

# PRACTICAL TECHNIQUES FOR DEFEATING BIOMETRIC DEVICES

By Mark Lane [REDACTED]

& Lisa Lordan [REDACTED]

MSc. Security and Forensics

Dublin City University

mark.lane@mail.dcu.ie

lisa.lordan@mail.dcu.ie

## FYI

Due to our liaison with [REDACTED] this document is to remain **CONFIDENTIAL**

## ABSTRACT

The storage and transmission of biometric data is becoming increasingly secure through the use of strong cryptography. However, advancements in this area rarely seem to address the biometric devices that are the corner stone of all biometric systems. This provides an exploitable avenue of attack. In this paper we present a number of practical techniques for fooling biometric devices that are commonplace in today's workplace where tampering with the device is impractical. In this paper we research fingerprint, iris and face recognition and aim to demonstrate why biometric devices should never be used as the only form of authentication on a system. We assess the most widely used biometric devices against these techniques in the context of a busy work environment. We attempt to demonstrate why two or more factor authentication should be used for mission critical systems and to circumvent identity theft.

## 1. Introduction

Biometric systems are a truly unique way of addressing the problems of identification and verification in a system, be it software access or physical access. In many organizations, implementing biometric devices in place of password control and/or physical security provides a more cost effective and conceptually secure solution. For high security systems this is implemented in parallel to other security measures such as a security guard monitoring the biometric authentication device. The purpose of such systems is to eliminate the "human error" factor when granting someone access. High profile examples of this type of authentication are the recent introduction of fingerprint readers at US immigration control, and the face recognition system recently

implemented in the [REDACTED]. Where such systems are implemented and monitored, the security of the biometric device becomes less of an issue as tampering and invalid authentication attempts will be easily noticed. Unfortunately the hardware of most biometric devices is designed with this particular scenario in mind. Ultimately the security of these devices is down to cost factors.

Even where "paranoid" security levels are not required, biometric devices are rapidly gaining ground, such as in the single factor authentication market. Such systems grant access based upon a single authentication system such as a password or biometric scan. It is primarily these systems that are most at risk from poor hardware design and equally poor implementation. Typical examples of these are fingerprint based door locks or unsupervised logins on computer systems. Combining biometric scans with passwords only adds partial security if an attacker has access to the hardware. In such cases a simple hardware key logger can be used, however for the purposes of this study, this would contradict our intention of authenticating without tampering with the hardware.

In this paper we will be primarily focusing on the use of fingerprint authentication systems. This is due to their prevalence in the marketplace as well as patent issues related to other forms of biometric scanners such as Iris. They provide a good illustration of how to attack a biometric device, regardless of how it is implemented. We shall also discuss some of the other forms of biometric devices, namely iris and face recognition systems, and also how to defeat them.

Herein, the person whose biometric data that we are trying to steal shall be known as the subject. Throughout this paper we will assume that there are two scenarios. Scenario one, that the subject is in cooperation with the attacker and scenario two, that the subject is unaware that their biometric data has been stolen or is not cooperating, i.e. non-cooperation. For each attack that we outline we will specify which scenario it is best suited for.

In order to ensure that the attack is relatively simple, we make a number of assumptions:

- The attacker has limited resources.
- The attack must not be costly to carry out and it should not require laboratory equipment.
- The attacker has limited time upon which to act.
- The attacker will have some sort of physical access to the device, typically this access will be under the supervision of a third party unless otherwise stated.
- The attacker cannot interfere with the normal operation of the device such as altering it physically or electronically in a noticeable or traceable way.
- The attacker knows the subject of the attack.
- In most circumstances the goal unless otherwise stated is to gain access to the system using the credentials of the subject.

## 2. BACKGROUND

### 2.1. What makes a good biometric?

Biometric authentication relies on any automatically measurable physical characteristic or personal trait that is distinctive to an individual [bf]. For a biological measurement to qualify as a biometric it should fulfil the following desirable properties [AP,T,AS]:

1. Universality: Every person should have the characteristic.
2. Uniqueness: No two people should be the same in terms of the characteristic, i.e. it should be distinct.
3. Permanence: The characteristic should not change over time.
4. Robustness: The characteristic can be measured consistently.

It is our opinion that there is one other factor that is equally important and is often overlooked to when defining a biometric:

5. Fraudulence: It must be extremely difficult to forge the biometric even with the cooperation of the subject.

There are two types of biometrics, hard biometrics and soft biometrics [y]. Hard biometrics are typically defined as biometrics that have a high level of uniqueness and are considered difficult to copy. Soft biometrics on the other hand, are ones where the level of uniqueness is relatively low. Soft biometrics are often more difficult to copy and reproduce than certain hard biometrics if they are combined.

Mistakes have been made in the past directly caused by choosing a soft biometric. In 1880 Parisian police officer, *Alphonse Bertillon* developed a system of anthropometry as a system of classifying criminals. The system worked on height, weight, length of arms, legs, index finger etc [as]. However this was later disproved in a prison

admission case where two unrelated men had identical measurements and identical names in the prison [1].

