DREAMLAB
TECHNOLOGIES

BYPASSING BIOMETRIC SYSTEMS WITH 3D PRINTING AND 'ENHANCED' GREASE ATTACKS

Yamila Levalle
Security Researcher at Dreamlab Technologies

June, 2020

INDEX

INTRODUCTION

Throughout the history of humanity, every restricted access has been determined by knowing or having a certain entity that proves that permission must be granted. Passwords are something that a person knows , while tokens are something that a person possesses . The years passed and researchers have encountered several shortcomings regarding the traditional authentication systems that represent the most frequently used approaches nowadays, leading to the adoption of new alternatives.

In 1971, A.J. Goldstein, L.D. Harmon, A.B. Lesk published the first paper that describes how human faces can be identified by humans and by computers, these studies form a foundation for continuing research on real-time man-machine interaction for computer classification and identification of multidimensional vectors specified by noisy components. The encounter between biometrics and computers created a new path for authentication systems in the following years.

Biometrics is the use of a person's unique physiological, behavioral, and morphological characteristics to provide positive personal identification. These examine fingerprints, iris, face, palmprint, vein patterns, voice, keystroke dynamics, signature, gait, ear shape, among others. Biometric authentication systems are pattern recognition systems that read biometric data as input, extract a feature set from such data, and finally compare it with a template set stored in a database. If the extracted feature set from the given input is matched to a template set stored in the database (and the attempt limit is not exceeded), then the user is granted access.

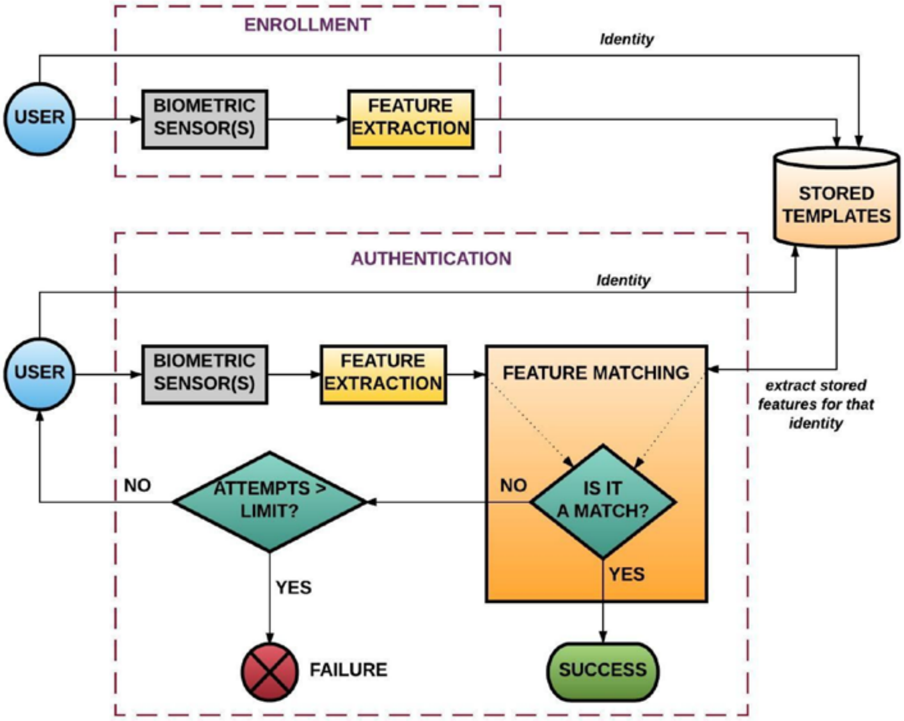


Figure 1 - Biometric Systems Recognition Process
https://www.researchgate.net/publication/332957276_A_Survey_on_Modality_Characteristics_Performance_Evaluation_Metrics_and_Security_for_Traditional_and_Wearable_Biometric_Systems

[1] IEEE, Identification of human faces, A.J. Goldstein ; L.D. Harmon ; A.B. Lesk, May 1971.
https://ieeexplore.ieee.org/document/1450184/authors#authors

The use of biometric authentication systems has introduced a convenient and efficient alternative to traditional schemes. However, we must keep in mind that as with any other technology, risks arise. Such systems are susceptible to a variety of security attacks that are aimed at undermining the integrity of the authentication process by either circumventing the security afforded by the system or deterring the normal functioning of the system. Common implementations of biometric authentication systems can be found on border controls, health care, welfare distribution and e-commerce among others. The abrupt adoption of biometric systems in commercial, government and forensic applications may lead to possible finance, privacy, and security breaches.

This paper presents an in-depth analysis of several types of software and hardware threats that exist in biometric authentication systems, describing how such vulnerabilities can be exploited with the help of 3D printing technology.

BIOMETRIC SYSTEM MODEL

In order to understand how biometric systems can be attacked, we must describe the biometric system model and the different modules that are part of it. Any biometric system consists of the following modules:

SCANNER

The scanner module in a biometric system is used to acquire the biometric data (e.g.: fingerprint, hand vein, palm print, voice, etc.) of an individual in the form of an image, video, audio or some other signal. The scanner module is vulnerable to a type 1 attack.

FEATURE EXTRACTOR

The feature extractor module in a biometric system operates on the signal sent by the scanner module to extract a feature set A, that represents the given signal. The extracted feature set A is sent to the matcher for processing. The feature extractor module is vulnerable to a type 3 attack.

STORED TEMPLATES

The stored templates module in a biometric system is usually a database that stores pre-acquired (usually during users' enrollment) feature sets called templates. These templates are queried by the matcher module to find a match for a given feature set A . The database that stores the templates is vulnerable to a type 6 attack.

MATCHER

The matcher is the most important module of the biometric system. It receives a feature set A from the feature extractor module and compares A with the templates stored in the database. Match scores are generated after each comparison and once all comparisons are done, the matcher processes these match scores in order to either determine or verify the identity of an individual. The matcher module is considered the main module in a biometric system as it evaluates if there is or not a match. It is vulnerable to a type 5 attack.

APPLICATION DEVICE

The application device module in a biometric system receives a Boolean answer from the matcher and acts accordingly denying or granting access. The application device can be vulnerable to a type 9 attack.

TYPES OF ATTACKS

TYPE 1: PRESENTATION ATTACK ON RECOGNITION SYSTEMS

In this attack a fake biometric trait can be created, like an artificial finger, in order to bypass fingerprint recognition systems, or well, present a photo or a video replay to bypass facial recognition systems.

TYPE 2: REPLAY ATTACK

When the scanner module in a biometric system acquires a biometric trait, the scanner module sends it to the feature extractor module for processing. In this attack the communication channel between the scanner and the feature extractor is intercepted to steal biometric traits and store it somewhere. The attacker can then replay the stolen biometric traits to the feature extractor to bypass the scanner.

TYPE 3: ATTACK ON THE FEATURE EXTRACTOR MODULE

In this attack the feature extractor module can be replaced with a malicious one. Therefore, the attacker can simply send commands to the malicious extractor in order to send to the matcher module feature values selected by him/her.

TYPE 4: ATTACK ON THE CHANNEL BETWEEN THE FEATURE EXTRACTOR AND MATCHER

This attack is similar to type 2, the main difference is that the attacker intercepts the communication channel between the feature extractor and the matcher to steal feature values of a legitimate user and replay them to the matcher later.

TYPE 5: ATTACK ON THE MATCHER

This attack is similar to type 3 described before, the main difference is that the attacker replaces the matcher with a malicious one. The attacker can send commands to the malicious matcher to produce high matching scores and send true values to the application to bypass the biometric authentication mechanism. The attacker can also send commands to the malicious matcher to produce low matching scores and send false values to the application all the time, causing a denial of service.

TYPE 6: ATTACK ON THE SYSTEM DATABASE

This attack compromises the security of the database where all the templates are stored. By doing this, the attacker can add new templates, modify existing templates or delete templates.

TYPE 7: ATTACK ON THE CHANNEL BETWEEN THE SYSTEM DATABASE AND MATCHER

This attack is similar to the attack described in type 2, the main difference is that the attacker intercepts the communication channel between the database and matcher to either steal and replay data or alter the data.

TYPE 8: COMMUNICATION INTERCEPTION BETWEEN MATCHER AND APPLICATION

This time, the attacker intercepts the communication channel between the matcher and the application to replay previously submitted data or alter the data.

TYPE 9: ATTACK ON THE APPLICATION

This attack is not focused in the biometric system itself but in the application that handles the authentication. Most biometric authentication systems use traditional authentication schemes as a backup. We can think about fingerprint readers as an example, they are shipped with laptops that force you to create a backup password that could be used to access the system if the fingerprint reader does not work accordingly. If the application in a biometric system is vulnerable due to having a critical bug (e.g.: buffer overflow, double free, etc.) then a skilled attacker can exploit this bug by sending the application a crafted input to change the control flow of the program.

In this paper we are going to focus on type 1 attacks: “Presentation Attacks”.

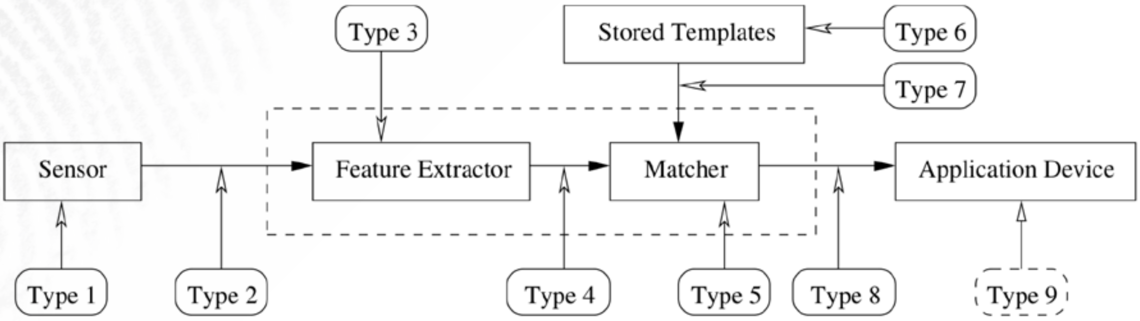


Figure 2 - Biometric Systems Attacks
https://www.semanticscholar.org/paper/How-to-Attack-Biometric-Systems-in-Your-Spare-Time-Obied/952bf27a58efd761a252bedd0b1d15aaa41cddeb

FINGERPRINT BIOMETRIC SYSTEMS

Fingerprint recognition is technically easier to achieve than the use of traditional authentication methods and it is widely more accepted by the public than other biometric authentication systems that use iris and retina. The industrialization and adoption of fingerprint sensors on common technology devices such as phones and laptops, have led to the development of products that are now quite small and affordable and have consequently became more widespread. As the market of fingerprint scanners increases, it is important to ensure and evaluate the security of such devices, establishing methods to measure how easy could be for the average criminal to circumvent the devices and how much effort, knowledge and resources are needed.

Most fingerprint scanner systems compare specific features of the fingerprint that are generally known as **“minutiae ”**. Investigators study the points where ridge lines end or where one ridge splits into two (bifurcations), deltas, cores, spurs, ridges endings, bridges and other distinctive features of the fingerprint. Collectively, these and other distinctive features are called **“typica ”**.

