Evolving world of biometric authentication

UNIVERSITY OF PLYMOUTH

Session Outline

- User authentication:
  - Passwords & tokens
  - Biometrics
  - Capabilities and limitations
  - Liveliness
- Tools for this session:
  - Biometric devices
  - Biometric worksheet

What is authentication?

Authentication is the process to confirm that only the right person can access a device, service, and/or application.

The authentication process includes three primary steps:

- Claim an identity: Users establish who they are typically through a username.
- Authentication: Typically, users prove they are who .
- Authorization: The system verifies that the users have permission to the system that they’re attempting to access.

Arguably the Gatekeeper of cyber security – bypass authentication and attackers can have open access to information and services!

Three forms of authentication

Passwords:

- A string of characters (letters, numbers, and other symbols) that are used to authenticate an identity or to verify access authorization.

Tokens:

- A portable, user-controlled, physical device (e.g., smart card or memory stick) used to generate a code that verifies the user's identity.

Biometrics:

- Measurable physical characteristics or personal behavioural traits used to identify, or verify the claimed identity of, an individual. Facial images, fingerprints, and handwriting samples are all examples of biometrics.

Source: https://csrc.nist.gov/glossary

Password authentication

- Passwords are often badly selected (and easily guessed):
- They might be too short, are made up of personal data such as names, birthdates or dictionary words.
- This makes them vulnerable to password cracking software.
- Passwords written down and discoverable, infrequently changed and used for multiple accounts across multiple systems.

Token authentication

Expensive to implement:

- Introducing token-based authentication could be cost prohibitive for an organization and cost would scale depending on the number of employees being enrolled.

Easily lost or stolen:

- A threat actor might be able to easily obtain a token if the user loses it or the threat actor has opportunity to steal it.

Verify the presence of the token *not* the person

Biometrics authentication

Biometric authentication is based upon something the user is…

- Theoretically biometrics are far more usable, there is nothing for the user to remember and nothing to them to lose or leave behind.

