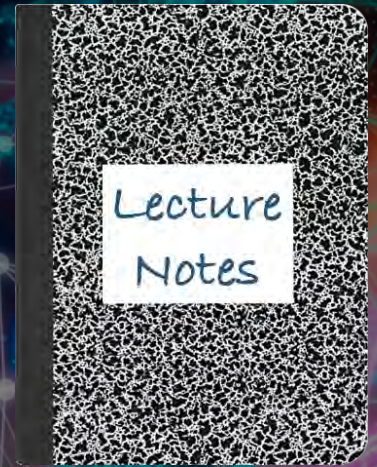


CS 419: Computer Security

# Week 9: Biometric Authentication



Paul Krzyzanowski

© 2022 Paul Krzyzanowski. No part of this content, may be reproduced or reposted in whole or in part in any manner without the permission of the copyright owner.

# Biometric Authentication

Identify a person based on physical or behavioral characteristics

```
scanned_fingerprint = capture();  
if (scanned_fingerprint == stored_fingerprint)  
    accept_user();  
else  
    reject_user();
```



We'd like to use  
logic like this

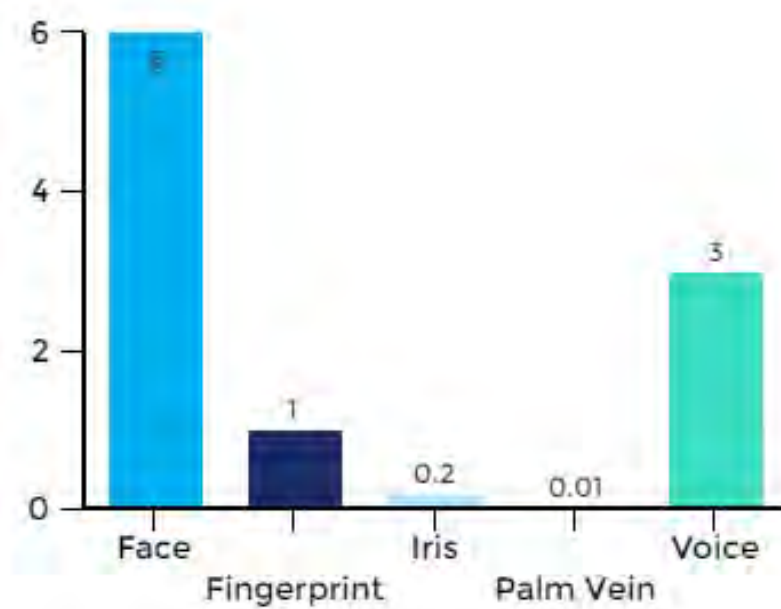
... but we can't!

# Biometric Authentication

- Rely on **statistical pattern recognition**
  - Thresholds to determine if the match is close enough
- **False Accept Rate (FAR)**
  - Non-matching pair of biometric data is *accepted* as a match
- **False Reject Rate (FRR)**
  - Matching pair of biometric data is *rejected* as a match

