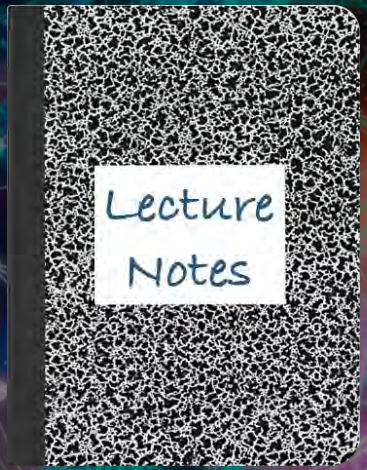
CS 419: Computer Security

Week 4:
Part 2: Biometric Authentication



Paul Krzyzanowski

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

Comparison of biometrics relies on pattern recognition & thresholds

- Determine if the match is close enough to a stored sample

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

False Accept Rate (FAR)

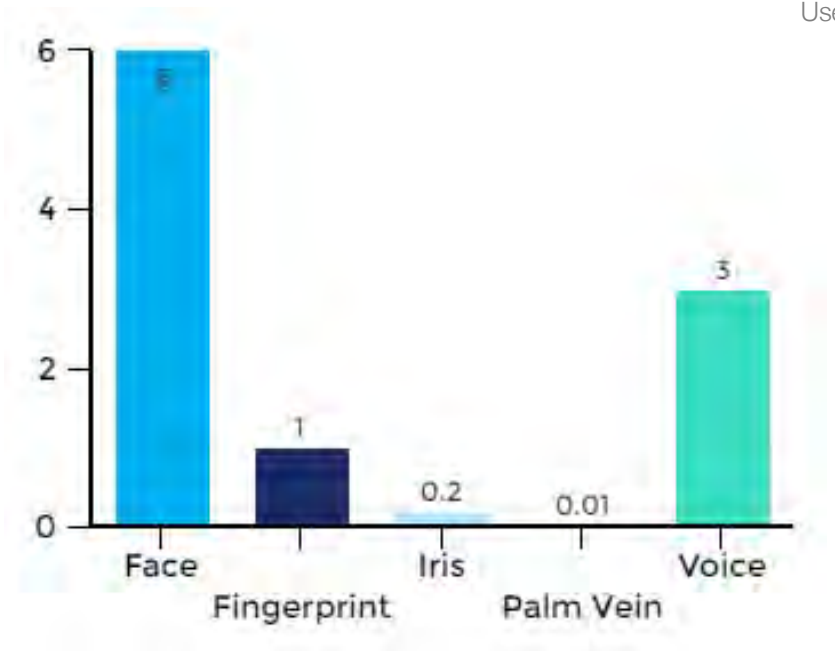
% non-matches accepted as a match

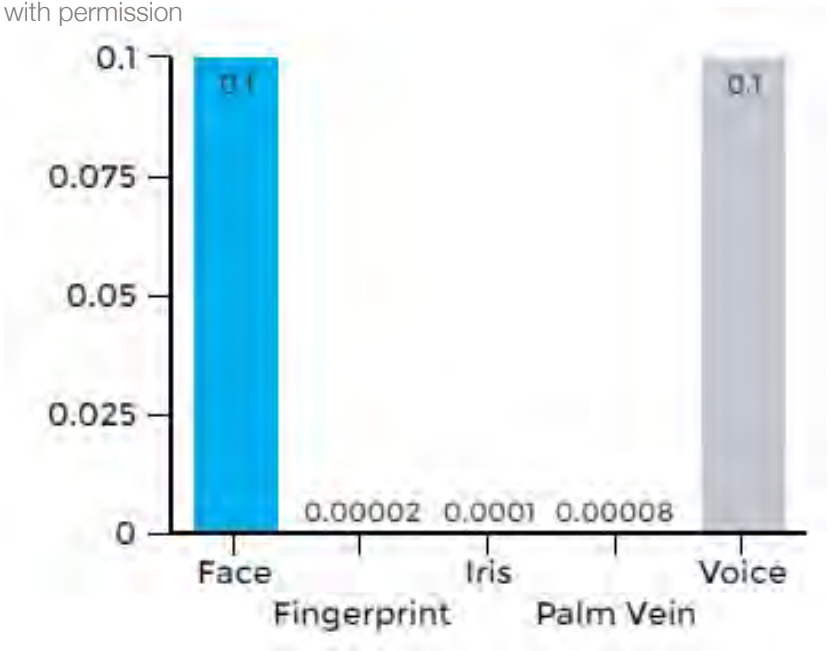
False Reject Rate (FRR)

