Biometric authentication systems today and in the future

Birgit Kaschte
Computer Science Department
University of Auckland
birgit@kaschte.de

24 October 2005

Abstract. Biometric data has been a widely discussed topic in the past and it still is. Recent discussions include proposals for storing biometric data on passports. In Germany, there are for example video stores using fingerprints for authentication, more and more laptops have a fingerprint sensor integrated, and banks are starting to use biometric data as well. However, despite this diverse range of trail uses and proposals biometric data is still not widely used for user authentication. This paper discusses why authentication using biometric data is not a common standard up to now. It also analyses if the use of biometric data makes systems more secure and if it is worth spending more money on such systems. The discussion and analysis in the paper leads to the conclusion that in most cases the trade-offs which need to be made are not good enough to consider biometric user authentication as a better alternative to usual methods such as login/password authentication. At the end the paper provides a short outlook about the future use of biometric data.

1 Introduction

As we all know, through personal experience or through reports in different media, software systems, using biometric data for authentication become more and more common. We find fingerprint sensors in laptops (see figure 1 on the following page) and PDAs, banks start using biometric authentication systems and there exist even video stores which use this technology. However, they are not yet widely used.

Systems using biometric data for authentication introduce a new and different user authentication paradigm - authentication is based on something that you are (e.g. fingerprint, iris or face) or that you can do or produce (e.g. handwriting or voice). Most

common user authentication systems use something that you have (e.g. smart card) or something that you know (e.g. password, PIN). [OGBRGR04]

Figure 1: Fingerprint sensor integrated in a laptop[1]

Authentication systems based on this paradigm must have some advantages, because otherwise nobody would spend money on the research and the development of such systems. What are the advantages? Does the use of biometric data make systems more secure? As biometric authentication systems are not yet widely used, this technology must also have some disadvantages, unsolved problems or maybe some security concerns. What are the disadvantages of such systems? Are they too expensive? There are many more questions like these and this paper tries to find some answers to them.

This paper is divided into three parts. Chapter 2 gives a short introduction into biometrics and especially into fingerprints and face recognition. Chapter 3 describes authentication systems in general and discusses different aspects of biometric authentication systems which provide answers to the above questions. Finally chapter 4 sums up the answers provided and has a look in the future.

2 Biometrics - What is it?

In the Internet on the pages of Wikipedia[2] the following definition of Biometrics can be found: "Biometrics is the study of automated methods for uniquely recognising humans based upon one or more intrinsic physical or behavioural traits". [Enc05]

In other words, the study of Biometrics explores ways to distinguish between individuals using physical characteristics (things we are) and personal traits (things we do). The most common physical characteristics explored and used are facial features, eyes (iris

[1] http://www.synaptics.com/img/usr/FingerPrint.jpg
[2] http://www.wikipedia.org

and retina), fingerprints and hand geometry. Handwriting and voice are examples of personal traits which could be used to distinguish between individuals.

The described characteristics and traits can be used to identify different individuals, because they all satisfy specific requirements. They are all universal and unique, which means that everybody has them and that the characteristics or traits are different for any two individuals. In addition to that they are all more or less permanently, which means that the characteristic or trait should not change with time. [JHPB97]

Fingerprints and face recognition are the two most common used characteristics to distinguish between individuals. The following two subsections give a more detailed insight in those two biometric recognition technologies.

2.1 Fingerprints

It is known since a long time that fingerprints of humans are unique. They can be distinguished by the epidermal ridge and furrow structure of each finger, which is used to categorise fingerprints as shown in figure 2. Even identical twins don't have the same fingerprint. Fingerprints are therefore widely used to identify people since a long time. They are even accepted by law to prove evidence, which makes them a powerful tool for forensics. [JHPB97]

For electronically processing fingerprints using image recognition algorithms, a fingerprint has to be scanned first. There exist different fingerprint scanners, e.g. capacitive, optical and thermal, each using a different technology. An images gained by a scanner is further processed by a feature extractor which reduces the image to a set of minutiae points (e.g. end points or bifurcation ridges). The set of these points is a compact and expressive representation of the fingerprint which is saved and used for the authentication process. [OGBRGR04]