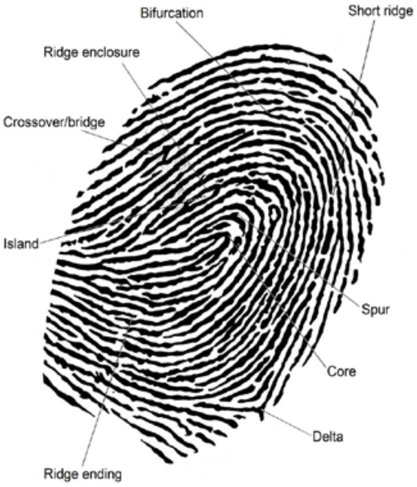


Figure 3 - Fingerprint Minutiae
https://datascienceprojects.wordpress.com/2018/08/04/fingerprint-classification-and-matching-using-deep-learning/

Through the usage of specific algorithms, the scanner can recognize and analyze these minutiae. It measures the relative positions of minutiae in the same way a human might recognize a part of the sky by the relative positions of stars. A simple way to think of it is to consider the shapes that various minutiae form if straight lines between them are drawn. If two prints have three ridge endings and two bifurcations forming the same shape with the same dimensions, there is a high likelihood they are from the same print. To get a match, the scanner system does not have to find the entire pattern of minutiae in the sample and in the print on record, it simply has to find a sufficient number of minutiae patterns that the two prints have in common. The exact number varies according to the scanner configuration.

Optical Fingerprint Scanners

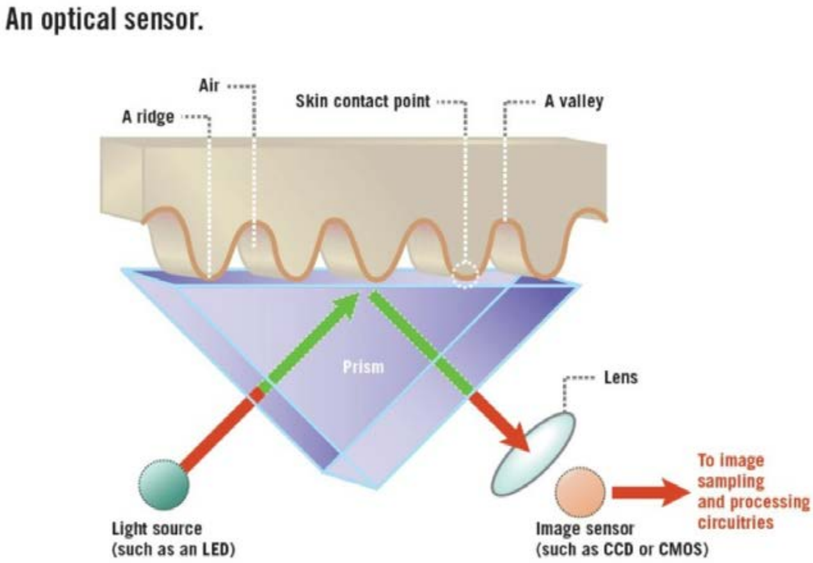

An optical sensor.
Air
A ridge
Skin contact point
A valley
Prism
Lens
To image sampling and processing circuitries
Light source (such as an LED)
Image sensor (such as CCD or CMOS)

Figure 4 - Optical Sensor
https://www.androidauthority.com/how-fingerprint-scanners-work-670934/

The main component in an optical scanner is the charge coupled device (CCD), the same light sensor system used in digital cameras and camcorders. A CCD is simply an array of light-sensitive diodes called photosites , which generate an electrical signal in response to light photons. Each photosite records a pixel, a tiny dot representing the light that hit that spot. Collectively, the light and dark pixels form an image of the scanned scene (a finger, for example) and then an analog-to-digital converter in the scanner system processes the analog electrical signal to generate a digital representation of this image.

The scanning process starts placing the fingers on a glass plate, and a CCD camera takes a picture. The scanner has its own light source that typically is an array of light-emitting diodes, to illuminate the ridges of the finger. The CCD system generates an inverted image of the finger, with darker areas representing more reflected light (the ridges of the finger) and lighter areas representing less reflected light (the valleys between the ridges).

Before comparing the print to the stored data, the scanner processor makes sure the CCD has captured a clear image. It checks the average pixel darkness or the overall values in a small sample and rejects the scan if the overall image is too dark or too light. If the image is rejected, the scanner adjusts the exposure time to let in more light, and then tries the scan again.

If the darkness level is precise, the scanner system checks the image definition (how sharp the fingerprint scan is). The processor looks at several straight lines moving horizontally and vertically across the image. If the fingerprint image has good definition, a line running perpendicular to the ridges will be made up of alternating sections of very dark pixels and very light pixels.

If the processor finds that the image is crisp and properly exposed, it proceeds to compare the captured fingerprint with fingerprints stored.

Capacitive Fingerprint Scanners

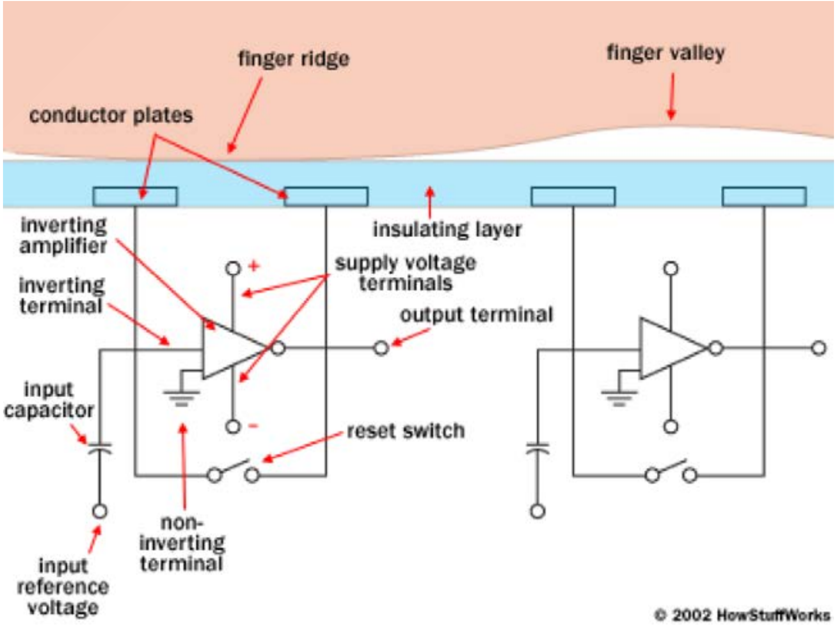


Figure 5 - Capacitive Sensor
https://computer.howstuffworks.com/fingerprint-scanner3.htm

Like optical scanners, capacitive fingerprint scanners generate an image of the ridges and valleys that make up a fingerprint. But instead of identifying the print using light, the capacitors use electrical current. The diagram above shows a simple capacitive sensor. The sensor is made up of one or more semiconductor chips containing an array of tiny cells. Each cell includes two conductor plates, covered with an insulating layer. The cells are tiny, smaller than the width of one ridge on a finger.

The sensor is connected to an IC, an electrical circuit built around an inverting operational amplifier. The inverting amplifier is a semiconductor device, made up of several transistors, resistors and capacitors. Like any amplifier, an inverting amplifier alters one current based on fluctuations in another current. Specifically, the inverting amplifier alters a supply voltage. The alteration is based on the relative voltage of two inputs, called the inverting terminal and the non-inverting terminal. In this case, the non-inverting terminal is connected to ground, and the inverting terminal is connected to a reference voltage supply and a feedback loop. The feedback loop, which is also connected to the amplifier output, includes the two conductor plates.

The two conductor plates form a basic capacitor, an electrical component that can store up charge.

The surface of the finger acts as a third capacitor plate, separated by the insulating layers in the cell structure and, in the case of the fingerprint valleys, a pocket of air. Varying the distance between the capacitor plates (by moving the finger closer or farther away from the conducting plates) changes the total capacitance (ability to store charge) of the capacitor. Because of this quality, the capacitor in a cell under a ridge will have a greater capacitance than the capacitor in a cell under a valley.

To scan the finger, the processor first closes the reset switch for each cell, which shorts each amplifier's input and output to "balance" the IC. When the switch is opened again, and the processor applies a fixed charge to the IC, the capacitors charge up. The capacitance of the feedback loop's capacitor affects the voltage at the amplifier's input, which affects the amplifier's output. Since the distance to the finger alters capacitance, a finger ridge will result in a different voltage output than a finger valley.

The scanner processor reads this voltage output and determines whether it is characteristic of a ridge or a valley. By reading every cell in the sensor array, the processor can put together an overall picture of the fingerprint, like the image captured by an optical scanner.

The main advantage of a capacitive scanner is that it requires a real fingerprint-type shape, rather than the pattern of light and dark that makes up the visual impression of a fingerprint. This makes the system harder to trick.

Ultrasonic Fingerprint Scanners

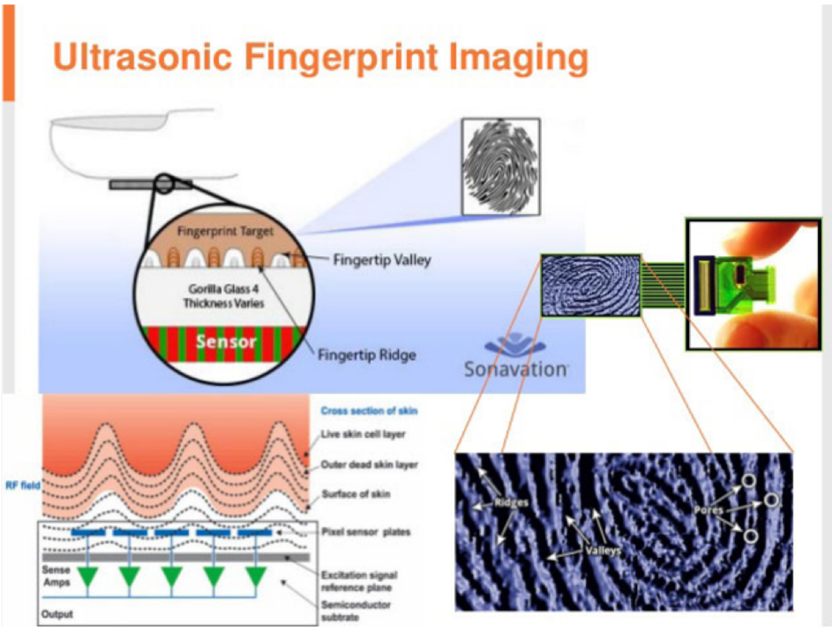


Figure 6 - Ultrasonic Sensor
https://circuitdigest.com/article/in-display-fingerprint-sensors

The latest fingerprint scanning technology to enter the smartphone space is an ultrasonic sensor. To capture the details of a fingerprint, the hardware consists of both an ultrasonic transmitter and a receiver. An ultrasonic pulse is transmitted against the finger that is placed over the scanner, some of this pulse is absorbed and some of it is bounced back to the sensor, depending upon the ridges, pores and other details that are unique to each fingerprint.

There is not a microphone listening out for these returning signals, instead, a sensor that can detect mechanical stress is used to calculate the intensity of the returning ultrasonic pulse at different points on the scanner. Scanning for longer periods of time allows for additional depth data to be captured, resulting in a highly detailed 3D reproduction of the scanned fingerprint. The 3D nature of this capture technique makes it an even more secure alternative to capacitive scanners.

In December 2018, Qualcomm announced its 3D ultrasonic in-display fingerprint sensor and this has been adopted inside Samsung's flagship Galaxy S10 and Galaxy S10 Plus. The drawback is that ultrasonic is not as snappy as other scanners yet, partly due to the reasons mentioned above. Ultrasonic technology is not compatible with some screen protectors, which limit the ability of the scanner to read fingerprints correctly. On the other hand, bezels are thinner than ever due to being able to hide the scanner under the display.