% of matches rejected as a non-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

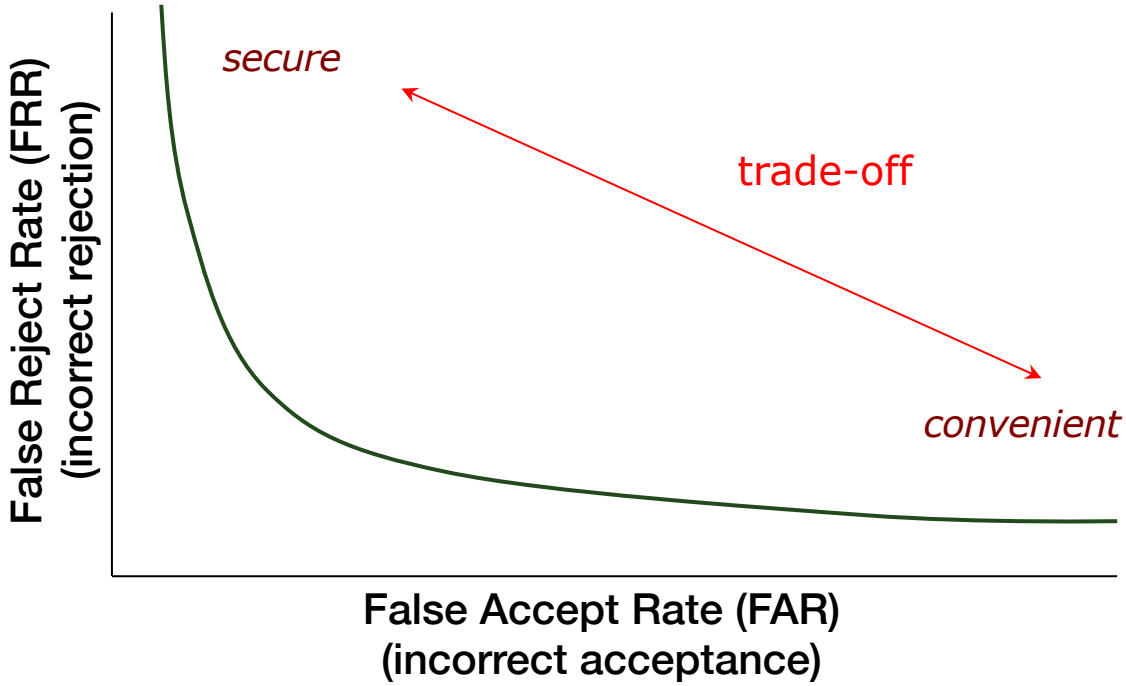
False Acceptance Rate (FAR)

