhindern. Zumindest *verdeckt angewandte* technisch unterstützte *Biometrie sollte unter Strafe gestellt werden*.

Was bedeutet dies nun in einer Welt, wo unterschiedliche Staaten mit höchst unterschiedlichen

Sicherheitsinteressen (und meistens ohne jede Beachtung der Datenschutzinteressen von Ausländern) Visafreiheit nur gegen Aufnahme maschinenles- und -prüfbarer digitaler Biometriemerkmale bieten?

Visa oder Reisepässe mit Biometrie?

Visa mit Biometrie sind hinsichtlich des Datenschutzes deutlich weniger gefährlich als Reisepässe mit Biometrie.

- Fremde Länder werden versuchen, über Besucher personenbezogene Biometrie-Datenbanken aufzubauen – wir sollten es ihnen weder durch Gewöhnung unserer Bürger an Biometrie erleichtern noch durch Maschinenlesbarkeit unserer Reisepässe verbilligen.
- Die organisierte Kriminalität wird versuchen, personenbezogene Biometrie-Datenbanken aufzubauen – wir sollten ihr nicht dabei helfen, indem wir das Abgeben biometrischer Merkmale an „fremden" Geräten zur Normalität erklären oder sogar noch durch unkontrollierte Maschinenlesbarkeit unserer Reisepässe unterstützen (vgl. Unsicherheit der RFID-Chips gegen unautorisiertes Auslesen [6]).
- Unterschiedliche Messungen und damit unterschiedliche Werte biometrischer Merkmale eignen sich – da biometrisches Identifizieren bei weitem nicht perfekt funktioniert – weniger als Personenkennzeichen als ein über zehn Jahre konstanter digitaler Referenzwert im Reisepass. Dies gilt natürlich nur, wenn die unterschiedlichen biometrischen Messergebnisse nicht sowieso immer von einem konstanten Personenkennzeichen wie beispielsweise der Passnummer „begleitet" werden.

Ausblick

Der Einsatz von Biometrie erfordert, wie bei jedem Sicherheitsmechanismus, Umsicht und ggf. Vorsicht. Um die möglichen Vorteile von Biometrie, wie bequeme Benutzung bei moderater (Un)Sicherheit zu nutzen, sollte Biometrie ausschließlich zwischen Menschen und ihren eigenen Geräten eingesetzt werden. Dies vermeidet, bei geeigneter Implementierung, nahezu alle genannten Probleme komplett und reduziert die übrigen erheblich.

In jedem Fall ist in Demokratien vor dem breiten Einsatz von Biometrie in Infrastrukturen, etwa in Reisepässen und Ausweisen, eine qualifizierte plurale Debatte nötig. Sie hat bisher höchstens ansatzweise stattgefunden und wird von den Innen- und Sicherheitspolitikern der westlichen Industriestaaten keineswegs gefördert, sondern verweigert oder – wo dies nicht möglich ist – durch unhaltbare Versprechungen oder grob einseitige Problemdarstellungen manipuliert. Diese Ausführungen zeigen bisher verschwiegene oder gar bisher unbekannte Argumente auf und möchten so einen grundlegenden Beitrag zu einer sowohl qualifizierteren als auch breiteren Diskussion zum Einsatz von Biometrie leisten.

In einer Güterabwägung zwischen innerer Sicherheit und Datenschutz (und danach der entsprechenden Gestaltungsdiskussion für technische Authentisierungs- und Identifizierungsinfrastrukturen) sollte Folgendes erwogen werden [4]:

- Eine Balancierung zwischen Überwachbarkeit und Datenschutz sollte nicht nur innerhalb einzelner Anwendungen (wie Telefon, E-Mail, Zahlungsverkehr, Überwachungskameras etc.), sondern über Anwendungen hinweg erfolgen.
- Genomdatenbanken werden möglicherweise die Sicherheit von Biometrie, die ererbte Körpermerkmale misst, untergraben.
- Genomdatenbanken und Ubiquitous Computing (= Pervasive Computing = vernetzte Rechner in allen Dingen) werden einen konsequenten Datenschutz in der physischen Welt weitgehend unmöglich machen.
- Freiräume sind notwendig. Sie sind in der digitalen Welt möglich und sollten deshalb dort geschaffen werden – anstatt mit hohen Kosten unsinnige (im Sinne einer Balancierung über Anwendungen hinweg) Erfassungsmöglichkeiten und Vorratsdatenspeicherungen anzustreben.

Danksagung

Rainer Böhme, Katrin Borcea-Pfitzmann, Arslan Brömme, Rüdiger Dierstein, Marit Hansen, Thomas Kriegelstein und zwei anonymen Gutachtern danke ich für ein kritisches Lesen dieses Textes und für viele konstruktive Verbesserungsvorschläge.

Literatur

1. Forastieri, V.: Evidence against a Relationship between Dermatoglyphic Asymmetry and Male Sexual Orientation. Hum. Biol. 74, 861–870 (2002)
2. Hall, J.A.Y., Kimura, D.: Dermatoglyphic Asymmetry and Sexual Orientation in Men. Behav. Neurosci. 108, 1203–1206 (1994) www.sfu.ca/~dkimura/articles/derm.htm
3. Jain, A., Hong, L., Pankanti, S.: Biometric Identification. Commun. ACM 43, 91–98 (2000)
4. Pfitzmann, A.: Wird Biometrie die IT-Sicherheitsdebatte vor neue Herausforderungen stellen? DuD, Datenschutz Datensicherheit 29, 286–289 (2005)
5. Schneier, B.: The Uses and Abuses of Biometrics. Commun. ACM 42, 136 (1999)
6. dud.inf.tu-dresden.de/literatur/BITKOM2005.06.29Biometrie.pdf