

BYPASSING BIOMETRIC SYSTEMS WITH 3D PRINTING

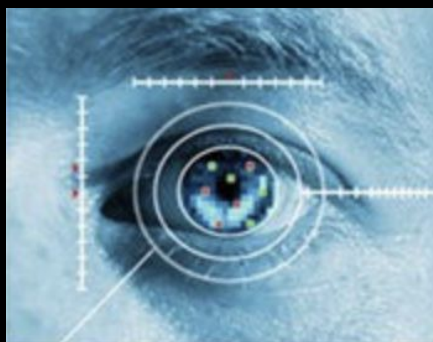


Yamila Levalle @ylevalle





WHAT IS A BIOMETRIC SYSTEM?



Physical Traits:

- Iris
- Fingerprint
- Ear Shape
- DNA
- Face
- Vein Pattern

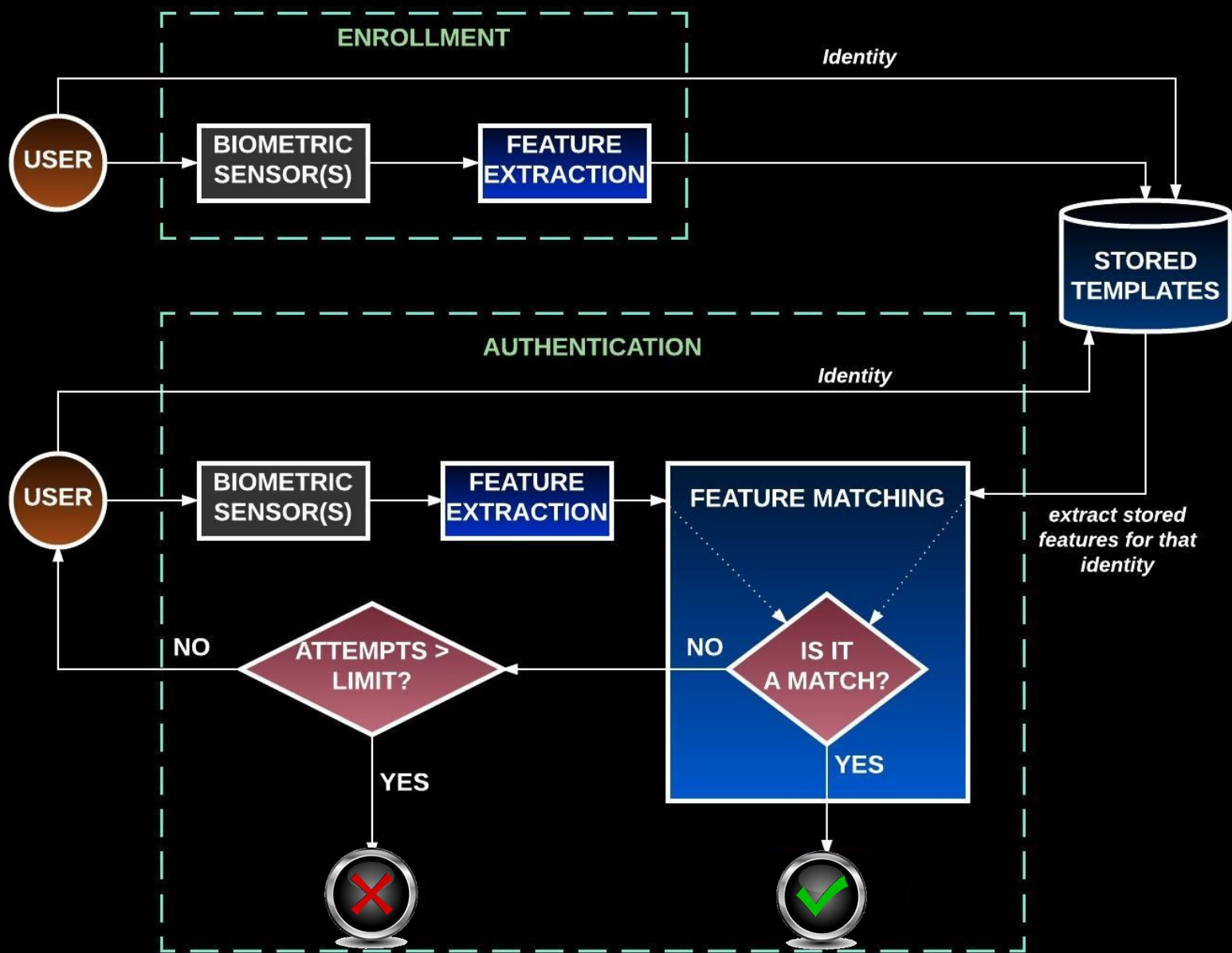
Behavioural Traits:

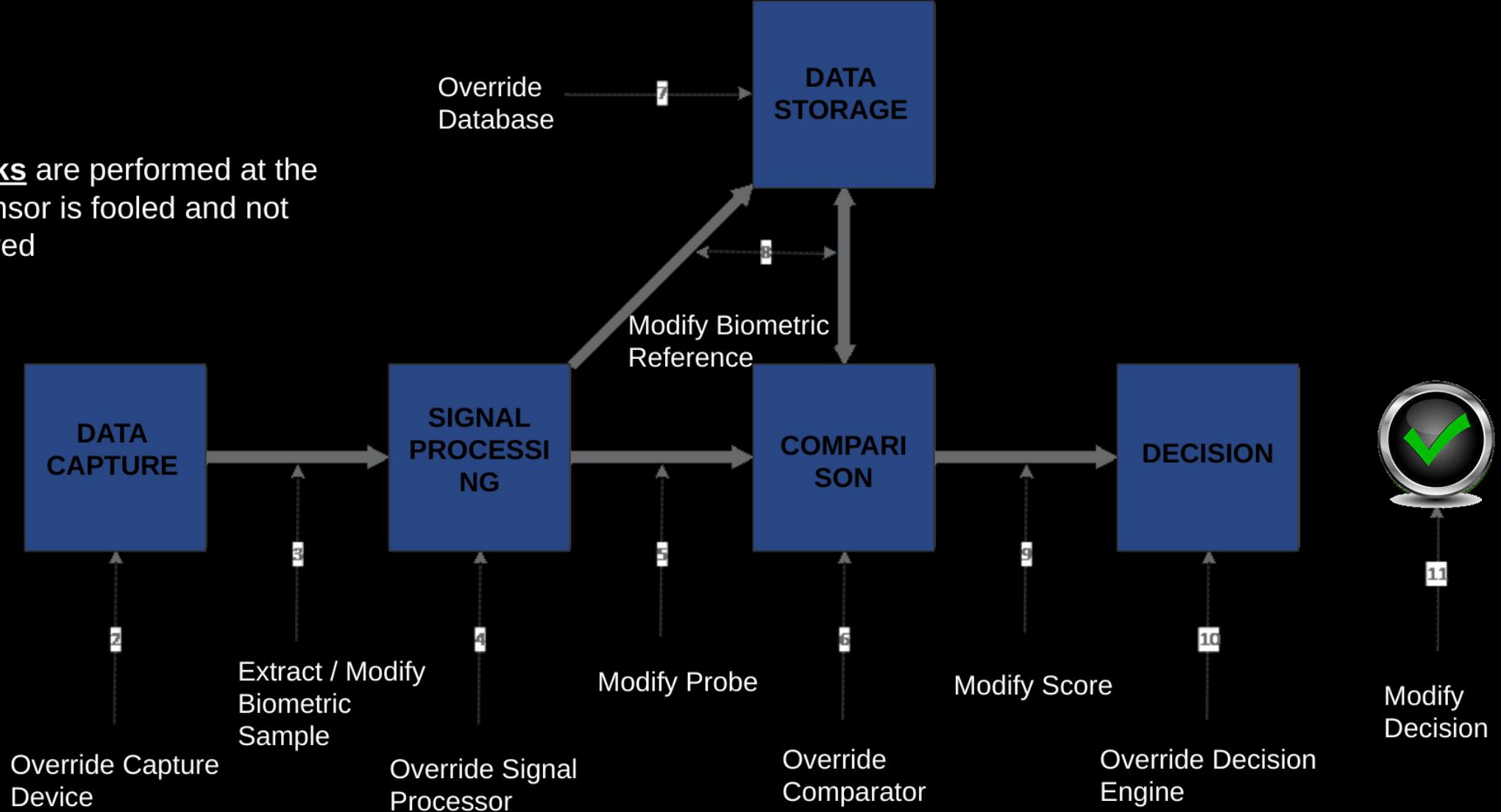
- Gait
- Voice
- Signature





HOW BIOMETRIC SYSTEMS WORK?







PRESENTATION ATTACKS IN REAL LIFE

BANK ROBBERY AND MASKED PLANE PASSENGER



UNITED STATES 2015



UNITED STATES 2010

Suspects on the
left and suspects
wearing masks
on the right



CANADA 2014



CHINA 2011



PRESENTATION ATTACKS IN REAL LIFE

FAKE FINGERS



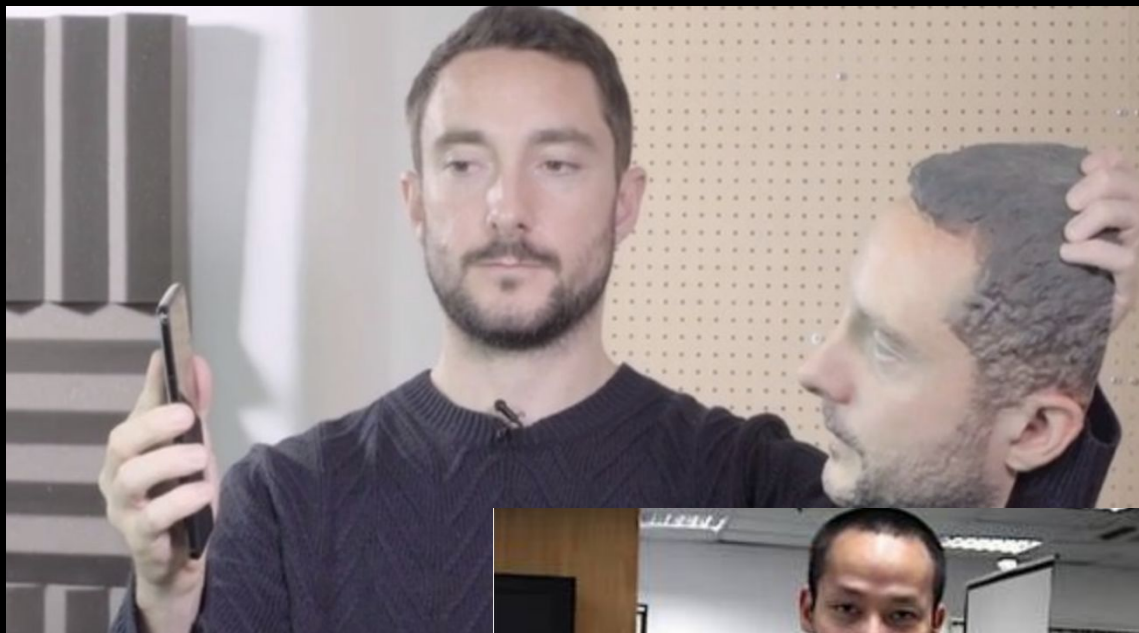
11 meses - Vía Buenos Aires

Echaron a seis empleados de Aerolíneas Argentinas que falseaban sus ingresos con dedos de silicona