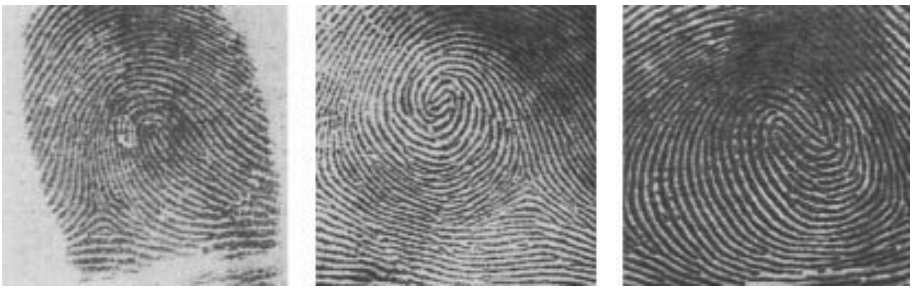

Figure 2: The picture shows 3 different categories of fingerprints - left loop, whorl and twinloop. [JHPB97]

2.2 Face recognition

The face of each individual is unique, although this is sometimes not obvious to other humans. Algorithms for face recognition usually use the shape and location of facial attributes to distinguish between different faces. Such facial attributes could be the shape and the distance of the eyes, eyebrows, lips, chin or nose (see [JHP00]). A lot of research has been done in this area. Face recognition is a promising technology which is accepted by society because people are used to staring into cameras. To make it a successful and widely used technology different problems have to be solved. It is for example not easy to recognise faces in different light or at different angles. In addition to that glasses, make-up, hairdressing and the ageing of faces can be a problem. [OGBRGR04]

3 Biometric authentication

3.1 Authentication in general

Before going into more detail about biometric authentication a general view on an access control model as described in [Lam04] can be helpful to understand how to keep a system secure. The diagram of the access control model shown in figure 3 on the following page is similar to the diagram Butler W. Lampson presents in his article. The guard in the middle of the diagram is responsible for deciding if a source requesting access to a resource of a system is granted this access or not. To decide, the guard uses authentication information for identifying the requesting source and authorisation information to find out if the identified source is allowed to access the requested resource. Each decision of the guard is logged in order to be able to backtrack decisions if necessary.

This paper talks only about the authentication process which is represented by the darker coloured parts of the diagram. The source is in this case a person who provides biometric information (usually in combination with other identification information) to a guard. The guard now uses some sort of algorithm to process the given biometric information and after a comparison with stored samples it decides to grant the person access or not.

Some articles like [PMWP00] distinguishes between biometric identification and biometric verification. Biometric identification means, that biometric data of an unknown individual is presented to a system. The system processes the data and compares it with all records in the systems internal database until one record matches the entered

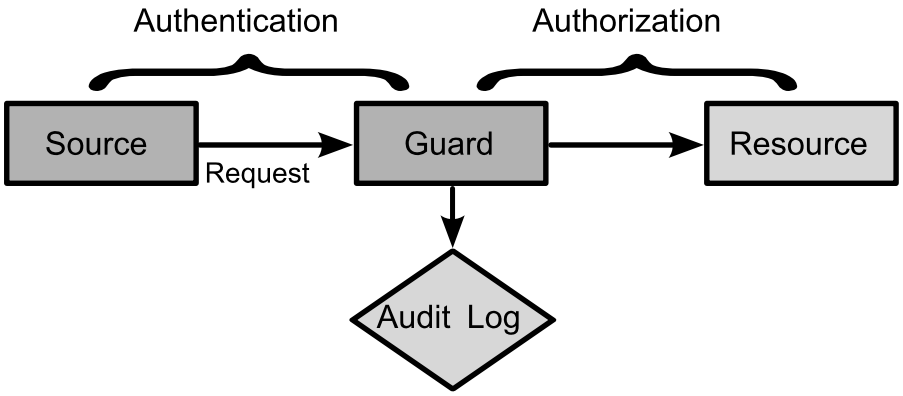

Figure 3: Access control model similar to the diagram in [Lam04]

data (one-to-many). Now the system is able to identify the unknown personality. This process takes much more time than the process of biometric verification. In this case a person provides biometric information to a system and claims that a particular identity belongs to this data (one-to-one). Now the system can reject the claim easily if no sample biometric data for the claimed identity can be found or if the provided biometric data and the sample data of the claimed identity don't match. In most authentication processes biometric verification is used.