Soft biometrics is define in [2 ] as

*“soft biometric traits are characteristics that provide some information about the individual, but lack the distinctiveness and permanence to sufficiently differentiate any two individuals.”*

## 2.2. Fingerprint

### 2.2.1. Formation of fingerprints

Ridges and furrows on the skin of the hands and feet are first formed approximately in the thirteenth week of development of a foetus in the womb. This pattern formed is the first level of identification. There are 3 general types of ridge pattern arch, loop and whorl [ao]. They all centre at a core, a central point of the fingerprint. A delta is a point where the three patterns come together in a triangular form [ap, aq]. The delta and the core are used to determine the pattern type and as a reference point for classification. The ridges vary in length and width, split, stop and fragment to form minutiae. These minutiae are the second level of identification. For identification Irish courts require 8 minutiae matches (“8 point rule”) and European courts require 12 minutiae (“12 point rule”) [8]. Also forming part of a fingerprint are the pores that are dotted throughout the skin. The distribution of these pores throughout the skin form a third level pattern on the fingertips. All three levels remain mostly intact throughout life and are the last thing to decay after death [at]. Deep cuts and the resulting scars can change a fingerprint but not beyond a recognizable state. Our research primarily focused on creating a fake finger capable of exceeding the 12 point rule.

### 2.2.2. How is the finger imaged

There are numerous techniques for imaging a finger. The appropriate technique for a system depends on whether you have a person’s cooperation and also the context in which the finger needs to be imaged.

In the law enforcement context there are typically three ways a finger can be imaged. The oldest and simplest way is to coat the finger with a black ink and “rolled” onto a piece of white paper. It requires cooperation from the person unless they are unconscious. This results in a square looking print that captures a 3D finger as a 2D image. This image is then scanned into the Automated Fingerprint Identification System (AFIS) and processed to produce a digital representation and an image of the finger.

The second way does not require cooperation from the owner of the finger. The sweat pores of the skin constantly produce sweat. When a person touches something with their hand they leave behind a fingerprint

caused by this moisture on the fingertips which may be visible to the naked eye. Powders such as graphite can be used that stick to the fats in sweat or to “develop it” so that it can be removed with lifting tape. This fingerprint is then scanned into the AFIS and processed in the same way as an inked fingerprint [aq].

The third way is through the use of a fingerprint scanner which can transmit the digital representation of the finger to the AFIS. This also requires cooperation from the subject.

For all commercially available fingerprint scanners the person’s cooperation is required as they must place their finger on the sensor of the scanner to gain access. There are six types of sensor that a fingerprint scanners use to image a finger. The sensor types are optical, ultrasound, solid state electric field, solid state capacitive, thermal and pressure.

In general fingerprint scanners only scan a small area that contains about thirty to forty minutiae. Typically this is plenty of information to make a match as minutiae based systems only need approximately eight to twelve distinct minutiae matches for verification [bh].

### 2.3. Face

#### 2.3.1. *Brief explanation of Face Recognition*

There have been many different approaches to designing face recognition systems. They range from neural nets, which mimic how the human brain performs pattern recognition to principle component analysis [an]. The process of enrolling and using a face recognition system is algorithm independent and quite simple as explained in [as]. It is this simplicity that compensates for their poor results.

#### 2.3.2. *How is the face imaged*

Facial recognition systems are quite flexible in relation to image capture. Some systems use a still image for recognition while others use video capture for a more accurate reading. The final way the face can be imaged is by using a livenesscan which perform liveness detection with the option of performing challenge and response techniques to prevent repeat attacks. The images taken and used by a face recognition system can include infrared, monochrome, colour or a combination of them [ap].

### 2.4. Iris

#### 2.4.1. *Brief explanation of Iris Recognition*

The iris forms during early gestation of the foetus and is fully formed by the eighth month with only the pigment left to fully develop afterbirth [ao,h]. The iris pattern is influenced by embryonic fluid and genetics which leads

to the iris pattern’s randomness [I]. When J. G. Daugman first applied for a patent on iris recognition algorithm in 1994 the algorithm appeared to be robust against attack as the eye is a complicated organ that is almost impossible to copy [25]. This patent has resulted in Daugman’s algorithm being the only iris recognition in use today. The algorithm takes an image of an iris and generates an iris code which can be used to compare irises.

#### 2.4.2. *How is the iris imaged*

As the colour of the iris is irrelevant for recognition monochrome cameras are used with infrared illumination. The infrared illumination is used to increase the contrast of the iris. The type of camera used is a charge-coupled device (CCD) camera. The smallest iris diameter that the algorithm can identify is 0.35 centimeters or 70 pixels wide [I], however the optimal size is an iris diameter of 0.5 to 1 centimeters (100 to 200 pixels) from a distance of 46 to 15 cm [as].

## 3. RESEARCH

### 3.1. Fingerprint

We had five strategic incremental objectives when we approached the problem of defeating fingerprint scanners.

