Biometrics – how to put to use and how not at all?

How to handle security problems of biometrics and how to handle security and privacy problems caused by biometrics?

Andreas Pfitzmann

TU Dresden, Fakultät Informatik, D-01062 Dresden
Phone: +49 351 463-38277, e-mail: pfitza@inf.tu-dresden.de, http://dud.inf.tu-dresden.de/

Structure of Talk

1. What is biometrics?
2. Biometrics for what purpose?
   - Authentication vs. Identification
3. Security problems of biometrics
   - FMR vs. FNR
4. Security problems caused by biometrics
   - Devaluation of classic forensic techniques
   - Safety problem: Stealing a finger to steal a car
   - Wanted multiple identities could be uncovered
5. Privacy problems caused by biometrics
   - Sensitive personal data, e.g. by retina scan or fingerprint
   - Processing of personal data without the data subject getting to know of it, e.g. face recognition
6. How to put to use and how not at all?
   - Only between the data subject and his/her devices!
7. Outlook

1. What is Biometrics ?

Measuring physiological or behavioral characteristics, e.g.:

- (Shape of) Face
- Facial thermograms
- Fingerprint
- Hand geometry
- Vein patterns of the retina
- Patterns of the iris
- DNA
- ...
- Dynamics of handwriting (e.g. handwritten signature)
- Voice print
- Gait
- ...

2. Biometrics for what Purpose ?

Physiological or behavioral characteristics are measured and compared with reference values to

- **Authenticate** (Is this the person (s)he claims to be?)

or even to

- **Identify** (Who is this person?).