Materials and devices for the experiments

DEVICES TO TEST

- Smartphone Samsung Galaxy S10 with ultrasonic fingerprint scanner and face recognition
- Smartphone Samsung Galaxy A30 with capacitive fingerprint scanner and face recognition
- Attendance System Hysoon FF395 with optical fingerprint scanner and face recognition
- Attendance System TA040 with optical fingerprint scanner

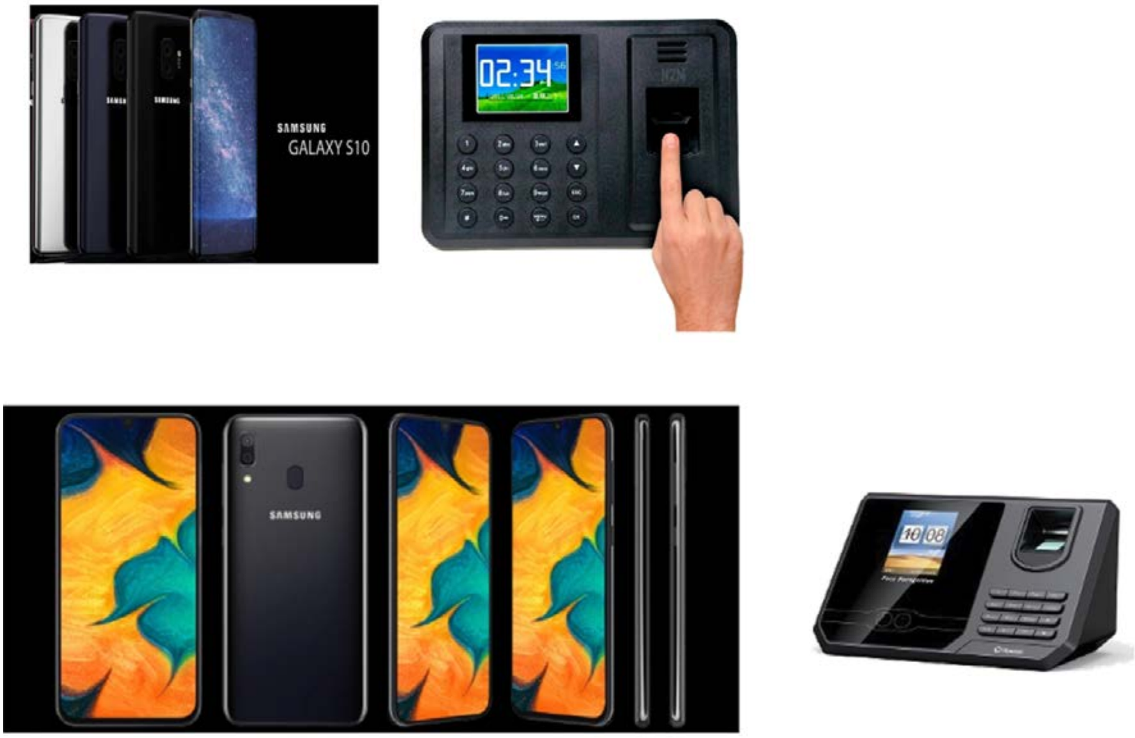


Figure 7 - Devices to test

Materials for fingerprint experiments

THE MATERIALS NEEDED FOR THE EXPERIMENTS INCLUDES:

- Gummy Bears
- Tinfoil
- Playdoh
- Latex Gloves
- Silicone Fingertips
- Alginate
- Epoxy putty
- Playdoh
- Hot Glue gun
- Silicone
- Gelatin Powder
- Liquid Latex
- Glycerin
- Synthetic Resin
- Wood glue
- UV Resin
- Isopropyl alcohol
- UV lamp
- Transparent Tape
- Transparency
- Hand Moisturizer
- Petrolatum Ointment
- Petrolatum + Paraffin Ointment
- Cocoa Butter Lip Balm
- Ethylcyanoacrylate Glue
- Fingerprint Powder and brush
- Digital Camera with macro functionality
- Fingerprint Ink Pad
- Paper and glass

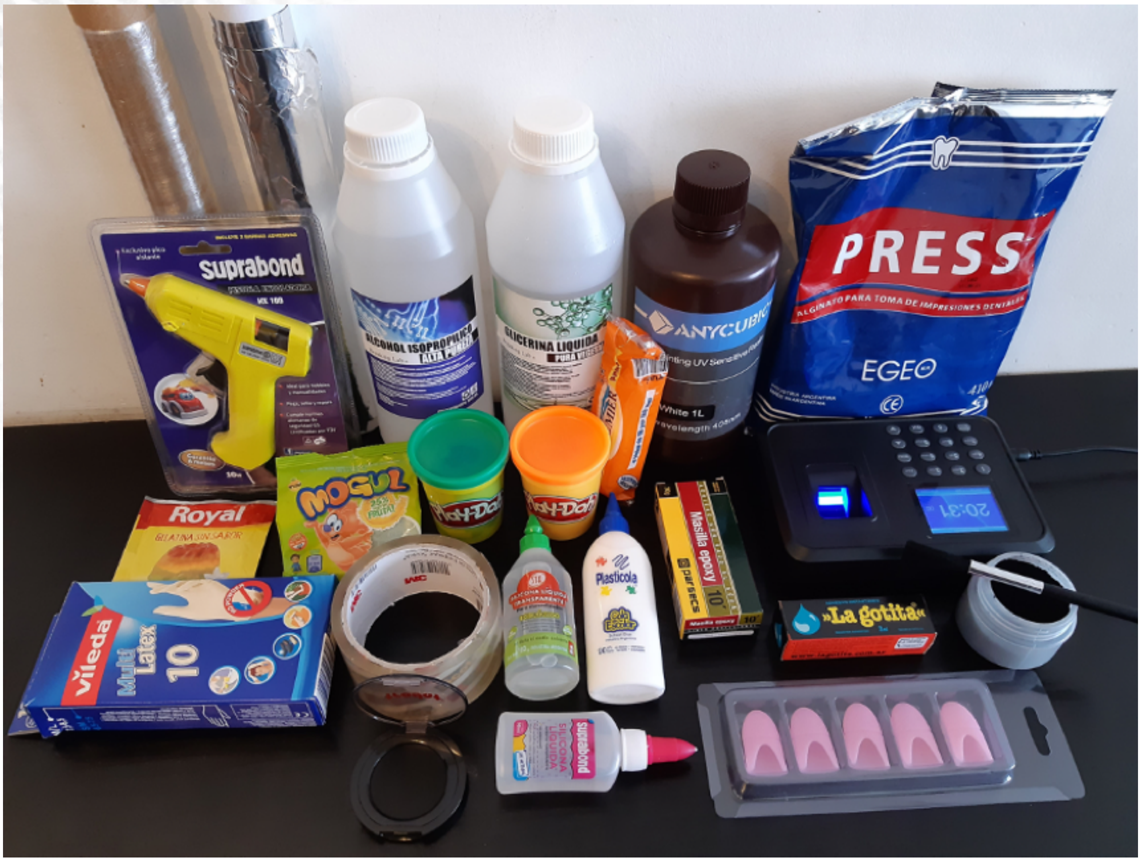


Figure 8 - Materials used for the experiments

FINGERPRINT BIOMETRIC SYSTEMS ATTACKS

Grease Attacks

PRECONDITIONS FOR THE ATTACK

To perform this attack, a requirement is to have a clear grease stain left on the surface of the scanner. This stain must have most of the important characteristics of the fingerprint left on the pad so that the scanner can reliably read the same line-ends and curves that it detected on the previous user.

REQUIREMENTS:

- Fingerprint scanner
- Legitimate user's enrolled fingerprint
- Applicable fingerprint stain on the scanner's pad left by the previous user.
- Temperature between 0-50°C (Scanner operating temperature)
- Gummy bears, silicone fingertips, playdoh, latex gloves, glycerin, paraffin ointment, petrolatum ointment, cocoa butter lip balm

Attack Methods

METHOD 1: MOIST BREATH

The idea behind this scheme is to breathe gently on the surface of the scanner and produce a substance that has enough capacitance to fool the scanner. As the small water particles hit the pad, the grease stain left on the surface does not hold them but the moist gathers up in between the small stained fingerprint lines. This could be enough for the scanner to measure the capacitance and faultily think that there is a finger.

How to perform this attack:

- Gently breathe at about 5 – 10 cm distance onto the surface of the pad.
- Try to control the amount of moist by breathing longer or shorter periods

METHOD 2: GUMMY BEAR

If the breathing does not work, a gummy bear could be used to represent a finger. This jelly candy has nearly the same capacitance as a finger's skin and can be soft enough to be placed evenly on the pad and still retain the stain in form.

How to perform this attack:

- Gently press the gummy bear against the pad. Be careful to do not ruin the stain.
- Try to control the pressure and keep gummy bear evenly flat against the pad.

METHOD 3: SILICONE FINGERTIPS

A silicone fingertip could be used to represent a finger. Silicone can be placed evenly on the pad and still retain the stain.

How to perform this attack:

- Gently press the silicone fingertip against the pad. Be careful to do not ruin the stain.
- Try to control the pressure and keep silicone fingertip evenly flat against the pad.

METHOD 4: LATEX GLOVES

Latex gloves could be used to represent a finger. Latex can be placed evenly on the pad and still retain the stain.

How to perform this attack:

- Gently press your finger wearing a latex glove against the pad. Be careful to do not ruin the stain.
- Try to control the pressure and keep the glove evenly flat against the pad, be careful if the latex glove is powdered because it will ruin the stain.

METHOD 5: PLAYDOH

A bit of playdoh could be used to represent a finger. Playdoh can be soft enough to be placed evenly on the pad and still retain the stain in form.

How to perform this attack:

- Gently press some playdoh against the pad. Be careful to do not ruin the stain.
- Try to control the pressure and keep the playdoh evenly flat against the pad.

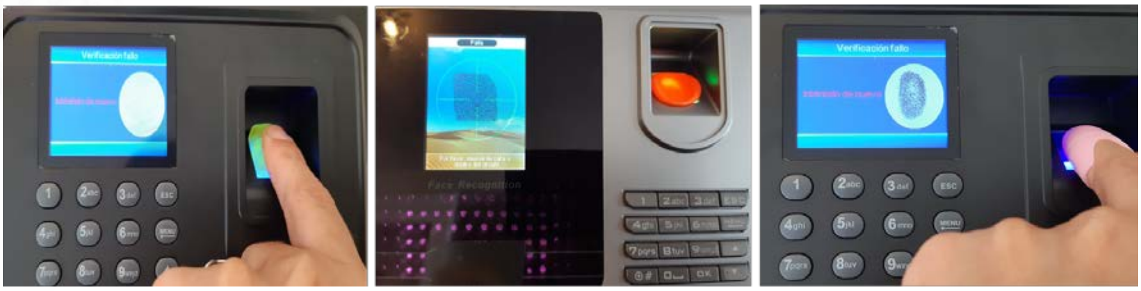
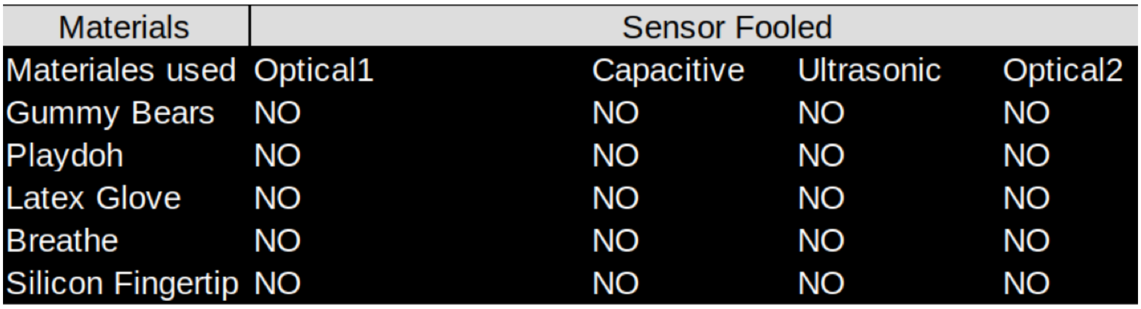


Figure 9 - Experiments with gummy bears, playdoh and silicone fingertips on Hysoon FF395

Grease attack results

With gummy bears, playdoh, latex gloves and silicone fingers, the scanner detected a finger. However, the fingerprint was not clear enough to fool the sensor, resulting in an unsuccessful attack on all the devices we tested.

