Biometric authentication today

Tjark Vandommele
Helsinki University of Technology
Tjark_Vandommele@gmx.de

Abstract

In the modern society, more and more people use online services in their everyday life. As some of these services, such as bank accounts, contain sensible data, they have to be protected. One way to do this is using biometric authentication.

This paper gives a general overview of biometric authentication today. It gives some basic information about the different kinds of biometrics and how to tell them apart.

Because of the increase of mobile devices with the possibility to connect to the Internet, mobile authentication is an important issue. Therefore we examine fingerprint scans and keystroke dynamics in detail, as examples of high potential biometrics that could be used in those use cases.

The second half of the paper focuses on vulnerabilities of biometric authentication. By using the framework of Bartlow and Cukic, we recognize possible attack points and explain different ways of exploiting them. Furthermore, we show how easy it is to create artificial fingerprint in order to trick a biometric authentication system and how a replay attack works.

Keywords: biometrics, authentication, vulnerabilities, mobile

1 What are biometrics and why are they important today?

"Biometrics" is a Greek word consisting of the syllable "bio" meaning "life" and "metric" meaning "to measure". It was first used in the 19th century [3], to describe the process of measuring and statistically analysing the lifespan of human, animals and plants. Nowadays "biometrics" has a second meaning. It is often used to describe the process of recognition of human beings by physical or behavioural characteristics.

In the modern world, mobility becomes more important every day. New mobile devices such as smart phones or netbooks help us to handle our tasks from wherever we are able to connect to the Internet. As mankind grows accustomed to this new way of using technology in its everyday life, the need for services that are highly sensitive increases. Examples of these services are online banking, management of personal data, e-mail accounts and so forth. Today these services are protected by passwords or "Transaction Numbers" (TAN) lists. However, the number of services that can be protected safely with passwords is limited, as humans can only memorize a certain quantity of passwords that are long and random enough to be considered secure. When there is a need to remember more passwords, humans tend to reuse old passwords or pick passwords that are easy to remember and therefore not secure. Biometrics attempts to solve this problem.

A human being has several indicators that make him or her unique. Popular examples are DNA, fingerprints and iris patterns. However there are many more characteristics that make a human being unique such as handwriting or dialect. These indicators can be used to identify someone and replace passwords for authentication. The challenge is to find such a characteristic that is at the same time unique to every human being, available on every human being, easy to obtain and hard to tamper with.

Biometrics are already used by several nations. For example on German passports not only personal data such as address and name are stored digitally, but also biometric characteristics of fingerprints and the face. Another well known example of a government using biometrics is the USA. Since September 11th 2001, the FBI has been collecting fingerprints, palm prints, scars, tattoos, iris patterns and facial shapes [2].

The purpose of this paper is to discuss biometrics in general and then take a closer look into biometrics, that could be used for authentication on a mobile device.

2 Different biometrics

2.1 Characteristics of biometrics

To determine if a biometric is suitable for the purpose it will be used for, certain attributes have been set [5]:

- Universality: Does every human being have the characteristic?
- Distinctiveness: How high is the chance that two or more people are having the same characteristic?
- Permanence: How much does the characteristic change over time?
- Collectability: How difficult is it to collect the characteristic?
- Performance: How difficult is it to read the characteristic by a machine?
- Acceptability: Is the used technology accepted by mankind?
- Circumvention: How difficult is it to tamper with the characteristic?