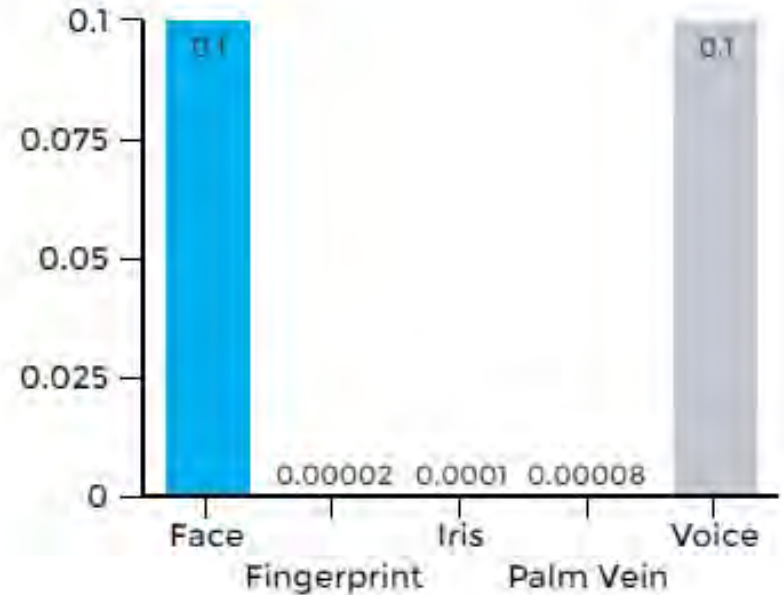
# FRR vs. FAR

Images from <https://www.bayometric.com/biometrics-face-finger-iris-palm-voice/>  
Used with permission



