School of

Engineering and Computer Science

Te Kura Mātai Pūkaha, Pūrorohiko

CYBR 171 T1 2024

Ngā whakapūtanga o Te Haumaru rorohiko

Cybersecurity Fundamentals

Authentication II

tokens (*software*) and biometrics

Learning goals

- How **software tokens** can be classified in terms of types of passwords and connectivity.
- Identify software token vulnerabilities.
- Explain why software tokens are more vulnerable than hardware tokens.
- Discuss why it is important to have 2FA and MFA.
- Explain biometric-based authentication techniques
- Identify biometrics vulnerabilities
- Discuss issues related to facial recognition systems

Ways to authenticate users

The four means of authenticating user identity are based on:

Something the individual **knows**

- Password, PIN, answers to prearranged questions

Something the individual **possesses** (token)

- Smartcard, electronic keycard, physical key

Something the individual **is** (static biometrics)

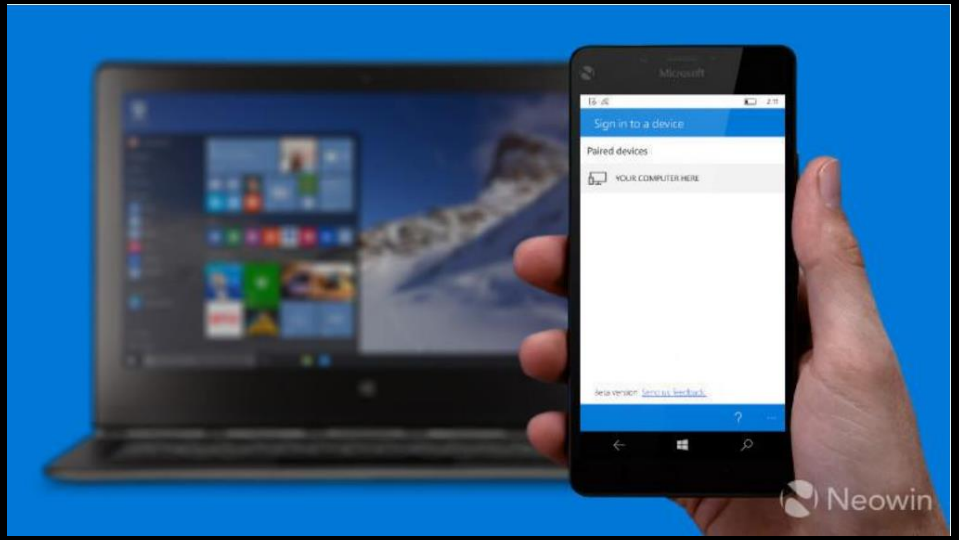
- Fingerprint, retina, face

Something the individual **does** (dynamic biometrics)

- Voice pattern, handwriting, typing rhythm

Can used **alone** or in **combination**, for example, **two-factor authentication**.

PART I:
Software Tokens



Ways to classify (*software*) tokens

- Password type
  - Fixed
  - Dynamic
    - One time password
    - Challenge-response

- Connectivity
  - Disconnected
  - Contact
  - Contactless

Example: Google Authenticator

Google authenticator supports both TOTP and the mathematical-based OTP

Supported by many websites and applications (for example, Wordpress above)

Loss and theft

- An attacker might gain access to the device
- As for hardware token can use for access
- **Easier to steal shared secrets from software**
  - Exploit tools for migrating from one phone to another
  - Get root on device and steal secrets directly

Virus infection

- The attacker installs **virus** on device running the software
- The attacker can **eavesdrop**, **control** what software token does, etc.
- Attacker might **remotely extract secrets** to allow copy of the software token to be created

> Stealing private keys is often accomplished with a computer virus. This type of malware emerged in early 2011, using keyloggers and other classic techniques to find data that looks like a bitcoin wallet private key, or a whole wallet data file full of them.
>
> The largest attack of this kind was conducted with the Pony botnet in 2014, which stole a variety of personal information from millions of users. The criminals behind the malicious code got away with about US$220,000 worth of various cryptocurrencies, from its many victims.

https://bravenewcoin.com/insights/bitcoin-stealing-malware-evolves-again

PART II:
2FA and *MFA*

2-Factor Authentication (2FA)

- Two factor because "**what you know**" (password) + "**what you have**" (device)
- Phone-based authentication uses SMS text message with **special code** and must enter this to complete verification
- WebAuth is browser standard to work with NFC tokens
- Google Authenticator for 2FA
- Increases the ***attacker workload*** – choose someone else.