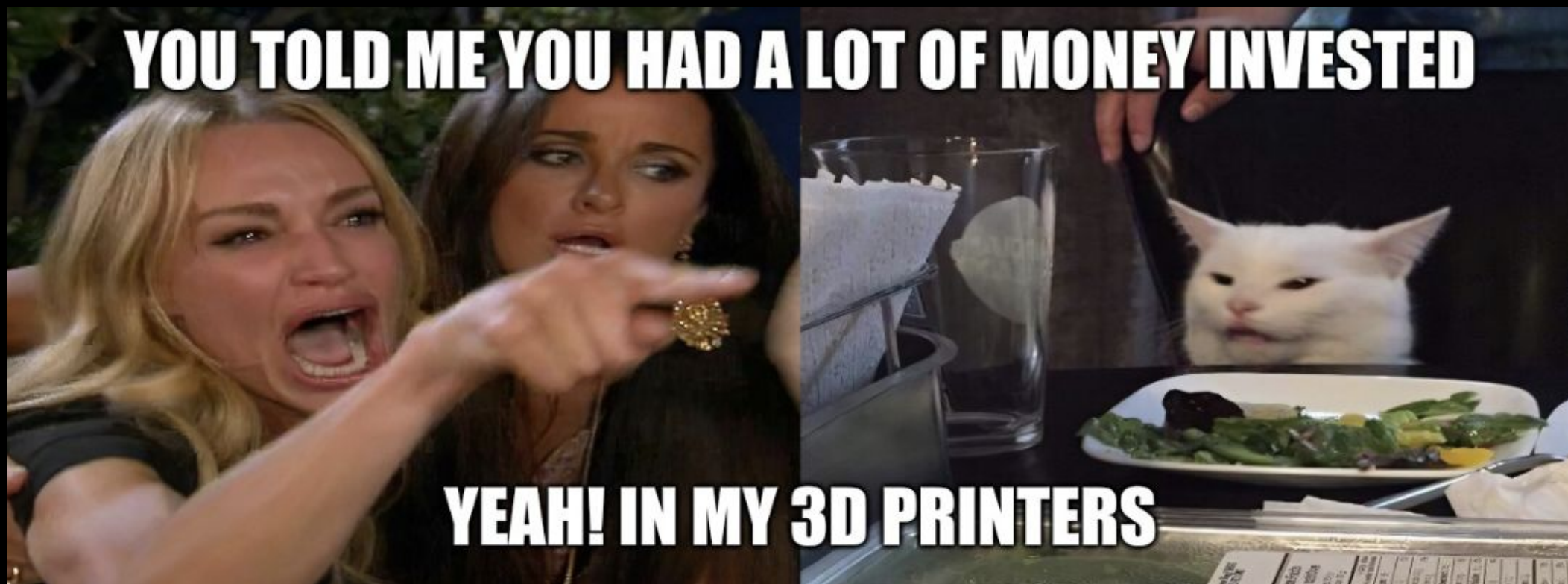


HOW 3D PRINTING COULD HELP TO BYPASS BIOMETRIC SYSTEMS





MAKING MY OWN EXPERIMENTS TO BYPASS BIOMETRIC SYSTEMS





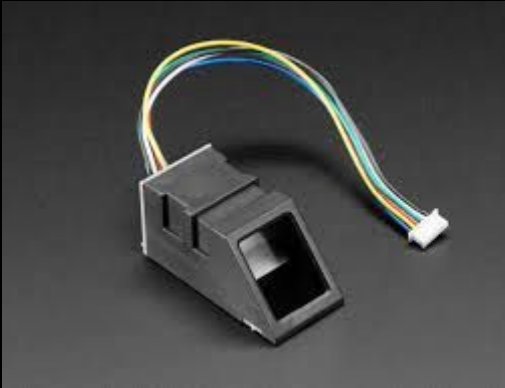
FINGERPRINT RECOGNITION



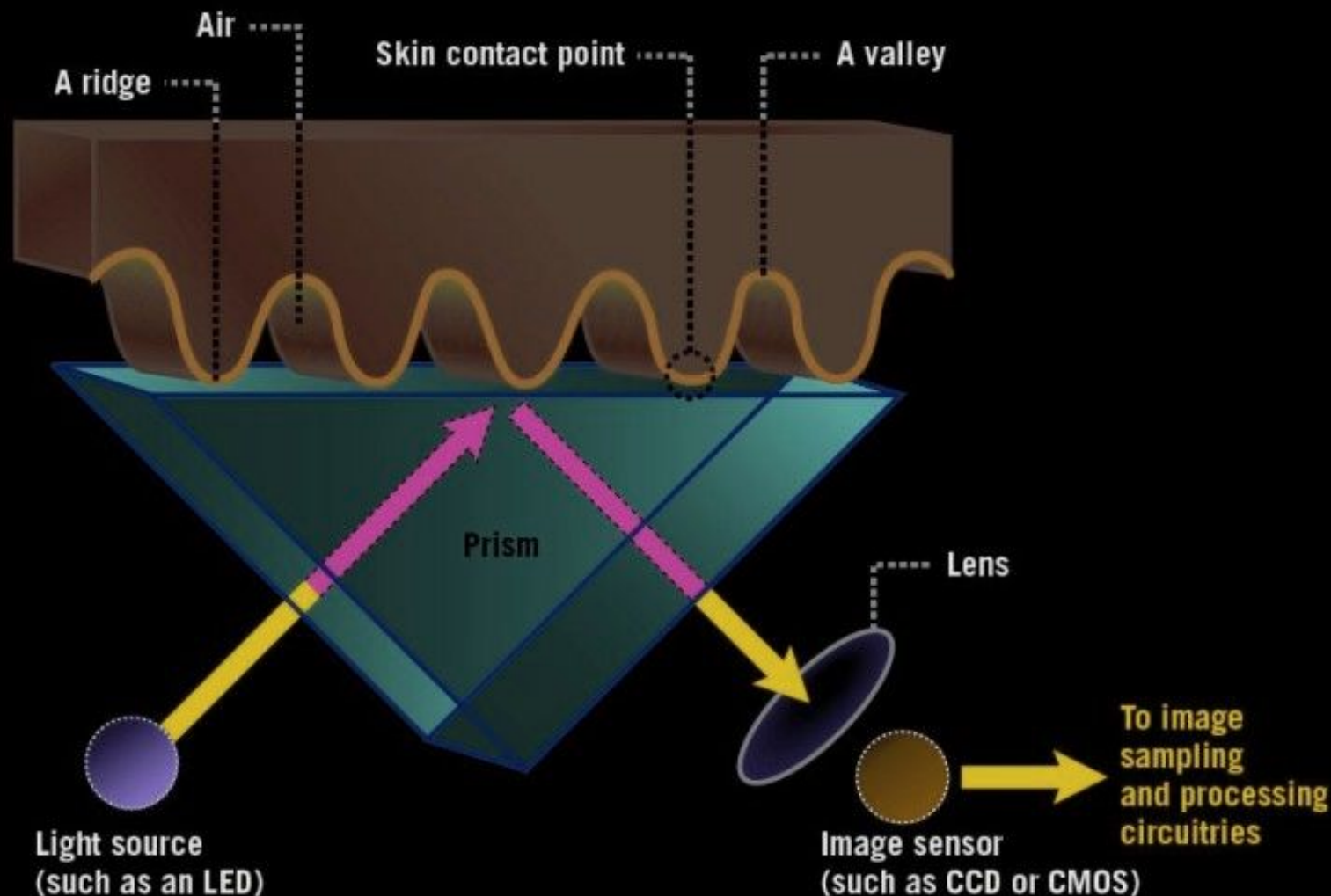
Minutiae and Typica



FINGERPRINT SENSORS



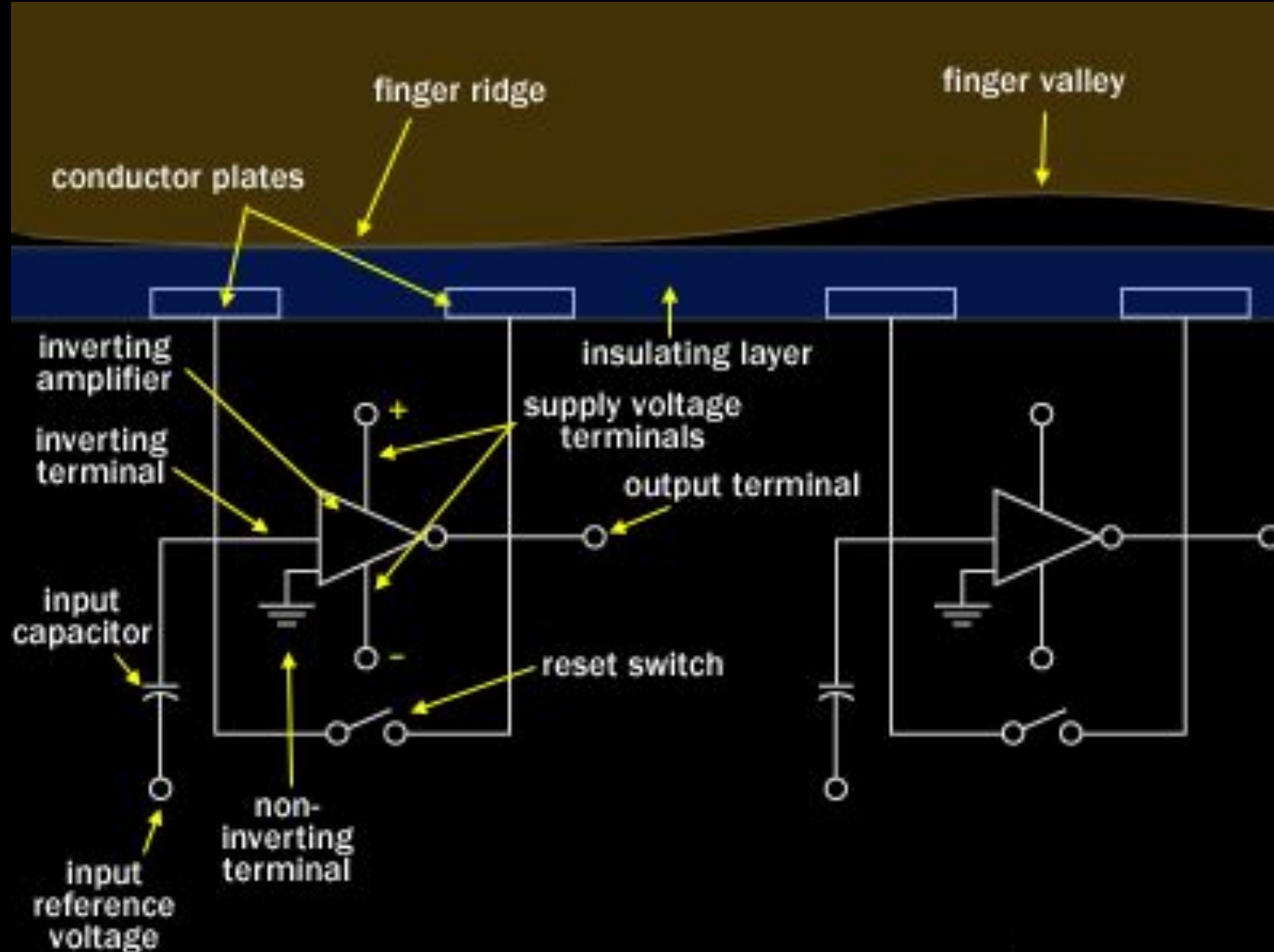
OPTICAL FINGERPRINT SENSOR



Optical fingerprint sensors are the oldest method of capturing and comparing fingerprints. This technique relies on capturing an optical image, essentially a photograph, and using algorithms to detect unique patterns on the surface, such as ridges or unique marks, by analyzing the lightest and darkest areas of the image.