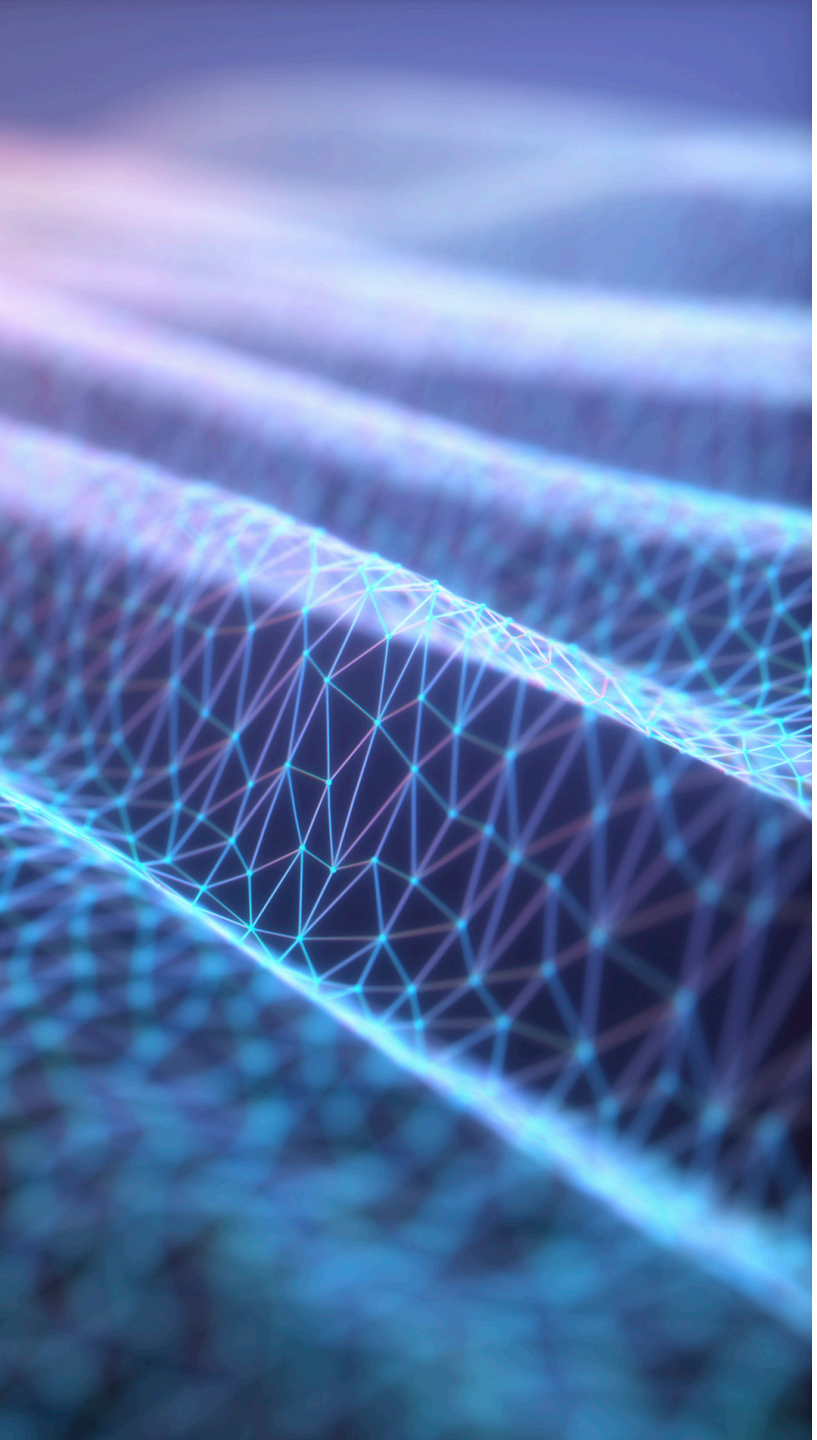
- Practical factors – additional hardware/software required, usability issues and performance concerns

Desirable features of biometrics

- **Uniqueness** - the ability to successfully discriminate people.
- **Universal** - the ability for a technique to be applied to a whole population of users.
- **Permanence** - the ability for the characteristics not to change with time.
- **Collectable** - the ease with which a sensor is able to collect the sample.
- **Acceptable** - the degree to which the technique is found to be acceptable by a person.
- **Circumventable** - the ability not to duplicate or copy a sample.