1. To authenticate as a valid user.
2. To enroll a fake finger into the system.
3. To enroll a fake finger that would authenticate to a real finger.
4. To leave a latent print from a fake finger.
5. To leave a latent print that would falsely identify the subject under [redacted].

We addressed these aims with in the context of the two scenarios of subject cooperation and non-cooperation. As fingerprint scanners are constantly developing and as minutia based scanners are the most secure route of this development, we chose to attempt to [redacted].

We worked closely with [redacted] to test our research against a purely minutia based system and the experts in this field. This system is comprised of a multi-million euro computer system by [redacted] with its results searched and verified by three experts before the fingerprint is deemed to be identified. The ultimate goal of our liaison was to create a fake finger mark capable of falsely identifying the subject. We also tested our results against seven of the leading fingerprint scanners on the market, namely:

- Targus Defcon Authenticator Fingerprint Scanner
- Compaq Fingerprint Scanner
- Sony Puppy Fingerprint Scanner
- Microsoft Fingerprint Scanner

- Touchchip Fingerprint scanner.
- Touchchip Fingerprint scanner with smart card reader.
- Lexar Jumpdrive USB memory with fingerprint scanner

All of the devices listed above use either optical or pressure sensors. There are other types of sensors, namely, ultrasonic, solid state electric field, solid state capacitive and thermal. These types of sensors are not widely available on the market and they have no real advantage over optical and pressure. The following attacks are identical for every type of sensor except thermal, where the fake finger should be heated to body temperature prior to application to the device.

### 3.1.1. Attacks with Cooperation

There are two attacks that can be used when you have the cooperation of the subject.

#### 3.1.1.1 Attack 1: Ask for a password

Most biometric authentication systems allow a user to supply a password without even attempting to verify their biometric. Simply obtaining the subjects password will allow the attacker to gain entry into the system. All but one of the fingerprint scanners that we tested worked in this way. This attack also makes an extremely valid point; there is no substitute for strong password security.

#### Results

Of the devices that we tested, the only scanner that did not function in this way was the Touchchip fingerprint scanner which had a smart card reader. It was possible to lock down the user interface to only allow logons where the smart card had been inserted into the device, however after obtaining the smart card it was still possible to verify using a password.

#### 3.1.1.2 Attack 2: Fake finger attack

This attack relies on the difficulty that fingerprint scanners have in distinguishing a real finger from a fake.

This is because the skin or epidermis is almost dead material. [Atos origin] Applying any other material with the same pattern and same texture has the same effect on the scanner as a real finger would. This attack involves trying to reproduce an exact copy of the ridges and furrows that appear in the subjects' finger. The best technique for this is to create a mould of the particular digit, and then create a cast from the mould which will become the fake finger. It is important that the mould and the cast accurately reflect the ridge patterns and minutia of the original finger. Our research primarily focused on techniques for achieving this.

For this attack we tested 15 different materials for moulding and 8 different materials for casting with some surprising results. The process for assessing the effectiveness of each moulding material was to create four individual moulds of a finger using the material in question. The material once hardened was then examined using a magnifying glass to assess the depth and sharpness of the ridges and furrows and the clarity of the minutia. The moulding materials that we tested were; oven-bake polymer clay, latex, air drying modelling clay, pva glue, candle wax, chewing gum, bubblegum, plasticine, bluetac, nail varnish, paint, microsils, cheese, gelatine and silicone. We choose to differentiate between bubblegum and chewing gum as the consistency of the two materials is quite different.

We found that the best materials for creating an accurate mould were; oven-bake polymer clay, plasticine and bluetac. They were fast, easy to obtain and extremely easy to create. Plasticine and bluetac took the longest to harden at thirty minutes in the freezer, while oven-bake polymer clay was hard and cool within 15 minutes. Wax was also found to be a good mould even though the creation process requires putting the subject's finger into the wax while it is still quite hot. See *Table 1* for a list of the materials used and the results that we obtained in descending order.

Mould Material	Ease of use	Durability	Time	Level 1, Ridge	Level 2, Minutia	Level 3, Pores
Oven Bake clay	Excellent	Excellent	15 min	Excellent	Excellent	Excellent
Bluetac	Excellent	Good	30 min	Excellent	Excellent	Good
Plasticine	Excellent	Good	30 min	Excellent	Excellent	Poor
Candle Wax	Poor	Excellent	20 min	Excellent	Excellent	Excellent
Microsil	Poor	Good	10 min	Excellent	Excellent	Excellent
Silicone	Good	Good	30 min	Excellent	Good	Poor
Nail Varnish	Fair	Good	90 min	Good	Excellent	Poor
PVA Glue	Poor	Fair	120 min	Excellent	Excellent	Excellent

Latex	Poor	Poor	90 min	Poor	Excellent	Excellent
Gelatine	Poor	Poor	60 min	Good	Good	Poor
Paint	Good	Poor	10 min	Good	Good	None
Air-Drying Clay	Excellent	Excellent	24 h	Fair	Fair	None
Bubblegum	Fair	Good	60 min	Good	Good	None
Chewing Gum	Fair	Poor	60 min	Good	Poor	None
Cheese	Poor	Poor	-	Good	Poor	None

*Table 1: Results of testing moulding materials*

To test the eight casting materials, we took the top three moulds, namely; oven-bake polymer clay, bluetac and plasticine, and then attempted to create a useable cast from each of these using each casting material. The analysis of the casting materials included a visual inspection followed by a physical test on a number of fingerprint scanners. The materials that we tested and the results obtained are ranked in descending order in *Table 2* below.