Likelihood that the authentication will accept an unauthorized user

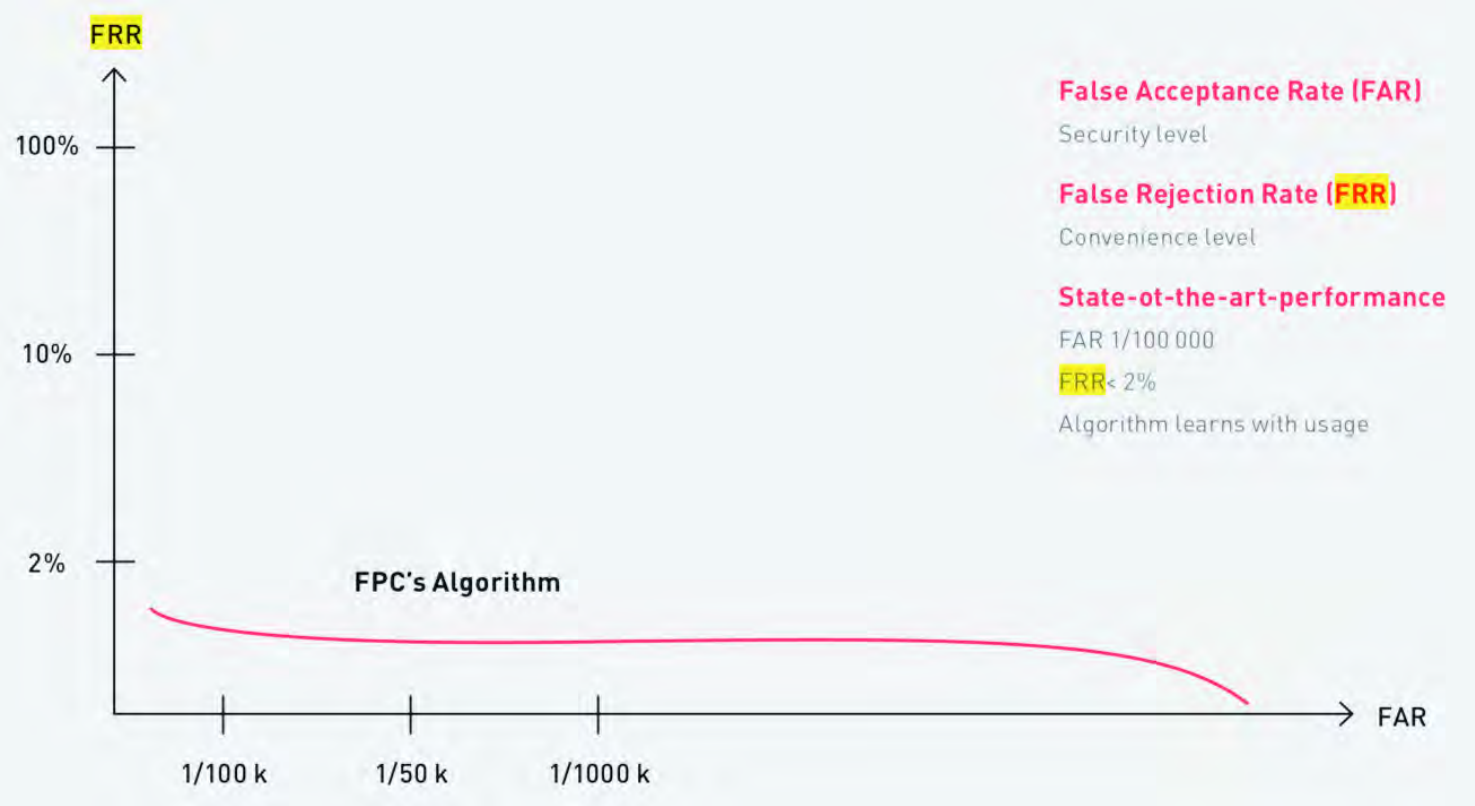
Biometric Authentication: ROC Curve

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

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

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.

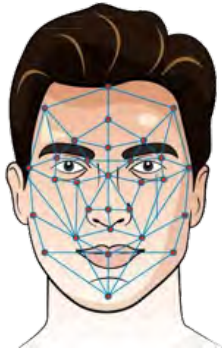
When unlocking your phone, it first will scan your face. If that fails to unlock the phone, the device then will check your irises. If both fail, Intelligent Scan will try to authenticate your identity using a combination of the two. And it all happens almost instantaneously.