Biometric identifier	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
DNA	+	+	+	-	+	-	-
Ear	o	o	+	o	o	+	o
Face	+	-	o	+	-	+	+
Facial thermogram	+	+	-	+	o	+	-
Fingerprint	o	+	+	o	+	o	o
Gait	o	-	-	+	-	+	o
Hand geometry	o	o	o	+	o	o	o
Hand vein	o	o	o	o	o	o	-
Iris	+	+	+	o	+	-	-
Keystroke	-	-	-	o	-	o	o
Odor	+	+	+	-	-	o	-
Palmprint	o	+	+	o	+	o	o
Retina	+	+	o	-	+	-	-
Signature	-	-	-	+	-	+	+
Voice	o	-	-	o	-	+	+

Table 1: Comparison of different biometrics. High, medium, and low are denoted by +, o, and -. [1]

As regards fingerprints, the uniqueness and the acceptability are quite good, but as one may lose a finger, the permanence could be a problem. In addition, there are known attacks on fingerprint readers, therefore circumvention may not be that good either. Table 1 shows an overview of the characteristics of the most common biometrics.

Biometrics are divided according to whether they are physiological and behavioural. Physiological biometrics are the kind of characteristics that refer to the shape of a body part, such as fingerprints. By contrast, behavioural biometrics refer to the behaviour of a human being. Examples are voice and gait.

2.2 Physical biometrics

As mentioned above, physical biometrics are body related biometrics. Most of these biometrics are available from birth, hardly change over time, are unique and almost every human being has them. A major problem with physical biometrics is theft. They can not be changed and therefore never used again, once they are stolen.

2.2.1 Fingerprints

Fingerprints have been used by law enforcement for over a century. Therefore, they are very well studied and society accepts their use in most cases. Moreover table 1 points out that fingerprints meet very high security demands, because distinctiveness and permanence are rated "high".

The word "fingerprint" commonly does not refer to a print of a whole finger, but to the structure of ridges and valleys on the surface of a fingertip. This structure is unique on every human being and does not change in lifetime. Even after the skin of a fingerprint has been cut of totally, the structure gets restored, as new skin grows. An image of these structures can be taken by applying ink to a finger tip and using it like a stamp on a blank piece of paper. Furthermore, as all human skin is always covered by a thin layer of fat, a fingerprint is left on every thing touched. These can be made visible by special kinds of powder. By comparing these images it is possible to determine if a specific human being has touched a certain object. Nowadays optical scanners and digital photography are also used to take images from fingerprints.

Since computers have become more powerful, they are used to compare the images of fingerprints. However some problems had to be solved first. The quality of images taken from fingerprints vary a lot as the light circumstances change, the finger is held in different ways, the finger is moved a little while the picture is taken, the device that took the picture changed, and so on. In contrary to a human, the computer cannot recognize that it is looking at two pictures of the same finger, and rejects the authentication.

To solve the problems mentioned above, a computer first extracts a pattern from each image of a fingerprint, and then compares these patterns. To create these patterns, the computer looks for features of the fingerprint, so called "minutiae". Figure 1 shows endings and fusion of ridges, which are the simplest minutiae to find. If not enough of those are found, the computer can look for other characteristics on the fingerprint, as is shown in Figure 2. A pattern consists of the relative location to each other, as well as the types of all minutiae found. These patterns can then be rotated and scaled to compensate the distinctions in two pictures of the same fingerprint. Furthermore these patterns need far less disk space than images themselves, which is a good thing when storing great quantities of fingerprints. [5] [1]

Figure 1: Ending and fusion of a ridge [7]

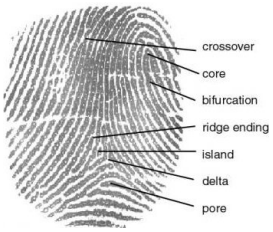

Figure 2: Different kinds of minutiae [7]

2.2.2 Other physical biometrics

Apart from fingerprints there are several other physical biometrics. For example, the analysis of DNA is also often used by law enforcement to identify human beings. As only identical twins share parts of their DNA, it is almost as unique as a fingerprint. However, the process to determine whether two samples are from the same person is very complex and can it only be done in a laboratory. Therefore, it is not suitable for authenticating on a mobile device. Furthermore it is very easy to steal a DNA sample of someone, because it can be found in every hair, every drop of saliva or in every scurf someone loses. [5] [1]