The results from our experiments have been listed here. The table shows the different materials we used along with which the sensors it fooled:



Materials	Sensor Fooled			
Materiales used	Optical1	Capacitive	Ultrasonic	Optical2
Gummy Bears	NO	NO	NO	NO
Playdoh	NO	NO	NO	NO
Latex Glove	NO	NO	NO	NO
Breathe	NO	NO	NO	NO
Silicon Fingertip	NO	NO	NO	NO

Figure 10 - Grease Attack Results

Due to the results using these known techniques have not been effective, we worked on improving them in order to achieve better results, in the following pages we will talk about the new techniques we have found to bypass these biometric controls.

Enhanced Grease Attacks

As observed, in most grease attack cases, a regular grease stain on the surface of the scanner is not enough to fool the sensor, it is needed to enhance it. We have discovered that it is possible to use other substances to obtain better results impersonating the legitimate users, these substances must be transparent for the user not to notice them and with ointment consistency to better enhance the fingerprint stain. We call this new type of attack “enhanced grease ”.

Attack Methods

METHOD 1: GLYCERIN OR HAND MOISTURIZER

We could use glycerin to enhance the stain and then a silicone fingertip or latex glove to represent a finger.

How to perform this attack:

- Spread a little bit of glycerin or hand moisturizer on the sensor pad.
- Wait for the legitimate user to put the finger in the sensor.
- Gently press your finger wearing a latex glove or a silicone fingertip against the pad.
- Try to control the pressure and keep your finger evenly flat against the pad.

METHOD 2: PETROLATUM OINTMENT

We could use petrolatum ointment to enhance the stain and then a silicone fingertip or latex glove to represent a finger.

How to perform this attack:

- Spread a little bit of petrolatum ointment on the sensor pad.
- Wait for the legitimate user to put the finger in the sensor.
- Gently press your finger wearing a latex glove or a silicone fingertip against the pad.
- Try to control the pressure and keep your finger evenly flat against the pad.

METHOD 3: PARAFFIN OINTMENT

We could use paraffin ointment to enhance the stain and then a silicone fingertip or latex glove to represent a finger.

How to perform this attack:

- Spread a little bit of paraffin ointment on the sensor pad.
- Wait for the legitimate user to put the finger in the sensor.
- Gently press your finger wearing a latex glove or a silicone fingertip against the pad.
- Try to control the pressure and keep your finger evenly flat against the pad.

METHOD 4: COCOA BUTTER LIP BALM

We could use cocoa butter lip balm to enhance the stain and then a silicone fingertip or latex glove to represent a finger.

How to perform this attack:

- Spread a little bit of cocoa butter lip balm on the sensor pad.
- Wait for the legitimate user to put the finger in the sensor.
- Gently press your finger wearing a latex glove or a silicone fingertip against the pad.
- Try to control the pressure and keep your finger evenly flat against the pad.

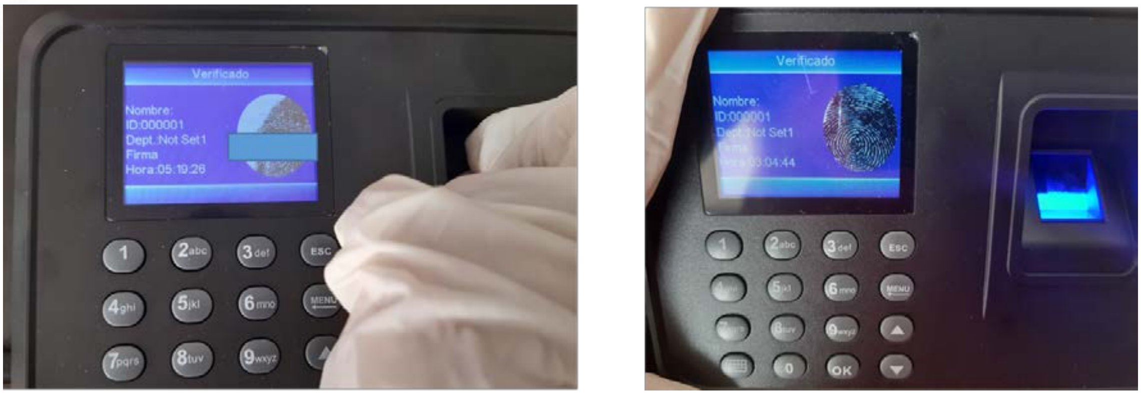
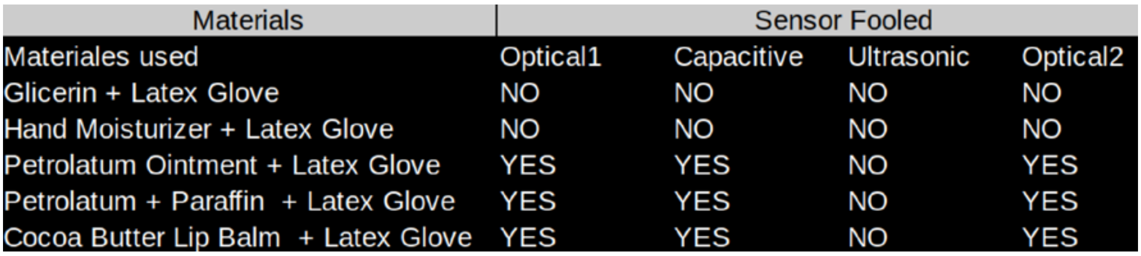


Figure 11 - Enhanced Grease Attacks with Petrolatum ointment and paraffin on TA040

Enhanced grease attack results

Using petrolatum ointment, paraffin or cocoa butter lip balm we successfully fooled the sensors and we were able to authenticate ourselves as the last user of the device, in optical and capacitive scanners, but not on ultrasonic scanners.

The results from our experiments have been listed here. The table shows the different materials we used along with which sensors it fooled:



Materials	Sensor Fooled			
Materiales used	Optical1	Capacitive	Ultrasonic	Optical2
Glicerin + Latex Glove	NO	NO	NO	NO
Hand Moisturizer + Latex Glove	NO	NO	NO	NO
Petrolatum Ointment + Latex Glove	YES	YES	NO	YES
Petrolatum + Paraffin + Latex Glove	YES	YES	NO	YES
Cocoa Butter Lip Balm + Latex Glove	YES	YES	NO	YES

Figure 12 - Enhanced Grease Attacks Results

Protection against Grease and Enhanced Grease Attacks

The best way to prevent this attack is to wipe the scanner after use. It is also recommended to use several fingers in the authentication. Implementing these recommendations will be impossible to use one stain on the scanner to pass two different fingerprint checks.

Modifications to equipment that might help:

- Live finger detection (pulse, sugar level, etc.)
- Small flap or cover over the pad that closes and clears the surface automatically after detection. Or at least scrambles it a bit.

Consensual Attacks

The term consensual suggests the user we are stealing the fingerprint from is aware of the process and actively participates by pressing his finger into a mold. Even though we have classified this approach as "consensual", there are not consensual ways to go about achieving the same. For example, one can make an imprint of a person's finger in their sleep or use social engineering techniques to fool a person into giving away an imprint. There are a multitude of ways to do this, however just a few can be done in such a way that the target does not know about it.

CREATING FINGERS MOLDS

- **Playdoh:** The first experiment performed was using plasticine as a mold. The playdoh was kneaded for a while to make it soft and easy to shape before pushing the finger into it to create the mold. It is needed to press the finger firmly against the playdoh for a few minutes to obtain a good mold.

- **Candle Wax:** The next item we tried to use as a mold was candle wax. We melted all the wax and put a little melted wax on aluminum foil. Then we let it dry for a while and pressed our finger against the wax. When the wax dried, we had a nice mold.

- **Epoxy Putty:** The next mold was made of the two-part epoxy putty type that dries at room temperature when exposed to air. Both parts were mixed according to the instructions, which resulted in an easy-to-form putty, then the putty was kneaded for 2 minutes and finally pressed the finger against it for 1 minute to create the mold. This mold is ready to use after it has dried.

- **Alginate:** The next mold was made of alginate, which is generally used to obtain dental impressions. We combined 20g of alginate with 50ml of water, then we mixed vigorously for 1 minute until a homogeneous paste was obtained. We put a little of this paste on aluminum foil and pressed a finger against it for one and a half minutes to create the mold. It is better to use the alginate molds right away.

- **Hot Glue:** The last mold which was pushed out of a glue gun onto a piece of aluminum foil and cooled down a bit. We dip our finger in water and then pressed it against the hot glue for a few minutes. When the glue had cooled off, it was usable as a mold:

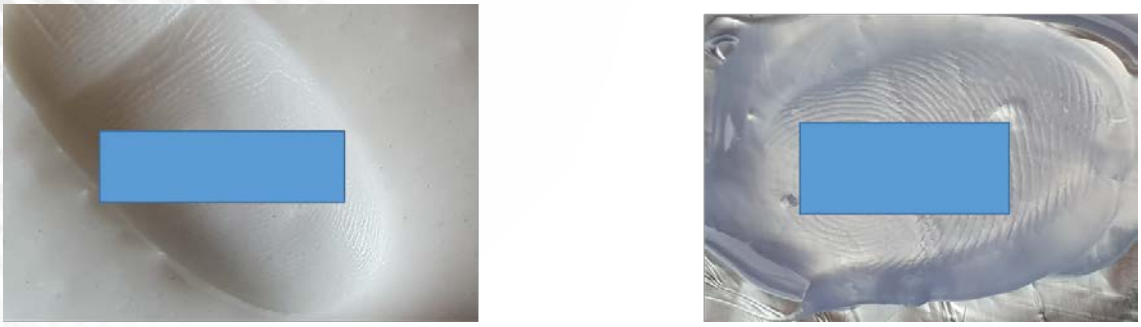


Figure 13 - Molds obtained from alginate and hot glue

CASTING ARTIFICIAL FINGERS

- **Liquid latex:** Liquid latex is a very good material to mold artificial fingers, it produces a light, detailed and flexible fingerprint. To cast the finger, the molds need to be filled with just a few drops of liquid latex. After conducting several experiments, we discovered that thin fake fingers work better than thicker ones. It takes from 10 minutes to one hour to dry depending on the thickness applied. As it dries, it solidifies to a rubbery consistency. To peel the fake fingerprint from the mold is recommended to use tweezers.

- **Silicone:** Silicone rubber is an ideal material for molding artificial fingers. As with liquid latex, it produces a light, flexible and detailed fingerprint, but has the added benefits of a longer life, resistance to chemicals and decomposition. To cast the finger we added the catalyst and mixed the catalyst together with the silicone for 3 minutes stirring continuously. Then, we let the mixture rest for 2 minutes and finally we filled the different molds. Once the silicone rubber is ready, you have 20 minutes of "work time" available before it starts to cure.