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 are

Signature, Voice

Behavioral vs. physiological biometrics

Others

- DNA
- Odor
- Gait
- Driving habits
- …

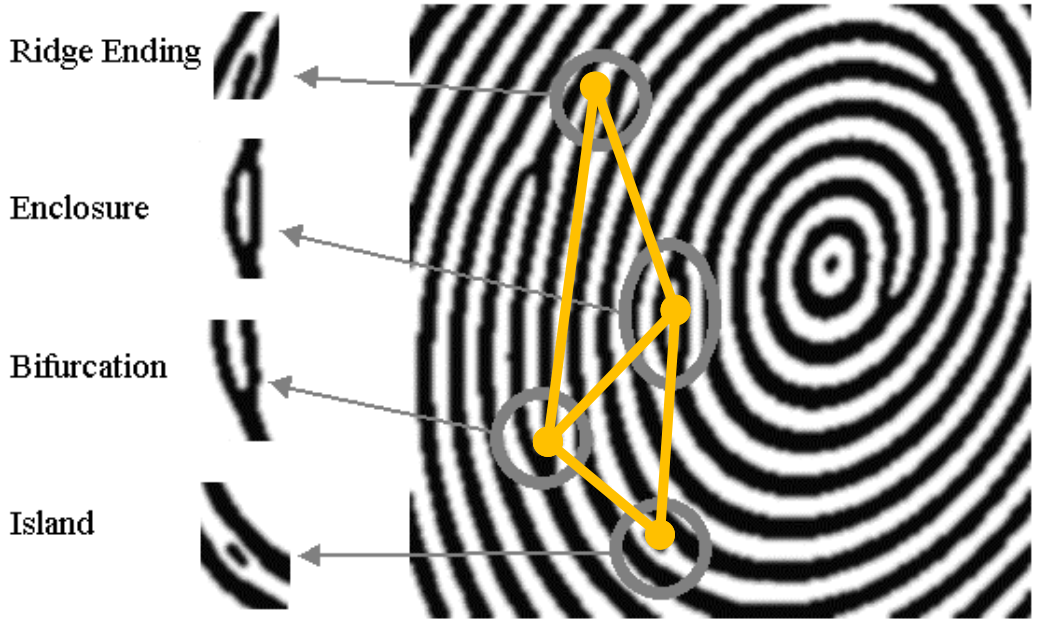
Feature Identification

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

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

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

Irises vs. Fingerprints

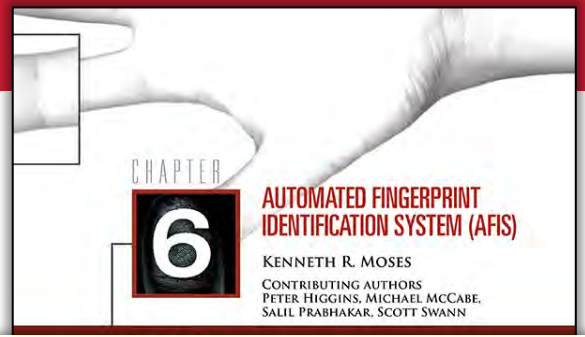
- **Number of features measured:**
  - High-end fingerprint systems: ~40-60 features
  - Iris systems: ~240 features

- **False accept/reject rates (FAR/FRR)**
  - Fingerprints: ~ 1:100,000 (varies by vendor; may be ~1:500)
    - FRR ≈ 0 – 66%, FAR ≈ 0.01%
  - Irises: ~ 1:1.2 million
    - FRR ≈ 1%, FAR ≈ 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 fully normalized
    1:many searches are difficult
  - Irises can be normalized to generate a unique IrisCode
    1:many searches much faster



Today's AFIS can often return a search of a million records in under a minute. As databases have expanded across the world, some AFIS engineers have expanded to searching four fingers or more in an effort to increase accuracy.

https://www.ojp.gov/pdffiles1/nij/225326.pdf

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

Malaysia car thieves steal finger

By Jonathan Kent
BBC News, Kuala Lumpur – 31 March, 2005

Police in Malaysia are hunting for members of a violent gang who chopped off a car owner's finger to get round the vehicle's hi-tech security system.

The car, a Mercedes S-class, was protected by a fingerprint recognition system.

Accountant K Kumaran's ordeal began when he was run down by four men in a small car as he was about to get into his Mercedes in a Kuala Lumpur suburb. The gang, armed with long machetes, demanded the keys to his car. It is worth around $75,000 second-hand on the local market, where prices are high because of import duties.

Stripped naked

The attackers forced Mr Kumaran to put his finger on the security panel to start the vehicle, bundled him into the back seat and drove off. But having stripped the car, the thieves became frustrated when they wanted to restart it. They found they again could not bypass the immobiliser, which needs the owner's fingerprint to disarm it.

