

BIOMETRIC AUTHENTICATION — SECURITY AND USABILITY

Václav Matyáš and Zdeněk Říha
Faculty of Informatics, Masaryk University Brno, Czech Republic
{matyas, zriha}@fi.muni.cz

Abstract We would like to outline our opinions about the usability of biometric authentication systems. We outline the position of biometrics in the current field of computer security in the first section of our paper. The second chapter introduces a more systematic view of the process of biometric authentication – a layer model (of the biometric authentication process). The third section discusses the advantages and disadvantages of biometric authentication systems. We also propose a classification of biometric systems that would allow us to compare the biometrics systems reasonably, along similar lines to Common Criteria [1] or FIPS 140-1/2 [4]. We conclude this paper with some suggestions where we would suggest to use biometric systems and where not.

Keywords: authentication, biometrics, classification, evaluation, security.

1. Introduction

This paper summarises our opinions and findings after several years of studying biometric authentication systems and their security. Our research on security and reliability issues related to biometric authentication started in 1999 at Ubilab, the Zurich research lab of bank UBS, and has been continuing at the Masaryk University Brno since mid-2000. This paper summarises our personal views and opinions on pros and cons of biometric authentication in computer systems and networks.

Proper *user identification/authentication* is a crucial part of the access control that makes the major building block of any system's security. User identification/authentication has been traditionally based on:

- * something that the user *knows* (typically a PIN, a password or a passphrase) or
- * something that the user *has* (e.g., a key, a token, a magnetic or smart card, a badge, a passport).

These traditional methods of the user authentication unfortunately do not authenticate the *user* as such. Traditional methods are based on properties that can be forgotten, disclosed, lost or stolen. Passwords often are easily accessible to colleagues and even occasional visitors and users tend to pass their tokens to or share their passwords with their colleagues to make their work easier. Biometrics, on the other hand, authenticate humans as such – in case the biometric system used is working properly and reliably, which is not so easy to achieve. Biometrics are automated methods of identity verification or identification based on the principle of measurable physiological or behavioural characteristics such as a fingerprint, an iris pattern or a voice sample. Biometric characteristics are (or rather should be) unique and not duplicable or transferable. While the advantages of biometric authentication definitely look very attractive, there are also many problems with biometric authentication that one should be aware of.

2. The layer model

Although the use of each biometric technology has its own specific issues, the basic operation of any biometric system is very similar. The separation of actions can lead to identifying critical issues and to improving security of the overall process of biometric authentication. The layer model was designed by our biometrics team (the authors, Hans-Peter Frei, Kan Zhang) during the Ubilab biometrics project, and its structure is also similar to some findings presented in other seminal works on biometric authentication (e.g., [3, 5]).

The whole process starts with the enrolment:

2.1. First measurement (acquisition)

This is the first contact of the user with the biometric system. The user's biometric sample is obtained using an input device. Quality of the first biometric sample is crucial for further authentications of this user. It may happen that even multiple acquisitions do not generate biometric samples with sufficient quality. Such a user cannot be registered with the system. There are also mute people, people without fingers or with injured eyes. Both these categories create a 'fail to enrol' (FTE) group of users. Users very often do not have any previous experience with the kind of the biometric system they are being registered with, so the first measurement should be guided by a professional who explains the use of the biometric reader.

2.2. Creation of master characteristics

The biometric measurements are processed after the acquisition. The number of biometric samples necessary for further processing is based on the nature of given biometric technology. Sometimes a single sample is sufficient, but often multiple (usually 3 or 5) biometric samples are required. The biometric characteristics are most commonly neither compared nor stored in the raw format (say as a bitmap).

2.3. Storage of master characteristics

After processing the first biometric sample(s) and extracting the features, we have to store (and maintain) the newly obtained master template. Choosing proper discriminating characteristic for the categorisation of records in large databases can improve identification (search) tasks later on. There are basically 4 possibilities where to store the template: in a card, in the central database on a server, on a workstation or directly in an authentication terminal. The storage in an authentication terminal cannot be used for large-scale systems, in such a case only the first two possibilities are applicable. If privacy issues need to be considered then the storage on a card (magnetic stripe, smart or 2D bar) has an advantage, because in this case no biometric data must be stored (and potentially misused) in a central database.