- **Ballistic Gelatin:** Gelatin powder needs to be mixed with water and glycerin to become a substance desirable in this kind of experiments. The thickness of this substance will vary with the ratio between gelatin and water. The original recipe for ballistic gelatin involves adding one tablespoon of unflavored gelatin powder to every 100 ml of water, adding a few drops of glycerin, heating, removing lumps until the gelatin powder dissolves, and then allowing the gelatin to cool in the molds. This recipe did not work properly, so we also tried other recipes with less water to compare the results: at first we tried with just one tablespoon of water and one tablespoon of gelatin powder without glycerin, but the recipe closest to the consistency we were looking for is the one that involved adding a tablespoon of gelatin, a tablespoon of glycerin and a tablespoon and a half of water, heating making sure that all the gelatin powder dissolves and then let the gelatin cool. Once the gelatin has cooled to a thick gel, melt it in the microwave, then let it cool to a gel again. Microwave repeatedly until the gelatin has no bubbles, and when a drop acts thick and rubbery. Once the gelatin is rubbery and bubble-free, melt it one final time, then pour the hot, liquid gelatin into the fingerprint mold, and put the mold into the freezer. Within a few minutes, the gelatin should harden into a solid, rubbery substance. Peel the gelatin carefully off the mold.

- **Synthetic Resin:** To cast the finger the molds were filled with just a few drops of synthetic resin. After conducting several experiments, it was deducted that thin fake fingers work better than thicker ones. It could take from 10 minutes to one hour to dry depending on the thickness applied. As it dries, it solidifies to a rubbery consistency.

- **Wood glue:** Wood glue produces a light and very detailed fingerprint. The molds were filled with just a little wood glue to cast the finger. After conducting several experiments, it was deducted that thin fake fingers work better than thicker ones as well. It takes from 20 minutes to several hours to dry depending on the thickness applied. To peel the fake fingerprint from the mold, we recommend using tweezers.

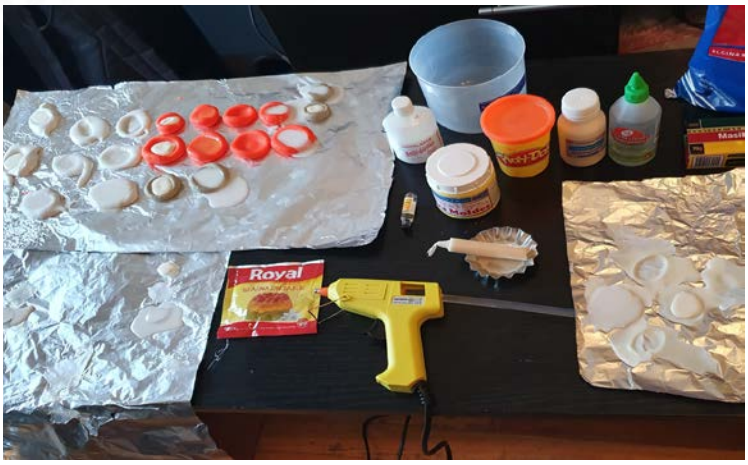


Figure 14 - Materials used for molds and casting

Results

For the molds, we obtained the best results with alginate and hot glue and for the casting we obtained the best results with liquid latex, wood glue and silicone. With the combination of a hot glue mold and wood glue casting we were able to fool all the sensors, the same with the combination of an alginate mold and liquid latex casting. Ballistic gelatin is not so easy to make at home, we tried several combinations of gelatin powder, water and glycerin, but the results were not enough to fool the scanners. Note that the working fingerprints are very thin, and, in some cases, we had to breathe on the fake fingerprint for the capacitive scanner to recognize it.

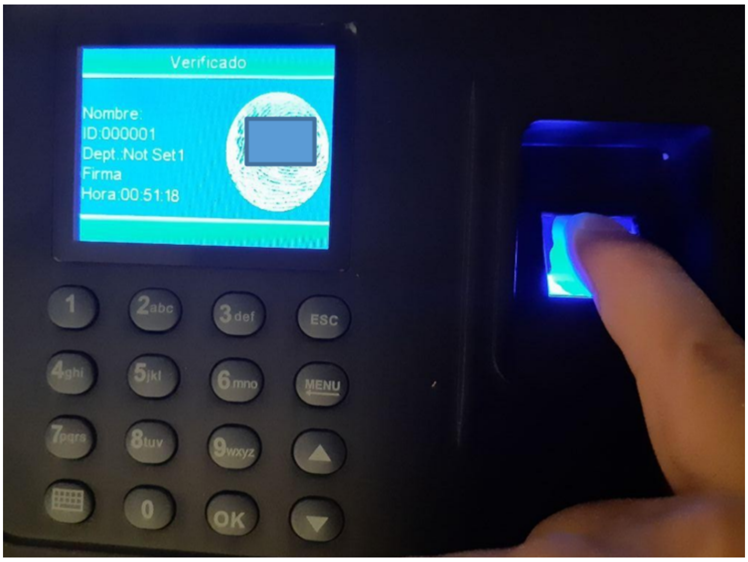
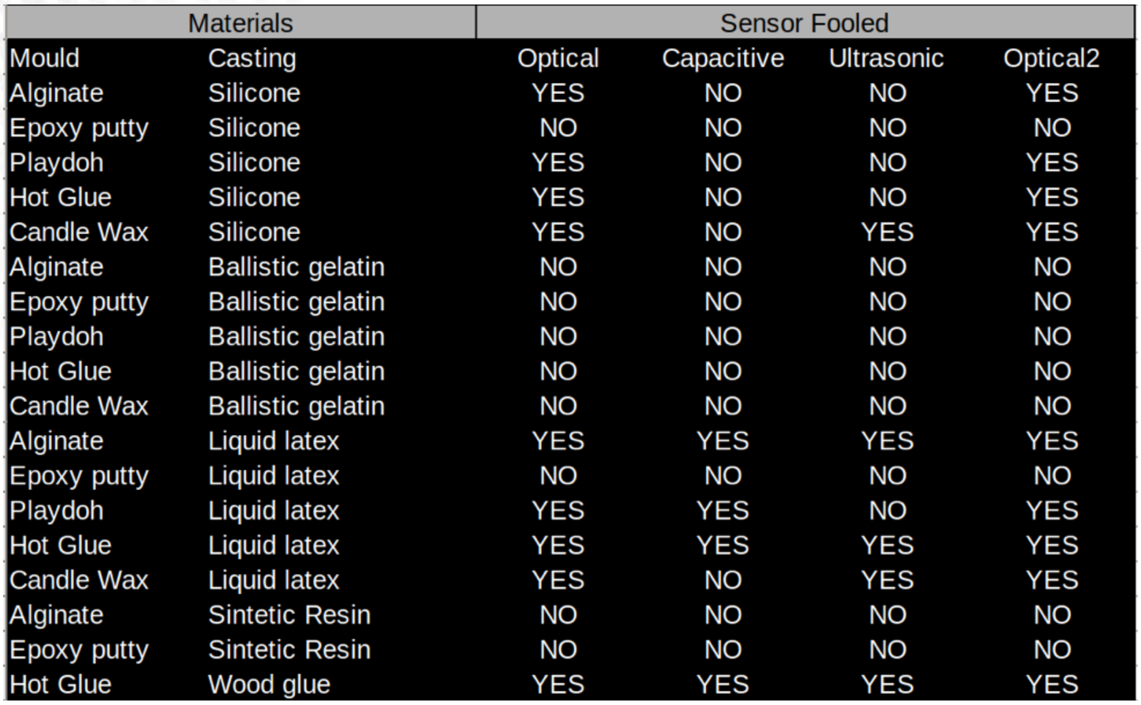


Figure 15 - Working fingerprint made of liquid latex from alginate mold in use

The results from our consensual experiments have been listed here. The table shows the different combinations of molds and castings we used along with which sensors it fooled:



Materials		Sensor Fooled			
Mould	Casting	Optical	Capacitive	Ultrasonic	Optical2
Alginate	Silicone	YES	NO	NO	YES
Epoxy putty	Silicone	NO	NO	NO	NO
Playdoh	Silicone	YES	NO	NO	YES
Hot Glue	Silicone	YES	NO	NO	YES
Candle Wax	Silicone	YES	NO	YES	YES
Alginate	Ballistic gelatin	NO	NO	NO	NO
Epoxy putty	Ballistic gelatin	NO	NO	NO	NO
Playdoh	Ballistic gelatin	NO	NO	NO	NO
Hot Glue	Ballistic gelatin	NO	NO	NO	NO
Candle Wax	Ballistic gelatin	NO	NO	NO	NO
Alginate	Liquid latex	YES	YES	YES	YES
Epoxy putty	Liquid latex	NO	NO	NO	NO
Playdoh	Liquid latex	YES	YES	NO	YES
Hot Glue	Liquid latex	YES	YES	YES	YES
Candle Wax	Liquid latex	YES	NO	YES	YES
Alginate	Sintetic Resin	NO	NO	NO	NO
Epoxy putty	Sintetic Resin	NO	NO	NO	NO
Hot Glue	Wood glue	YES	YES	YES	YES

Unconsensual Attacks

In these attacks the user does not participate actively, and latent fingerprints are obtained in a non-cooperative way. The procedure from the discovery of a latent fingerprint to having an artificial recreation of the fingerprint is not trivial. First and foremost, there is a problem identifying the correct finger. Lifting a latent fingerprint from a finger not included in a fingerprint recognition process will end being a wasted effort. Assuming the correct latent fingerprint has been identified, various methods for obtaining it were presented, which have already been tested through experimentation. The following steps are recommended:

1. Enhance the latent fingerprint with glue fumes or fingerprint powder: The fingerprint will have to be enhanced in some way so that it can be lifted.
2. Lift the latent fingerprint with a digital camera or transparent tape: After enhancement, the fingerprint must in some way be transferred to a different, but fitting, medium from which it was discovered and enhanced.
3. Digitally enhance the fingerprint with software: After having lifted and digitized the fingerprint, it needs to be digitally enhanced, so that acceptable molds can be made from the digitized fingerprint.
4. Create a mold: Create a usable mold, preferably over a long period of time.
5. Cast artificial fingers with silicone, liquid latex or wood glue: Final step is to make an artificial finger with silicone rubber, liquid latex or wood glue.

MATERIALS NEEDED:

- Ethylcyanoacrylate Glue
- Fingerprint Powder and brush
- Digital Camera with macro functionality
- Transparent Tape
- Fingerprint Ink Pad
- Transparency
- Plastic wrap
- Latex glove
- Silicone Rubber
- Liquid Latex
- Wood glue
- Paper

Latent Fingerprint Enhancement

Fingerprint Powders: Fingerprint powders are fine powders used in dusting for fingerprints by crime scene investigators and others in law enforcement. The process of dusting for fingerprints involves various methods intended to get the particles of the powder to adhere to residue left by friction ridge skin on the fingers. Powders may be applied with a fingerprint brush, a brush with extremely fine fibers designed to hold powder, and deposit it gently on the fingerprint to be revealed, without rubbing away the delicate residue of the fingerprint itself.

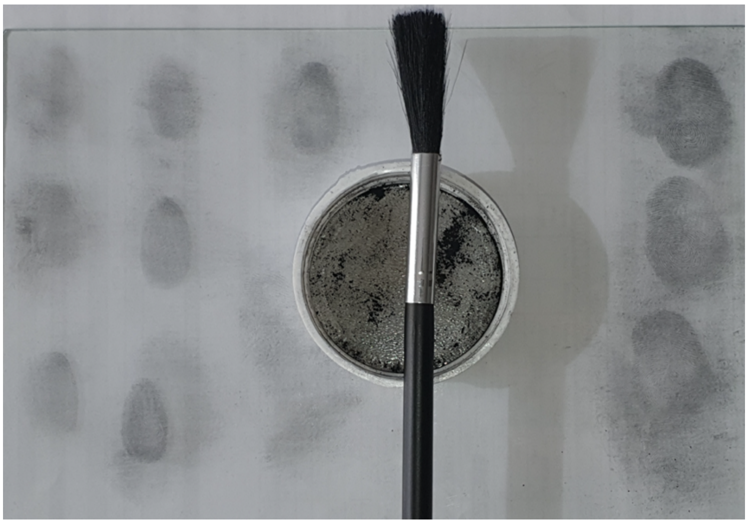


Figure 16 - Dusting fingerprints with fingerprint brush and powder

Ethylcyanoacrylate Fumes: By encapsulating the latent print with a container containing instant glue, the working agent in the glue (ethylcyanoacrylate) will evaporate, fumes from the glue will be attached to the ridges of the latent fingerprint, making possible to lift it.