Resistance to 2FA

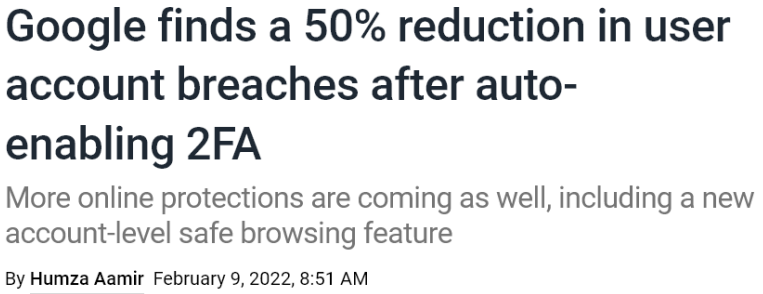
- Must **carry your device** with you
- Can **lock yourself out** of your services
- Take up can be **slow** forcing autoenrollment

Over 90 percent of Gmail users still don't use two-factor authentication

53

The security tool adds another layer of security if your password has been stolen

By Thuy Ong | @ThuyOng | Jan 23, 2018, 8:30am EST



Google finds a 50% reduction in user account breaches after auto-enabling 2FA

More online protections are coming as well, including a new account-level safe browsing feature

By **Humza Aamir** February 9, 2022, 8:51 AM

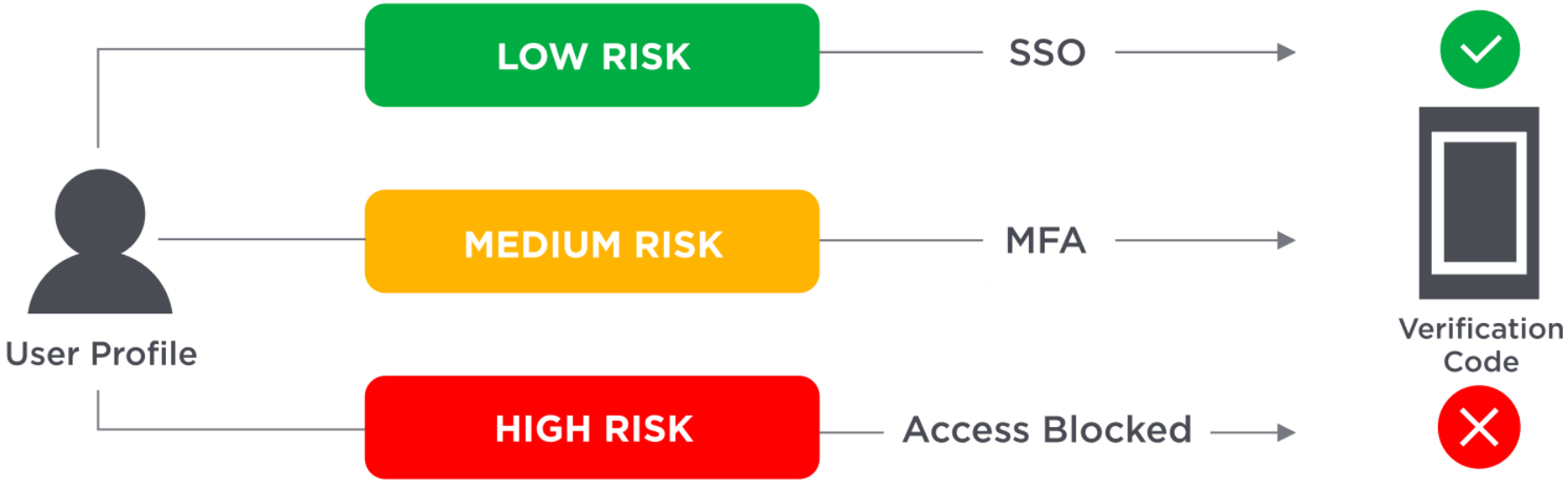
Phone-based Authentication (SMS)

