BIOMETRICAL FINGERPRINT RECOGNITION: DON'T GET YOUR FINGERS BURNED

Ton van der Putte and Jeroen Keuning
Esire, an Origin Extended Enterprise
P.O. Box 543, 3740AM Baarn, The Netherlands
Ton.vanderPutte@esire.net and Jeroen.Keuning@esire.net

Abstract One of the most critical issues to solve when building multi-accessible systems, such as computer applications, cars or physical buildings, is to determine the identity of a person. A system protecting confidential information, or items of value, puts strong security demands on the identification. Biometry provides us with a user-friendly method for this identification and is becoming a competitor for current identification mechanisms, especially for electronic transactions. However, there are ways to compromise a system based on biometric verification. This article focuses on the drawbacks and risks of biometric verification, specifically verification based on fingerprints. It shows how all currently available fingerprint scanners can be fooled by dummies that are created with very limited means and skills.
This article should be read as a warning to those thinking of using new methods of identification without first examining the technical opportunities for compromising the identification mechanism and the associated legal consequences. This is especially true for people working with smart cards since it is quite common to store fingerprints on smart cards and due to the developments in solid state fingerprint scanners, integration of a fingerprint scanner on a smart card is possible.

Keywords: Biometry, Identification, Verification, Fingerprints, Fraud, Compromise

1. INTRODUCTION

Identification systems based on biometrics are capable of identifying persons on the basis of either physical or behavioural characteristics. Currently, there are over ten different techniques available to identify a person based on biometrics. The following techniques are applied within the main categories physical and behavioural characteristics:

Behavioural characteristics	Physical characteristics
keystrokes dynamics	iris recognition
voice recognition	retina recognition
signature dynamics	vein pattern recognition
	face recognition
	recognition of hand or finger geometry
	fingerprint recognition

Before a system is able to verify the specific biometrics of a person, it of course requires something to compare it with. Therefore, a profile or template containing the biometrical properties is stored in the system. Recording the characteristics of a person is called enrolment. In order to get a profile that corresponds most with reality, the biometrical characteristics are scanned several times. In case of fingerprint recognition the finger is scanned three to four times to get a profile that is independent of variations that occur in practice, such as the angle of placement of the finger on the scanner. Since storage capacity for the profiles in these systems is usually limited (for example if used in combination with smart cards), it is common to use data compression before storing the profile. Storing profiles in tokens requires a combination of token and biometry for verification and therefore gives a higher level of security.

When a biometrical verification is to occur, a scan of the biometrics of a person is made and compared with the characteristics that are stored in the profile. In general, a certain margin of error is allowed between the observed and stored characteristics. If this margin is too small, the system will reject a righteous person more often while if this margin is too large, malicious persons will be accepted by the system. The probabilities that a righteous person will be rejected and that a malicious person will be accepted, are called False Reject Rate (FRR) and False Accept Rate (FAR) respectively. When using a biometric system, one would of course want to minimise both rates, but unfortunately these are not independent. An optimum trade-off between FRR and FAR has to be found with respect to the application.

2. BIOMETRIC IDENTIFICATION BASED ON FINGERPRINTS

In this chapter the techniques for fingerprint identification will be explored. After explaining the theory of fingerprint verification, all current scanning technologies are described in more detail. Once it is known how these scanners identify a person by means of a fingerprint, two methods to counterfeit fingerprints are shown. All additional methods implemented by scanner manufacturers to prevent counterfeits from be-

ing successful are also described together with proposed methods how these systems could also be fooled into accepting dummy fingerprints. The consequences for systems using fingerprint verification are discussed at the end of the chapter. First, an example for fingerprint verification from practice will be given. This example also illustrates how difficult it can be to find an optimum trade-off between FAR and FRR. From a security point of view, one would want to have the FAR as small as possible. However, for acceptance of a biometry system, a large FRR is worse.

