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
   - Favored 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?).

The aims are to

- prevent successful impersonation (shall even hold if the impersonated person might try to help) and
- provide user-friendliness to the legitimate users, i.e., no need to remember passphrases and the like nor any need to carry tokens like metal keys, chip cards or paper documents and to take care of them.

3. Security problems of biometrics

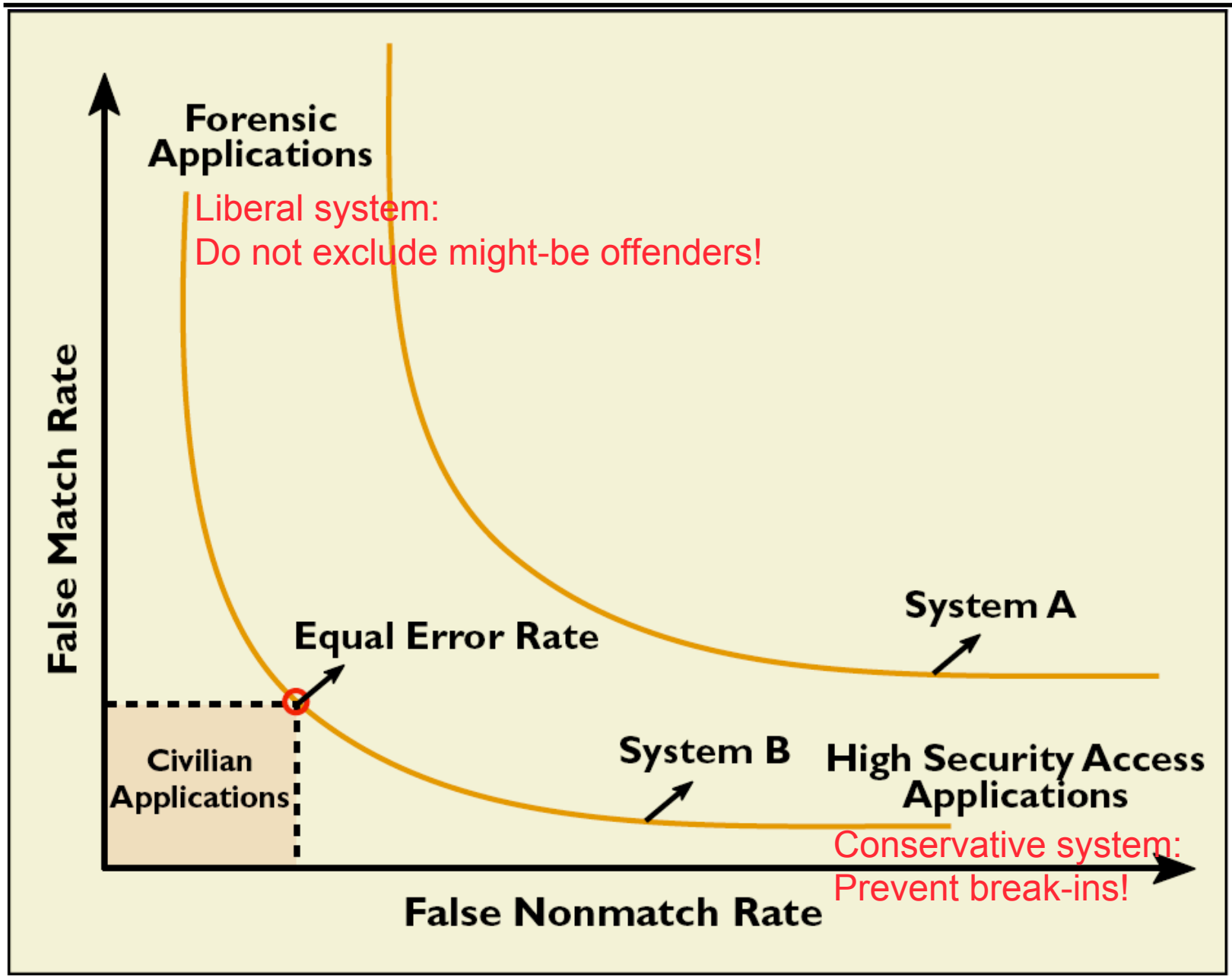

Figure taken from:

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 compromises overall security**
  - **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 a Mercedes S-class.
  - 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.

- **Favored 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.
  - Biometric encryption, i.e., generating encryption keys which can be recovered from biometrics alone, stays an option - even if futuristic nowadays.
- Active biometrics (i.e., person does something explicitly) in passports and/or towards third-party devices can be avoided and should be!
- Passive biometrics by third-party devices cannot be prevented – regrettably.

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

Stand-alone 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 including machine-readable biometrics in our passports.
- **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 third-party devices, 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, e.g., the passport number.

→ **Countries** taking privacy of their citizens seriously should **mutually agree to not include any data usable as a universal personal identifier in stand-alone visas**.

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 which are **predictable from these data**.
- **Genome databases** and **ubiquitous computing** (= pervasive computing = networked computers in all physical things) will **undermine privacy primarily in the physical world.**
- **Privacy spaces in the digital world are possible** (and 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.

- Andreas Pfitzmann: Biometrics – How to Put to Use and How Not at All? In: S. M. Furnell, S. K. Katsikas, and A. Lioy (Eds.): TrustBus 2008, LNCS 5185, Springer-Verlag, Berlin Heidelberg 2008, 1-7.