As soon as the user is enrolled, she can use the system for successful authentications or identifications. This process is typically fully automated and takes the following steps:

2.4. Acquisition(s)

Current biometric measurements must be obtained for the system to be able to make comparison with the master template. These subsequent acquisitions of the user's biometric measurements are done at various places where authentication of the user is required. It is often up to the reader to check that the measurements obtained really belong to a live persons (the liveness property). In many biometric techniques (e.g., fingerprinting) the further processing trusts the biometric hardware to check the liveness of the person and provide genuine biometric measurements only. Some other systems (like the face recognition) check the user's liveness in software (time-phased sampling).

2.5. Creation of new characteristics

The biometric measurements obtained in the previous step are processed and new characteristics are created. Only a single biometric sam-

ple is usually available. This might mean that the number or quality of extracted features is lower than at the time of enrolment.

2.6. Comparison

Currently computed characteristics are compared with the characteristics obtained during enrolment. If the system performs (identity) verification then these newly obtained characteristics are compared only to the master template. For an identification request the new characteristics are matched against a large number of master templates.

2.7. Decision

The final step in the verification process is the yes/no decision based on a threshold. This security threshold is either a parameter of the matching process or the resulting score is compared with the threshold value. Although the error rates quoted by manufactures (typical values of equal error rate (ERR)¹ do not exceed 1%) might indicate that biometric systems are very accurate, the reality is much worse. Especially the false rejection rate is quite high (very often over 10%) in real applications. This prevents legitimate users to gain their access rights and stands for a significant problem of biometric systems.

3. What are the advantages of biometric authentication

The primary advantage of biometric authentication methods over other methods of user authentication is that they really do what they should, i.e., they *authenticate the user*. These methods use real human physiological or behavioural characteristics to authenticate users. These biometric characteristics are (more or less) permanent and not changeable. It is also not easy (although in some cases not principally impossible) to change one's fingerprint, iris or other biometric characteristics.

Users cannot pass their biometric characteristics to other users as easily as they do with their cards or passwords.

Biometric objects cannot be stolen as tokens, keys, cards or other objects used for the traditional user authentication, yet biometric characteristics can be stolen from computer systems and networks. Biometric characteristics are not secret and therefore the availability of a user's fingerprint or iris pattern does not break security the same way as availability of the user's password. Even the use of dead or artificial biometric characteristics should not let the attacker in.

Most biometric techniques are based on something that cannot be lost or forgotten. This is an advantage for users as well as for system administrators because the problems and costs associated with lost, reissued or temporarily issued tokens/cards/passwords can be avoided, thus saving some costs of the system management.

Another advantage of biometric authentication systems may be their *speed*. The authentication of a habituated user using an iris-based identification system may take 2 (or 3) seconds while finding your key ring, locating the right key and using it may take some 5 (or 10) seconds.

3.1. Disadvantages of biometric authentication

So why do not we use biometrics everywhere instead of passwords or tokens? Nothing is perfect, and biometric authentication methods also have their own shortcomings. First of all the performance of biometric systems is not ideal (yet?). Biometric systems still need to be improved in the terms of accuracy and speed. Biometric systems with the false rejection rate under 1% (together with a reasonably low false acceptance rate) are still rare today. Although few biometric systems are fast and accurate (in terms of low false acceptance rate) enough to allow identification (automatically recognising the user identity), most of current systems are suitable for the verification only, as the false acceptance rate is too high².

The fail to enrol rate brings up another important problem. Not all users can use any given biometric system. People without hands cannot use fingerprint or hand-based systems³. Visually impaired people have difficulties using iris or retina based techniques. As not all users are able to use a specific biometric system, the authentication system must be extended to handle users falling into the FTE category. This can make the resulting system more complicated, less secure or more expensive. Even enrolled users can have difficulties using a biometric system. The FTE rate says how many of the input samples are of insufficient quality. Data acquisition must be repeated if the quality of input sample is not sufficient for further processing and this would be annoying for users.

Biometric data are not considered to be secret and security of a biometric system cannot be based on the secrecy of user's biometric characteristics. The server cannot authenticate the user just after receiving her correct biometric characteristics. The user authentication can be successful only when user's characteristics are fresh and have been collected from the user being authenticated. This implies that the biometric input device must be trusted. Its authenticity should be verified (unless the device and the link are physically secure) and user's liveness would be

checked. The input device also should be under human supervision or tamper-resistant. The fact that biometric characteristics are not secret brings some issues that traditional authentication systems need not deal with. Many of the current biometric systems are not aware of this fact and therefore the security level they offer is limited.