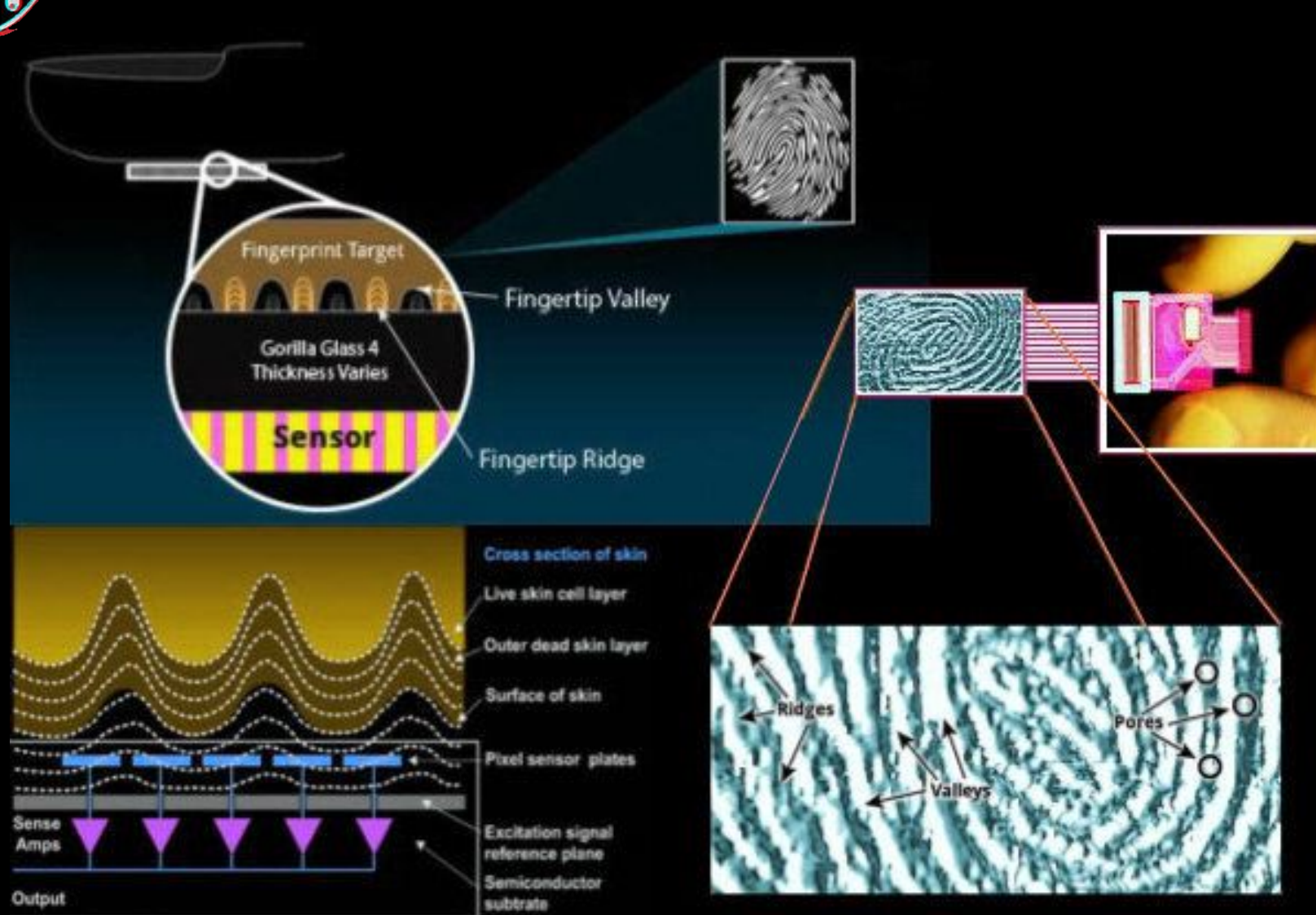
CAPACITIVE FINGERPRINT SENSOR



Capacitive fingerprint sensors use tiny capacitor circuits to collect data about a fingerprint. As capacitors can store electrical charge, connecting them up to conductive plates on the surface of the scanner allows them to be used to track the details of a fingerprint.

The charge stored in the capacitor will be changed slightly when a finger's ridge is placed over the conductive plates, while an air gap will leave the charge at the capacitor relatively unchanged. An integrator circuit is used to track these changes.

ULTRASONIC FINGERPRINT SENSOR



The hardware consists of 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.



DEVICES TO TEST: CELLPHONES AND ATTENDANCE SYSTEMS

Samsung Galaxy S10
Ultrasonic Fingerprint
Scanner
Face Recognition



SAMSUNG
GALAXY S10



Hysoon FF395
Optical Fingerprint
Scanner
Face Recognition

TA040
Optical Fingerprint
Scanner



Samsung Galaxy A30
Capacitive Fingerprint
Scanner
Face Recognition





GREASE ATTACKS

Preconditions for the attack

For using this kind of attack one needs to have a clear grease stain left on the surface of the scanner. This stain has to 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 enrolled fingerprint
- Applicable fingerprint stain on the scanner's pad left by the previous user
- Temperature between 0-50°C (scanners operating temperature)
- Gummy bears, silicone fingertips, playdoh, latex gloves





GREASE ATTACK RESULTS

Materials Tested and Results:

- Gummy Bears: Finger recognized
- Playdoh: Finger recognized
- Latex Glove: Finger recognized
- Moist Breathe: No Finger recognized
- Silicon Fingertip: Finger recognized

Materials	Sensor Fooled			
Materiales used	Optical1	Capacitive	Ultrasonic	Optical2
Gummy Bears	NO	NO	NO	NO
Tinfoil	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





“ENHANCED” GREASE ATTACKS AND RESULTS

The problem with grease attacks is that in most cases, a regular grease stain on the scanner surface is not enough to fool the sensor. We need to enhance it with other substances to obtain better results impersonating legitimate users, these substances must be transparent so that the user does not notice them and with ointment consistency to better enhance the fingerprint stain. This substance could be spread in the legitimate user fingerprint or on the fingerprint sensor.



**Researchers
Fingerprints are
Blurred**

Materials	Sensor Fooled			
Materiales used	Optical1	Capacitive	Ultrasonic	Optical2
Glicerín + 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





CONSENSUAL ATTACKS (WITH COOPERATION)

Preconditions for the attack

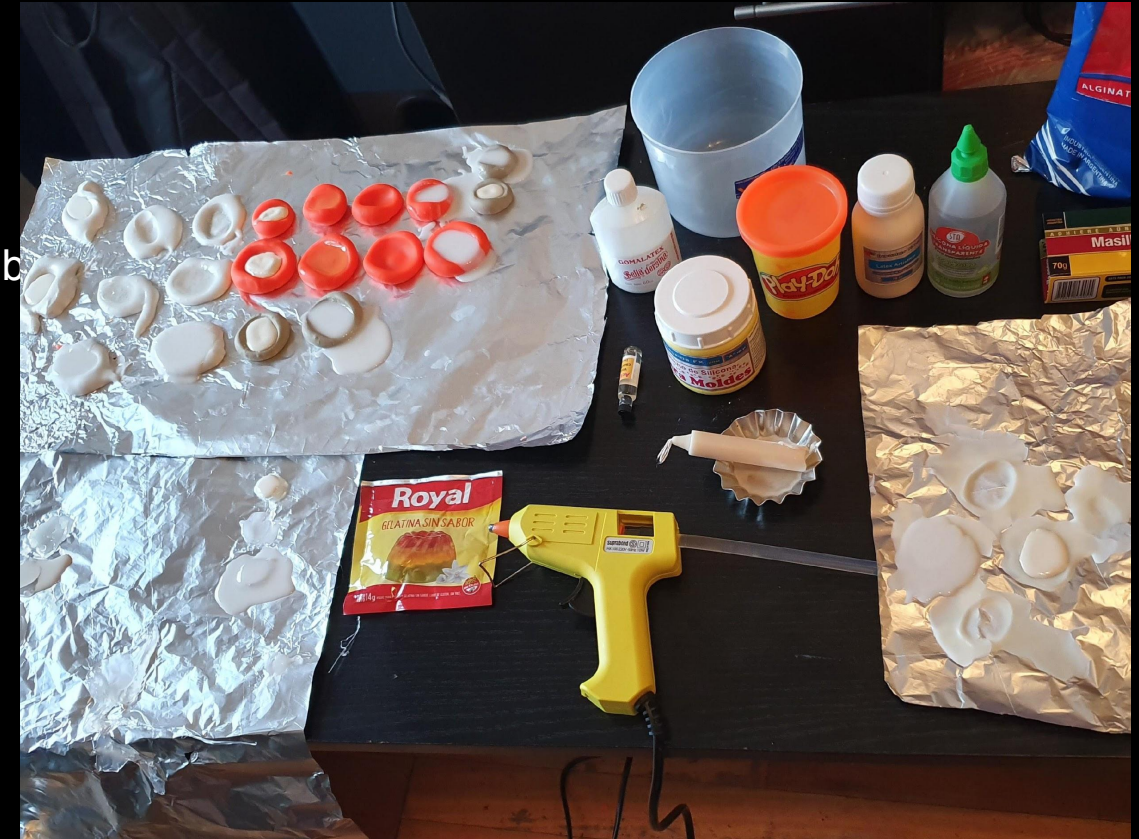
The term consensual suggests the user we are taking the fingerprint from is aware of the process and actively participates by pressing his finger into some kind of a mold. Even though we have classified this approach as “consensual”, there are unconsensual ways to go about achieving the same.