3. Security Problems of Biometrics

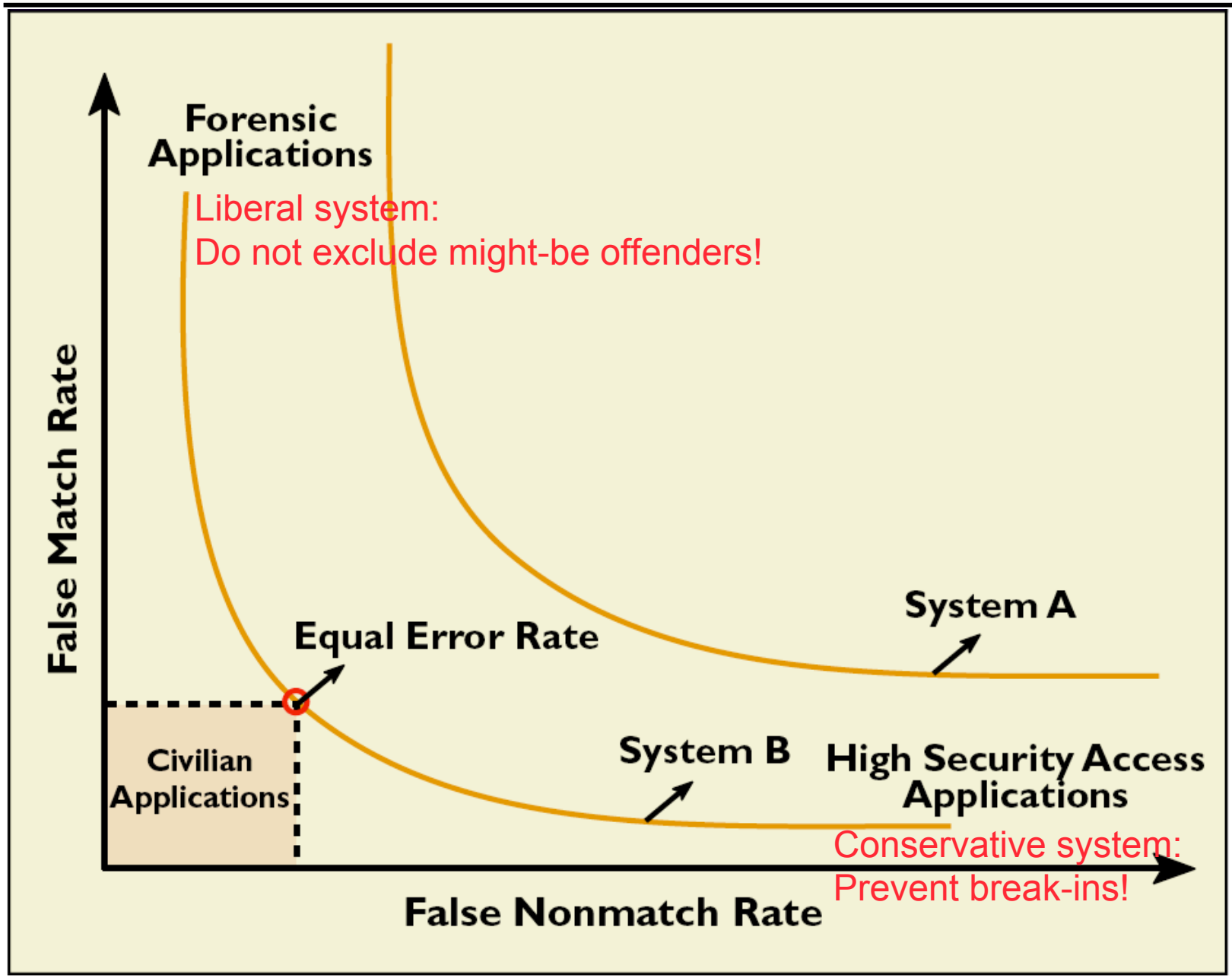


Figure taken from:

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

Low FMR causes high FNR and vice versa !

4. Security Problems caused by Biometrics (1)

- **Devaluation of classic forensic techniques**
  - **Databases of fingerprints or common issuing of one's fingerprint** essentially ease the fabrication of finger replicas and thus **leaving someone else's fingerprints at the site of crime**.
    The more fingerprints a forger has at his discretion and
    the more he knows about the holder of the fingerprints
    the higher the plausibility of somebody else's fingerprints he will leave ...
  - If biometrics employing fingerprints is used to secure huge values, an **"industry" fabricating replicas of fingers** will arise.
    If fingerprint biometrics are rolled out to the mass market,
    huge values to be secured arise by accumulation automatically.
  - As infrastructures, e.g. for border control, cannot be upgraded as fast as single machines to fabricate replicas of fingers, a **loss of security** is to be expected **overall**.

4. Security Problems caused by Biometrics (2)

- **Stealing body parts** (Safety problem of biometrics)
  - Example: **Cut off a finger**, to steal an S-class Mercedes.
  - Even a **temporary** (or only an **assumed**) **improvement** of "security" by biometrics is not necessarily an advance, but endangers physical integrity of persons.
  - If checking that the **body part** measured biometrically is **still alive** really works, **kidnapping** and **blackmailing** will replace the stealing of body parts.

- **Wanted multiple identities could be uncovered as well:**
  - **Agents of secret services** – each country will set up person-related biometric databases of all "foreign" citizens.
  - **Undercover agents** and **persons in witness-protection programs** – in particular organized crime will set up person-related biometric databases.

5. Privacy Problems caused by Biometrics

- **Sensitive personal data**, e.g.
  retina scan reveals information on consumption of alcohol, fingerprint might reveal data on homosexuality.

- Processing of personal data **without the data subject getting to know of it**, e.g. face recognition

- **Employing several kinds of biometrics in parallel** to cope with the insecurity of each single kind, multiplies the privacy problem (cf. mosaic theory of data protection).

Data protection by erasing personal data does not work on the Internet, since it is necessary to erase *all* copies. Therefore even the possibility to gather personal data has to be avoided.

6. How to put to Use and how not at all ? (1)

- Between **data subject** and **his/her devices**
  - Authentication by possession and/or knowledge *and* biometrics
  - No devaluation of classic forensic techniques
  - No privacy problems caused by biometrics
  - But: Safety problem remains unchanged
    ⇒ Provide possibility to switch off biometrics after successful biometric authentication.

- Active biometrics (i.e. person does something explicitly) in passports and/or towards “foreign” devices can be avoided and should be!

- Passive biometrics by “foreign” devices cannot be prevented – regrettably.

6. How to put to Use and how not at all ? (2)

- **Visas including biometrics** do much less endanger privacy than **passports including biometrics**.
  - **Foreign countries** will try to build up person-related **biometric databases** of visitors – we should not ease it for them nor should we make it cheaper for them by making our passports machine readable.
  - **Organized crime** will try to build up person-related **biometric databases** – we should not ease it for them by establishing it as common practice to deliver biometric data to “foreign” machines, nor should we help them by making our passports machine readable without keeping the passport holder in control (cf. insecurity of RFID-chips against unauthorized reading).
  - Since **biometric identification is all but perfect**, **different measurements** and thereby **different values** of biometric characteristics are **less** suited to become **a universal personal identifier** than a digital reference value constant for 10 years in your passport. Of course this only holds if these different values of biometric characteristics are not always “accompanied” by a constant universal personal identifier like the number of your passport.