Cast Material	Ease of use	Durability	Time	Level 1, Ridge	Level 2, Minutia	Level 3, Pores
Gelatine	Fair	Poor	20 min	Excellent	Excellent	Excellent
Latex	Excellent	Good	40 min	Excellent	Excellent	Excellent
Microsil	Good	Good	10 min	Excellent	Excellent	Excellent
Silicone	Good	Good	10 min	Excellent	Excellent	Excellent
PVA Glue	Excellent	Excellent	10 min	Excellent	Excellent	Excellent
Bubblegum	Fair	Good	-	Good	Good	Poor
Chewing Gum	Fair	Poor	-	Good	Poor	Poor
Cheese	Good	Poor	-	Good	Poor	None

*Table 2: Results of testing casting materials*

After numerous trials at perfecting the right technique we found the following procedure to be optimal.

*Steps used to create a fake finger*

Although each material had its own individual methods of hardening and optimal thickness, the general process is material independent.

1. Create a base layer of material approximately 40mm square and 5mm thick. At this point the finger should be firmly pressed into the material to leave an impression to create the mould. This material is then hardened according to directions supplied.
2. A thin layer of lubricant is then applied to stop the casting layer from sticking to the mold. We found that fine clock oil was best suited for this. The finer the lubrication the more detailed the cast will be.
3. A layer of liquid casting material was then densely painted onto a piece of backing material such as cotton. This layer should be at least 1-2mm thick. This provides strength and durability to the cast. If the fingerprint scanner is optical then use a uniform colour fabric otherwise the colours affect the reading.

4. Apply another thin layer of casting material to the back of the fabric. This minimizes the effect that the pattern of the weave has on the reading. It also further strengthens the fake finger.
5. Allow to set.
6. Finally carefully peel the newly formed cast from the mold and analyze it for defects

A fake finger can also be created by applying the casting substance directly to the finger using casting materials such as latex, pva glue, microsil and silicone. The resulting mould is an inverse of the finger, i.e. what was a ridge on the finger is now a furrow on the mould. To our amazement, simply applying this mould directly to many of the fingerprint scanners would still verify to the subject. Specific examples were using PVA glue, allowed to set on the subjects finger, then verified on the Targus and Compaq fingerprint scanners. This appears to be a major flaw in their design as they are not able to detect when the print has been inverted.

After testing we found to best combination of materials were the oven-bake polymer clay or bluetac with gelatine or latex.

1.1. Tests performed

To test to see if our fake finger would meet all of our objectives we divided our tests into two distinct groups. Firstly we aimed to test it against the market leading brands of fingerprint authentication devices, and secondly we had our fake finger analysed by the [REDACTED].

Testing Objectives 1-3

There were four tests performed for each scanner using the top two casts. The tests are based on tests performed in [12]. These are;

1. Subject enrolled by the fingerprint system. Subject verified by the fingerprint system. This will form our control test.
2. Subject enrolled by the fingerprint system. Attempt to verify the fake finger as the subject in the system.
3. Fake finger enrolled by the fingerprint system. Fake finger is verified by the system.
4. Fake finger enrolled by the fingerprint system. Subject's finger verified by the fingerprint system as the fake finger.

The control test was performed ten times. Each of the verification tests were performed thirty times, enrolling, then verifying and then re-enrolling for the next test to ensure an accurate result. We had to recreate the casts frequently as typically a cast will only last less than ten enrolment/verification attempts before beginning to deteriorate.

Oven Bake polymer Clay Mould with Gelatine Cast				
Device	Enroll Real	Enroll Real	Enroll Fake	Enroll Fake
	Verify Real	Verify Fake	Verify Real	Verify Fake
Lexar	10%	1 = 3%	1 = 3%	1 = 3%
Targus	80%	22 = 73%	18 = 60%	21 = 70%
Touchip	80%	17 = 56%	6 = 19%	10 = 33%
Compaq	40%	9 = 30%	6 = 19%	13 = 43%
Microsoft	90%	20 = 67%	14 = 47%	7 = 23%
Sony	80%	19 = 63%	4 = 13%	10 = 33%

Table 3. Tests on fingerprint scanners using the oven bake polymer clay mould and gelatine cast.