Case: Within the car industry a biometric verification system is under evaluation. Some manufacturers of expensive cars are considering using fingerprint recognition as a requirement for ignition of the engine. To arm against car theft, the FAR should be as small as possible. On the other hand, suppose that the righteous owner of a car cannot use his car because his fingerprint is rejected (i.e. FRR is too high). He will consider this to be a much more serious flaw in the system than a technical failure which prevents the car from being started. This is especially true if he compares the advantages of this system with this rejection: the advantages are that the driver does not (necessarily) have to have a key to his car and a perception of higher security with respect to theft of his car. Whether indeed the security improves is questionable. Right now, we do not see car thieves trying to copy the key of your car, instead they try to by-pass the ignition mechanism where the car key is involved. Furthermore, as this article will show, it might decrease security since it is fairly easy and cheap to copy a fingerprint from a person, even without the person knowing this.

2.1. THEORY OF FINGERPRINT VERIFICATION

The skin on the inside of a finger is covered with a pattern of ridges and valleys. Already centuries ago it was studied whether these patterns were different for every individual, and indeed every person is believed to have unique fingerprints [2]. This makes fingerprints suitable for verification of the identity of their owner. Although some fingerprint recognition systems do the comparison on the basis of actual recognition of the pattern, most systems use only specific characteristics in the pattern of ridges. These characteristics are a consequence from the fact that the papillary ridges in the fingerprint pattern are not continuous lines but lines that end, split into forks (called bifurcation), or form an island. These special points are called minutiae and, although in general a fingerprint contains about a hundred minutiae, the fingerprint area that is scanned by a sensor usually contains about 30 to 40 minutiae [5].

For over hundred years law enforcement agencies all over the world use minutiae to accurately identify persons [2]. For a positive identification that stands in European courts at least 12 minutiae have to be identified in the fingerprint. The choice of 12 minutiae is often referred to as "the 12 point rule" (see also [1]). This 12 point rule is not based on statistical calculations but is empirically defined based on the assumption that, even when a population of tens of millions of persons are considered, no two persons will have 12 coinciding minutiae in their fingerprints (see [3]). Most commercially available fingerprint scanners give a positive match when 8 minutiae are found. Manufacturers claim a FAR of one in a million based on these 8 minutiae, which seems reasonable.

2.2. FINGERPRINT SCANNING TECHNOLOGIES

Technologies for scanning fingerprints have evolved over the past years. The traditional method which is used by law enforcement agencies for over a hundred years now is making a copy of the print that is found at a crime scene or any other location and manually examining it to find minutiae. These minutiae are compared with prints from a database or specific ink prints, which could be taken at a later time. This method is of course based on the fact that the person who left the fingerprints is not co-operating by placing his finger on a fingerprint scanner. For systems that are commercially available (and deployed) people are required to co-operate in order to gain access to whatever is protected by the verification system.

The first generation fingerprint scanners appeared on the market in the mid eighties, so the technology is about fifteen years old. Over the past few years the technology for scanning fingerprints for commercial purposes has evolved a lot. While the first generation sensors used optical techniques to scan the finger, current generation sensors are based on a variety of techniques. The following techniques are deployed in commercial products that are currently available:

- Optical sensors with CCD or CMOS cameras
- Ultrasonic sensors
- Solid state electric field sensors
- Solid state capacitive sensors
- Solid state temperature sensors

The techniques will be described in greater detail in this section. The solid state sensors are so small that they can be built into virtually any

machine. Currently a sensor is in development that will be built in a plastic card the size of a credit card, not only with respect to length and width but also with respect to thickness! It is clear that this type of sensor will give a boost to the number of applications using fingerprint technology.

Optical Sensors

With optical sensors, the finger is placed or pushed on a plate and illuminated by a LED light source. Through a prism and a system of lenses, the image is projected on a camera. This can be either a CCD camera or, its modern successor, a CMOS camera. Using frame grabber techniques, the image is stored and ready for analysis.

Ultrasonic Sensors

Ultrasonic techniques were discovered when it was noticed that there is a difference in acoustic impedance of the skin (the ridges in a fingerprint) and air (in the valleys of a fingerprint). The sensors that are used in these systems are not new, they were already being deployed for many years in the medical world for making echo's. The frequency range, which these sensors use, is from 20kHz to several GigaHertz. The top frequencies are necessary to be able to make a scan of the fingerprint with a resolution of about 500 dots per inch (dpi). This resolution is required to make recognition of minutiae possible.