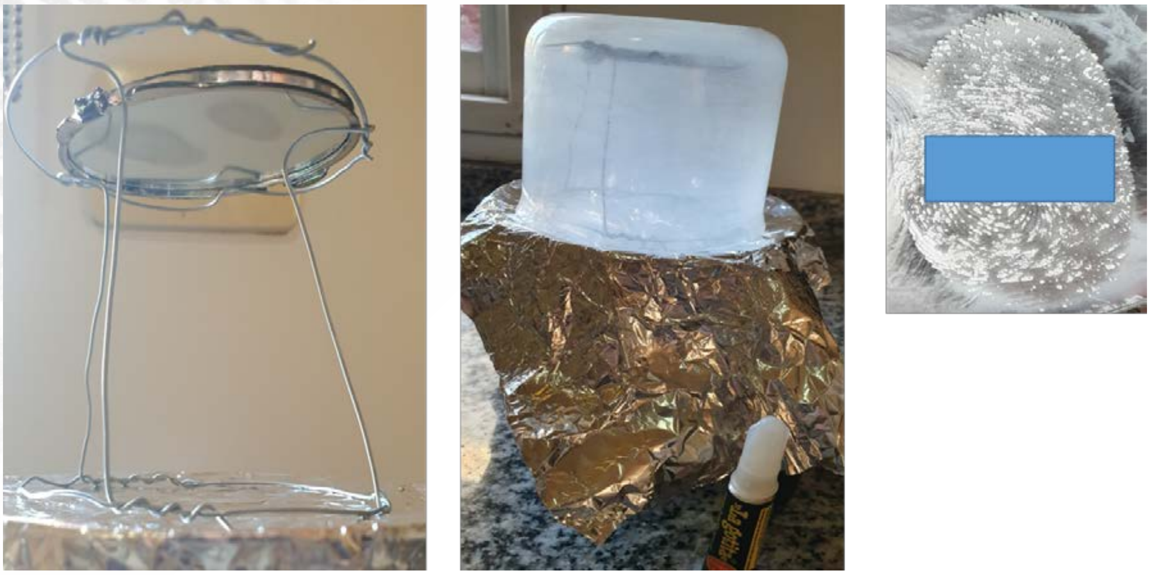


Figure 17 - Ethylcyanoacrylate fuming chamber construction, use and results obtained

Lifting a Latent Fingerprint

Digital Camera: The first method of fingerprint digitizing we tried was using the digital photo camera from the Samsung Galaxy S10 smartphone, which was able to take images up to 12 mega pixels in size. It was important to be able to get close enough to the fingerprint while getting a clear shot. The camera had nice macro functionality which made it possible to get good, in-focus images of close objects.

Transparent Tape: This method will only work on dusted fingerprints. By using a broad transparent tape, we are able to lift the laser toner powder which had stuck to the latent fingerprint. Having the powder fastened to the tape, we then transferred it to a white sheet of paper by simply attaching the transparent tape onto it. Having the latent fingerprint now transferred to a white sheet of paper enables us to easily digitize it by taking a photo with the digital camera or using a scanner. Transparent tape was also tested with the latent fingerprint itself on the different devices, with the objective of impersonating the legitimate user.

DIGITALLY ENHANCING THE FINGERPRINT

We planned to use https://github.com/Utkarsh-Deshmukh/Fingerprint-Enhancement-Python, as a base for digitally enhancing the fingerprint using oriented gabor filters in Python, but the tool didn't work so we had to adapt it to make it functional. The new functional version is on my public github account: https://github.com/ylevalle/Fingerprint-Enhancement-Python.

CREATING A MOLD FOR FINGERPRINT REPRODUCTION

Transparencies: One way to create a mold is to use a transparency, in which the enhanced digitized fingerprint is printed upon with a laser printer. When printing, care must be taken so that the printed fingerprint is roughly the same size of the real-life fingerprint. The resolution of the printer is also an important aspect. When the fingerprint is printed on the transparency, the laser toner powder which is burnt onto the transparency will create an impression some micrometers high. This enables us to use it as a mold.

Offset Plate: The offset printing plates used in offset printing are thin -up to about 0.3 mm- and they mostly have a mono-metal aluminum or sometimes multi-metal. The fingerprints in the offset printing plate used to print the transparency have some micrometers high and could be used as a mold.

Fingerprint Ink: Other techniques involve using fingerprint ink on different materials such as paper, plastic wrap and latex gloves to impersonate the legitimate user.

CASTING ARTIFICIAL FINGERS

- Liquid latex: we applied a few drops of liquid latex to the transparency and offset plate molds.
- Silicone: we applied a very thin layer of silicone, prepared as we explained in previous sections on this paper, to the transparency and offset plate molds.
- Wood glue: we applied a very thin layer of wood glue to the transparency and offset plate molds.

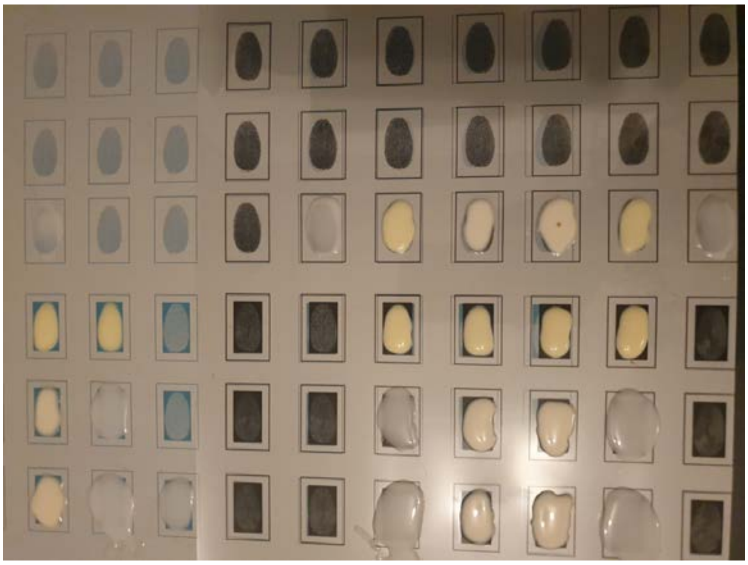


Figure 18 - Casting the transparency and offset plate with liquid latex, silicone and wood glue

RESULTS

The best results were obtained lifting the latent fingerprint with a digital camera, using an oriented Gabor filter implementation in python to digitally enhance the fingerprint image, offset printing a transparency, using the transparency as a mold and casting it with liquid latex. With this procedure optical sensors were easily fooled. The fingerprint ink on a latex glove technique also worked on capacitive and ultrasonic sensors.

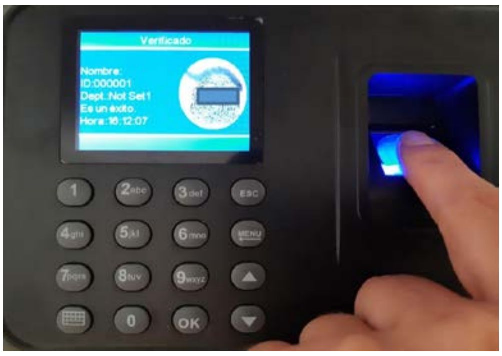
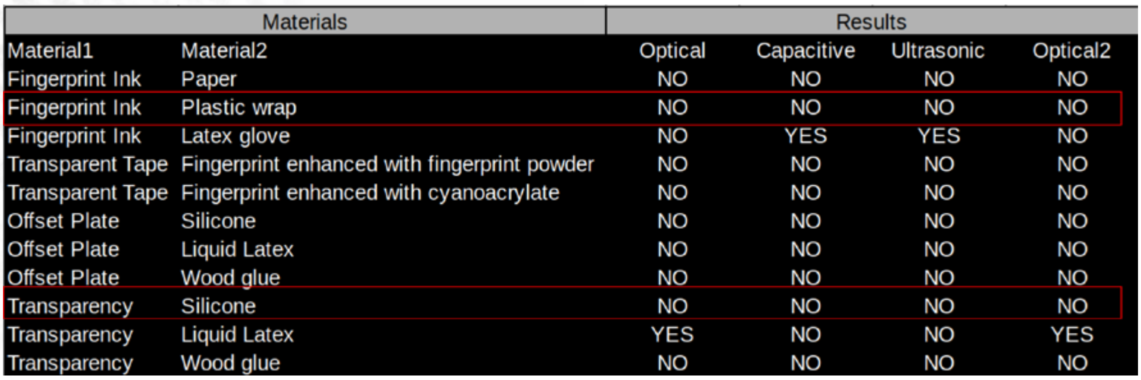


Figure 19 - Working fingerprint made of liquid latex from the transparency in use

The results from our unconsensual experiments have been listed here. The table shows the different combinations of molds and castings we used along with which sensors it fooled:



Materials		Results			
Material1	Material2	Optical	Capacitive	Ultrasonic	Optical2
Fingerprint Ink	Paper	NO	NO	NO	NO
Fingerprint Ink	Plastic wrap	NO	NO	NO	NO
Fingerprint Ink	Latex glove	NO	YES	YES	NO
Transparent Tape	Fingerprint enhanced with fingerprint powder	NO	NO	NO	NO
Transparent Tape	Fingerprint enhanced with cyanoacrylate	NO	NO	NO	NO
Offset Plate	Silicone	NO	NO	NO	NO
Offset Plate	Liquid Latex	NO	NO	NO	NO
Offset Plate	Wood glue	NO	NO	NO	NO
Transparency	Silicone	NO	NO	NO	NO
Transparency	Liquid Latex	YES	NO	NO	YES
Transparency	Wood glue	NO	NO	NO	NO

Figure 20 - Unconsensual attacks results

Unconsensual Attacks with 3D Printing

To obtain a working fingerprint through 3D printing, we need to follow these steps:

1. Lift the latent fingerprint with a digital camera with macro functionality: We used the digital photo camera from the Samsung Galaxy S10 smartphone, which was able to take images up to 12 mega pixels in size to obtain a photo of a latent fingerprint on glass or a fingerprint inked on paper. It was important to be able to get close enough to the fingerprint while getting a clear shot. The camera had nice macro functionality which made it possible to get good, in-focus images of close objects.

2. Use a tool based on https://github.com/Utkarsh-Deshmukh/Fingerprint-Enhancement-Python, , for digitally enhancing fingerprints using oriented Gabor filters in Python, the tool is shared in my public GitHub account: https://github.com/ylevalle/Fingerprint-Enhancement-Python.

