Biometrics – How to Put to Use and How Not at All?

Andreas Pfitzmann

TU Dresden, Faculty of Computer Science, 01062 Dresden, Germany
Andreas.Pfitzmann@tu-dresden.de

Abstract. After a short introduction to biometrics w.r.t. IT security, we derive conclusions on how biometrics should be put to use and how not at all. In particular, we show how to handle security problems of biometrics and how to handle security and privacy problems caused by biometrics in an appropriate way. The main conclusion is that biometrics should be used between human being and his/her personal devices only.

1 Introduction

Biometrics is advocated as *the* solution to admission control nowadays. But what can biometrics achieve, what not, which side effects do biometrics cause and which challenges in system design do emerge?

1.1 What Is Biometrics?

Measuring physiological or behavioral characteristics of persons is called biometrics. Measures include the *physiological characteristics*

- (shape of) face,
- facial thermograms,
- fingerprint,
- hand geometry,
- vein patterns of the retina,
- patterns of the iris, and
- DNA

and the *behavioral characteristics*

- dynamics of handwriting (e.g., handwritten signatures),
- voice print, and
- gait.

One might make a distinction whether the person whose physiological or behavioral characteristics are measured has to participate explicitly (*active* biometrics), so (s)he gets to know that a measurement takes place, or whether his/her explicit participation is not necessary (*passive* biometrics), so (s)he might not notice that a measurement takes place.

S.M. Furnell, S.K. Katsikas, and A. Lioy (Eds.): TrustBus 2008, LNCS 5185, pp. 1–7, 2008.

1.2 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?).

Both decision problems are the more difficult the larger the set of persons of which individual persons have to be authenticated or even identified. Particularly in the case of identification, the precision of the decision degrades with the number of possible persons drastically.

2 Security Problems of Biometrics

As with all decision problems, biometric authentication/identification may produce two kinds of errors [1]:

False nonmatch rate: Persons are wrongly not authenticated or wrongly not identified.
False match rate: Persons are wrongly authenticated or wrongly identified.

False nonmatch rate and false match rate can be traded off by adjusting the decision threshold. Practical experience has shown that only one error rate can be kept reasonably small – at the price of a unreasonably high error rate for the other type.

A biometric technique is more secure for a certain application area than another biometric technique if both error types occur more rarely. It is possible to adapt the threshold of similarity tests used in biometrics to various application areas. But if only one of the two error rates should be minimized to a level that can be provided by well managed authentication and identification systems that are based on people's knowledge (e.g., passphrase) or possession (e.g., chip card), today's biometric techniques can only provide an unacceptably high error rate for the other error rate.

Since more than two decades we hear announcements that biometric research will change this within two years or within four years at the latest. In the meantime, I doubt whether such a biometric technique exists, if the additional features promised by advocates of biometrics shall be provided as well:

- user-friendliness, which limits the quality of data available to pattern recognition, and
- acceptable cost despite possible attackers who profit from technical progress as well (see below).

In addition to this decision problem being an inherent security problem of biometrics, the implementation of biometric authentication/identification has to ensure that the biometric data come from the person at the time of verification and are neither replayed in time nor relayed in space [2]. This may be more difficult than it sounds, but it is a common problem of all authentication/identification mechanisms.

3 Security Problems Caused by Biometrics

Biometrics does not only have the security problems sketched above, but the use of biometrics also creates new security problems. Examples are given in the following.

3.1 Devaluation of Classic Forensic Techniques Compromises Overall Security

Widespread use of biometrics can devaluate classic forensic techniques – as sketched for the example of fingerprints – as a means to trace people and provide evidence:

Databases of fingerprints or common issuing of one's fingerprint essentially ease the fabrication of finger replicas [3] and thus leaving someone else's fingerprints at the site of crime. And 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. Plausible fingerprints at the site of crime will cause police or secret service at least to waste time and money in their investigations – if not to accuse the wrong suspects in the end.