Materials for Molds:

- Alginate
- Epoxy putty
- Playdoh
- Hot Glue
- Candle Wax

Materials for Casting:

- Silicone
- Ballistic gelatin
- Liquid latex
- Synthetic Resin
- Wood glue



Researchers
Fingerprints are
Blurred again





CONSENSUAL ATTACKS RESULTS



Materials		Sensor Fooled			
		Optical	Capacitive	Ultrasonic	Optical2
Mould	Casting				
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 (WITHOUT COOPERATION)

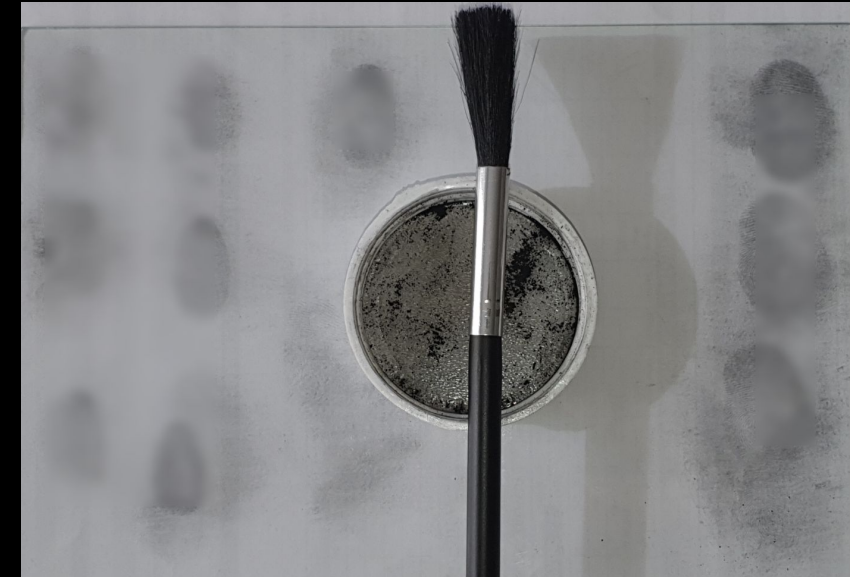
In these attacks the user does not participate actively and latent fingerprints are obtained in a non-cooperative way. Assuming the correct latent fingerprint has been identified, the following are the steps to follow:

Procedure

1. Enhancing the latent fingerprint with glue fumes or fingerprint powder
2. Lifting the latent fingerprint with digital camera or transparent tape
3. Digitally enhancing the fingerprint with software
4. Creating a mold
5. Casting artificial fingers with silicone, liquid latex or wood glue

Materials

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



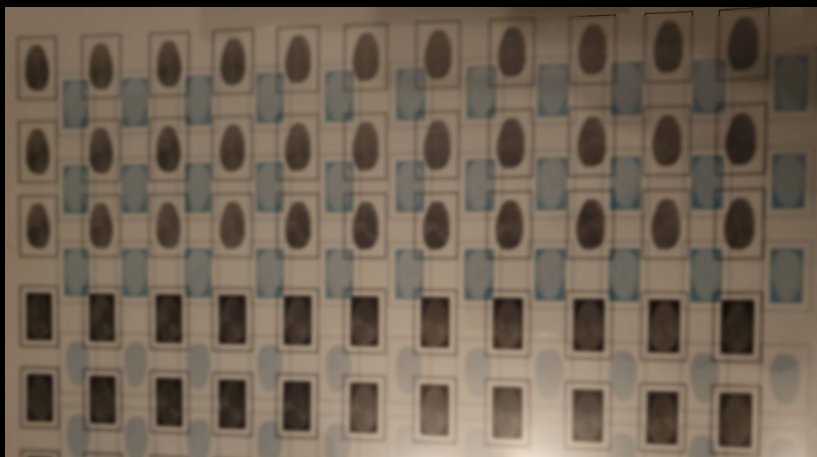
**MY OWN CYANOACRYLATE
FUMING CHAMBER XD**





UNCONSENSUAL ATTACKS RESULTS

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

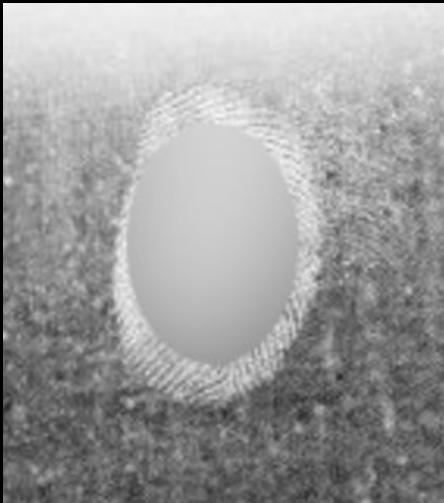




UNCONSENSUAL ATTACKS WITH 3D PRINTING: MATERIALS AND SOFTWARE

```
yl@ws17:~/tools/Fingerprint-Enhancement-Python/src$ ls
enhanced2bw.jpg  image_enhance.py      ridge_freq_2.py      ridge_segment.py
enhanced2.jpg    image_enhance.pyc     ridge_freq.py        ridge_segment.pyc
enhanced.jpg     main_enhancement.py  ridge_freq.pyc       ridge_orient.py
frequest.py      ridge_filter.py       ridge_orient.pyc
frequest.pyc     ridge_filter.pyc
yl@ws17:~/tools/Fingerprint-Enhancement-Python/src$
```

The precision of a domestic UV Resin printer is 25 microns. Human papillary ridges in general have a height between 20-60 microns.