Another biometric that is almost unique on every human

being is the iris. It can be scanned using an ordinary digital camera, as long as the resolution is high enough. It is quite hard to tamper with, as surgery is very expensive and difficult and fake irises are easy to recognize. The only problem with using a scan of the iris for authentication is that the quality of the scans vary a lot more than on fingerprint scans. This is because an eye cannot be pressed on the scanning device like a finger can. Therefore light conditions, scale, objects in between the scanner and the eye and so on can prevent a successful authentication via iris scan. [5] [1]

The same problems as for iris scans appear on ear or face recognition. In addition it is possible to tamper with the scanning systems, as they cannot recognize fake additions to the face or ear.

2.3 Behavioural biometrics

All biometrics that refer to habits and behavioural features of a person belong to this category. They are a lot easier to collect then physical biometrics and their usage is accepted by most people. On the other hand behavioural biometrics can change either over time or even on purpose by training.

2.3.1 Keystroke dynamics

On the side of behaviour biometrics, the analysis of keystroke dynamics has a lot potential for mobile authentication. Alike the handwriting of a person has certain characteristics that can be analysed and almost perfectly matched to him, the way someone is using a keyboard has too.

The most obvious characteristic of typing is speed. If someone is able to write 50 words per minute on average, it is very doubtful that the same person can identify himself as someone who is able to type 100 words per minute. However, this characteristic can only be used in one direction because it is easy to slow down one's typing speed, in order to pretend to be someone else. Therefore, more characteristics of keystroke dynamics have to be considered. One is the "dwell time", which describes how long a key is pressed down until released. This dwell time varies for every letter on a keyboard, as different fingers in different positions are used to press it. In addition to that the so called "flight time", the time the user needs to hit the next key after he released the previous one, can be used to identify someone.

Furthermore, it is possible to determine whether a person is right or left handed, by analysing the keystroke dynamics. This can be done by comparing the flight and dwell time for the letters that are typically pressed with the right hand, to those pressed with the left. In most cases, a right hander is faster with his right hand, which has an impact on these measurements.

In some cases, it can even be determined what native language the person typing has. As certain combination of letters are often used in one language and rarely in another, a native speaker of the first language is faster on these combinations of letters. For example, the combination "t - h - e" is very common in English, but rarely ever used in German. That is why an English person would type these letters faster than a German, even if English is not the language used at that moment. In addition to that, it could also be guessed from which region of a country someone is by analysing his choice of words or spelling of certain words. Someone from the United Kingdom would write "colour" while someone from the USA would spell it "color".

When combining all these characteristics of keystroke dynamics, it is possible to identify a person by his typing. Although some of these may be easy to tamper with, others are not and it takes a lot effort to fully adept the typing behaviour of someone else. The only problem is that some of these characteristics may change over time. Typing speed increases when one gets a lot of practice, flight and dwell time differ if the keyboard layout changes or the keys respond differently on different keyboards.

Due to the typing characteristics mentioned above, there are two ways of monitoring one's typing behaviour. The first approach is the static observation of typing habits. The keystrokes are being watched, while the user tries to authenticate with a service. This approach is more secure than only using a password, but as soon as the user is logged in, there is no way to be sure that it is still him using the service. That is why the continuous observation of typing behaviour might be the better choice. At this approach the system monitors the keystrokes at all time. Therefore, it can determine that the person using the computer changed, even if the authentication with a service was already successful. This way, it would be possible to block an email account if it is not used by the owner because he forgot to log out at a public computer. The continuous approach can also be used to compensate minor changes in the characteristics, such as speeding up.