According to the article [OGBRGR04] each biometric system consists of an enrolment and a testing phase. The sample biometric data sets which are used for comparison in an authentication process are produced and saved in an enrolment phase. Each authorised user has to go through this step in which for example a fingerprint is taken, processed and saved for example in a database or on an identification card. In the testing phase, when an individual seeks access to a system, the sample saved in the enrolment phase is used by the guard of the system to decide whether to grant access or not. The enrolment phase is much more important for a biometric system than for a system using user name and password. If the sample taken from a person is for example not good enough, the probability that the system refuses access to this person is much higher.

3.2 Performance and security considerations

As we all know old systems get only replaced by new ones, if the new systems have some advantages. For example if they are faster, more secure, cheaper or easier to use. So this section has a look at the performance and the security of biometric authentication systems, before the next section discusses some more advantages and disadvantages.

The performance of a biometric authentication system is difficult to measure. The accuracy of a system is a strong factor which can indicate a good or a bad performance. Other factors like speed, storage, cost and ease-of-use should be considered as well. [JHP00]

Unfortunately biometric systems are not perfect and so sometimes errors occur. It is possible that an authorised person is rejected by the system or that a not-authorised person gets access to it. The probability of these two types of errors are called false rejection (FR) and false acceptance (FA) (see [OGBRGR04]). For most systems it is possible to trade off these types of errors against each other. This can be done for example by increasing a threshold used to decide whether there is a match between two biometric data or not. The FR rate and the FA rate are dependant of each other. In a perfect system both rates would be zero. A very secure system tries to increase the FA rate to almost zero which would result in a very high FR rate. A more convenient system would try to decrease the FR rate which would result in a higher FA rate.

The time an authentication system needs to say whether a person is authorised or not is also a major factor which can be used to determine the performance. For most systems it is important that the authentication system can find an answer in almost real time. It would be for example not acceptable to wait in front of an ATM for half a minute until access is granted or not. The time needed for the authentication process is often connected with the accuracy and therefore with the security of the biometric system. If the FA rate is very high (high security) the system could for example use more characteristic points of the biometric which need to be compared in an authentication process or the algorithm used to compare two biometric samples could be much more complicated. So a more secure biometric authentication process tends to need more time than one with lower security. In the case of an ATM a very secure and a very fast biometric authentication process would be needed. In other cases the speed might not be a concern.

The above discussion shows that all biometric authentication systems have a FR and a FA rate which needs to be traded off against each other and which consequently affects the time taken by the authentication process and the security. But developers or other people who need to decide whether to use a biometric authentication process or not and if yes, which technology to use, should also take other factors like those mentioned above into account.

The list below presents some factors, including the factors the article [OGBRGR04] talks about, which should be considered in such a decision process:

- Vulnerability to fraud the system - Is it easy to fool the system by fraudulent methods? Is it possible to steal a biometric characteristic or trait of another person?
- Distinctiveness and uniqueness of the biometric characteristic or trait - How probable is it that two persons have the same characteristic? Can biometric traits be distinguished easily and accurately?
- Variation of the biometric characteristic or trait - How fast do the biometric characteristics or traits change? What happens if a user looses the used biometric characteristic, e.g. looses eyesight or looses a finger? Can a face be recognised after 20 years?
- Intrusiveness of the system - How intrusive is the system when taking the biometric sample? Is the authentication process rather comfortable of rather uncomfortable for the user?
- Cooperation of the customer - How much cooperation is needed by the user when taking the biometric sample? Do the users have to buy extra hardware? If yes, will they do that?
- Amount of support for the running system - What kind of support will be necessary? Do the biometrics samples need to be updated regularly? Is a support hotline required?

Decision makers have to use test reports and statistics to find answers to these questions as it is not possible to test the available technologies on their own. The first of the above points is the most important one concerning the security of a system. The article [TKZ02] of the German magazine c't presents some test results on biometric recognition systems. Here is a very short summary of their results.

The article describes the test and the results of several capacitive, optical and thermal fingerprint scanners, one iris scanner and one face recognition system. The main focus is on the fingerprint scanners and the face recognition system. The authors describe three scenarios about how it might be possible to fool the biometric system. In the first scenario the regular sensor technology is used and the system is tricked by artificial created data. The second scenario is again about using artificially created data which is this time gained for example by sniffer programs. The so achieved data is then played

back to the system. In the third scenario the database is attacked directly. The article and the following summary of the test results focuses on the first scenario.