Electric Field Sensors

This solid state sensor has the size of a stamp. It creates an electric field with which an array of pixels can measure variations in the electric field, caused by the ridges and valleys in the fingerprint. According to the manufacturer the variations are detected in the conductive layer of the skin, beneath the skin surface or epidermis.

Capacitive Sensors

Capacitive sensors are, just as the electric field sensors, the size of a stamp. When a finger is placed on the sensor an array of pixels measures the variation in capacity between the valleys and the ridges in the fingerprint. This method is possible since there is a difference between skin-sensor and air-sensor contact in terms of capacitive values.

Temperature Sensors

Sensors that measure the temperature of a fingerprint can be smaller than the size of a finger. Although either width or height should exceed the size of the finger, the other dimension can be fairly small since a temperature scan can be obtained by sweeping the finger over the sensor. The sensor contains an array of temperature measurement pixels which make a distinction between the temperature of the skin (the ridges) and the temperature of the air (in the valleys).

2.3. COUNTERFEITING FINGERPRINTS

The biggest problem when using biometrical identification on the basis of fingerprints is the fact that, to the knowledge of the authors, none of the fingerprint scanners that are currently available can distinguish between a finger and a well-created dummy. Note that this is contrary to what some of the producers of these scanners claim in their documentation. We will prove the statement by accurately describing two methods to create dummies that will be accepted by the scanners as true fingerprints. The two methods vary based on the co-operation of the fingerprint owner. Although there will without doubt be more ways to counterfeit fingerprints, the methods described in this article should suffice to show that all current scanners can be fooled. Results of tests of current scanners can be found in Appendix C.

Duplication With Co-operation

Duplication of a fingerprint with co-operation of its owner is of course the easiest method since it is possible to compare the dummy with the original fingerprint in all aspects and adapt it accordingly. First, a plaster cast of the finger is created. This cast is then filled with silicone rubber to create a wafer-thin silicone dummy (see also Figure 1). This dummy can be glued to anyone's finger without it being noticeable to the eye. For a thorough description of how to create such a dummy, we refer to Appendix A which describes the materials and tools that can be used. From the appendix it follows that creation of this type of dummy is possible with very limited means within a few hours.

Duplication Without Co-operation

For duplication of a fingerprint without co-operation of its owner it is necessary to obtain a print of the finger from, for example, a glass or another surface. One of the best ways to obtain such a print could be the fingerprint scanner itself. If the scanner is cleaned before a person will

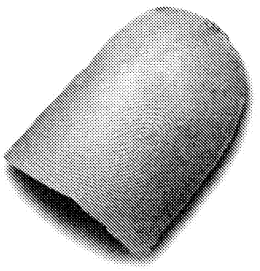

Figure 1 A wafer-thin silicone dummy of a fingerprint

be using it, an almost perfect print is left on the scanner surface since people tend to press their finger (which is the verification finger!) firmly on the scanner. Some more expertise is required to create a dummy from such a print, but every dental technician has the skills and equipment to create one. An accurate description of how to create a dummy of the fingerprint can be found in Appendix B. A picture of a stamp that is created using this method can be found in Figure 2.

Figure 2 A stamp type dummy of a fingerprint

2.4. ADDITIONAL TESTS OF SCANNERS

The main problem that challenges scanner manufacturers is making a distinction between dummy material that is not alive (i.e. silicone rubber) and material that is in fact not alive as well, the epidermis of a finger. Much research is done to make sure that a living finger is behind the epidermis. This research focuses on properties such as temperature, conductivity, heartbeat, blood pressure etc.. Although the methods are able to distinguish between dummies and real fingers, their operation margins have to be adjusted so radically to effectively operate indoors, outdoors, summer and winter, that a wafer-thin silicone rubber that is glued to a real finger easily passes these additional tests of scanners. For each of the possible additional tests for living fingers, a description will be given how dummies can be accepted by these systems.