Besides to the benefits of continuous authentication, the biggest advantage of using keystroke dynamics is that it is very cheap. There is no additional hardware needed on notebooks, netbooks and desktop computer. Furthermore as research in this area goes on, the different ways of typing on cellphones etc. might be used for a keystroke analysis as well. [4]

2.3.2 Other behavioural biometrics

Apart from keystroke dynamics, the voice of a user can be analysed to identify him. Technically speaking the voice is not a behavioural biometric, but more a combination of physiological and behavioural biometrics. The vocal chords, the mouth, the throat and the nasal cavity affect the voice. Moreover, characteristics of the voice depend on the region where one grew up, when it comes to dialect or accent. The upside of using voice analysis for authentication is that it is highly accepted and most mobile devices are already equipped with the necessary hardware, a microphone. Furthermore, it is a very intuitive way to recognize people. On the other hand there are some major downsides to voice analysis. Sickness, emotions and time can change the voice significantly. Furthermore background noises could prevent a successful authentication. Also, there are some security issues, because a recording of someone's voice might be enough to steal their identity, when the words spoken for authentication never change. This could be prevented by a text-independent voice recognition system, where a different text is used for every authentication, but these systems are even more difficult to design and often reject users falsely. [5] [1]

Another behavioural biometrics is the gait. Although it is not very distinct, it may help in the identification process. As a video sequence is needed to analyse the gait of a human being, it may be combined with face recognition. It is obvious that this is not suitable for authentication on a mobile device, as making a video of themselves is not very practical. However it could be used in public locations to identify people. An additional downside of the analysis of gait is, that it changes a lot due to injuries, weight gain or loss, different shoes and so on. [5] [1]

3 Attacks on biometrics

3.1 Possible weak points

To analyse possible threats to a biometric authentication system Figure 3 by Bartlow and Cukic is used. It is based on an earlier framework by Wayman [10] and divides a biometric authentication system into eight subsystems:

- The *Administration* needed for every biometric authentication system is represented by this unit.
- The *IT Environment* unit is the supersystem which the biometric authentication system is a part of.
- A *Token* with additional information is required by some biometric authentication systems, in addition to the biometric presented to the scanning device.
- *Data Collection* is the part of the system that scans the biometric characteristic on the person that wants to authenticate himself to the service.
- *Transmission* transports the collected data to the other units that need it.
- *Signal Processing* processes the received data and compares it to the data in the storage.
- *Storage* for all the data needed for the authentication.
- The *Decision* subsystem makes the boolean decision between "accept" and "reject".

By using this framework, we determined 20 different possible weak points on biometric authentication systems labelled 1 - 20 in Figure 3. In addition to that, we identified 20 different possible vulnerabilities [8] [6], which can be categorized in six groups:

- Insider: People that already have access to the system, such as a *Bad Admin* or a *Bad User*, can cause security leaks. This could happen by accident, because humans tend to make mistakes, or on purpose, if someone tries to operate out of his rights, abuse their position to break into the system or try to upgrade his account to a higher level of security.
- Processing Weaknesses: An attacker could exploit weaknesses in the processing of the biometric presented to the scanning device. The system could be tricked by confronting it with disturb signals, called *Noise*. Furthermore, if the quality control accepts *Poor Images* of biometric characteristic with low quality, it could be possible to gain access by using ones own biometrics, which the system might mistake for a noisy picture. Similar to the poor image attack a *Weak ID* pattern for the pattern matching could be exploited. In addition to that, an attacker might perform an *Casual* attack by trying to authenticate with the system with a rejected biometric characteristic over an over again, until he eventually succeeds, due to a high false accept rate. Moreover the attacker could try to get a *Fake Template* into the system, so that his own biometrics get accepted.
- Scanner: There are several ways an attacker could try to trick the scanning device. If his biometric characteristic is identical or close to identical to someone's with higher security level, he could use this fact to break into the system. This is called an *Evil Twin* attack. Furthermore it might be possible to *Mimic* the biometric characteristic needed for authentication, such as slowing down the typing speed. In addition to that, for some biometric characteristics it is not too hard to make an *Artificial* copy of a real one. Specially so called *Residual* biometrics, meaning that they leave a trace behind, are sensitive to this kind of attack.
- Hardware: Some weaknesses are caused by insecure hardware. If the *Power* on any part of the system falls out, security might not be available anymore. Furthermore the attacker could try to *Tamper* with the hardware for the biometric authentication system.
- System: If the authentication system is designed or implemented improperly, more attacks might be possible. The attacker could record the data sent during a valid authentication and later use this data in a *Replay Attack*. Furthermore, he could try to break the encryption of the transmission in a *Crypt Attack*, in order to get the biometric data. Moreover the attacker could try to *Corrupt* the software of the system in order to make it more vulnerable. Some attacks on the system remain *Undetected*. These attacks could be preparations for future attacks.
- Environment: Some weaknesses result in the fact, that most authentication systems are part of a bigger supersystem, which might not be secure enough. For example it could be possible, that the attacker is able to install software in the supersystem, in order to *Degrade* total security. Furthermore if the supersystem is not secure enough against *Fail secure* attacks, such as denial of service attacks, buffer overflow etc., security might suffer. Moreover an attacker can get access to the service without using the biometric authentication system at all. This is called a *Bypass*.