- Most common 2FA but **not appropriate** for high-value targets and deprecated by NIST since 2016
- SIM swap scams
  - port number to new phone
  - in person or over the phone
  - Twitter's CEO Jack Dorsey (2019)
- Cell network hack
  - Signalling System 7 protocol
  - Connects mobile phone roaming globally
  - German banks (2017) and UK Metro Bank (2019)

Multifactor Authentication

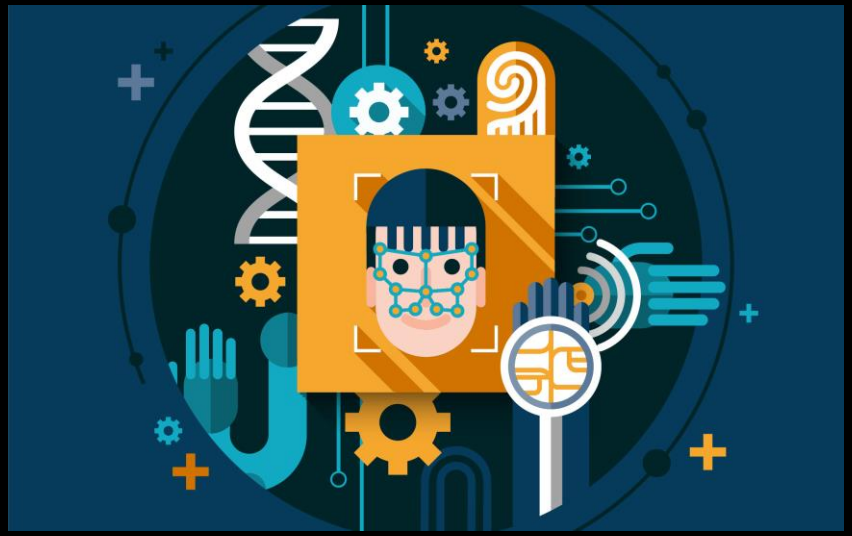
- Increase workload further using multiple factors instead of two.
  - Email, location, tokens
- **Adaptive authentication** is also a subset of MFA
  - Where are you
  - When is it happening
  - What device is used
  - Connection via a private or public network
- Calculate risk level and choose the authentication method or multiple factors to use
- Also known as **risk-based authentication**

Multifactor Authentication



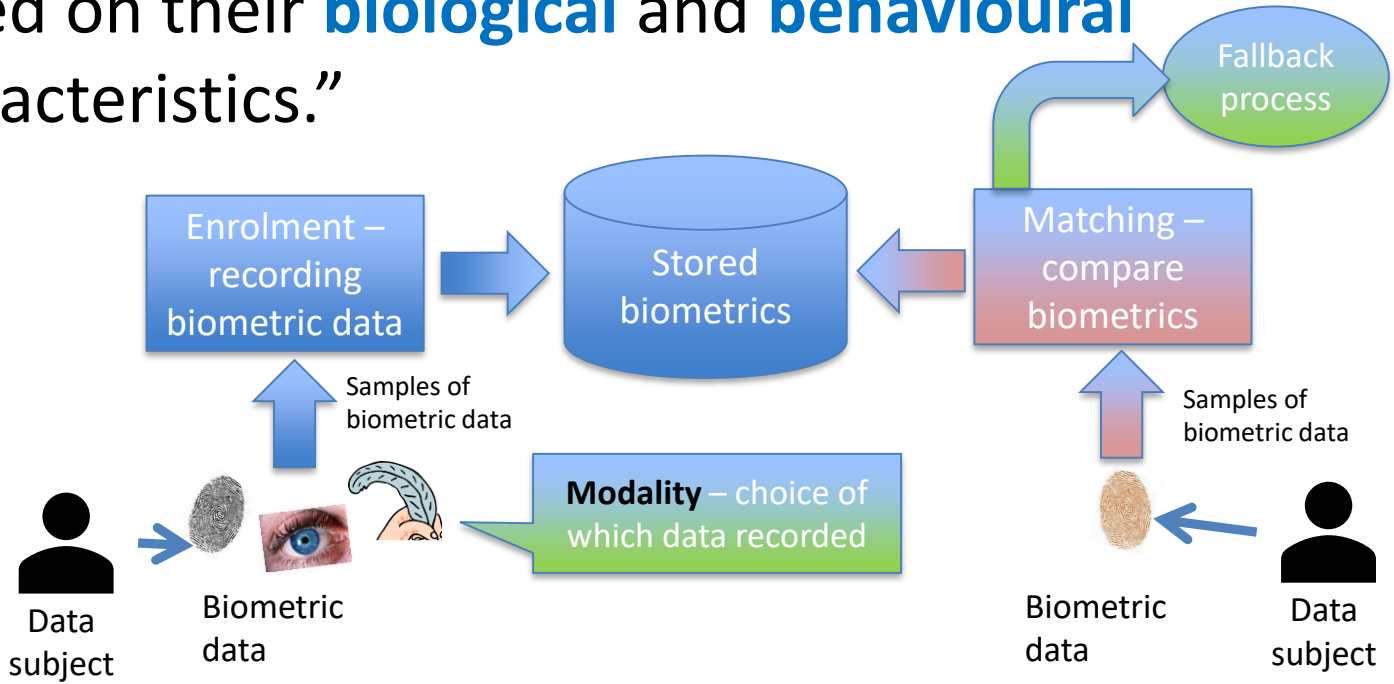
https://www.onelogin.com/learn/what-is-mfa