Temperature

In a normal environment the temperature of the epidermis is about 8-10 degrees Celsius above the room temperature (18-20 degrees Celsius). By using the silicone rubber as described in Appendix A, the temperature transfer to the sensor decreases by at most 2 degrees if compared to a regular finger. It is clear that the difference falls with normal margins that are used on this system (at least 26-30 degrees). Sensors that are also capable of working outdoors are set to accept finger temperatures in an even broader range. Even when these sensors are compensating the fact that they are used outdoors, wafer-thin silicone rubbers won't be detected.

Conductivity

With most fingerprint scanners it is possible to add sensors which measure the conductivity of the finger. The conductivity of a regular finger is dependent on the type of skin (normal or dry). A normal conductivity value is about 200k Ohm (also dependent on the type of sensor), but the same finger will have a conductivity of several mega-Ohms during dry freezing winter weather and only several kilo-Ohms during summer when it is sweaty. Taking this into account, it is obvious that the margins are so large that putting some saliva on the silicone dummy will fool the scanners into believing it is a real finger.

Heartbeat

Several scanner manufacturers claim to detect a living finger by detecting the heartbeat in the tip of the finger. This is very well possible,

although some practical problems arise from this. People actively participating in a sport can have heart rhythm of less than forty beats per minute, meaning that they should keep their finger motionless on the sensor for at least four seconds for the rhytmh to be detectable. Also, the diversity in heart rhythm of a single person makes it virtually impossible to use it to take a person's heart rhythm into account when scanning the fingerprint. For example, the next day the same sportsman can have a heart rhythm of eighty beats per minute (doubled) if he decides to take the stairs instead of the elevator, just before his fingerprint is scanned. Moreover, the heartbeat of the underlying finger will be detected and accepted when a wafer-thin silicone rubber is used.

Relative Dielectric Constant

The dielectric constant of a specific material reflects the extent to which it concentrates the electrostatic lines of flux. Some manufacturers use the fact that the Relative Dielectric Constant (RDC) of human skin is different from the RDC of, for example, silicone rubber. Just as with conductivity measurement in fingerprint scanners, the RDC is influenced by the humidity of the finger. To prevent an unacceptably high FRR, the margin of operation should be rather large. Putting some spirit on the silicone rubber with a wad of cotton wool before it is pressed on the fingerprint scanner fools the additional dielectric sensor. Spirit consists of 90% alcohol and 10% water. The RDCs of alcohol and water are 24 and 80 respectively, while the RDC of a normal finger is somewhere between these two values. Since the alcohol in the spirit will evaporate quicker than the water, the rate alcohol/water in the evaporating spirit will go to 0 (i.e. spirit slowy turns into water). During evaporation the RDC of the dummy will go up until it falls within the margins of the scanner and will be accepted as a real finger.

Blood Pressure

There are sensors available with which the blood pressure can be measured by using two different places on the body. They require a measurement of the heartbeat on two different places to determine the propagation speed of the heart pulse through the veins. Apart from the disadvantages that were already mentioned with the heartbeat sensors, this technique has an additional disadvantage in requiring measurement on two different places, i.e. on two hands. Similar to the heartbeat sensors, this method is not susceptible to a wafer-thin silicone rubber glued to a finger. Single point sensors are available but they must be entered di-

rectly in a vein, which obviously makes them unusable as a biometric sensor.

Detection Under Epidermis

Some systems focus on detection of the pattern of lines underneath the epidermis. The pattern of lines on this layer is identical to the pattern of lines in the fingerprint. Although this type of sensors look underneath the first layer doesn't mean that they cannot be fooled by dummy fingers, once it is known how they distinguish between the epidermis and the underlying layer.
Some methods use the fact that the underlying layer is softer and more flexible than the epidermis (ultrasonic sensors could use this), while others focus on the higher electric conductivity of the underlying layer. Once it's known which property the sensor uses, a second silicone rubber with matching properties can be created. It is more difficult to create a dummy that is wafer-thin as described in Appendix A, but for a dummy as described in Appendix B it is rather easy. First, a conductive, soft or more flexible rubber print is made which can be used as the basis to which the regular silicone rubber is attached. Making sure that the two line patterns are in exact matching positions is no problem for a dental technician.