As well as the units of which a biometric authentication system consists of, not all attack points and the different vulnerabilities are part of every system. The framework is a general structure used to show a possible attacks.

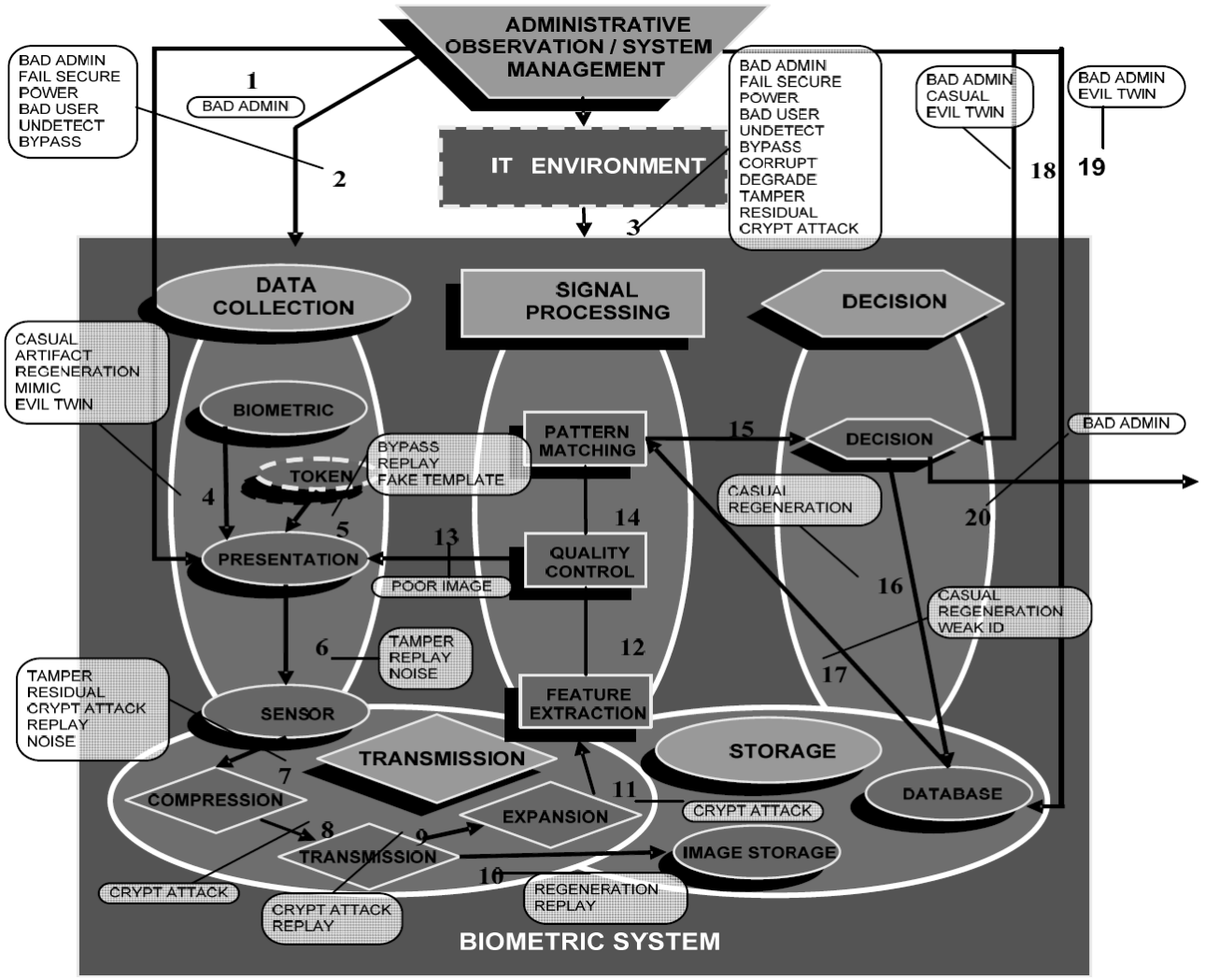

Figure 3: Bartlow and Cukic's Framework [6]

3.2 Examples of attacks

In this section we will discuss two examples of attacks on biometric authentication systems. The attack on fingerprint scanners is particularly easy and can be performed by most people, even with basic knowledge about computers. To realize a replay attack good knowledge in hacking, such as decrypting and signal fetching, is required, but it can be applied to almost every biometric authentication system.

3.2.1 Artificial fingerprints

Artificial biometrics are vulnerabilities that most biometrics have in common. The attacker tries to obtain an image or some other representation of an accepted biometric and creates a copy of it. Afterwards, the copy is used to pass the biometric authentication system. The usage of fingerprints is particularly susceptible to these kind of attacks, because it is quite easy for the attacker to obtain an image of a valid fingerprint.

The first step of attacking fingerprint authentication is to find a user that has the rights the attacker wants to obtain. The best choice is the administrator of the service, because he has all rights there are. An easier target is a regular user, who might not be as careful as the administrator is, but still has all the rights the attacker needs.

Then the attacker has to find out which finger the user uses to identify himself to the biometric authentication system. This can easily be done by watching the user during the authentication.