PART III:
Biometrics



Always need a fallback process

- Biometrics "The automated recognition of individuals based on their **biological** and **behavioural** characteristics."



https://www.ncsc.gov.uk/collection/biometrics/understanding-biometrics

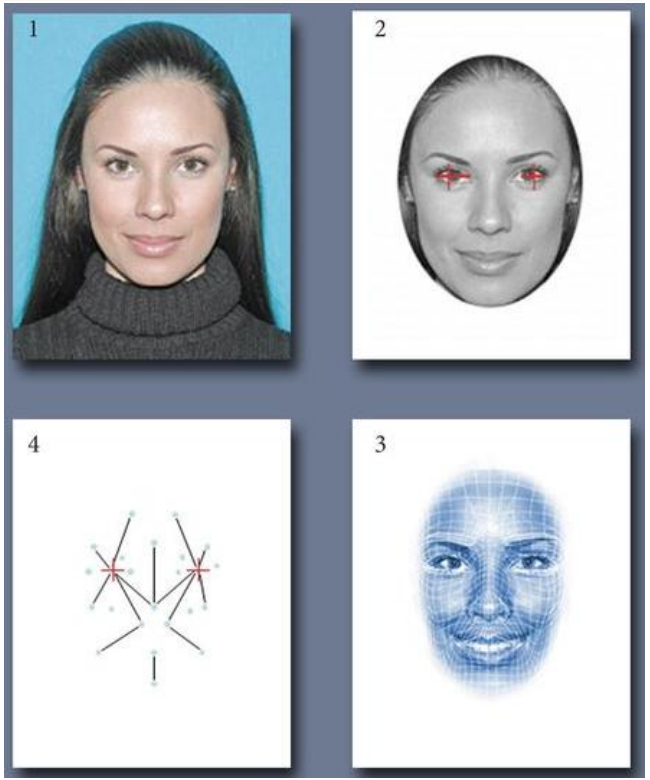
Static versus dynamic and multimodal

- **Static**
  - Requires capturing a single sensor reading
  - Photo, hand geometry etc.
- **Dynamic**
  - Requires capturing multiple sensor readings
  - Voice, gait (way you walk)
  - Harder to fake (currently)
- **Multimodal**
  - Two or modes required e.g. fingerprint and photo
  - Can be combined with MFA to be multimodal MFA