If biometrics based on fingerprints is used to secure huge values, quite probably, an "industry" fabricating replicas of fingers will arise. And if fingerprint biometrics is rolled out to the mass market, huge values to be secured arise by accumulation automatically. It is unclear whether society would be well advised to try to ban that new "industry" completely, because police and secret services will need its services to gain access to, e.g., laptops secured by fingerprint readers (assuming both the biometrics within the laptops and the overall security of the laptops get essentially better than today). Accused people may not be forced to co-operate to overcome the barrier of biometrics at their devices at least under some jurisdictions. E.g., according to the German constitution, nobody can be forced to co-operate in producing evidence against himself or against close relatives.

As infrastructures, e.g., for border control, cannot be upgraded as fast as single machines (in the hands of the attackers) to fabricate replicas of fingers, a loss of security is to be expected overall.

3.2 Stealing Body Parts (Safety Problem of Biometrics)

In the press you could read that one finger of the driver of a Mercedes S-class has been cut off to steal his car [4]. Whether this story is true or not, it does exemplify a problem I call the safety problem of biometrics:

- Even a temporary (or only 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.

If we assume that as a modification of the press story, the thieves of the car know they need the finger as part of a functioning body, they will kidnap the owner of the car and take him and the car with them to a place where they will remove the biometric security from the car. Since such a place usually is closely connected to the thieves and probably gets to be known by the owner of the car, they will probably kill the owner after arriving at that place to protect their identities. So biometrics checking that the measured body part of a person is still alive may not solve the safety problem, but exacerbate it.

3.3 Favored Multiple Identities Could Be Uncovered as Well

The naive dream of politicians dealing with public safety to recognize or even identify people by biometrics unambiguously will become a nightmare if we do not completely ignore that our societies need multiple identities. They are accepted and often useful for agents of secret services, undercover agents, and persons in witness-protection programs.

The effects of a widespread use of biometrics would be:

- To help uncover agents of secret services, each country will set up person-related biometric databases at least for all foreign citizens.
- To help uncover undercover agents and persons in witness-protection programs, in particular organized crime will set up person-related biometric databases.

Whoever believes in the success of biometric authentication and identification, should *not* employ it on a large scale, e.g., in passports.

4 Privacy Problems Caused by Biometrics

Biometrics is not only causing security problems, but privacy problems as well:

1. Each biometric measurement contains potentially sensitive personal data, e.g., a retina scan reveals information on consumption of alcohol during the last two days, and it is under discussion, whether fingerprints reveal data on homosexuality [5,6].
2. Some biometric measurements might take place (passive biometrics) without knowledge of the data subject, e.g., (shape of) face recognition.

In practice, the security problems of biometrics will exacerbate their privacy problems:

3. Employing several kinds of biometrics in parallel, to cope with the insecurity of each single kind [7], multiplies the privacy problems (cf. mosaic theory of data protection).

Please take note of the principle that data protection by erasing personal data does not work, e.g., on the Internet, since it is necessary to erase *all* copies. Therefore even the possibility to gather personal data has to be avoided. This means: no biometric measurement.

5 How to Put to Use and How Not at All?

Especially because biometrics has security problems itself and additionally can cause security and privacy problems, one has to ask the question how biometrics should be used and how it should not be used at all.

5.1 Between Data Subject and His/Her Devices

Despite the shortcomings of current biometric techniques, if adjusted to low false nonmatch rates, they can be used between a human being and his/her personal devices. This is even true if biometric techniques are too insecure to be used in other applications or cause severe privacy or security problems there:

- Authentication by possession and/or knowledge *and* biometrics improves security of authentication.
- No devaluation of classic forensic techniques, since the biometric measurements by no means leave the device of the person and persons are not conditioned to divulge biometric features to third-party devices.
- No privacy problems caused by biometrics, since each person (hopefully) is and stays in control of his/her devices.
- The safety problem of biometrics remains unchanged. But if a possibility to switch off biometrics completely and forever after successful biometric authentication is provided and this is well known to everybody, then biometrics does not endanger physical integrity of persons, if users are willing to cooperate with determined attackers. Depending on the application context of biometrics, compromises between no possibility at all to disable biometrics and the possibility to completely and permanently disable biometrics might be appropriate.