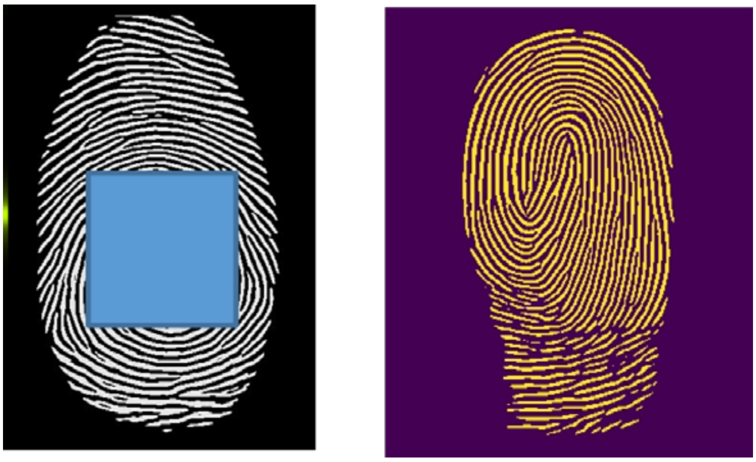


Figure 21 - Enhanced fingerprint results using the fingerprint enhancement tool

3. Convert the enhanced.JPG file to an SVG (Scalable Vector Graphics file) with a free online tool like https://convertio.co/ar/jpg-svg/, import the SVG file into Tinkercad https://www.tinkercad.com or another 3D CAD design software to create a 3D model of the fingerprint. Configure the fingerprint length and width according to the measures of the original latent fingerprint, put a thin back block with 0.5 mm height or more behind the fingerprint, configure the ridge height and create two different 3D models: one negative or hollow for casting and one positive for direct tests. Human papillary ridges, in general have a height between 59.0 +/- 19.2 micrometers, that is between 0.00398 cm and 0.00782 cm.

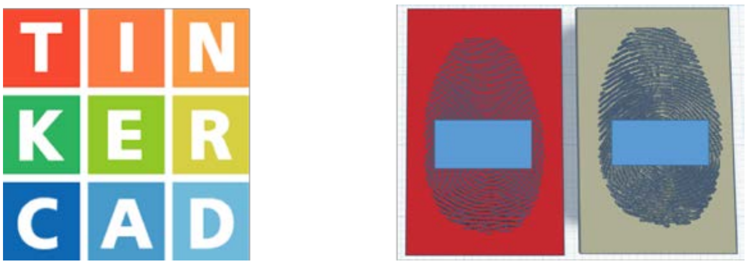


Figure 22 - Tinkercad logo and 3D models of the fingerprint

4. Export the 3D model file in a 3D printable file format (STL) and upload it on the Anycubic Photon 3D DLP / SLA printer. You need to configure the printer settings according to the UV resin that you are going to use, as it is explained in the following pdf https://dwn.alza.cz/files/infolist/5593793/anycubic_resin_settings.pdf. We printed the models in different positions and orientations, it took us 6 retries to achieve the optimal printer settings and ridge height.

Figure 23 - Anycubic Photon 3D Printer and Resin

5. Once the printing is completed, the 3D printed molds require rinsing in Isopropyl alcohol (IPA) to remove any uncured resin from their surface. After rinsed parts dry, the molds require post-curing using an UV-post curing lamp or direct sunlight, which helps parts to reach their highest possible strength and stability.

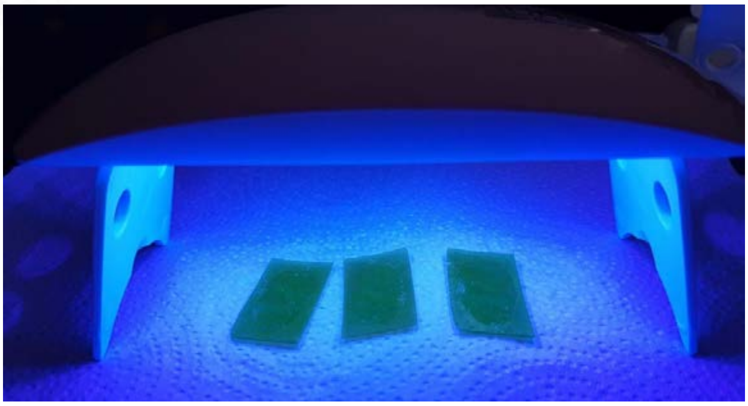


Figure 24 - UV Post Curing Lamp

6. Fill the 3D printed negative or hollow molds with:

   a. **Liquid latex:** To cast the finger we filled the 3D printed molds with just a few drops of liquid latex, in our experience, thin fake fingers work better than thicker ones. It takes from 10 minutes to one hour to dry depending on the thickness applied, but it is best to leave it on longer just to be sure. As it dries, it solidifies to a rubbery consistency.

   b. **Wood glue:** To cast the finger we filled the 3D printed molds with just a little wood glue. It takes from 20 minutes to several hours to dry depending on the thickness applied, but it is best to leave it on longer just to be sure.

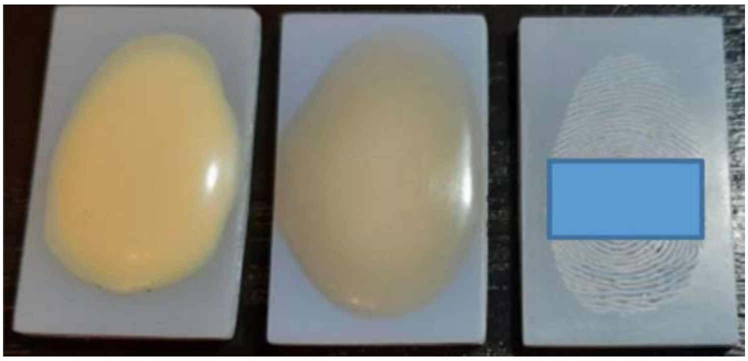


Figure 25 - Casting the 3D printed molds with liquid latex and wood glue

RESULTS

The fingerprint obtained from the 3D mold with liquid latex or wood glue casting worked on all sensors, and the positive fingerprint printed directly on UV resin worked on the ultrasonic sensor and in one of the optical sensors. In the optical sensor we had to spread the fingerprint with cocoa butter lip balm or petrolatum for the sensor to recognize it.

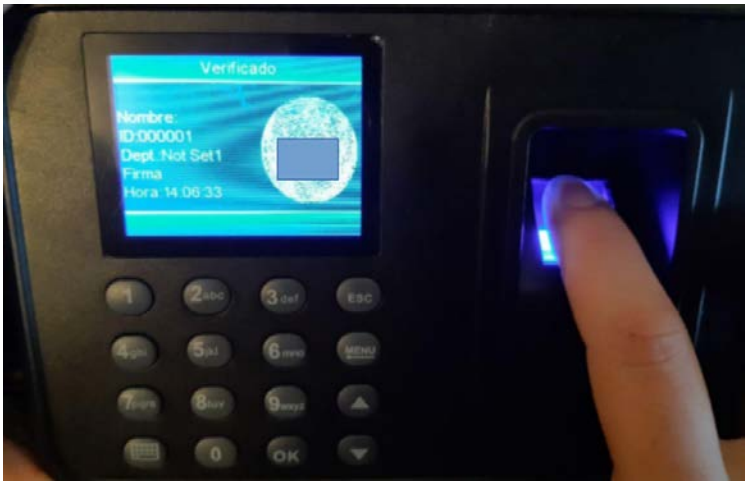
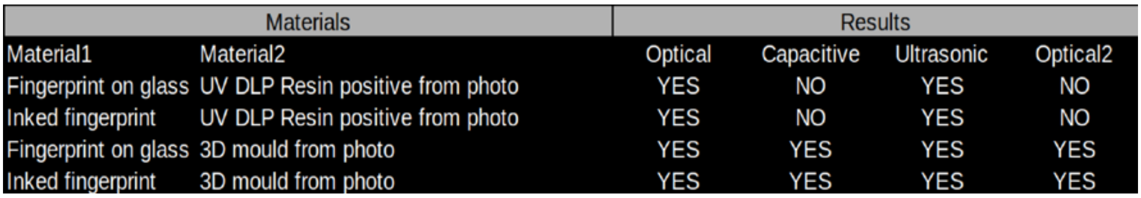
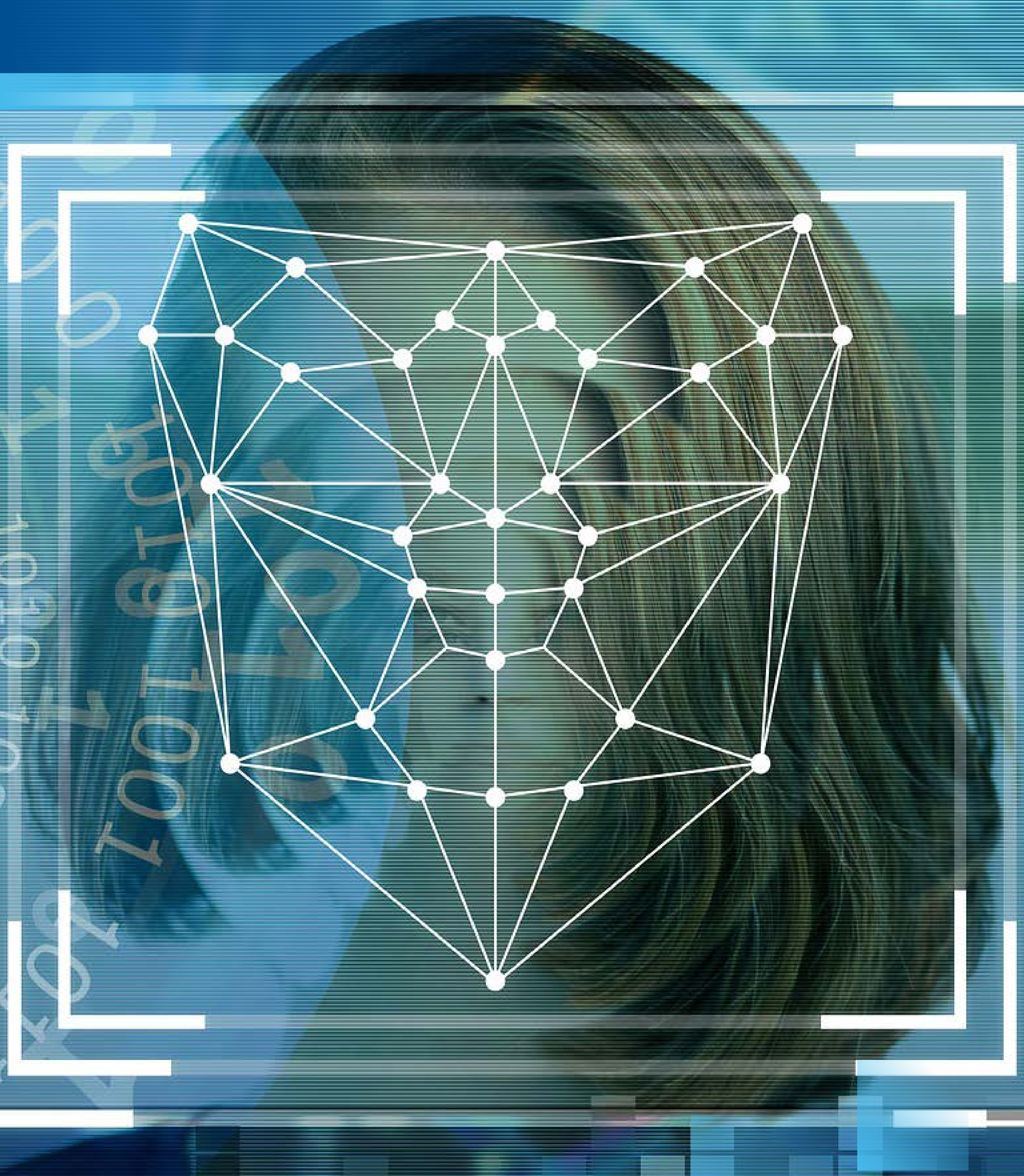


Figure 26 - Working fingerprint made of liquid latex from the 3D mold in use

The results from our not consensual experiments with 3D printing have been listed here. The table shows the different combinations of molds and castings we used along with which sensors it fooled:



Materials		Results			
Material1	Material2	Optical	Capacitive	Ultrasonic	Optical2
Fingerprint on glass	UV DLP Resin positive from photo	YES	NO	YES	NO
Inked fingerprint	UV DLP Resin positive from photo	YES	NO	YES	NO
Fingerprint on glass	3D mould from photo	YES	YES	YES	YES
Inked fingerprint	3D mould from photo	YES	YES	YES	YES



The goal of a presentation attack in facial recognition systems is to fool the system by presenting a facial biometric artifact.