The next step is obtaining an image of the fingerprint used. On some biometrics this would be hard to do, but for fingerprints this is not. On some models of fingerprint scanners, like the one in Figure 4, the needed fingerprint is even left on the surface of the scanner. That is because the user has to press his whole finger onto a solid surface where it will leave a fingerprint. A better design is used on some modern notebooks and can be seen in Figure 5. The user has to drag his finger slowly over the scanner while this is taking an image. As the finger is not pressed to a solid surface no fingerprint will be left behind. But it is still very easy for the attacker to obtain the needed fingerprint, as they can be found all over the keyboard of the notebook where the scanner is build-in. If the fingerprint scanner is not part of a notebook, there still are lots of opportunities for the attacker to obtain an image of the fingerprint. All he has to do is watch what items the user touches.

Figure 4: A fingerprint scanner

Figure 5: Another model of a fingerprint scanner

Once the needed fingerprint is found, there are several ways to copy it. One of the easiest, but the still best, has been described by the Chaos Computer Club in 2004 [9]. After the fingerprint has been made visible with graphite powder or super glue, a picture is taken with a digital camera. This picture is enhanced a little on the computer and then printed in the right size with a laser printer on a transparent slide. The toner of the laser printer builds up a three dimensional negative of the fingerprint.

All the attacker has to do now is to build a dummy fingerprint from this negative. This is done by carefully sweeping it with a thin layer of wood glue. The wood glue forms the ridges of the fingerprint, by filling up the valleys of the negative. When the wood glue hardened, the dummy can be pulled of the transparency slide, cut to the right size and attached to a finger with skin friendly glue. Now, the attacker can use his artificial fingerprint to pass the biometric authentication system unnoticed.