Some biometric sensors (particularly those having contact with users) also have a *limited lifetime*. While a magnetic card reader may be used for years (or even decades), the optical fingerprint reader (if heavily used) must be regularly cleaned and even then the lifetime need not exceed one year.

Biometric systems may violate user's *privacy*. Biometric characteristics are sensitive data that may contain a lot of personal information. The DNA (being the typical example) contains (among others) the user's preposition to diseases. This may be a very interesting piece of information for an insurance company. The body odour can provide information about user's recent activities. It is also told [3] that people with asymmetric fingerprints are more likely to be homosexually oriented, etc.

Use of biometric systems may also imply loss of anonymity. While one can have multiple identities when authentication methods are based on something the user knows or has, biometric systems can sometimes link all user actions to a single identity.

Biometric systems can potentially be quite troublesome for some users. These users find some biometric systems *intrusive* or personally invasive. Even if no biometric system is really dangerous, users are occasionally afraid of something they do not know much about. In some countries people do not like to touch something that has already been touched many times (e.g., biometric sensor), while in some countries people do not like to be photographed or their faces are completely covered.

Lack of *standards* (or ignorance of standards) may also possess a serious problem. Two similar biometric systems from two different vendors are not likely to interoperate at present.

4. Possible classification of biometric systems

Classifications help to compare systems. The famous Orange Book [2] divided systems into four categories (A – D) with additional subcategories. All the security features (such as access control or auditing) get attention. The higher security level the more sophisticated protection is required. But the higher levels also have more stringent assurance requirements. There must be more reason to believe that the system functions as designed.

The ITSEC also classifies the security of systems, so does the Common Criteria. A product or a system can be certified for a particular security class. The vendor asks an independent organisation to evaluate properties of a particular product/system and if this *Target of Evaluation* complies with the criteria, the label is granted. Although an obtained security label does not automatically imply that the product is secure, it helps in product categorisation and comparison.

In this chapter we categorise biometric systems according to the level of protection they offer. Our classification proposal divides systems into four levels. We first introduce the model of a biometric system. Then adjustable and/or optional parameters of biometric systems are discussed and at the end four security levels are described.

4.1. Modules of a biometric system

Any biometric system is basically made of the following components:

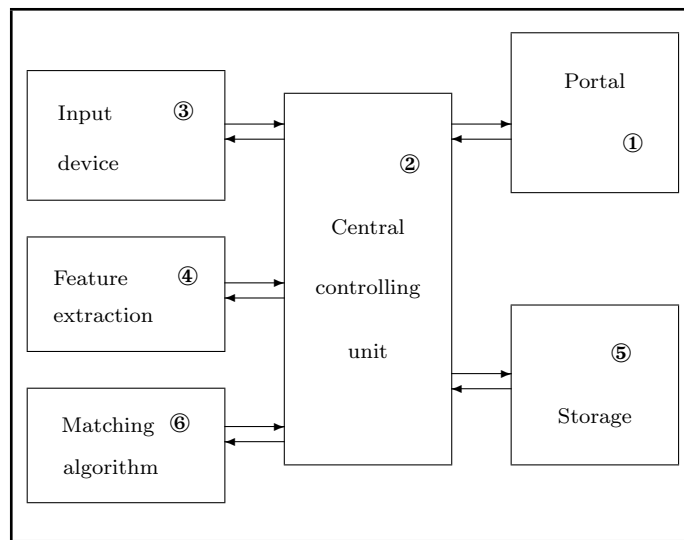


Figure 1. The model of a biometric system.

- 1 *Portal*. Its purpose is to protect some assets. An example of a portal is the gate at an entrance of a building. If the user has been successfully authenticated and is authorised to access an object then access is granted.
- 2 *Central controlling unit* receives the authentication request, controls the biometric authentication process and returns the result of user authentication.

- 3 *Input device.* The aim of the input device is biometric data acquisition. During the acquisition process user's liveness and quality of the sample may be verified.
- 4 *Feature extraction* module processes the biometric data. The output of the module is a set of extracted features suitable for the matching algorithm. During the feature extraction process the module may also evaluate quality of the input biometric data.
- 5 *Storage* of biometric templates. This will typically be some kind of a database. Biometric templates can also be stored on a user-held medium (e.g., smartcard). In that case a link between the user and her biometric template must exist (e.g., in the form of an attribute certificate).
- 6 The biometric *matching* algorithm compares the current biometric features with the stored template. The desired security threshold level may be a parameter of the matching process. In this case the result of the matching will be a yes/no answer. Otherwise a score representing the similarity between the template and the current biometric sample is returned. The central unit then makes the yes/no decision.