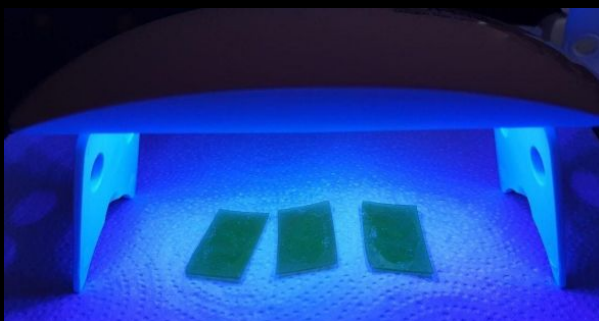
UNCONSENSUAL ATTACKS WITH 3D PRINTING



Procedure

1. Lift the latent fingerprint with a digital camera with macro functionality
2. Use a tool for digitally enhance the fingerprints, for example this Python tool based on the Utkarsh-Deshmukh tool: <https://github.com/ylevalle/Fingerprint-Enhancement-Python>
3. Convert the enhanced JPG file to an SVG file, import the SVG file into Tinkercad to create a 3D model of the fingerprint
4. Configure the fingerprint length and width according to the measures of the original latent fingerprint, put a thin back block 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.
5. Export the 3D models file in a 3D printable file format (STL) and upload it on the Anycubic Photon 3D Printer.
6. Once the printing is completed, the 3D printed molds require rinsing in Isopropyl alcohol. After rinsed parts dry, the molds require post-curing using an UV lamp or direct sunlight.
7. Fill the 3D printed negative or hollow molds with:
 - liquid latex or wood glue