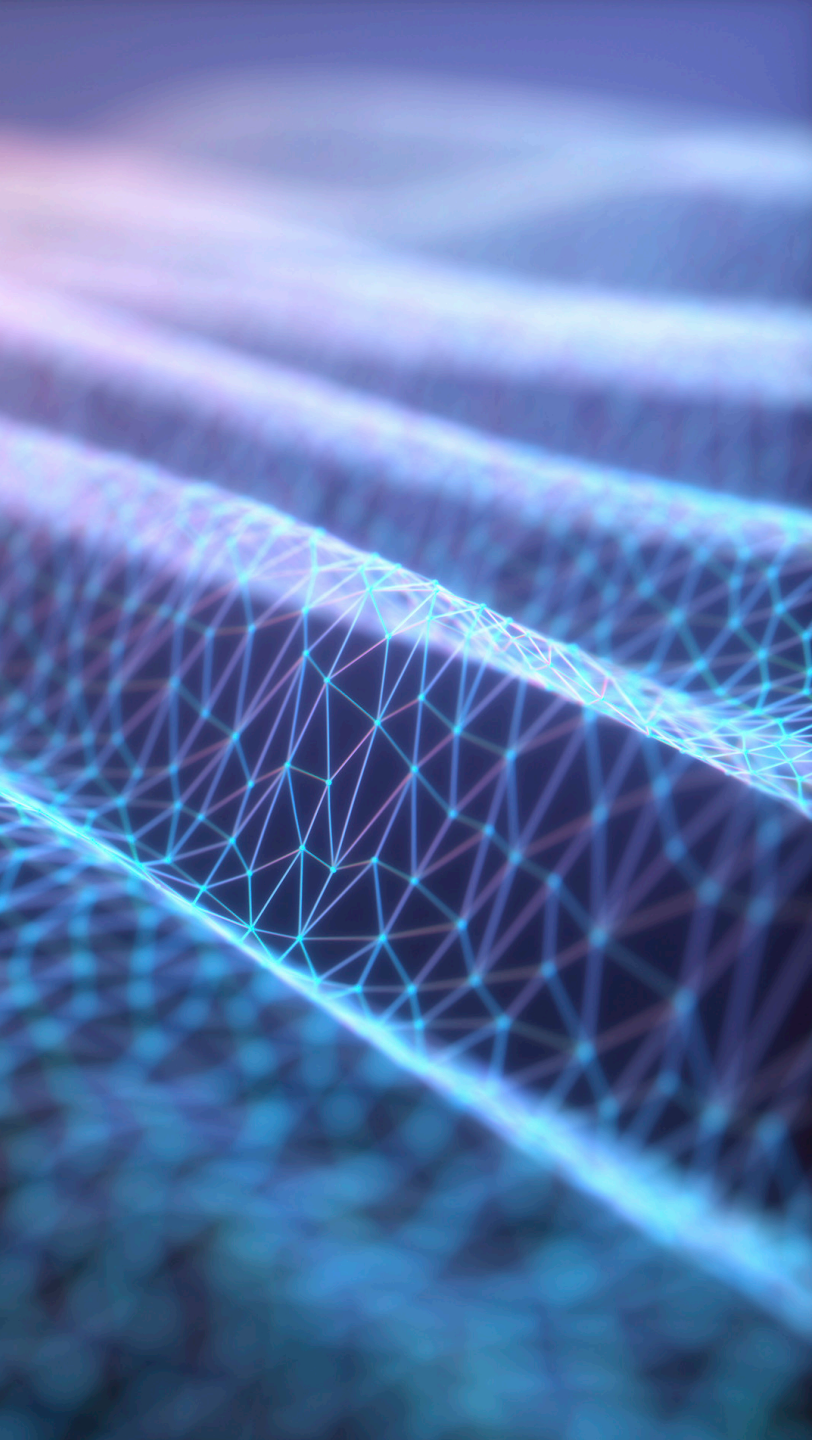
Biometric modalities

Physiological	Behavioural
Fingerprint Recognition	Speaker Recognition
Hand Geometry	Signature Recognition
Vascular Pattern Recognition	Keystroke Analysis
Iris Scanning	Mouse Dynamics
Retinal Scanning	Gait Recognition
Facial Recognition	Stylometry
Facial Thermogram	
Ear print	



Activity: Enrolment on biometric systems

Using the biometric peripherals, have a go at enrolling on each of the systems.



Discuss: Usability and preferences

How usable do you think the three biometric options are?

Do you have a preference to one method in particular?

How do you think each of the modalities are used in practice?