4.2. Parameters of biometric systems

What does it take for one biometric system to be more secure than another one? What are the differences among various systems?

Liveness testing: Incorporation of a liveness test makes an attack against the biometric system more difficult. There are various liveness tests offering various levels of protection. Most of the tests, however, can be easily cheated. A combination of multiple liveness tests can make the system more secure.

Tamper resistance: If the biometric system is not under constant human supervision it has to rely on tamper resistance. Without tamper resistance or supervision the system can be tampered with and forged/replied biometric data can be injected into the system.

Secure communication: Biometric system components can be either standalone and communicate with each other over an external insecure medium or can be coupled in a tamper-resistant box. The communication among modules within a tamper-resistant cover need not be secured, but the communication over an insecure line should be authenticated and encrypted.

Security threshold level: Lower false acceptance rate means higher level of security (and unfortunately, in most cases, also higher false rejection rate causing user frustration). A proper value must be set in accordance with goals of the biometric system.

Fall-back mode: In some systems the biometric authentication may be sufficient for the user authentication. In some systems an additional authentication method must be used and the biometric authentication is only a necessary part of user authentication. Successful authentication using this additional method may but need not be sufficient for user authentication.

4.3. Proposal of classification

Our proposal of classification divides biometric systems into four categories according to the level of security they offer. The higher security category the higher level of protection the system offers. Which level to choose depends heavily on the purpose of the biometric system, its threats and on available funds.

Level 1 – Very simple systems: Systems falling into this category are more or less very simple. They offer only restricted level of protection and can be easily cheated. Such systems have no liveness test incorporated and no part of the system has to be tamper-resistant. The communication among particular components need not be authenticated nor encrypted. Successful biometric authentication is sufficient means of authentication and after an unsuccessful biometric authentication some traditional authentication method is offered.

Such biometric systems are subject to easy attacks such as unplugging the biometric input device and injecting previously eavesdropped biometric data (because of no encryption or authentication), misuse of high false acceptance rate or faked trivial copies of biometric characteristics.

Level 2 – Simple systems: Biometric systems at level two require mutual authentication of particular components and encrypted communication. Still no liveness testing or tamper resistance is required. The biometric authentication is sufficient authentication. A traditional authentication method as a sufficient authentication method is offered only in the case of biometric system malfunction.

Systems on level two offer a certain level of security and still remain relatively cheap. Some of the easiest attacks are eliminated,

but the systems still can be tampered with or cheated with faked biometric characteristics.

Level 3 – Intermediate systems: Level three systems already do have some kind of liveness test. Exposed components of the system (typically the biometric input device) must be guarded or tamper-resistant against moderate attacks. The communication must be authenticated and encrypted. The biometric authentication is sufficient, and the system never offers traditional authentication as a sufficient authentication method.

Such biometric systems will be able to resist moderate attacks. Advanced tampering methods or advanced faked biometric characteristics, however, will still be able to cheat the biometric systems.

Level 4 – Advanced systems: For systems of level four more than one advanced liveness test method are required. Exposed and unguarded components must be tamper-resistant. Such tamper resistance must be able to resist advanced tampering attacks. Communication among particular components (except within a tamper-resistant box) must be mutually authenticated and encrypted. Successful biometric authentication is necessary but not sufficient part of the user authentication. A supplemental traditional authentication method must be a necessary part of the authentication, too. Preferably multiple biometric techniques should be involved in the biometric authentication.

Biometric systems falling into the level four should be able to resist even professional and well-funded attacks. But nothing is bullet-proof and designing a system resistant to (for example) very well funded attacks of intelligence services is rather difficult.

| Level | Liveness | Tamper res. | Secure Comm. | Traditional auth method |
|-------|----------|-------------|--------------|-------------------------|
| 1 | no | no | no | sufficient/any time |
| 2 | no | no | yes | sufficient/malfunction |
| 3 | yes | moderate | yes | not sufficient |
| 4 | multiple | advanced | yes | not sufficient/required |

Table 1. Brief overview of classification proposal.

5. Conclusions

Let us discuss where the use of biometric systems may be an advantage and where not. Biometrics are a great way of authenticating users. The user may be authenticated by a workstation during the logon, by a smart card to unlock the private key, by a voice verification system to confirm

a bank transaction or by a physical access control system to open a door. All of these cases are typical and correct places where to deploy a biometric system.