Oven Bake polymer Clay Mould with Latex Cast				
Device	Enroll Real	Enroll Real	Enroll Fake	Enroll Fake
	Verify Real	Verify Fake	Verify Real	Verify Fake
Lexar	10%	0%	0%	0%
Targus	80%	10 = 33%	22 = 73%	16 = 53%

Touchip	80%	14 = 47%	9 = 30%	16 = 53%
Compaq	40%	4 = 13%	6 = 20%	13 = 43%
Microsoft	90%	20 = 67%	3 = 10%	7 = 23%
Sony	80%	17 = 57%	6 = 20%	10 = 33%

Table 4. Tests on fingerprint scanners using the oven bake polymer clay mould and latex cast.

Testing Objectives 4 & 5

We tested the top two fake fingers against the [REDACTED] to test how accurate our technique was. These were fake fingers cast from oven-bake polymer clay, using gelatine and latex. The fake fingers were subject to two tests by the fingerprints department.

As the latex fake finger is not naturally moist, moisture was applied to the fake finger and pressed onto an acetate sheet in six separate places. The gelatine fake finger was also applied to the same acetate along side these marks. This was then given to [REDACTED] for analysis. They treated the acetate with superglue by placing it in a fumigation chamber. This chamber releases superglue fumes that stick to the moisture that is left behind by our fake finger. The results from this test showed that our gelatine fake finger met objective number 4, and that it had left a latent print behind.

The subject's fingerprints were then taken using ink and paper as per the current procedure in [REDACTED] for taking fingerprints. These fingerprints were then uploaded to the "[REDACTED]" fingerprint system at which point a trained expert performed quality control to remove any misidentified minutia. The computer system was searched using both the inked marks taken from the fake fingers and the marks left on the acetate. The results from the AFIS system were then analysed and verified by three experts, all of which produced an exact match to the subject. The conclusion of this test showed that the gelatine fake finger naturally left a good quality latent print that easily identified the subject.

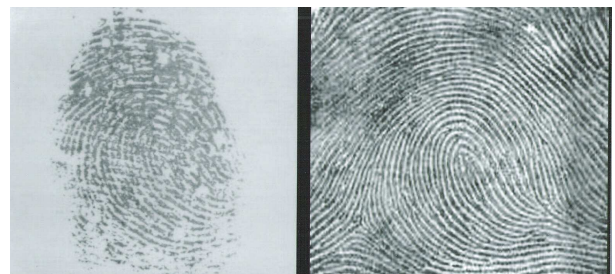
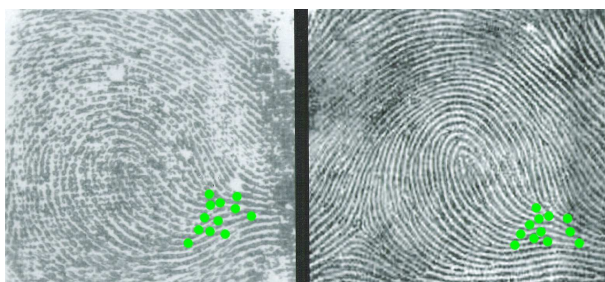


Figure A. This shows the latent print (left) developed from the acetate using the superglue fumigation

*technique. The inked print on the right is the one belonging to the subject, returned by the AFIS system.*

The inked prints left behind by the fake fingers had over 100 minutia matches with some layer 3 detail (pores). Figure B shows the 12 point minutia match necessary for identification under European law.

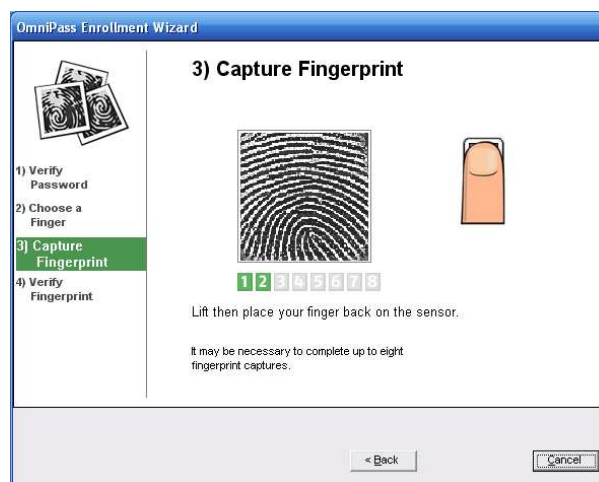


*Figure B. This shows the inked print (left) that was inputted into the AFIS system. The print on the right is the one returned as a match. The twelve green dots on each image show some of the matching minutia.*

### 3.1.2. Attacks without cooperation

There are three ways to obtain a print without the cooperation of the subject. The first way is to engineer a situation that calls for the subject to place their finger in a mould and leave an impression. The second way is by taking the subject's latent print. To do this reliably the attacker has to ensure that the latent print is in fact the subject's. A typical example might be to lift a print from the subject's mouse whether by dusting with graphite powder [13] and lifting the print with lifting tape or lifting the dusted latent print with microsil [14]. A latent print could also be lifted directly from the fingerprint scanner itself.