Digitally
enhanced
test
fingerprint

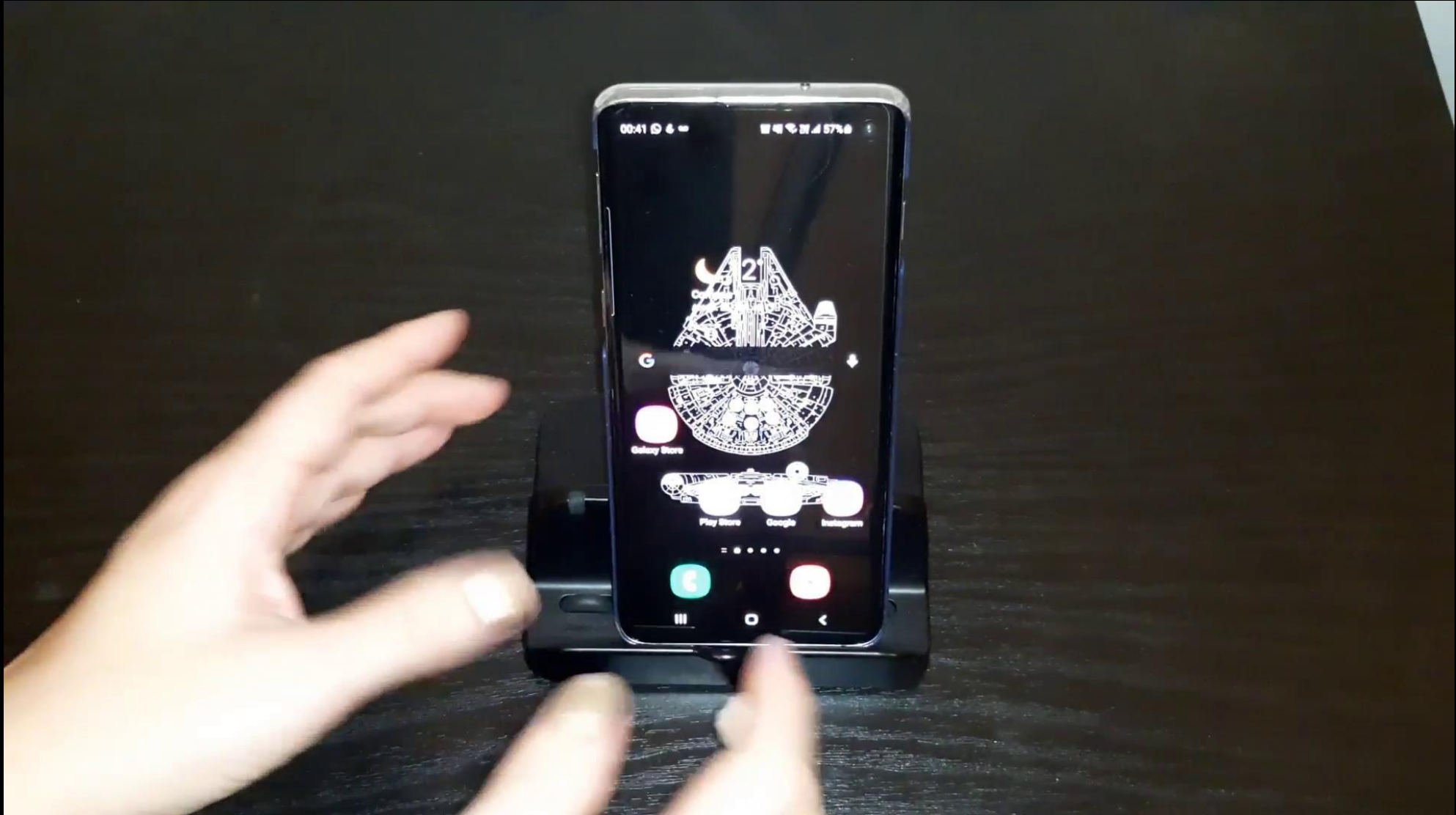




UNCONSENSUAL ATTACKS WITH 3D PRINTING: RESULTS

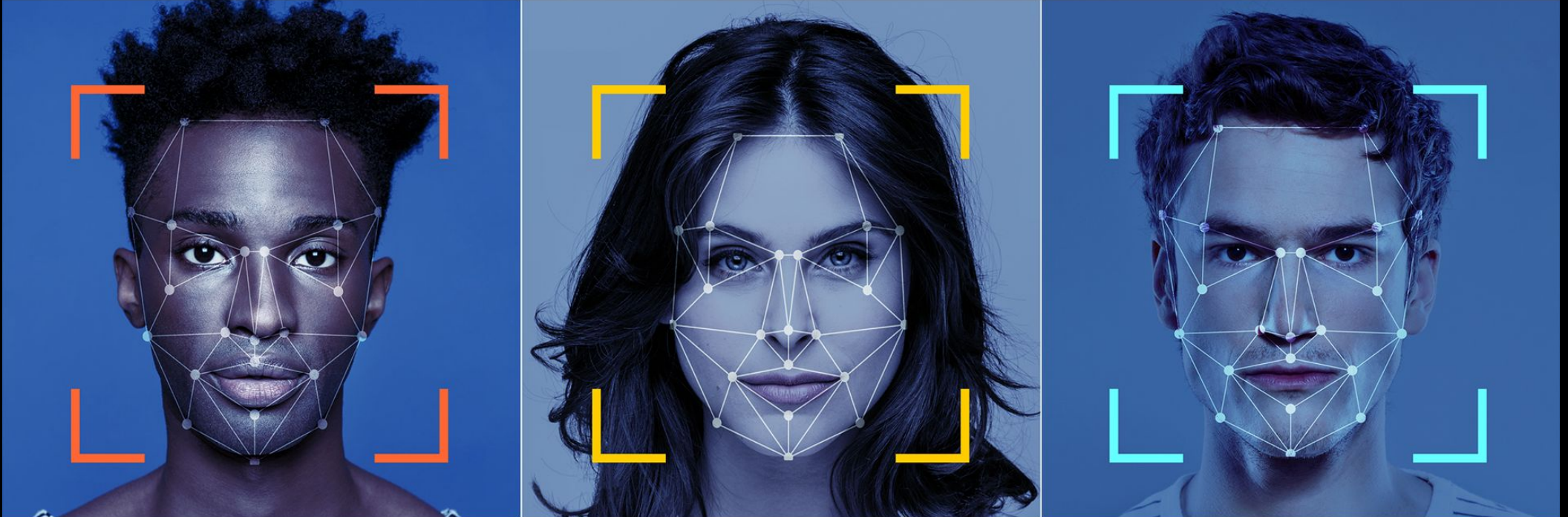


Materials		Results			
Material1	Material2	Optical	Capacitive	Ultrasonic	Optical2
Fingerprint on glass	UV DLP Resin positive from photo	YES	NO	YES	NO
Inked fingerprint	UV DLP Resin positive from photo	YES	NO	YES	NO
Fingerprint on glass	3D mould from photo	YES	YES	YES	YES
Inked fingerprint	3D mould from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





NEXT STAGE OF THE RESEARCH: FACIAL RECOGNITION SYSTEMS



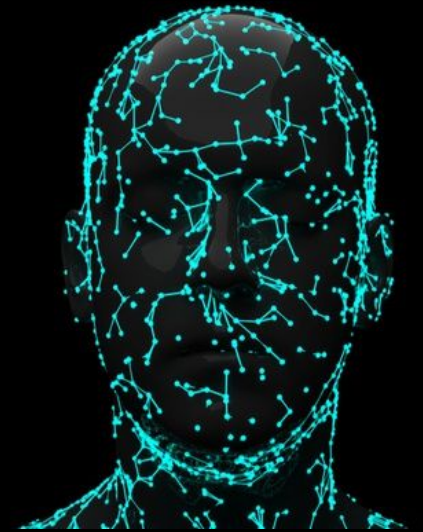


REFERENCE MATERIALS AND RECOMMENDED LECTURES

- <https://blog.talosintelligence.com/2020/04/fingerprint-research.html>
- <https://msutoday.msu.edu/news/2017/real-or-fake-creating-fingers-to-protect-identities/>
- http://biometrics.cse.msu.edu/Publications/Fingerprint/CaoJain_HackingMobilePhonesUsing2DPrintedFingerprint_MSU-CSE-16-2.pdf
- Chugh, Tarang & Jain, Anil. (2018). Fingerprint Presentation Attack Detection: Generalization and Efficiency.
- Pakutharivu, P. & Srinath, M.V.. (2017). Analysis of Fingerprint Image Enhancement Using Gabor Filtering With Different Orientation Field Values. Indonesian Journal of Electrical Engineering and Computer Science. 5. 427-432. 10.11591/ijeecs.v5.i2.pp427-432.
- Galbally, Javier & Marcel, Sébastien & Fierrez, Julian. (2014). Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint and Face Recognition. IEEE Trans. on Image Processing. 23. 710-724. 10.1109/TIP.2013.2292332.
- Wiehe, Anders & Org, Anders@wiehe & Søndrol, Torkjel. (2005). Attacking Fingerprint Sensors.
- Costa-Pazo, Artur & Bhattacharjee, Sushil & Vazquez-Fernandez, Esteban & Marcel, Sébastien. (2016). The Replay-Mobile Face Presentation-Attack Database. 10.1109/BIOSIG.2016.7736936.
- Erdogmus, Nesli & Marcel, Sébastien. (2014). Spoofing Face Recognition With 3D Masks. Information Forensics and Security, IEEE Transactions on. 9. 1084-1097. 10.1109/TIFS.2014.2322255.
- Bhattacharjee, Sushil & Marcel, Sébastien. (2017). What You Can't See Can Help You - Extended-Range Imaging for 3D-Mask Presentation Attack Detection. 1-7. 10.23919/BIOSIG.2017.8053524.



**THANK YOU DEFCON SAFE MODE!
AND TO ALL THE COWORKERS AND FRIENDS
THAT HELPED ME WITH THIS RESEARCH @laspibasdeinfosec**



Yamila Levalle @ylevalle