It was possible for them to trick all fingerprint scanners using artificial gained data. With some scanners is was more difficult than with others. The following methods (some of them are shown in figure 4) were successful in tricking the system:

- Reactivate the fat traces of a finger (latent fingerprint) left on the sensor's surface by breathing on it.
- Reactivate latent fingerprints by placing a bag filled with warm water on the fingerprint sensor.
- Adhesive film is slightly pressed on the sensor's surface after the latent fingerprint is dusted with normal graphite powder to gain access to the system.
- Instead of using a latent fingerprint left on the sensor the fatty residue on a CD and a glass was used. These prints were dusted with graphite powder and then secured with adhesive film. This was placed with small pressure on the scanner to log into the system.
- For the optical and the thermal scanners they produced artificial silicon fingerprints which were placed on the scanner to access the system successfully.

Figure 4: The three pictures from the article [TKZ02] show three different methods how it is possible to fool a fingerprint scanner.

The following points describe three methods which were used to successfully trick the face recognition tool:

- The tested system takes a small number of images of the new person in the enrolment phase. Each time this person logs into the system, the image taken for the

authentication process is added to the existing set of images. These images are not encrypted and can be read once access to the system is gained. In the first test the authors used such images to gain access to the system. They presented them on a laptop at the correct distance (see figure 5) to the camera of the system.

- For the second approach they used several pictures (different light condition) of an authorised person taken by a normal digital camera. These pictures were also presented to the camera on a laptop at the correct distance to gain access. The access rate was very high.
- After increasing the security level of the face recognition tool the above described methods were no longer successful, because in this level a "Live-Check" is performed. This means that the software tries to recognise small movements of the face in order to find out if a picture is presented to the camera or if a real human is standing in front of it. The authors managed to fool the system anyway. They simply used a small video clip of an authorised person presented to the camera on a laptop.

Figure 5: A face recognition is fooled by presenting the camera a simple picture of an authorised user on a laptop. [TKZ02]

The tests described in this article show clearly that the tools tested are not very secure and most of them can be tricked quite easily by non experts. By now the vendors of such products might have been able to improve them, but a risk always remains. So this paper and most of the other referenced papers conclude that biometric data should not yet be used on its own in an authentication process. A more secure authentication process could combine biometrics with other technologies. For example password and fingerprint or smart card and fingerprint.

3.3 Advantages and Disadvantages

Besides the already mentioned concerns about accuracy and security of biometric authentication systems there are some more disadvantages which are shortly mentioned in the following paragraphs. But besides all disadvantages the advantages which make biometric systems so desirable are described in the second half of this section.

Acceptability is one more disadvantage of biometric authentication systems. New systems can only be successful if they are accepted. In the case of biometric authentication systems some people are concerned about their acceptance in society. Nataliya B. Sukhai for example writes in her article that there are many people who would hesitate using fingerprints for authentication because fingerprints are associated with criminals. Other people would never use an iris scanner, because they are afraid that the light used to scan the iris is harmful for the eyes. [Suk04]

Another disadvantage is the high cost of biometric authentication technologies. The article [Hir05] claims that "Biometric systems do impose the highest costs of any authentication technology." The high cost results on the one hand from higher costs for hardware and software and on the other hand from high costs for integrating biometric authentication into the current network. [Suk04]

The varying reliability of biometric systems is another disadvantage, which is already shortly mentioned above. The biometrics of people can change when they age or suffer physical injuries or diseases. This might for example affect their fingers or their eyes. In addition to that environmental conditions might affect the reliability of biometric systems. Background noise for example might hinder voice recognition systems or a cut in a finger might result in not being able to access a system using fingerprint recognition. [Hir05]

One more disadvantage not yet mentioned, is the problem of integrating biometric authentication into corporate infrastructures. According to the article of Clare Hist [Hir05] the support for platforms and applications is very limited and current standards are not or only poorly supported.

Besides all mentioned disadvantages, biometric authentications systems are very desireable because of the following advantages.

The most obvious advantage is that biometric data can't get lost, stolen, duplicated or forgotten like keys or access cards. They also can't be forgotten, compromised, shared, observed or guessed like passwords, secret codes or PINs [Woo97]. In addition to that

people can't write them down ("25% of the people appear to write their PIN on their ATM card" [JHP00]) which would make is easy for other people to steal it. People also don't have to change the data used for authentication every three months like we sometimes have to do with passwords. Therefore authentication systems using biometric data are more convenient to use.