Very promising are solutions where the cryptographic functions as well as the biometric matching, the feature extraction and the biometric sensor are all integrated in one (ideally also tamper-resistant) device. Such devices provide a very high protection of the secret/private key as the biometric data as well as the secret/private key will never have to leave the secure device.

We believe that biometric authentication is a good *additional* authentication method. Even cheap and simple biometric solutions can increase the overall system security if used *on top* of existing traditional authentication methods.

Biometrics can be used for dozens of applications outside the scope of computer security. Facial recognition systems are often deployed at frequently visited places to search for criminals. Fingerprint systems (AFIS) are used to find an offender according to trails left on the crime spot. Infrared thermographs can point out people under influence of various drugs (different drugs react in different ways). Biometric systems successfully used in non-authenticating applications may but also need not be successfully used in authenticating applications.

5.1. Where not to use biometrics?

Although good for user authentication, biometrics cannot be used to authenticate computers or messages. Biometric characteristics are not secret and therefore they cannot be used to sign messages or encrypt documents. If my fingerprint is not secret there is no sense in adding it to documents we have written. Anyone else could do the same. Cryptographic keys derived from biometric data are nonsense, too.

Remote biometric authentication is not trivial at all. The assumption that anyone who can provide my fingerprint can also use my bank account in the homebanking application is not a good idea. Remote biometric authentication requires a trusted biometric sensor. Will a bank trust your home biometric sensor to be sufficiently tamper resistant and provide trustworthy liveness test? Although remote biometric authentication may work in the theory, few (if any) current devices are trustworthy enough to be used for remote biometric authentication.

While using biometrics as an additional authentication method does not weaken the security of the whole system (if users do not rely on the biometric component so much to ignore the traditional authentication method, e.g., by using simple passwords), replacing an existing system

with a biometric one may be more risky. Users as well as administrators and system engineers tend to overestimate security properties of biometric systems; such a decision must be based on and confirmed by a risk analysis. Particularly, reviewing the process of the biometric data capture and transfer is very important. Sometimes biometric authentication systems replace traditional authentication systems not because of higher security but because of higher comfort and ease of use.

False rejects – the unpleasant property of biometric systems causing authorised users to be rejected – may prevent biometric systems to spread into some specific applications, where inability of a user to authenticate herself (and run an action) may imply serious problems.

Few basic conclusions at the very end:

- * *Different biometric samples of the same person will never be same.*
- * *Biometric systems make errors.*
- * *Biometric data are not secret.*
- * *The role of the input device is crucial, and this device must be trusted or well secured.*
- * *The biometric system should check user's liveness.*
- * *Biometrics are good for user authentication. They cannot be used to authenticate data or computers.*

Notes

1. There are two kinds of errors that biometric systems do: *false rejection* occurs when a legitimate user is rejected and *false acceptance* occurs when an impostor is accepted as a legitimate user. The number of false rejections/false acceptances is usually expressed as a percentage from the total number of authorised/unauthorised access attempts. *The equal error rate (ERR)* is the point where FAR and FRR are equal. The ERR value as such does not have any practical use, but it can be used as indicator of the biometric system accuracy.

2. Both the FAR and FRR are functions of the threshold value and can be traded off, but the set of usable threshold values is limited. For example a system with the ERR of 1% may be set to operate at the FAR of 0.01%, but this would imply the FRR to jump over 90 or 95%, which would make system unusable.

3. The FTE rate is estimated as 2% for fingerprint based systems and 1% for iris based systems. Real values of the FTE rate are dependent on the input device model, the enrolment policy and the user population.

References

- [1] Common Criteria for Information Technology Security Evaluation, v 2.1, 1999.
- [2] Department of Defense (1985). Trusted Computer System Evaluation Criteria.
- [3] Jain, A., Bolle, R. and Pankanti S. (1999). *BIOMETRICS: Personal Identification in Networked Society*. Kluwer Academic Publishers.

- [4] National Institute of Standards and Technology (1994 and 2001). *Security Requirements for Cryptographic Modules, FIPS PUB 140-1/2*.
- [5] Newham, E. (1995). *The biometric report*. SBJ Services.
- [6] Matyáš, V., Říha, Z. (2000). *Biometric Authentication Systems*. Technical report. <http://www.ecom-monitor.com/papers/biometricsTR2000.pdf>.
- [7] Mansfield, T. (2001) *Biometric Product Testing – Final Report*, National Physical Laboratory, 2001, <http://www.npl.co.uk/>.