The third way of gaining the subject's print is by accessing the fingerprint system itself. Most fingerprint recognition software does not store an image of the fingerprint specifically for this reason. One work around is if the attacker can gain access to the system while the subject is enrolling, and if they could take a screen shot at the precise moment that the fingerprint was displayed by the system they would then have an image of the subject's fingerprint already pre-processed. All of the systems we tested displayed an image of the fingerprint as it enrolled.



*Figure C. This shows an image as the subject is being enrolled into the Targus fingerprint scanner*

Regardless of how the latent print is obtained the technique is the same. The lifted latent print is digitized by the attacker and processed using an image editor package such as paint shop pro [15] or adobe Photoshop [16]. The resulting image is then printed onto a transfer or an acetate sheet. The image is then transferred onto moulding material. A small drill or router is then used to chisel out the ridges and furrows into the moulding material. Once a sufficient number of ridges and furrows have been excavated a casting material is then applied to the mould. As with the previous attack we found that the best material to use was oven-bake polymer clay and gelatine. Blue tack was also good for this purpose however due to time constraints we were unable to cover a large enough surface using this technique to create a large enough fake finger for testing. We estimate that it would take approximately one week to complete this attack successfully on the average fingerprint scanner.

This attack has been carried out successfully in the past [proper 20] and we are confident that given enough time and patience it would be easy to defeat all of the fingerprint scanners that we have tested. Our results show that the resulting mould is extremely accurate and detailed if somewhat time consuming. This attack will remain an extremely credible threat to fingerprint scanners for the foreseeable future.



**Figure D. This shows how an image printed on a moulding material is being chiselled out to create a three dimensional mould**

### *.1.2. Tests performed*

Two tests were performed for this particular attack. For the first test we took latent prints from a piece of glass that the subject was asked to touch. The glass was then dusted with graphite powder and lifting tape was used to lift the print.

We also took latent prints from the scanners that we tested. The scanner was wiped clean of other fingerprints. The subject was already enrolled in the system and was asked to verify themselves to the system. The fingerprint was then dusted with graphite powder and the dusted print was lifted using microsil.

These latent prints then were scanned in and preprocessed in adobe photoshop. The processed prints were then printed on to an inkjet transparency using the highest quality on Hewlet Packard photosmart 1350 [19]. Latex was applied to one set of prints on acetate while the ink was still wet. Gelatin prints were applied to another set of prints on acetate. These were allowed to dry and then tested against the fingerprint scanners however the particular scanners that we had were not susceptible to this particular attack as they were mainly pressure based.

For the second test we printed a fingerprint image onto a transparency. While the ink was still wet we pressed the image onto a piece of hardened oven-bake polymer clay. We then used a magnifying glass and a drimel to create the ridges and furrows in the clay. We found that this gave more than enough contrast to begin the long process of shaping the mould.

## **3.2. Iris**

According to John Daugman in [ap] he states that his algorithm for iris recognition is impervious to attacks from photographs and printed irises. His defence against this attack is to apply a 2D Fourier transform to the iris image and determine if there is a specific pattern left by printing on the iris pattern. If this pattern is present then the iris is denied access [21]. This is however impossible as there is a max resolution to all cameras. So long as the individual pixels of the print are greater than twice the resolution of the camera then the camera is unable to perceive any noticeable difference between the image and a real iris (Niquists theorem). It is more likely that the use of infrared light is providing an added layer of security against the print than Fourier transform. We tested this using a Panasonic BMET100 iris scanner. We used a Nikon Coolpix 7900 [17] with a resolution of 3072x2304 (7 megapixels) to take a macro close-up

picture of the subject's iris. Another way of capturing the iris is by taking a video of the iris. This captures the eye movement that some iris scanners use for liveness detection. We used a Sony Handycam to capture a video of the iris.

### *3.2.1. Printing*

The iris image was printed using the highest resolution of the Hewlet Packard photosmart 1350 series [19] (600dpi). We printed the iris onto photo paper and inkjet transparency [20].

### *3.2.2. The attack*

The attacks on an iris scanner are the same with or without the cooperation of the subject. The simplest attack is to hold a high resolution picture of the iris with the pupil cut out up to the attacker's eye and present to the iris scanner. This results in the scanner seeing the iris pattern of the subject but performing liveness detection using the pupil of the attacker.

### *3.2.3. Tests*

Ten subjects were tested. The subjects ranged from twelve to subjects in their seventies with different eye colour. We tested a panasonic Authenticam BM-ET100US iris scanner [22]. Firstly we enrolled and authenticated the subject to ensure that the iris recognition system could authenticate the subject. Then we attempted to authenticate the fake iris (photograph) to the enrolled subject. Thirdly we enrolled the fake iris and attempted to authenticate the fake iris. Finally we enrolled the fake iris and attempted to authenticate the subject to the fake iris. Although iris scanners only use monochrome images we tested all the attacks with both monochrome and colour images to test for a difference.