Other Claims

Some manufacturers claim to use even more exotic detection methods and techniques than the ones described above, making claims to having built a sensor which is not even known or being used in medical science. Additionally, they refuse to reveal the detection method claiming it is a company secret. Claims by these manufacturers should, without a doubt, be considered nonsense! In general, security by obscurity (trust that, by keeping specifications secret, the system will not be broken) should never be used. Although obscurity can make it more difficult for people to break the system in a brief period after introduction, most systems can be reverse engineered or worked around in ways the designers never expected.

2.5. CONSEQUENCES OF COUNTERFEIT POSSIBILITIES

The possibility to make a dummy, which will be accepted by the fingerprint scanners, makes the system weak with respect to some different attacks:

1 A malicious person who wants to gain access, inconspicuously intercepts a fingerprint from someone who is granted access. With this print, a dummy is created.

2 If a righteous person is willing to co-operate, one or several dummies can be created with which this individual can give access to whomever he wishes.

3 If a righteous person handles a transaction, he can claim to be framed by a malicious person as described in point 1.

While the first two attacks on the system are possible with most verification systems, the third claim can usually be disproved since the person making the claim must have revealed something. An example is fraud with a PIN protected credit card. If the fraud is committed using the PIN code, the probability that its owner has not been careful with the PIN is much higher than the probability that the PIN system is broken. But the fingerprint verification system is very susceptible to this attack since we all leave behind fingerprints everyday, everywhere without noticing it. As long as it is still possible to use either the methods from this article, or other methods to work around a fingerprint verification system, deployment of such systems is unsuitable for virtually any application.

Case: Suppose that a bank decides that for transactions, which exceed a certain amount of money, identification of the employee performing the transaction is required. The argumentation to use fingerprint verification instead of for example username/password combinations are that in case of fingerprint verification, the employee has to be present and cannot transfer his username/password to a colleague to perform transactions for him. Other systems that are considered, such as smart cards, can also not prevent the employee from letting other people perform a transaction. The bank trusts on the solution presented to them and decides to roll-out the fingerprint verification system throughout all offices.
An employee of the bank knows that these systems can be circumvented and decides to make a dummy from a fingerprint of a colleague. The risks are small since using the fingerprint of a colleague cannot be traced back to him. To obtain the fingerprint he asks the colleague who's fingerprint he intents to use to hand him a glass or plate. This will almost certainly leave a perfect print on a clean surface, with which a dummy can be created and the fraudulent transactions can be performed. In case the malicious employee is not capable of creating a good dummy, he can always perform transactions using his own finger and claim that he is framed by a colleague the same way as described above.

3. CONCLUSION

Manufacturers of fingerprint scanners currently cannot deliver convincing evidence that they can make a distinction between a real, living finger and a dummy created from silicone rubber or any other material. Therefore, our advice is not to use fingerprint verification with applications where the identification serves as proof of presence. Comparing all biometric verification possibilities, fingerprint scanners are (perhaps apart from keystroke dynamics) the least secure means of verification. It is the only system where the biometrical characteristic can be stolen without the owner noticing it or reasonably being able to prevent it.

Even in a case where confidential computer data are protected by means of fingerprint verification we advise use of this verification only in combination with a token, for example a smart card, on which the user's template is stored. This prevents unnoticed access by someone using a dummy when the template, with which the scanned finger is compared, is stored on the computer's hard disk. The security level of the combination of fingerprint verification and smart card should be compared to username/password security. The former can be considered more user-friendly.

With all applications that are considered to be protected by using biometric verification, techniques to compromise the system such as described in the appendices of this article should be very thoroughly examined. It should of course be taken into account that someone can break into a system if they put enough effort and resources into it (which is of course common with security issues). A problem with fingerprints is that neither the resources nor the skills to create a dummy are uncommon. Furthermore, the possibility of someone claiming to have been framed by someone else using methods that could not reasonably be prevented, must be eliminated. Otherwise the system is not suitable for the application.

4. DISCLAIMER

This article is based on private material and information that was released by fingerprint scanner manufacturers (also [4]). Many of the statements in this article are based on technology that is currently available. New technologies may evolve to a full fingerprint scanner between the submission deadline of this article and the actual CARDIS conference. These results or proof from fingerprint manufacturers that they can actually make a distinction between living fingers and well created dummies will of course be discussed at the conference.