## False Rejection Rate (FRR)

Likelihood that the authentication will reject an authorized user

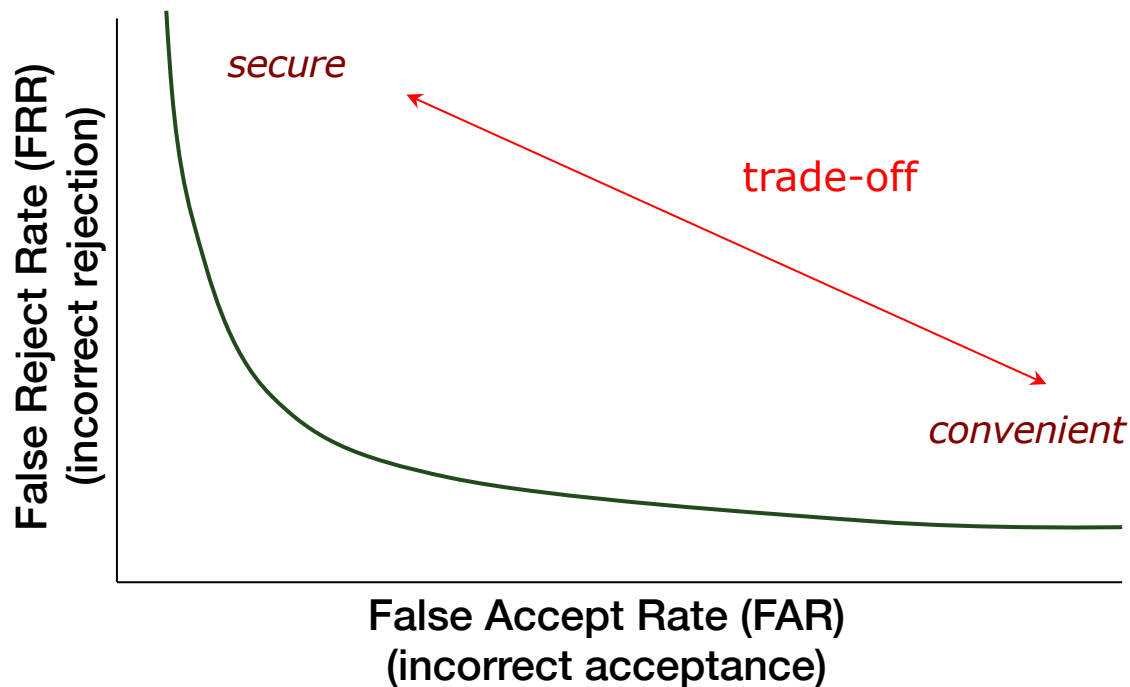


## False Acceptance Rate (FAR)

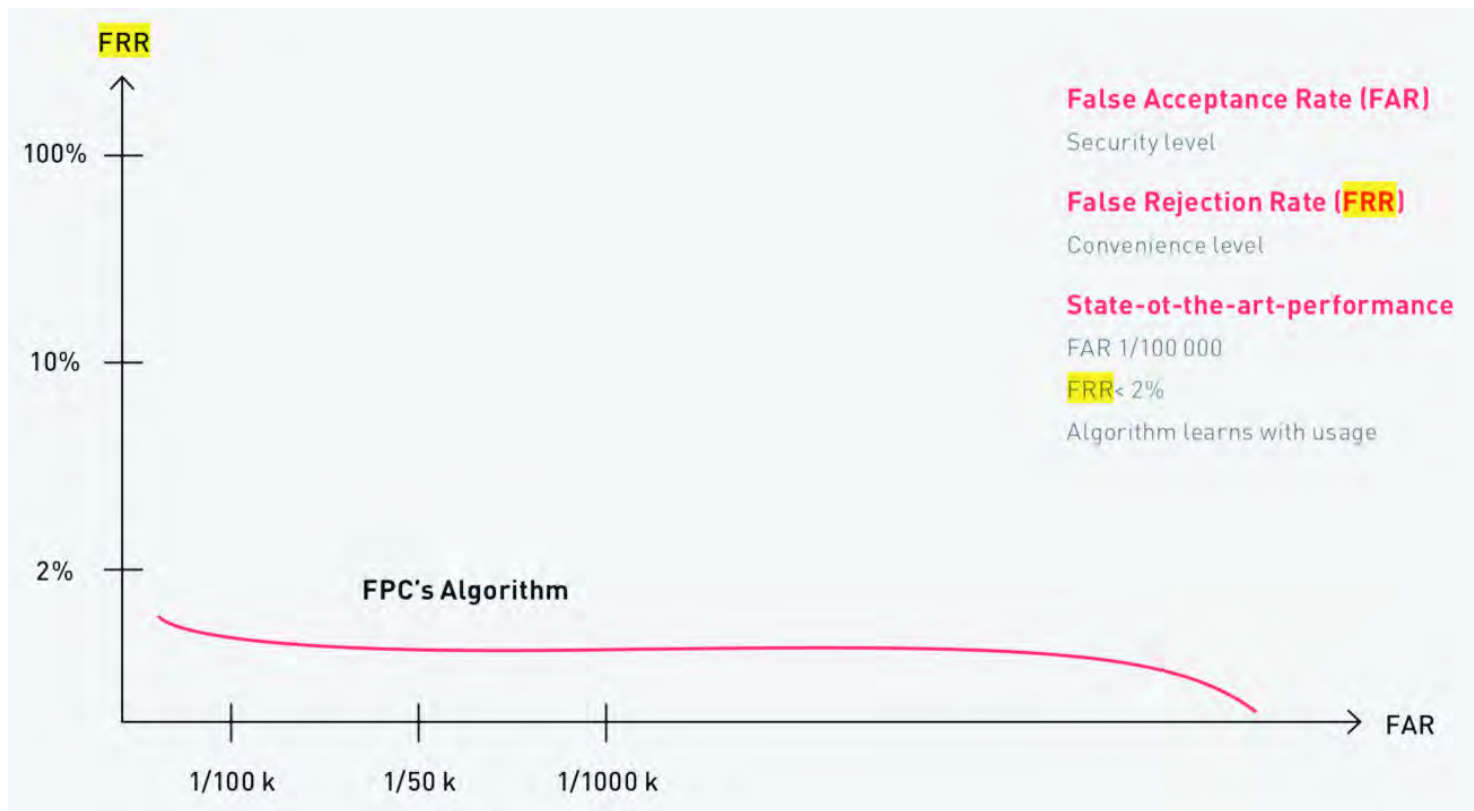
Likelihood that the authentication will accept an unauthorized user

# Biometric Authentication: ROC Curve

**Each biometric system has a characteristic ROC curve**  
(*receiver operator characteristic*, a legacy from radio electronics)



# Sample ROC curve for an advanced capacitive fingerprint sensor



Source: [https://www.fingerprints.com/uploads/2019/10/fpc\\_white\\_paper\\_digital.pdf](https://www.fingerprints.com/uploads/2019/10/fpc_white_paper_digital.pdf)