### *3.2.4. Results*

We were unable to create a fake iris pattern that would authenticate as a real iris however we were able to enrol a fake iris that would authenticate to itself. This was primarily due to the differences introduced by the printing process and the way the image looked under infra red light. It highly likely that after some fine tuning such as altering the colour of the print so that it looks similar under Infrared light that we would have greater success. This attack has been completed successfully on this particular range of devices by a number of people [proper 20].

## **3.3. Face**

In launching an attack on face recognition systems we found that there was little difference between the attacks where the attacker has cooperation from the subject and

where they do not have cooperation. We tested our attacks against the Recognix FaceCode face recognition software available from [24] which requires a video capture device. We used the web camera as part of the Panasonic Authenticam BM-ET100US iris scanner [22].

### 3.3.1. Attack 1: Ask for a password

Most biometric recognition systems allow the user to bypass submitting a biometric by allowing the option of entering a password. If the attacker has the cooperation of the subject then all the attacker has to do is ask for the password. If the attacker does not have the cooperation of the subject, there are many other techniques to determine the password. These techniques include social engineering, attacking the password file on servers, using a password cracking program or even checking if the password has been written down near the subject's desk. FaceCode allowed the subject to circumvent submitting their face by choosing to use a password instead.

### 3.3.2. Attack 2: Photograph of subject

This attack works on the principle that the face recognition software has no physical access to the subject. Face recognition systems find it difficult to distinguish between a 2D face and a 3D face.

The attack is as follows;

1. Take a clear photograph of the subject
2. Print the photograph in high resolution. The photograph need only be the size of a passport photograph.
3. Present the photograph to the system holding it near the camera.

As part of our test we tested that the FaceCode was working correctly and could recognize our subjects under normal conditions by enrolling and verifying all the subjects. We then used different photographs of the subjects to attack the system. We used a photograph of each subject taken at a distance of ten metres, a photograph taken at a distance of three metres and passport photograph on an ID card or in a passport. These photographs can be obtained with and without the subject's cooperation. An attacker could even use a computer virus which takes images using the subject's machine's web camera, one such virus is the Rbot-GR virus [23].

Type of photograph	Enroll Real	Enrole Fake	Enroll Fake
	Verify Fake	Verify Real	Verify Fake
Subject at 10m	0%	0%	0%
Subject's face only at 1m	0%	0%	100%

Passport photograph on ID card	87%	93%	100%
--------------------------------	-----	-----	------

**Table T: Results of attack on FaceCode face recognition software using photographs**

We were surprised to find how simple it was to fool the face recognition system as can be seen from table T above. It was just a matter of finding the appropriate photograph. We found that a passport style photograph worked best. Even a passport style photograph that is not of excellent quality can suffice, as can be seen in figure R below which worked 100% of the time.



**Figure R: Example of a subject's ID card to attack Face Recognition Software**

## 4. CONCLUSIONS

### 4.1. Two or more factor authentication

We have successfully shown that biometric devices are not nearly as secure as we all hoped. While advancements in the area have improved greatly, biometric devices are still somewhat in their infancy. We have demonstrated that they can be extremely useful when addressing the problem of identification but not yet advanced enough at addressing the problem of verification. We have also shown that even when they are used for identification it is relatively simple for a malicious attacker to falsely leave an identifying mark.

It is our conclusion that using a biometric device on its own does not provide sufficient levels of security for even the simplest systems. While combining biometrics makes the task for an attacker much harder, it does not eliminate the problem completely, after all, you can choose never to divulge a password however you cannot choose not to leave a fingerprint.

### 4.2. Why a password isn't much better

Although a password can be a lot harder to steal than a biometric, if the attacker has access to the keyboard then it can be as good as useless. If the attacker can gain access to the keyboard just before and immediately after the user has logged in, then there is a simple attack that doesn't require any software or hardware key loggers.

The key is to lightly coat the keyboard with a fluorescent dust that is hard to notice under normal lighting conditions. Once the user has logged in the attacker simply uses an ultraviolet light to try and deduce which keys have been pressed. This dramatically reduces the key space that the attacker has to search. Feeding this information into a program that matches characters to English language words could rank the results in order of probability. We successfully tested this theory using an ultraviolet lamp and different types of fluorescent powder on a keyboard. We found that mustard powder a simple and effective powder for this particular task.

#### 4.2.1. Possible solution

Devices such as the RSA Secure ID tags [27] are extremely effective at avoiding some of the pitfalls of biometric authentication systems while also addressing the problems of password security. The principal works on generating a different, un-guessable password every minute. This password is used half of the password required to log in, the user memorizes the other half. These devices are “uncloneable” according to their manufacturers and are already the industry leaders in authentication systems for medium and enterprise solutions.