Appendix: A - Duplication With Co-operation

This appendix describes, step by step, how to create a wafer-thin silicone dummy of a fingerprint if the owner of the fingerprint is willing to co-operate. The method requires only a limited amount of time (a few hours) and limited means (only cheap and easy accessible materials are used).

1 Beforehand, the finger should be washed with soap to make plaster flow more easily through the valleys of the print.

2 Using modelling-wax a kind of saucer or bowl is formed at the nail side of the finger and around the tip of the finger (like a thimble with an opening where the actual fingerprint is). This bowl is filled with plaster to obtain a print of the finger. Preferably the plaster should be of a good quality (such as used by dental technicians or kits for creating plaster figures sold in hobby shops).

3 The dried plaster is a bowl with a perfect fingerprint inside. In order to make a very thin dummy, a pounder that fits the mould (apart from a 1 mm distance for the dummy) can be created using plaster.

4 Silicone waterproof cement (available in any do-it-yourself shop) or liquid silicone rubber is placed in the mould and the pounder is pressed firmly on top of this layer.

5 When the silicone has hardened, the dummy should be very carefully removed and is ready.

Appendix: B - Duplication Without Co-operation

In order to make a dummy from a fingerprint without co-operation of its owner, a remake of a fingerprint that was left behind somewhere has to be made. The resulting dummy can of course be no better than the print itself so that for a good dummy a good print is required.

1 First the print has to be copied from the material it is left on. The method used by the police can very easily be used for this. Visualisation of the print is done with a very fine powder put on the print with a brush. Some scotch tape is used to remove the powder from the underground.

2 A camera and film are used to create a photo of the print by placing the tape on the photosensitive side of the film and making a picture using a diffuse light source.

3 After developing the film, the negative is attached to a photosensitive printed circuit board (PCB). This is exposed to UV light after which the negative is removed and the PCB will be developed. Using an etching bath, the parts of the PCB that were exposed to the UV light are washed away. A final etching bath (sour) etches the copper layer. The result is a very slim profile (about 35 micron) that is an exact copy of print, copied in step 1.

4 After deepening the profile (with for example a Dremel) to resemble the depth of a regular fingerprint, a silicone waterproof cement stamp can be created.

This method creates an almost perfect copy of the finger in about eight hours, using materials that are available in do-it-yourself shops and electronics shops. It requires more skills to create this dummy than the one described in Appendix A, but again, any dental technician or handyman has the necessary skills.

Appendix: C - Tested Fingerprint Sensors

From 1990 several fingerprint sensors have been tested using dummy fingers, as described in this article. All tested sensors accepted a dummy finger as a real finger, almost all at the first attempt. The following table shows the tested scanners, the date on which it has been tested and the number of attempts required to get a dummy finger accepted.

Manufacturer	Model	Technology	Date	Difficulty
Identix	TS-520	Optical	Nov. 1990	First attempt
Fingermatrix	Chekone	Optical	Mar. 1994	Second attempt
Dermalog	DemalogKey	Optical	Feb. 1996	First attempt
STMicroelectronics	TouchChip	Solid state	Mar. 1999	First attempt
Veridicon	FPS110	Solid state	Sep. 1999	Second attempt
Infineon	FingerTip	Solid state	Sep. 1999	First attempt
Identicator	DFR200	Optical	Oct. 1999	First attempt

In the period 1994 till 1998, more optical sensors have been tested on various fairs (mainly the CeBIT fair in Hannover, Germany). All sensors accepted the silicone dummy finger at the first attempt. The tested sensors are not listed in the table since no thorough list of manufacturers and models has been made at that time.

References

[1] Kingston, C.R. and P.L. Kirk, "Historical Development and Evaluation of the '12 Point Rule' in Fingerprint Identification," International Criminal Police Review, 1965.

[2] Lee, H.C. and R.E. Gaensslen, "Advances in Fingerprint Technology," Elsevier, New York, 1991.

[3] Zeelenberg, A.J., "Het identificatieproces van dactyloscopische sporen," VUGA, 's-Gravenhage, 1993 (in Dutch).

[4] http://www.biometrics.org

[5] http://www.infineon.com