They stripped Mr Kumaran naked and left him by the side of the road - but not before cutting off the end of his index finger with a machete. Police believe the gang is responsible for a series of thefts in the area.

http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm

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

Remember That DNA You Gave 23andMe?

The Atlantic

The company is in trouble, and anyone who has spit into one of the company's test tubes should be concerned.

Kristen V. Brown • September 27, 2024

23andMe is not doing well. Its stock is on the verge of being delisted. It shut down its in-house drug-development unit last month, only the latest in several rounds of layoffs. Last week, the entire board of directors quit, save for Anne Wojcicki, a co-founder and the company's CEO. Amid this downward spiral, Wojcicki has said she'll consider selling 23andMe—which means the DNA of 23andMe's 15 million customers would be up for sale, too.

23andMe's trove of genetic data might be its most valuable asset. For about two decades now, since human-genome analysis became quick and common, the A's, C's, G's, and T's of DNA have allowed long-lost relatives to connect, revealed family secrets, and helped police catch serial killers. Some people's genomes contain clues to what's making them sick, or even, occasionally, how their disease should be treated.

https://www.theatlantic.com/health/archive/2024/09/23andme-dna-data-privacy-sale/680057/

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/

THE VERGE

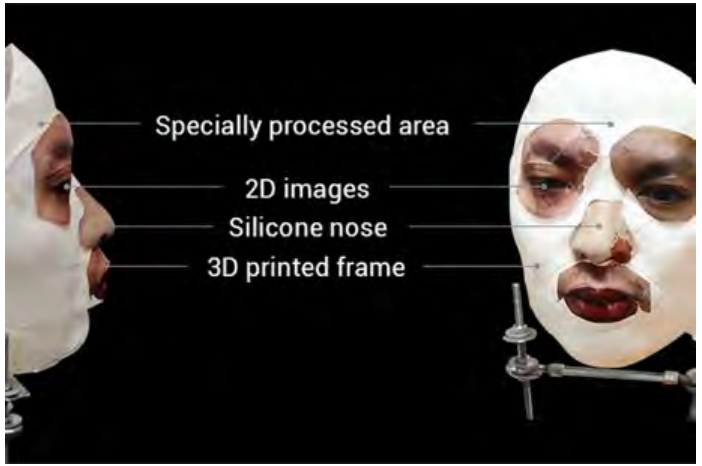
This $150 mask beat Face ID on the iPhone X

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

FINDBIOMETRICS
GLOBAL IDENTITY MANAGEMENT

Researchers Use Tape and Glasses to Spoof Face ID Liveness Detection

August 12, 2019

A team of
Tencent researchers has managed to get past Face ID's liveness detection with a pair of glasses and some tape. To execute the attack, the researchers placed a strip of black tape on each lens. The tape mimics the outline of the eye, while a dot of white tape in the center imitates the iris.

The technique is effective because the Face ID algorithm does not make a complete scan when the user is wearing glasses. Tencent's researchers were able to use the "X-Glasses" to unlock someone's phone and authorize a financial transaction, and presented their findings at the recent Black Hat conference in Las Vegas.

"If you are wearing glasses, [Face ID] won't extract 3D information from the eye area when it recognizes the glasses," explained Tencent's Zhuo Ma.

https://findbiometrics.com/biometrics-news-researchers-use-tape-and-glasses-to-spoof-face-id-liveness-detection/

BBC NEWS

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/

THE VERGE

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

Deepfake Software Fools Voice Authentication With 99% Success Rate

Creating a fake voice to trick authentication systems has never been so easy or effective.

Matthew Humphries • June 28, 2023

Computer scientists at the University of Waterloo figured out how to successfully fool voice authentication systems 99% of the time using deepfake voice creation software.