To oppose the artificial fingerprint attack, modern fingerprint scanners try to detect dummies. This is done by measuring pulse and / or electrical conductivity of the finger during the scan process. However, tests have shown that if the dummy is thin enough, the attacker will still be granted access. Furthermore, there are materials more suitable to imitate a finger than wood glue.

3.2.2 Replay attack

A replay attack can be used if a biometric authentication system cannot be cheated with an artificial copy of the biometric. This could happen either because the scanner recognizes dummies or because it is not possible or too expensive to make a copy.

The attack usually takes place in the transmission part of the system. The attacker tries to listen to the communication between the scanning device and the rest of the system, in order do copy the data of a valid authentication. As soon as he achieved that, he resends this data to the system to authenticate himself with it without using the scanning device.

It is possible to prevent the attacker from obtaining authentication data by encrypting the communication, but this might cause other problems, as secure encryption is not always achievable. For example the process could be slowed down, because the chip used for the encryption is too slow. However, using several encryption chips could speed the process up, but it would require a larger scanning device, which is not desirable for mobile authentication. Another approach is a very specialized chip, which on the other hand would increase the cost. Furthermore a faster encryption algorithm that is not totally secure could be used, but that would give the attacker possibilities to apply his replay attack anyway. In addition to the encryption a handshake protocol must be used to guarantee that the attacker cannot use a copy of the encrypted communication. This would result in the same drawbacks as the encryption. [8]

4 Conclusion

As we have seen, biometrics have a lot of potential to replace passwords in protection of the critical services. Some of the biometrics are distinct enough to protect even high security services, such as bank accounts. Others are well accepted by society, and therefore they could be used for day to day services.

However, on the other hand many problems exist when using biometrics to secure these services. Specially, when biometrics are used on mobile devices, they could mean a serious threat to security, as ordinary users are more sloppy than those in high security facilities. Because of that, it is easy for attackers to abuse one of the many possible weaknesses. For example the use of artificial fingerprints does not even need higher skills of computer hacking, which enables even more people to tamper with the security systems.

Therefore we come to the conclusion that even though biometric authentication systems have a lot of potential, they should not be exaggerated as much as they are. Rather there should be a lot of research to enhance the existing methods or find new ones, so that soon we do not need to remember passwords anymore and still sleep peacefully, as we know our services are protected.

References

[1] S. P. Anil K. Jain, Arun Ross. An introduction to biometric recognition. In *Circuits and Systems for Video Technology, IEEE Transactions on*, 2004.

[2] K. Arena and C. Cratty. Fbi wants palm prints, eye scans, tattoo mapping. February 2008. `http://edition.cnn.com/2008/TECH/02/04/fbi.biometrics/`.

[3] C. Bernoulli. *Handbuch der Populationistik: oder der Völker- und Menschenkunde : nach statistischen Ergebnissen*. Verlag der Stettin'sche Buchhandlung, 1841.

[4] A. D. R. Fabian Monrose. Keystroke dynamics as a biometric for authentication. 1999.

[5] M. G. Kresimir Delac. A survey of biometric recognition methods. 2004.

[6] B. N. Bartlow. The vulnerabilities of biometric systems; an integrated look at old and new ideas. Technical report, West Virginia University, 2005.

[7] N. Science and T. Council. Fingerprint recognition. Technical report, National Science and Technology Council, 2007.

[8] D. Speicher. Vulnerability analysis of biometric systems using attack trees. Technical report, Lane Department of Computer Science and Electrical Engineering Morgantown, West Virginia, 2006.

[9] Unknown. How to fake fingerprints? Technical report, 2004.

[10] J. L. Wayman. Technical testing and evaluation of biometric identification devices. In A. K. Jain, R. Bolle, and S. Pankanti, editors, *Biometrics*, pages 345–368. Springer US, 2002.