# Sample ROC data for FaceTec facial recognition

False Acceptance Rate (FAR)	False Rejection Rate (FRR)
1/1,000,000	0.0022 (0.22%)
1/2,000,000	0.0030 (0.30%)
1/4,200,000	0.0040 (0.40%)
1/10,000,000	0.0080 (0.80%)
1/12,800,000	0.0099 (0.99%)

[https://www.facetec.com/FaceTec\\_3D\\_Face\\_Matching\\_Whitepaper.pdf](https://www.facetec.com/FaceTec_3D_Face_Matching_Whitepaper.pdf)

# Galaxy S9 Intelligent Scan favors unlocking ease over security



An in-depth look at Samsung's new biometrics verification system -- and how it stacks up against the iPhone X's Face ID — shows it's not quite safe enough for mobile payments.

Shara Tibken, Alfred Ng March 1, 2018 5:00 AM PST

Unlocking the Galaxy S9 might be faster -- but that doesn't mean it's more secure.

Samsung's newest smartphones, the Galaxy S9 and S9 Plus, include a new feature the company calls Intelligent Scan. The technology combines Samsung's secure iris scanner with its less-secure facial recognition unlock technology.

When unlocking your phone, it first will scan your face. If that fails to unlock the phone, the device then will check your irises. If both fail, Intelligent Scan will try to authenticate your identity using a combination of the two. And it all happens almost instantaneously.

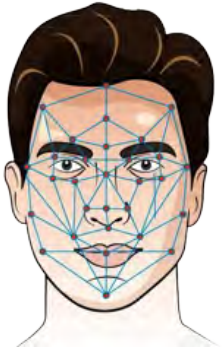
<https://www.cnet.com/news/samsung-galaxy-s9-intelligent-scan-unlock-favors-ease-over-security/>



# Biometric Authentication Modalities

## Face

- Face geometry
- w/ 3-D imaging
- Thermographs
- Ear imaging



## Eyes

- Iris - spokes
- Retinal scans



## Hands

- Fingerprints
- Vein scans
- Hand geometry
  - Finger length
  - Contours
  - Surface area



## Signature, Voice

Behavioral vs. physiological biometrics



## Others

- DNA
- Odor
- Gait
- Driving habits
- ...