7. Outlook

- **Balancing** surveillance and privacy should not only happen concerning single applications, but **across applications**.
- **Genome databases** will possibly **undermine the security** of biometrics **measuring inherited physiological characteristics**.
- **Genome databases** and **ubiquitous computing** (= pervasive computing = computers in all physical things connected to a network) will **undermine privacy primarily in the physical world.**
- **Privacy spaces in the digital world are possible** (and probably needed, cf. story of my Christian youth group) **and should be established** – instead of trying to gather and store traffic data for a longer period of time (data retention) at high costs and for (very) limited use (in the sense of balancing across applications).

Literature

- Andreas Pfitzmann: Biometrie – wie einsetzen und wie keinesfalls? Informatik-Spektrum 29/5 (2006) 353-356.

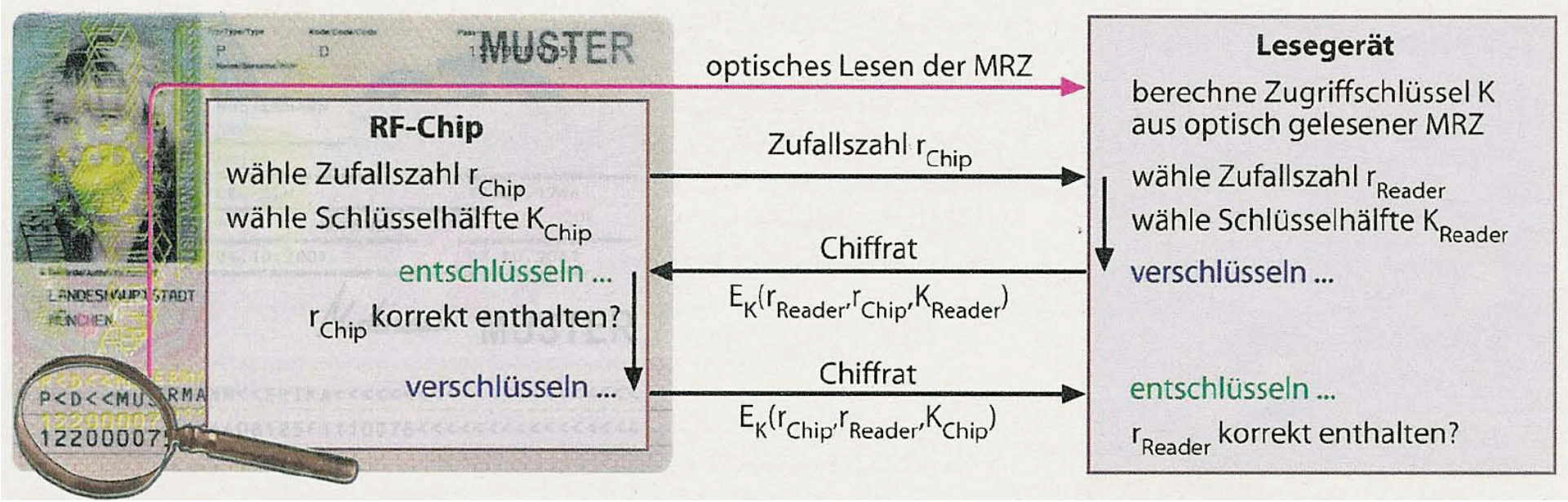
- Andreas Pfitzmann: Der ePass – innovativ, aber ein Sicherheitsrisiko; iX, Magazin für professionelle Informationstechnik /10 (Oktober 2007) 48.

Another Hot Topic w.r.t. ID-documents: RFIDs

- **RFIDs integrated into passports** (starting autumn 2005 in Germany) **and identity cards** (starting 2009 ?) **support** not only the creation of movement profiles, but also **building ID-document specific bombs** detonating exactly when (the holder of) the ID-document is in close proximity.

- The **improvement of the German BSI et al. w.r.t. the security of RFIDs in ID-documents (basic access control) does not change this**:
  Whoever did have access to the paper part of the ID-document (issuing country, immigration offices at immigration or emigration; sellers of pre-paid mobile phones requiring a photocopy of the buyer's ID-document) or colludes with someone who did, can read the RFID whenever it is in close proximity.

Security Improvement of RFIDs by BSI et al. is Insufficient



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.