Example: Face Recognition

How facial identification works

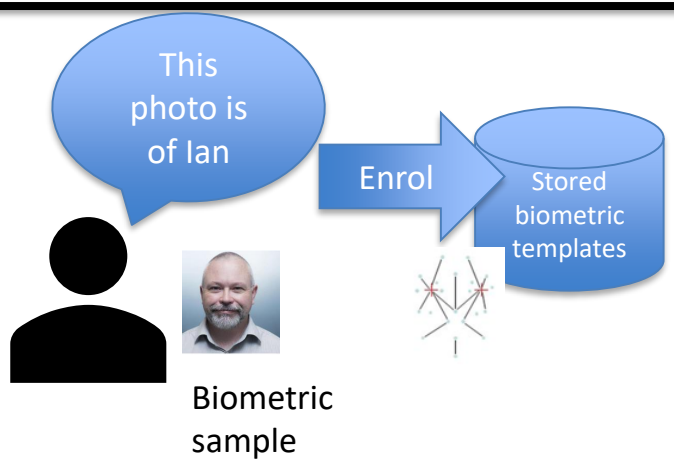
1. Image is captured
2. Eye locations are determined
3. Image is converted to grayscale and cropped
4. Image is converted to a template used by the search engine for facial comparison results
5. Image is searched and matched using a sophisticated algorithm to compare the template to other templates on file
6. Duplicate licenses are investigated for fraud

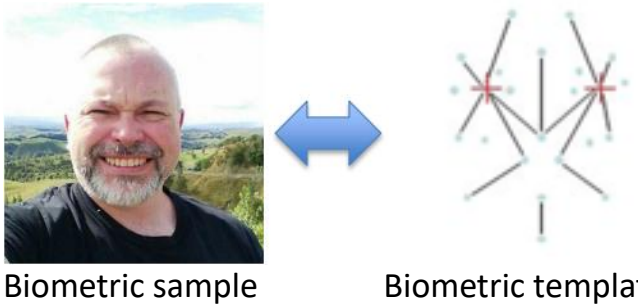


https://www.eff.org/pages/face-recognition

Identity and Authentication

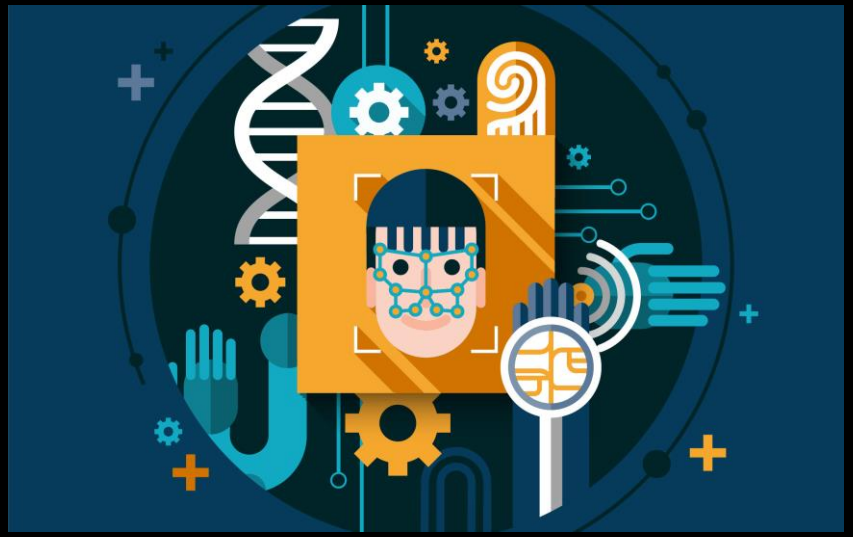
- Two related but distinct concepts.
- **Identity** "This is Ian's photo," e.g. Proving to someone that the biometric does belong to that individual. **Used at enrolment time**.
- **Authentication** "I claim to be Ian" e.g. Matching a picture to a template stored in a database. **Used when verifying the claim**.





PART IV:

Biometrics are not black and white



Biometrics doesn't always work

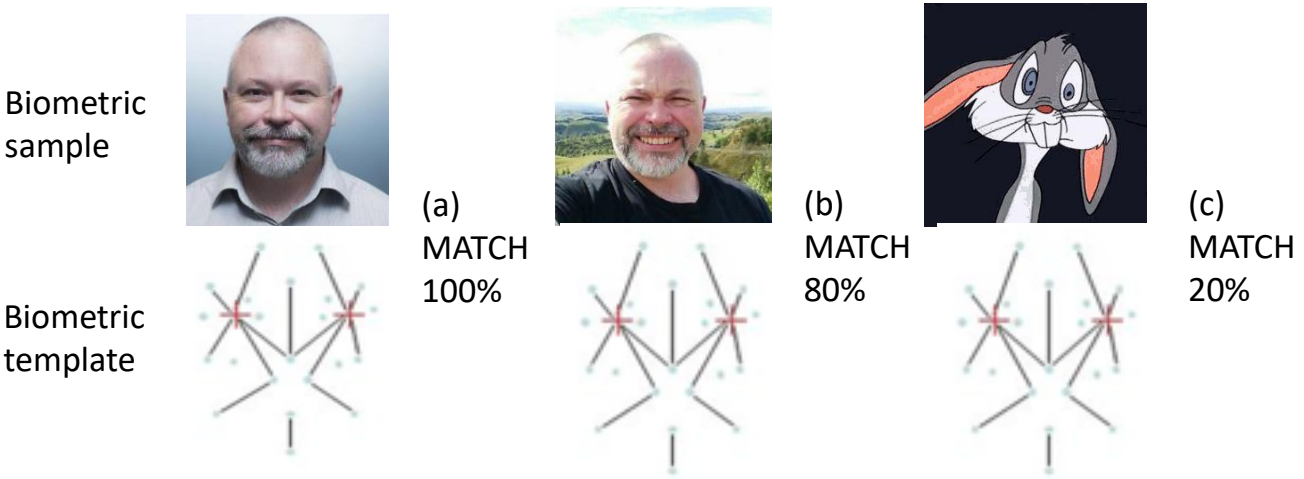
https://www.youtube.com/watch?v=WQxRfbxFnnw&t=7s

How biometric matching works

- Specific to the biometric and implementation, e.g.
  - **fingerprints** - position and number of ridges
  - **voice** – model for each speaker patterns
  - **Iris** – infrared light reveals iris pattern
  - **Face recognition** – 3D, 2D, digital photographs & video
- The **matching score** is calculated based on comparing the **biometric sample** with the **user's template** e.g.
  - Percentage
  - The ratio of matched to unmatched features
  - Dimensionless number
- The **match threshold** is the value at which reasonably certain there is a match

Example: Choosing a threshold

- Threshold of 100% - yes to (a) but not (b) and (c)
- Threshold of 80% - yes to (a) and (b) not (c)
- Threshold of 15% - yes to (a), (b) and (c)



Biometric errors

- **Matching is not TRUE of FALSE**
  - Compare this with "**secret you know**" or "**secret you have**"
  - Match score compared with the template
  - Tunable threshold for match or no-match
- **False match** – individual presents themselves to a biometric system and is matched with someone else's record (**=> false acceptance**)
- **False non-match** – enrolled individual presents themselves to a biometric system, but is not matched to their own record (**=> false rejection**)