# Feature Identification

## Example: Fingerprints

Identify minutiae points and their relative positions

### Minutiae (features)

Arches

Loops

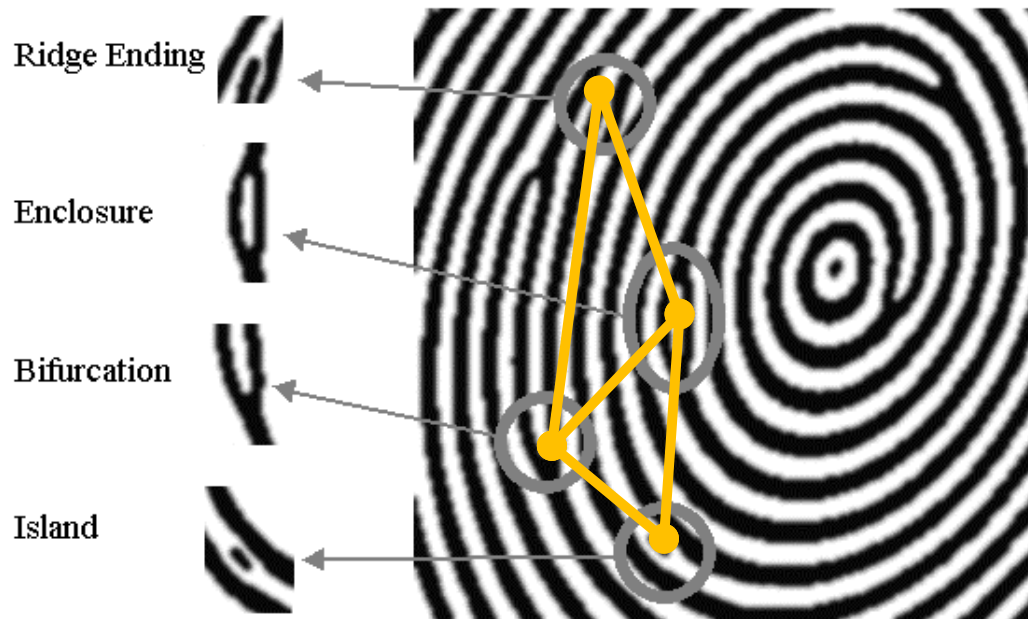
Whorls

Ridge endings

Bifurcations

Islands

Bridges



source: [http://anil299.tripod.com/vol\\_002\\_no\\_001/papers/paper005.html](http://anil299.tripod.com/vol_002_no_001/papers/paper005.html)

# Desirable Characteristics

- **Robustness**

- Repeatable, not subject to large changes over time
- Fingerprints & iris patterns are more robust than voice

- **Distinctiveness**

- Differences in the pattern among population
- Fingerprints: typically 40-60 distinct features
- Irises: typically >250 distinct features
- Hand geometry: ~1 in 100 people may have a hand with measurements close to yours

# Desirable Characteristics

<b>Biometric</b>	<b>Robustness</b>	<b>Distinctiveness</b>	<b>Ease of Use</b>	<b>User Acceptance</b>
<b>Fingerprint</b>	Moderate	High	Medium	Medium
<b>Face</b>	Moderate	Low	High	High
<b>Hand Geometry</b>	Moderate	Low	Medium	Medium
<b>Voice</b>	Moderate	Low	High	High
<b>Iris</b>	High	Ultra high	Medium	Medium
<b>Retina</b>	High	Ultra high	Low	Low
<b>Signature</b>	Low	Moderate	Low	High

# Irises vs. Fingerprints

- **Number of features measured:**
  - High-end fingerprint systems: ~40-60 features
  - Iris systems: ~240 features
- **False accept/reject rates (FAR/FRR)**
  - Fingerprints: ~ 1:100,000 (varies by vendor; may be ~1:500)
    - FRR  $\approx$  0 – 66%, FAR  $\approx$  0.01%
  - Irises: ~ 1:1.2 million
    - FRR  $\approx$  1%, FAR  $\approx$  0.1%
  - Retina scan ~1:10,000,000

# Irises vs. Fingerprints

- **Ease of data capture**

- More difficult to damage an iris ... but lighting is an issue
- Feature capture more difficult for fingerprints:
  - Smudges, gloves, dryness, ...

- **Ease of searching**

- Fingerprints cannot be normalized
  - 1:many* searches are difficult
- Irises can be normalized to generate a unique IrisCode
  - 1:many* searches much faster

# Biometric Authentication Process

## 0. Enrollment

- The user's entry in a database of biometric data needs to be initialized
- Initial sensing and feature extraction
- May be repeated to ensure good feature extraction



# Biometric Authentication Process

## 1. Sensing

- User's characteristic must be presented to a sensor
- Output is a function of:
  - Biometric measure
  - The way it is presented
  - Technical characteristics of sensor

## 2. Feature Extraction

- Signal processing
- Extract the desired biometric pattern
  - remove noise and signal losses
  - discard qualities that are not distinctive/repeatable
  - Determine if feature is of “good quality”





# Biometric Authentication Process

## 3. Pattern matching

- Sample compared to original signal in database
- Closely matched patterns have “small distances” between them
- Distances will hardly ever be 0 (perfect match)

## 4. Decision

- Decide if the match is close enough
- Trade-off:
  - ↓ false non-matches leads to ↑ false matches