Taken from:
Dr. Dennis Kügler: Risiko Reisepass? Schutz der biometrischen Dater im RF-Chip; ct 5/2005, page 88

Does PKI for RFID-readers help ?

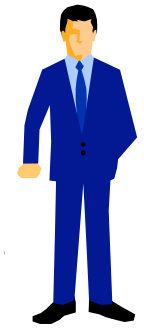
Reader identifies itself against the RFID-chip (e.g. signs a challenge and sends PKI-certificate of its public key) before the RFID-chip sends any chip-specific information.

- If PKI is only used for **access control to some of the data fields**, there is only a small gain w.r.t. creation of movement profiles and **no gain w.r.t. building ID-document specific bombs** (extended access control).
- If **PKI is used for each access** and **no cloning of readers** possible and **no failed state** participating (which for reasons of global validity of ID-documents means: no failed state on earth), then the **RFID access problem is solved**.
- Very advisable: **Output by the ID-document** or (in a way which can not be manipulated!) by the reader, whether the holder of the ID-document shall cooperate to give his/her biometric data to the reader.

Resulting political agenda

- **Biometrics** should not be pushed, but **only introduced with great care**.
- Gathering and storing biometric information **outside devices operated by the person him/herself** poses a **high security and privacy risk** and should be avoided whenever possible.
- Before incorporating digitized biometric data into **passports and identity cards**, a thorough **cost/benefit analysis** has to be conducted and discussed in the public.
  Maybe the plans to incorporate biometrics have to be revised.
- Even with the security enhancements (basic/extended access control) developed by the German BSI et al. implemented **RFIDs in ID-documents endanger body and life of their holders**. RFIDs in ID-documents either have to be completely avoided or they have to be protected against unauthorized access by physical shielding.

Identification of human beings by IT-systems



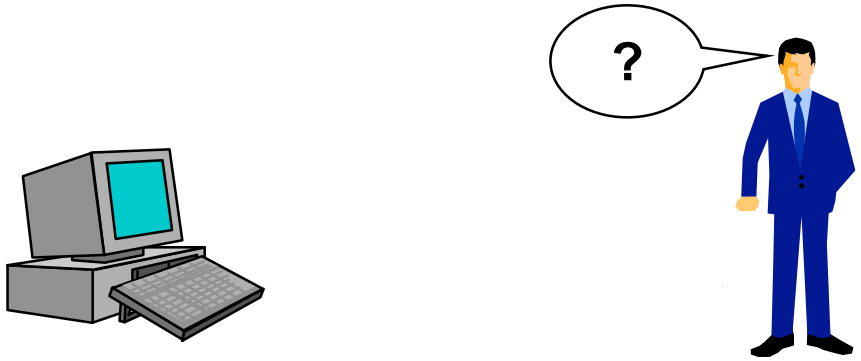
What one *is*
- hand geometry
- finger print
- picture
- hand-written signature
- retina-pattern
- voice
- typing characteristics

has
- paper document
- metal key
- magnetic-strip card
- smart card (chip card)
- calculator

knows
- password, passphrase
- answers to questions
- calculation results for numbers

picture + hand-written signature + paper document → **ID-card**

Identification of IT-systems by human beings

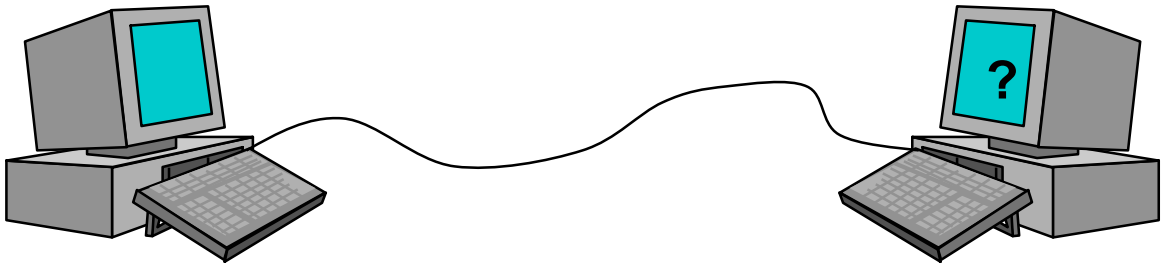


What it *is*
- casing
- seal, hologram
- pollution

knows
- password
- answers to questions
- calculation results for numbers

Where it *stands*

Identification of IT-systems by IT-systems



What it *knows*

- password
- answers to questions
- calculation results for numbers
- **cryptography**

Wiring *from where*