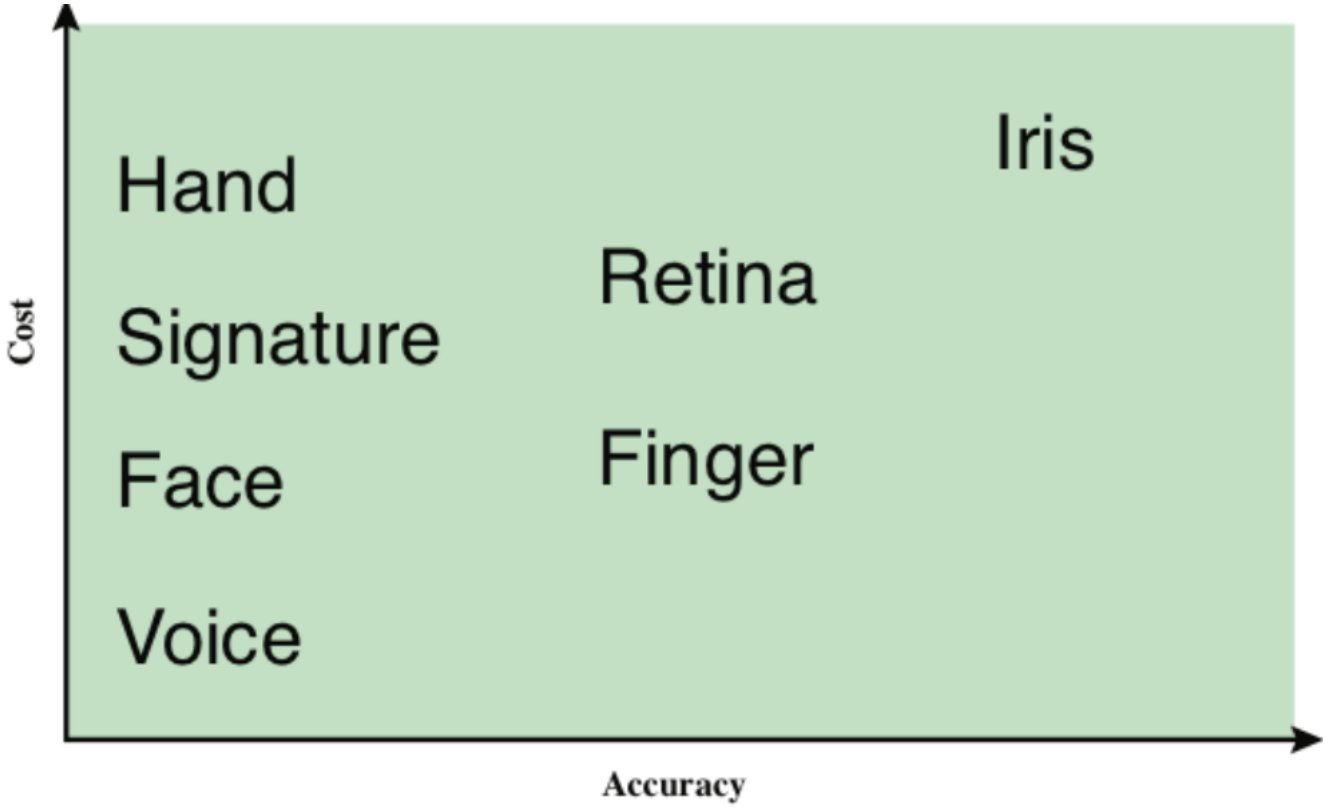
We want to know how often it happens

- **False match rate (FMR)** – the average measure of the propensity of the system **to make the error**
- **False non-match rate (FNMR)** – the average measure of the propensity of the system **to make this error**

Modality	Authentication False match rate (approx.)
Good-quality fingerprints	1 in 100,000
Face recognition	1 in 1000
Single iris recognition	1 in 1,000,000
Voice prints	1 in 10,000

Inverse relationship ***FMR*** and ***FNMR***

Biometrics—*Cost* versus *Accuracy*



PART V:
Spoofing biometrics

What is spoofing?

- Imitate people, companies and even computers.
- Examples:
  - Identify
  - Emails
  - Phone calls
- Attack on **authenticity**
- Potential problem for **biometric** systems

Spoofing Fingerprints

https://www.youtube.com/watch?v=VYI9XNO4XzU

Spoofing Fingerprints

- Key problem is collecting the prints to copy
- Collect latent print from target.
- Latent prints are invisible
- Traces of sweat, oil or natural secretions
- Found on various surfaces e.g. glass
- Hard to get **good-quality prints** without cooperation