# Identification vs. Authentication

- **Identification:**      *Who is this?*
  - Requires a *1:many* search
  
- **Verification:**      *Is this Bob?*
  - Present a name, PIN, token
  - Then you only need a *1:1* (or *1:small #*) search

# Essential Sensor Characteristics

- **Trusted sensor**
- **Liveness & decoy testing**
- **Tamper resistance**
- **Secure communication**
- **Acceptable thresholds**



# Other Biometric Authentication Characteristics

- **Cooperative systems (multi-factor)**
  - User provides identity, such as name and/or PIN
- **vs. Non-cooperative**
  - Users cannot be relied on to identify themselves
  - Need to search large portion of database
- **Overt vs. covert identification**
  - Example: have a user look directly into a camera or use a hidden camera
- **Habituated vs. non-habituated**
  - Do users regularly use (train) the system

# Problems With Biometric Authentication

- **Requires a sensor**
  - Camera works OK for iris scans & facial detection  
(but a good Iris scan will also use infrared light; a face sensor may project an infrared grid for texture mapping or capture a thermal image)
- **Tampering with device or device link**
  - Replace the sensed data – or just feed it new data directly where the device talks to the computer
- **Tampering with stored biometric data**
- **Biometric data cannot be compartmentalized**
  - You cannot have different data for your Amazon & bank accounts
- **Biometric data can be stolen**
  - Photos, lifting fingerprints
  - Once biometric data is compromised, it remains compromised
    - You cannot change your iris or finger

# A photo will unlock many Android phones using facial recognition

By John E Dunn

08 JAN 2019 5

Security threats, Vulnerability

How easy is it to bypass the average smartphone's facial recognition security?

According to the Dutch consumer protection organisation Consumentenbond, in the case of several dozen Android models, it's a lot easier than most owners probably realise.



Its researchers tested 110 devices, finding that 42 could be beaten by holding up nothing more elaborate than a photograph of a device's owner.

Consumentenbond offers little detail of its testing methodology but it seems these weren't high-resolution photographs – almost any would do, including those grabbed from social media accounts or selfies taken on another smartphone.

While users might conclude from this test that it's not worth turning on facial recognition, the good news is that 68 devices, including Apple's recent XR and XS models, resisted this simple attack, as did many other high-end Android models from Samsung, Huawei, OnePlus, and Honor.

<https://nakedsecurity.sophos.com/2019/01/08/facial-recognition-on-42-android-phones-beaten-by-photo-test/>

# Google Pixel 4 Face Unlock works if eyes are shut

Chris Fox • Technology reporter • 17 October 2019

Google has confirmed the Pixel 4 smartphone's Face Unlock system can allow access to a person's device even if they have their eyes closed. One security expert said it was a significant problem that could allow unauthorised access to the device.

By comparison, Apple's Face ID system checks the user is "alert" and looking at the phone before unlocking.

Google said in a statement: "Pixel 4 Face Unlock meets the security requirements as a strong biometric."

<https://www.bbc.com/news/technology-50085630>

# Samsung Galaxy S8 iris scanner tricked by photo, contact lens



Turns out the sophisticated tech can't tell the difference between your eye and a picture with a contact lens over the iris, a hacking club says.

Alfred NG. May 24, 2017 8:34 AM PDT

You won't believe your eyes. But maybe the Samsung Galaxy S8 will.

In the month since Samsung released its flagship device, hackers in Germany have figured how to break the phone's iris recognition lock. Samsung has touted the biometric technology as "one of the safest ways to keep your phone locked," claiming that a person's iris patterns are "virtually impossible to replicate."

But that's exactly what the hackers from the Chaos Computer Club say they did. The hackers used a photo shot in night mode and from a medium distance, about the same range that would pop up in a Facebook profile picture or a selfie. They then printed out a closeup of the person's eye and put a contact lens over the iris on the paper.

The lens is there to replicate the eye's curvature, the Chaos Computer Club said in a blog post this week. Someone then held up the piece of paper to the Samsung Galaxy S8's iris scanner, and it unlocked as if a real person had looked at it.