## 5. REFERENCES

- [1] Woodward Jr, J.D. Orlans, N. M. and Higgins, P. 2002. *Biometrics*. McGraw-Hill Professional.
- [2] Jain, A. Bolle, R. and Pankanti, S (eds). 1998. *Biometrics Personal Identification in networked society*. Boston: Kluwer Academic Publishers.
- [3] Prabhakar, S. Pankanti, S. and Jain, A.K. 2003. Biometric Recognition: Security and privacy concerns. *IEEE Security & Privacy*, 3 (March/April), pp33-42.
- [4] Wayman, J. Jain, A. Maltoni, D. and Maio, D. (eds). 2005. *Biometric systems technology, design and performance evaluation*. London: Springer.
- [5] Zewail, R. Saeb, M. and Hamdy, N. 2004. Soft and hard biometrics fusion for improved identity verification. *IN: The 47<sup>th</sup> IEEE Midwest Symposium on circuits and systems*. IEEE pp 2255-228.
- [6] Redi, P. 2004. *Biometrics for network security*. New Jersey: Prentice Hall PTR.
- [7] Maltoni, D. Maio, D. Jain, A.K. and Prabhakar, A. 2003. *Handbook of fingerprint recognition*. New York: Springer.
- [8] 8
- [9] Blomme, J. 2003. *Evaluation of biometric security systems against artificial fingers*. PhD Thesis. Linköping university.
- [10] Van der putte, T. and Keuning, J. 2000. Biometrical fingerprint recognition: Don't get your fingers burned. *IN: Proceedings of the fourth working conference on smart card research and advanced applications*, September 2000. Kluwer Academic Publishers. pp289-303.
- [11] Uwechue, O.A. and Pandya, A.S. 1997. Boston: Kluwer Academic Publishers.
- [12] Sanderson, S. and Erbetta, J.H. “Authentication for secure Environments based on Iris Scanning Technology” IEEE Colloquium on Visual Biometrics, vol.8, pp.1-7, 2000.
- [13] Daugman, J. G. 2004. How iris recognition works [pdf]. Available from: [www.cl.cam.ac.uk/users/jgd1000/irisrecog.pdf](http://www.cl.cam.ac.uk/users/jgd1000/irisrecog.pdf) [Accessed on 5 May 2005].
- [14] Daugman, J.G. March 1994. *United states, Biometric Personal Identification System based on Iris Analysis*. patent No. 5,291,560.
- [15] Van der Putte, T. 2001 Spoofing fingerprints. As easy as 1, 2, 3? [Online]. Available from: [http://www.keuning.com/biometry/Biometrics\\_2001.pdf](http://www.keuning.com/biometry/Biometrics_2001.pdf) [Accessed 5 June 2005].
- [16] Cryptome. (Homepage). [Online]. Available from: <http://cryptome.org/> [Accessed on 10 June 2005].
- [17] Reade Advanced Matrials. (graphite powder page). [Online]. Available from: <http://www.reade.com/Products/Carbons/graphite.html>. [Accessed on 20 August 2005].
- [18] Sctrace international Ltd. (homepage) [Online]. Available from: <http://www.cstrace.com> [Accessed on 20 August 2005].
- [19] (transfer paper page). [Online]. Available from: [http://www.databazaar.com/Inkjet\\_Cartridge/Product/Specialty\\_Paper\\_HEWQ1974A.html](http://www.databazaar.com/Inkjet_Cartridge/Product/Specialty_Paper_HEWQ1974A.html). [Accessed 19 August 2005].
- [20] Thalheim, L. Krissler, J. and Ziegler, P. 2002. Body Check. Biometric access protection devices and their programs put to the test. *C't*. [Online]. Vol. 11 p114-Biometrie. Available from: <http://www.heise.de/ct/english/02/11/114/>. [Accessed 3 March 2005].
- [21] Amazon. (HP PhotoSmart 1350 All-In-One Printer page). [Online]. Available from: <http://www.amazon.co.uk/exec/obidos/ASIN/B000DIODE/202-9741844-9898250>. [Access on 20 August 2005].
- [22] Daugman, J.G. (countermeasures). [Online]. Available from:

- <<http://www.cl.cam.ac.uk/users/jgd1000/countermeasures.pdf>> [Accessed 5 May 2005].
- [23] Shoplet. (inkjet transparency page). [Online]. Available from: <<http://www.shoplet.com/office/db/AVE05277.html>>. [Accessed 20 August 2005].
- [24] Panasonic. (Authenticam page). [Online]. Available from: <<http://catalog2.panasonic.com/webapp/wcs/stores/servlet/ModelDetail?displayTab=O&storeId=11201&catalogId=13051&itemId=63725&catGroupId=14469&modelNo=BM-ET100US&surfModel=BM-ET100US>> [Accessed 20 August].
- [25] Recognix FaceCode (homepage). [Online]. Available from: <<http://www.facecode.recognix.com>> [Accessed 10 June 2005].
- [26] Farrell, N. 2004. Worm turns on webcams. [Online]. Available from: <<http://www.theinquirer.net/?article=18039>> [Accessed 13 June 2005].
- [27] RSA security. (Secure ID page). [Online]. Available from: <<http://www.rsasecurity.com/node.asp?id=1156>>. [Accessed 25 August 2005].