5.2 Not at All between Data Subject and Third-Party Devices

Regrettably, it is to be expected that it will be tried to employ biometrics in other ways, i.e. between human being and third-party devices. This can be done using active or passive biometrics:

- Active biometrics in passports and/or towards third-party devices is noted by the person. This helps him/her to avoid active biometrics.
- Passive biometrics by third-party devices cannot be prevented by the data subjects themselves – regrettably. Therefore, at least *covertly employed passive biometrics should be forbidden by law.*

What does this mean in a world where several countries with different legal systems and security interests (and usually with no regard of foreigners' privacy) accept entry of foreigners into their country only if the foreigner's country issued a passport with machine readable and testable digital biometric data or the foreigner holds a stand-alone visa document containing such data?

5.3 Stand-Alone Visas Including Biometrics or Passports Including Biometrics?

Stand-alone visas including biometrics do much less endanger privacy than passports including biometrics. This is true both w.r.t. foreign countries as well as w.r.t. organized crime:

- Foreign countries will try to build up person-related biometric databases of visitors – we should not ease it for them by conditioning our citizens to accept biometrics 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[1]

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.

Therefore, countries taking privacy of their citizens seriously should

- not include biometric characteristics in their passports or at least minimize biometrics there, and
- mutually agree to issue – if heavy use of biometrics, e.g., for border control, is deemed necessary – stand-alone visas including biometric characteristics, but not to include any data usable as a universal personal identifier in these visas, nor to gather such data in the process of issuing the visas.

6 Conclusions

Like the use of every security mechanism, the use of biometrics needs circumspection and possibly utmost caution. In any case, in democratic countries the widespread use of biometrics in passports needs a qualified and manifold debate. This debate took place at most partially and unfortunately it is not encouraged by politicians dealing with domestic security in the western countries. Some politicians even refused it or – if this has not been possible – manipulated the debate by making indefensible promises or giving biased information.

This text shows embezzled or unknown arguments regarding biometrics und tries to contribute to a qualified and manifold debate on the use of biometrics.

[1] cf. insecurity of RFID-chips against unauthorized reading, `http://dud.inf.tu-dresden.de/literatur/Duesseldorf2005.10.27Biometrics.pdf`

7 Outlook

After a discussion on how to balance domestic security and privacy, an investigation of authentication and identification infrastructures [8] that are able to implement this balance should start:

- Balancing surveillance and privacy should not only happen concerning single applications (e.g. telephony, e-mail, payment systems, remote video monitoring), but across applications.
- Genome databases, which will be built up to improve medical treatment in a few decades, 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 – we will leave biological or digital traces wherever we are.
- Privacy spaces in the digital world are possible (and needed) and should be established – instead of trying to gather and store traffic data for a longer period of time at high costs and for (very) limited use (in the sense of balancing across applications).

Acknowledgements

Many thanks to my colleagues in general and Rainer Böhme, Katrin Borcea-Pfitzmann, Dr.-Ing. Sebastian Clauß, Marit Hansen, Matthias Kirchner, and Sandra Steinbrecher in particular for suggestions to improve this paper and some technical support.

References

1. Jain, A., Hong, L., Pankanti, S.: Biometric Identification. Communications of the ACM 43/2, 91–98 (2000)
2. Schneier, B.: The Uses and Abuses of Biometrics. Communications of the ACM 42/8, 136 (1999)
3. Chaos Computer Club e.V.: How to fake fingerprints? (June 12, 2008), http://www.ccc.de/biometrie/fingerabdruck_kopieren.xml?language=en
4. Kent, J.: Malaysia car thieves steal finger (June 16, 2008), news.bbc.co.uk/2/hi/asia-pacific/4396831.stm
5. Hall, J.A.Y., Kimura, D.: Dermatoglyphic Asymmetry and Sexual Orientation in Men. Behavioral Neuroscience 108, 1203–1206 (1994) (June 12, 2008), www.sfu.ca/~dkimura/articles/derm.htm
6. Forastieri, V.: Evidence against a Relationship between Dermatoglyphic Asymmetry and Male Sexual Orientation. Human Biology 74/6, 861–870 (2002)
7. Ross, A.A., Nandakumar, K., Jain, A.K.: Handbook of Multibiometrics. Springer, New York (2006)
8. Pfitzmann, A.: Wird Biometrie die IT-Sicherheitsdebatte vor neue Herausforderungen stellen? DuD, Datenschutz und Datensicherheit, Vieweg-Verlag 29/5, 286–289 (2005)