<https://www.cnet.com/news/samsung-galaxy-s8-iris-scanner-tricked-photo-contact-lens/>



# Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case

Scams using artificial intelligence are a new challenge for companies

By Catherine Stupp • August 30, 2019

Criminals used artificial intelligence-based software to impersonate a chief executive's voice and demand a fraudulent transfer of €220,000 (\$243,000) in March in what cybercrime experts described as an unusual case of artificial intelligence being used in hacking.

The CEO of a U.K.-based energy firm thought he was speaking on the phone with his boss, the chief executive of the firm's German parent company, who asked him to send the funds to a Hungarian supplier. The caller said the request was urgent, directing the executive to pay within an hour, according to the company's insurance firm, Euler Hermes Group SA.

<https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402>

# Massive biometric security flaw exposed more than one million fingerprints

The system is used by banks, police and defence companies.

August 14, 2019 – Rachel England, @rachel\_england



A biometrics system used by banks, UK police and defence companies has suffered a major data breach, revealing the fingerprints of more than one million people as well as unencrypted passwords, facial recognition information and other personal data.

Biostar 2, the biometrics lock system managed by security company Suprema, uses fingerprints and facial recognition technology to give authorised individuals access to buildings. Last month the platform was integrated into another access system -- AEOS -- which is used by 5,700 organizations across 83 countries, including the UK Metropolitan Police.

<https://www.engadget.com/2019/08/14/biometric-security-flaw-fingerprints>

## Samsung's Galaxy S10 fingerprint sensor fooled by 3D printed fingerprint

It took 13 minutes to print up the fake

By Andrew Liptak • April 7 2019

... user darkshark outlined his project: he took a picture of his fingerprint on a wineglass, processed it in Photoshop, and made a model using 3ds Max that allowed him to extrude the lines in the picture into a 3D version. After a 13-minute print (and three attempts with some tweaks), he was able to print out a version of his fingerprint that fooled the phone's sensor.

<https://www.theverge.com/2019/4/7/18299366/samsung-galaxy-s10-fingerprint-sensor-fooled-3d-printed-fingerprint>

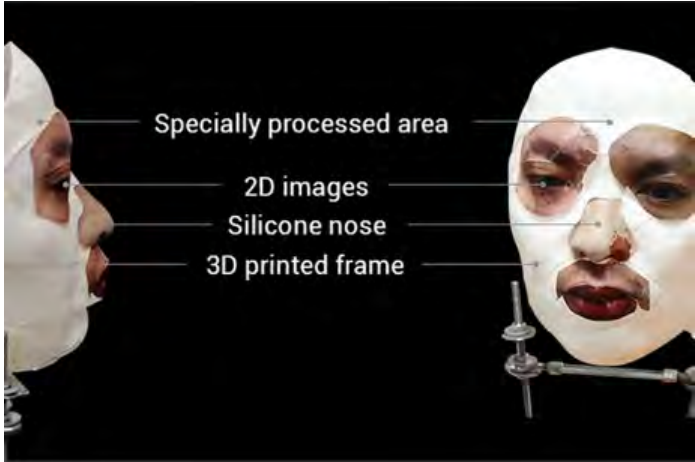
Video: <https://imgur.com/gallery/8aGqsSu>

## This \$150 mask beat Face ID on the iPhone X It's just a proof of concept at the moment

By Thuy Ong • Nov 13 2017

Vietnamese cybersecurity firm Bkav claims it's been able to bypass the iPhone X's Face ID feature using a mask. The mask is made to trick Apple's depth mapping and the result is a kind of creepy hybrid monster head with realistic cutouts for the eyes, nose and mouth.

Bkav says the mask is crafted through a combination of 3D printing, makeup, and 2D images.



<https://www.theverge.com/2017/11/13/16642690/bkav-iphone-x-faceid-mask>

The End