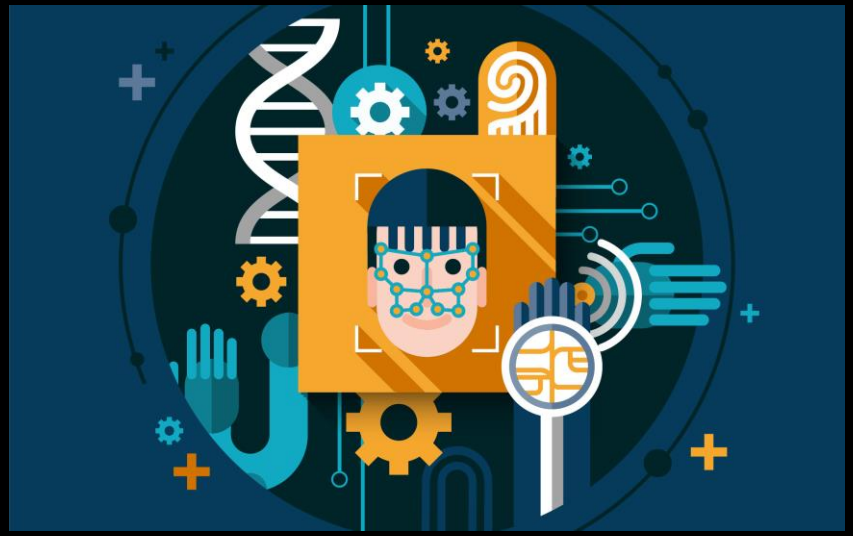
Spoofing Face Recognition

- Face recognition
  - Use a photo of someone else
  - Take a photo or use Facebook
  - Windows Hello face recognition spoofed with photographs – Naked Security (sophos.com)
  - **Adding extra security** through IR and 3D measurements
  - Capture from **live video** and challenge-response

Deep Fakes

- Video and/or audio of a person
- Face or body digitally altered
- For spoofing or to spread false information
- Research into detecting deepfakes using machine learning
- **Guard against by combining with other authentication methods**

PART VI:
Problems related to facial recognition



Identification of individuals

- Identification “Do we recognize these people?”
- Search database for match against biometric

Find criminals, counterterrorism, human trafficking, airport security

Catching a Suspected New York City Subway Terrorist

New York City Police Department (NYPD) detectives used facial recognition technology to identify a man who sparked terror by leaving a pair of rice cookers in the Fulton Street subway station. Within minutes, detectives pulled still images of the suspect from security footage and used facial recognition software to compare them to mug shots in the NYPD’s arrest database. The system returned several hundred potential matches, and after multiple stages of human review, it took NYPD only one hour to identify the suspect.

Is facial recognition discriminatory?

- Facial recognition rates over 90%
- Error rates vary across demographic groups
- “Gender Shades” project 2018
- Similar results when NIST (2019) reviewed 189 algorithms

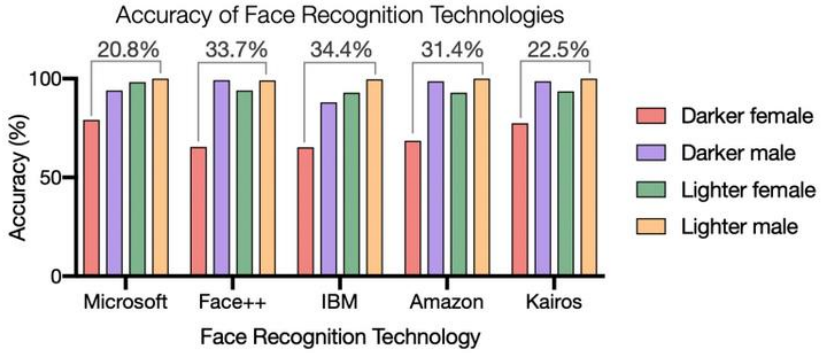


Figure 1: Auditing five face recognition technologies. *The **Gender Shades project** revealed **discrepancies** in the classification accuracy of face recognition technologies for different skin tones and sexes. These algorithms consistently demonstrated the poorest accuracy for darker-skinned females and the highest for lighter-skinned males.*

Training data is predominantly white and male

https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/

In US has led to wrongful arrest

Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match

A New Jersey man was accused of shoplifting and trying to hit an officer with a car. He is the third known Black man to be wrongfully arrested based on face recognition.

Aotearoa context

TE AO MĀORI / TECHNOLOGY

Police facial recognition discrimination against Māori a matter of time - expert

6:41 pm on 2 September 2020

Share this

Meriana Johnsen, Journalist
meriana.johnsen@rnz.co.nz

It is only a matter of time before a Māori person is wrongfully arrested because of a false match on facial recognition software, a Māori technology expert says.

https://www.police.govt.nz/news/release/police-release-findings-independent-expert-review-facial-recognition-technology

PART VII:
What’s next

Advantages and Disadvantages

Advantages	Disadvantages
Strong link with biometric and individual	Determined attackers can defeat them
Find multiple records belonging same individual	Some people are excluded from using it
Some cases biometrics faster and more convenient	Variability between two captures lead to errors
Additional security measure	Cannot replace compromised biometric characteristics
	Results can be discriminatory against some demographics

What's up next

- Lab2 was out yesterday, please continue to work on it
- Friday – guest lecture Jack Moran and Jim Rush
- Next week, we will look at **software threats** in the form of malware and viruses.