FACIAL RECOGNITION SYSTEMS

Biometric Face Recognition is the process and ability to identify and recognize the face of an individual, either to grant access to a secure system or to find out the details of a person by matching the face with the data in a biometric database. Generic face recognition systems comprise three major modules: face detection and alignment, visual feature extraction, and face recognition. What the biometric face reader does is map and extract the features of a person's face that can be used for recognition and stores the data in a biometric database along with the identity of a certain individual.

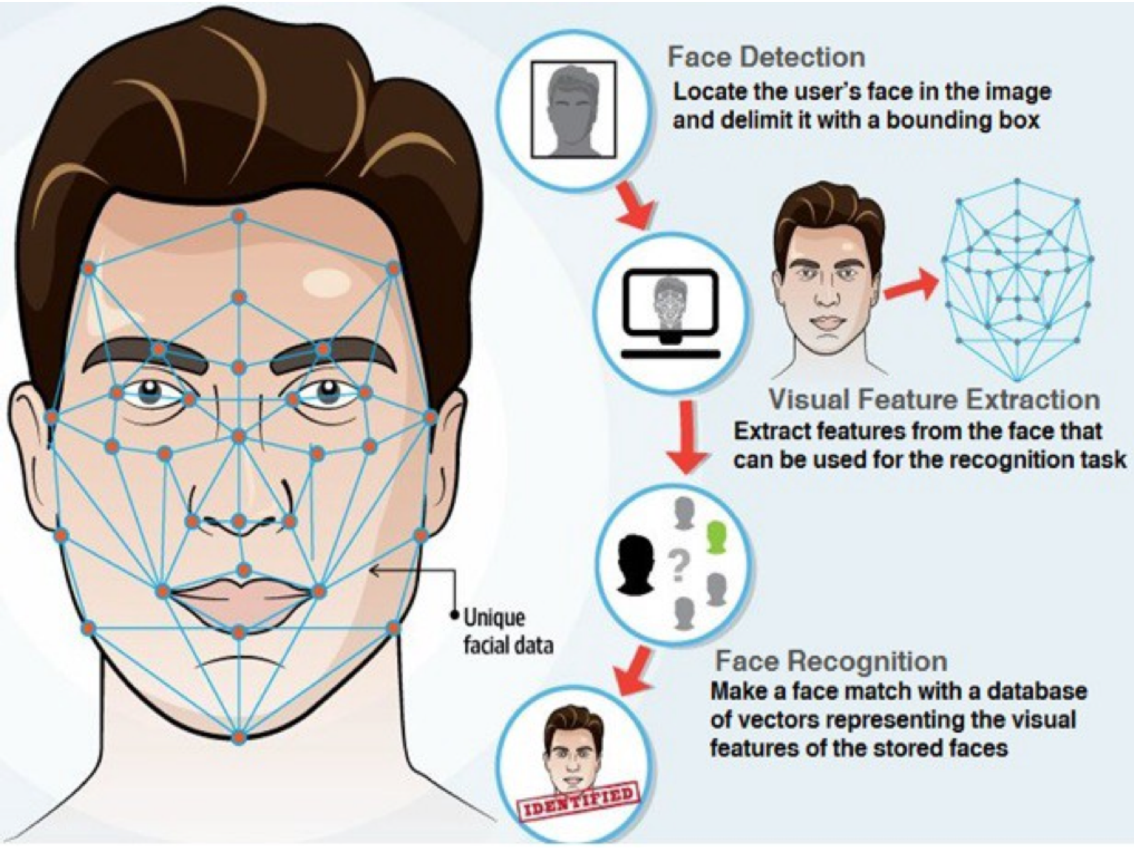

Face Detection
Locate the user's face in the image and delimit it with a bounding box
Visual Feature Extraction
Extract features from the face that can be used for the recognition task
Face Recognition
Make a face match with a database of vectors representing the visual features of the stored faces
Unique facial data
IDENTIFIED

Figure 27 - Facial recognition process
https://medium.com/adalab/facial-recognition-system-5642f57c220a

FACIAL RECOGNITION SYSTEMS ATTACKS

The goal of a presentation attack in facial recognition systems is to fool the system by presenting a facial biometric artifact.

Printed or Displayed Photo

Popular face biometric artifacts include a printed photo, the electronic display of a facial photo and replaying a video using an electronic display.

- **Printed or Displayed Photo:** The attacker uses someone's photo. The image is printed or displayed on a digital device. This is the most common type of attack since most people have facial pictures available on the internet or photos could be obtained without any permission.

Printed photo attacks exhibit reduced image texture, mechanical artifacts like horizontal lines, no facial motion (like eye blinks) and borders of the image may be visible. To overcome the facial motion limitations, there are other attacks that allow the attacker to simulate eye blink or facial motion:

- **Eye-cut photo attack:** Eye regions of a printed photo are cut off to exhibit blink behavior of the impostor.
- **Warped photo attack:** Consist in bending a printed photo in any direction to simulate facial motion.

Electronic display of facial photos attacks exhibits blurred image texture, moiré effect (artifact of images produced by various digital imaging and computer graphics techniques) and reduced color diversity.

Video Replay

A more sophisticated way to trick the system, which usually requires a looped video of a victim's face. This approach ensures behavior and facial movements to look more 'natural' compared to holding someone's photo. This type has physiological signs of life that are not presented in photos, such as eye blinking, facial expressions, and movements in the head and mouth, and it can be easily performed using tablets or large smartphones.

Video replay attacks exhibit blurred image texture, moiré effect (artifact of images produced by various digital imaging and computer graphics techniques) and reduced color diversity.

3D Masks

Other popular face biometric artifacts are 3D masks, these masks can be rigid or silicone, with or without eye holes, generic or custom made.

- **A rigid 3D mask attack:** exhibits vivid colors, no facial motion (no lips or eye movement) and no texture in NIR (near infrared reflectance). These masks cost about USD $300.

- **A 3D silicone mask attack:** exhibits skin-like appearance and reflection, facial motion, thermal imaging and texture in NIR, these artifacts are difficult to detect for a facial recognition system. A generic silicone mask cost about 600 dollars and custom-made 3D silicone masks costs around 3000 dollars.

Other attacks

Another attack to facial recognition systems includes makeup. This type of attack exhibits: skin-like appearance and reflection, facial motion, thermal imaging and texture in NIR.

Another novel attack on facial recognition systems is **“X-glasses”** . Researchers last year discovered that the abstraction of the eye for liveness detection in FaceID renders a black area (the eye) with a white point on it (the iris). And then, they discovered that if a user is wearing glasses the system will not extract 3D information from the eye area. Putting these two factors together, researchers created a prototype of glasses, dubbed “X-glasses”, with black tape on the lenses, and white tape inside the black tape. Using this trick, they were able to unlock a victim’s mobile phone by placing the tape-attached glasses above the sleeping victim’s face to bypass the liveness detection mechanism of FaceID.

In the attack called **morphed face**, morphing techniques are used to create artificial biometric samples, which resemble the biometric information of two (or more) individuals in image and feature domain. If morphed biometric images are infiltrated to a biometric recognition system, for example during the issuance process of an electronic passport, the subjects contributing to the morphed image will be successfully verified against that single enrolled template.

PRESENTATION ATTACKS DETECTION

The most used techniques for detecting presentation attacks in facial recognition systems are the use of eye blinking or motion challenges. Other techniques that could be used to detect presentation attacks instruments in such systems are texture analysis, frequency analysis, image quality analysis, thermal imaging analysis and active flash.

For presentation attacks detection on fingerprint systems you need to analyze the degree of sharpness, color and luminance levels of the sample, entropy, structural distortions, local artifacts, light absorbance, material elasticity and moisture content.

REFERENCES AND PREVIOUS WORK

- https://i.blackhat.com/USA-19/Wednesday/us-19-Chen-Biometric-Authentication-Under-Threat-Liveness-Detection-Hacking.pdf
- https://www.blackhat.com/presentations/bh-dc-09/Nguyen/BlackHat-DC-09-Nguyen-Face-not-your-password-slides.pdf
- https://pdfs.semanticscholar.org/4de8/6f7d8e5d7461d17e6995a5e3fc6b957b3c26.pdf
- https://pdfs.semanticscholar.org/952b/f27a58efd761a252bedd0b1d15aaa41cddeb.pdf
- https://www.idiap.ch/~marcel/lectures/lectures/marcel-tutorial-tabularasa-icb2015.pdf
- https://project.inria.fr/wifs2017/files/2017/12/tutorial-biometric-spoofing-WIFS-2017-part1-reduce.pdf
- https://project.inria.fr/wifs2017/files/2017/12/tutorial-biometric-spoofing-WIFS-2017-part2-reduce.pdf
- https://www.synaptics.com/sites/default/files/sentrypoint-anti-spoofing-wp.pdf
- https://www.researchgate.net/publication/330035636_Fingerprint_Presentation_Attack_Detection_Generalization_and_Efficiency
- http://biometrics.cse.msu.edu/Publications/Fingerprint/CaoJain_HackingMobilePhonesUsing2DPrintedFingerprint_MSU-CSE-16-2.pdf
- https://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid
- https://www.ccc.de/en/updates/2017/iriden
- https://www.researchgate.net/publication/260974477_Image_Quality_Assessment_for_Fake_Biometric_Detection_Application_to_Iris_Fingerprint_and_Face_Recognition
- https://www.researchgate.net/publication/308795497_The_Replay-Mobile_Face_Presentation-Attack_Database
- https://www.researchgate.net/publication/262605045_Spoofing_Face_Recognition_With_3D_Masks
- https://www.researchgate.net/publication/320177829_What_You_Can’t_See_Can_Help_You_-_Extended-Range_Imaging_for_3D-Mask_Presentation_Attack_Detection
- https://www.researchgate.net/publication/316681277_Analysis_of_Fingerprint_Image_Enhancement_Using_Gabor_Filtering_With_Different_Orientation_Field_Values/link/5a2009abaca272088b23f65b/download
- https://arxiv.org/pdf/1909.08848.pdf

Secure. Today and Tomorrow.

Over the last 20 years, Dreamlab Technologies has established itself as both a pioneer and a source of constant innovation within the cybersecurity landscape.

DREAMLAB
TECHNOLOGIES

DREAMLAB SWITZERLAND

Dreamlab Technologies AG
Monbijoustrasse 36
CH – 3011 Bern

contact@dreamlab.net
dreamlab.net

DREAMLAB CHILE

Dreamlab Technologies Chile
Villavicencio 361
Oficina 113
CLE – 8320154
Santiago de Chile

DREAMLAB BOLIVIA

Dreamlab Technologies Bolivia
c/o Cetus Group
Av. 20 de Octubre 402
Edificio Torre Zafiro Piso 2
BOL – 3520 La Paz

DREAMLAB PERU

Dreamlab Technologies Peru
Av. Salaverry 3240
Piso 4
San Isidro, Lima 27

DREAMLAB GERMANY

Dreamlab Technologies Germany
c/o KDAB
Reuchlinstraße 10 -11
DE – 10553 Berlin

DREAMLAB OMAN

Dreamlab Technologies Oman
Tosca Business Center
2nd Floor, Office No. 233
P.O. Box 55
OM – 133, Al Khuwair

DREAMLAB MALAYSIA

Dreamlab Technologies Malaysia
Level 29-01, Tower A,
Vertical Business Suite
Bangsar Sourth, Jalan Kerinchi
MY – 59200 Kuala Lumpur