Andre Kassis, a Computer Security and Privacy PhD candidate at Waterloo, who is also the lead author of this research study, explains how voice authentication works:

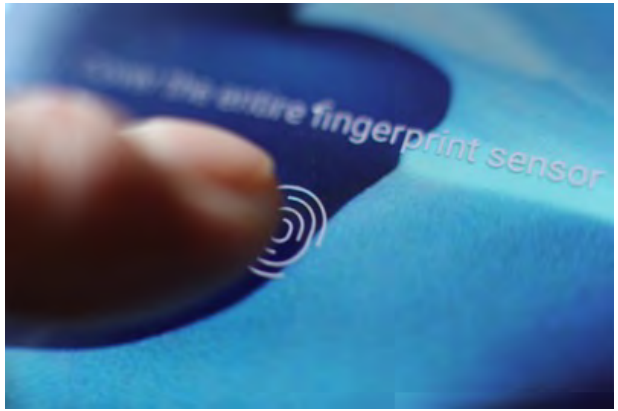
"When enrolling in voice authentication, you are asked to repeat a certain phrase in your own voice. The system then extracts a unique vocal signature (voiceprint) from this provided phrase and stores it on a server ... For future authentication attempts, you are asked to repeat a different phrase and the features extracted from it are compared to the voiceprint you have saved in the system to determine whether access should be granted."

The team at Waterloo beat the authentication by using machine learning-enabled deepfake software to generate a copy of a voice. All the software needs is five minutes of recorded voice audio from which to learn to be a convincing fake. Even spoofing countermeasures employed by the voice authentication systems don't flag the fake voice because a program written by the team removes markers from the deepfake audio that "betray it is computer-generated."

https://www.pcmag.com/news/deepfake-software-fools-voice-authentication-with-99-success-rate

engadget

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

State government fixes bug exposing Aadhaar biometric records

BIOMETRIC UPDATE.COM

Philippines responds to breach allegations

Chris Burt • Oct 13, 2023

Fingerprint biometrics submitted to India's national ID system, Aadhaar, have been exposed by the West Bengal state government website, TechCrunch reports.

Security researcher Sourajeet Majumder found and reported a bug that exposed Aadhaar digital ID numbers, identity documents, photographs and images of fingerprints on the e-District web portal. Soon after he reported the bug to government cybersecurity body CERT-In and the West Bengal government, it was fixed, according to the report.

The bug allowed a prospective attacker to guess sequences of 16-digital deed application numbers, and publicly available tools enabled valid numbers to be identified based on responses from the server.

The fear is that a malicious attacker may have discovered the path to people's biometrics before Majumder reported it and could use the data to mount spoof attacks. The Unique Identification Authority of India (UIDAI) recently implemented liveness detection for fingerprint biometrics to stem incidents of fraud carried out with presentation attacks against the Aadhaar-enabled Payment System.

https://www.biometricupdate.com/202310/state-government-fixes-bug-exposing-aadhaar-biometric-records

Risk-Based Authentication

Multi-factor authentication is more secure

…but more of a pain for users

What's the likelihood that a user's account was compromised

… if they're connecting from their laptop at home?

… if they're connecting from a remote country?

… if they're connecting at an odd time of day?

Does it matter if they're connecting to a company server with highly sensitive information or something mundane?

Can we assess the risk of access being malicious and adjust our authentication policy?

Risk-Based Authentication (RBA)

RBA is a form of Adaptive Authentication

- **Assess risk of access**
  - Depending on the level of risk:
    - Use credentials stored in a browser's cookies
    - Accept just a password or a push notification for a one-time password
  - Or ask the user for additional information:
    - Password
    - App-generated one-time password
    - Email/SMS one-time password
    - Security question
    - Biometric information

How do we assess risk?

Risk score = *f*(user, device, location, destination, connection, time)

- **User**
  - High-value user: e.g., admin, executive – someone with lots of access?
  - Past history: past compromises, training
- **Device**
  - Corporate managed device (e.g., a user can't install random crap)?
  - Known device for that user?
  - Status of anti-malware software and malware reports
- **Location**
  - IP address, geolocation (if mobile)
- **Connection**
  - Is it a point-to-point encrypted connection?
  - Is the user connecting via an anonymizing proxy?
- **Time**
  - Is the time or frequency of the connection unexpected for the user?
- **Is the connection to a high-value service?**

Major benefits of RBA

- Balance security and convenience – reduce friction for users most of the time
- Make access difficult for suspicious user
- Rule-based configuration allows an organization to determine which risk factors are the most significant

The End