The most important advantage is that biometric authentication systems can increase the security of the system, if the accuracy is high, the hardware used can't be cheated easily and if it is used together with other authentication methods. Clare Hist states for example that biometrics used in conjunction with smart cards "can provide strong security for PKI credentials held on the card."[Hir05]

In addition to that biometric authentication systems reduce costs because it is possible to eliminate overheads resulting from password management [Hir05]. The reason for this is that people can't forget their passwords anymore and so the queries at help desks become less. Besides reducing the mentioned overhead this also saves money because there are no more costs for distributing new passwords in a secure way.

4 Conclusion and Outlook

There seem to exist more disadvantages than advantages for using biometric authentication systems. This is one reason why such systems are not yet widely used. But the advantages mentioned above are so important and people want to benefit from them that the disadvantes will be more and more reduced in the future. However, some sort of trade-offs, like between the FA rate and the FR rate will always need to be made.

The discussion above shows that biometric authentication is an interesting topic that a lot of reasearch is going on in this area and that it can be used for secure systems despite all disadvantages. At the moment it is recommended to combine biometric authentication with any other authentication technology. Such multi-factor authentication systems are always more secure and it is also common practice to use combinations of different authentication methods. ATMs require for example a PIN and a bank card with additional authentication information saved on a chip.

When talking about biometric data questions about the privacy of personal data come up automatically. This paper has not considered this topic but there are many article dealing with these conserns. It is a difficult topic but it is obvious that biometric authentication systems have to store the biometric samples in a secure way and it has

to be ensured that such data cannot be used otherwise. The best would be if biometric data is kept under the control of the person to which it belongs. This could be done for example by saving the biometric sample only on a smart card which is used in combination with the biometric in an authentication process.

To sum up it can be clearly said that the usage of biometric authentication will increase more and more in the future. This will be supported among other things by the steady improvement of the technologies and the reduction of the prices for hardware and software. Biometric authentication can and probably will be used in many areas, for example ATMs, access to Personal Computers, PDAs and mobile phones, DRM systems, access to buildings and cars and many more we can't even think about.

Acknowledgement

I wish to thank Daniel Weisser for his help. He helped me finding the topic for this term paper as well as spelling and logical errors. Thanks to him I used LaTeX for writing this paper which proved to be a good decision.

References

[Enc05] Wikipedia: The Free Encyclopedia. Biometrics. URL: http://en.wikipedia.org/wiki/Biometrics, September 2005.

[Hir05] Clare Hirst. The pros and cons of using biometric systems in business. Technical Report G00126400, Gartner, March 2005.

[JHP00] Anil Jain, Lin Hong, and Sharath Pankanti. Biometric identification. *Commun. ACM*, 43(2):90–98, 2000.

[JHPB97] Anil K. Jain, Lin Hong, Sharath Pankanti, and Ruud Bolle. An identity-authentication system using fingerprints. In *Proceedings of the IEEE*, volume 85 of *9*, pages 1365–1388, September 1997.

[Lam04] B.W. Lampson. Computer security in the real world. *Computer*, (37):37–46, June 2004.

[OGBRGR04] J. Ortega-Garcia, J. Bigun, D. Reynolds, and J. Gonzalez-Rodriguez. Authentication gets personal with biometrics. *Signal Processing Magazine, IEEE*, pages 50–62, March 2004.

[PMWP00] P.J. Phillips, A. Martin, C.L. Wilson, and M. Przybocki. An introduction to evaluating biometric systems. *Computer*, 33:56–632, February 2000.

[Suk04] Nataliya B. Sukhai. Access control & biometrics. In *InfoSecCD '04: Proceedings of the 1st annual conference on Information security curriculum development*, pages 124–127, New York, NY, USA, 2004. ACM Press.

[TKZ02] Lisa Thalheim, Jan Krissler, and Peter-Michael Ziegler. Body check. *c't*, November 2002. translated by Robert W. Smith.

[Woo97] John D. Woodward. Biometrics: Privacy's foe or privacy's friend? In *Proceedings of the IEEE*, volume 85 of *9*, pages 1480–1492, September 1997.