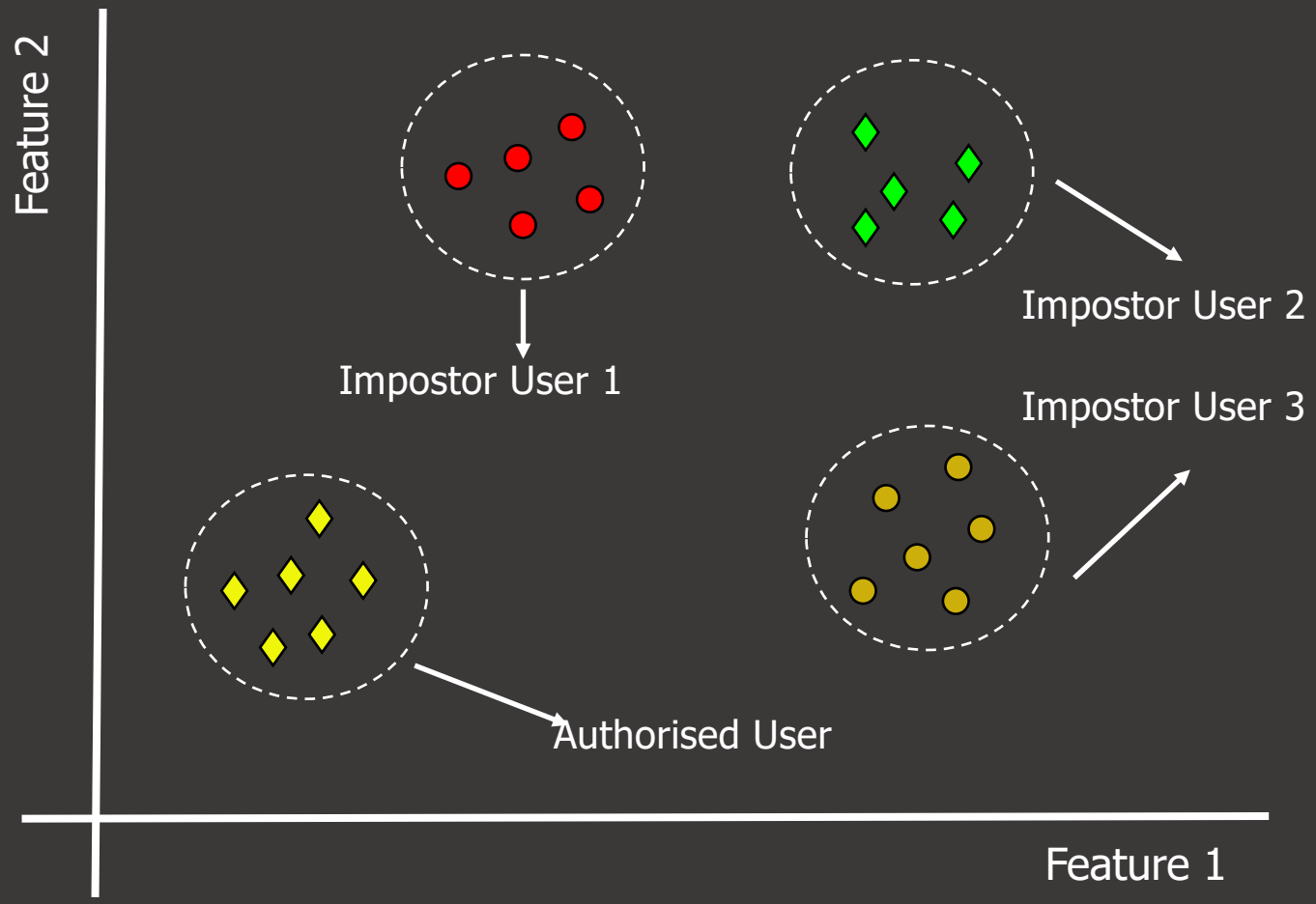
Feature vectors

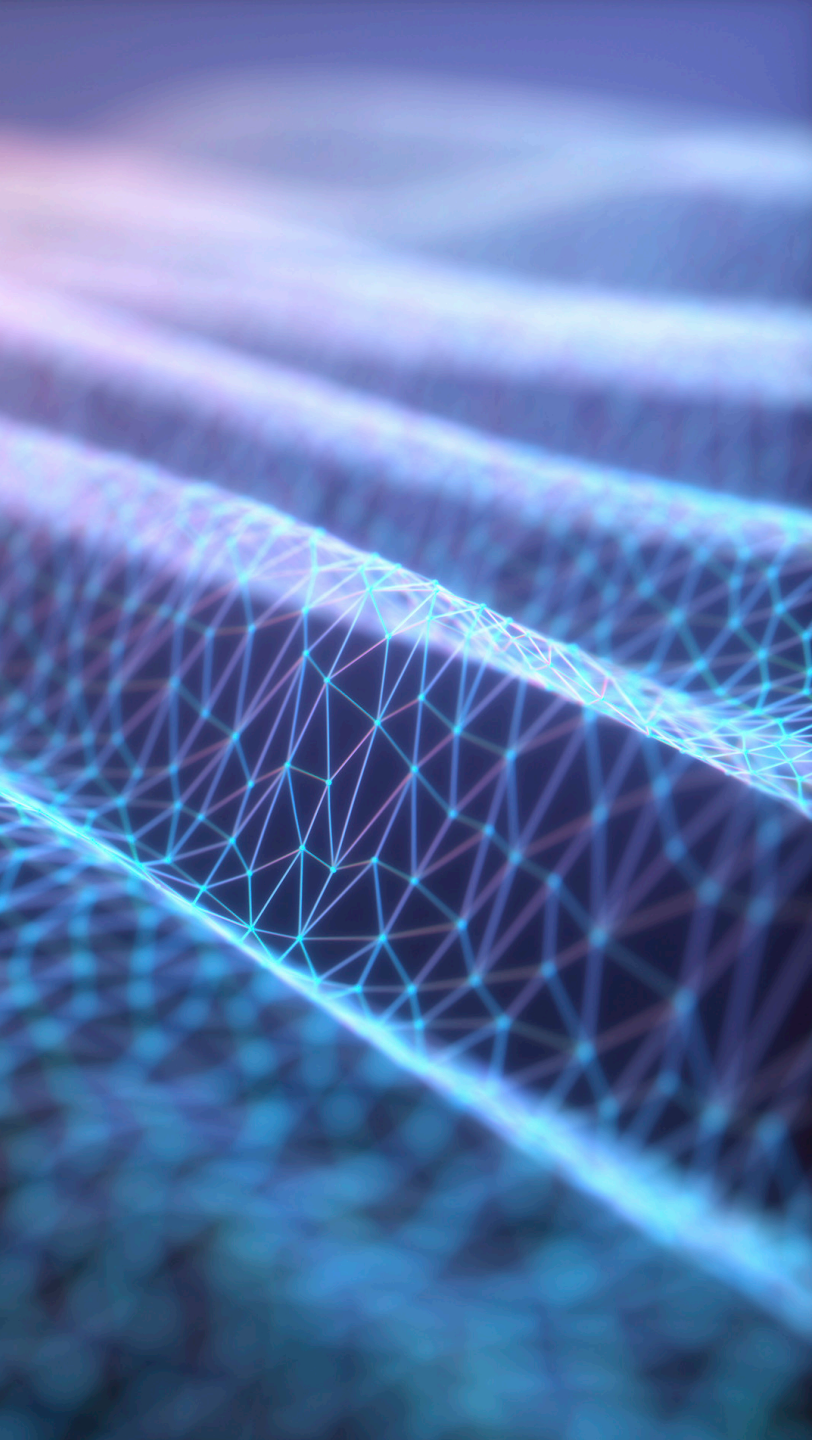
A biometric feature vector is a representation of the unique characteristics or features from a given biometric sample.

Each element in a feature vector represents an aspect of the modality:

- The texture from a fingerprint can be measured using the ridges and bifurcations that are unique to everyone.
- Specific sections of the human iris can be isolated and compared using high resolution imagery.
- In facial recognition, an algorithm might measure the location of different facial features (e.g. the distance between an individual's eyes or the distance between their nose and mouth).

Pattern Classification





Activity: Biometric scores

Going back to the biometric technologies, verify on each of the biometric systems and compare the scores that you get for each.

Fill out the worksheet as you try each of the different systems.

Biometric decision boundaries

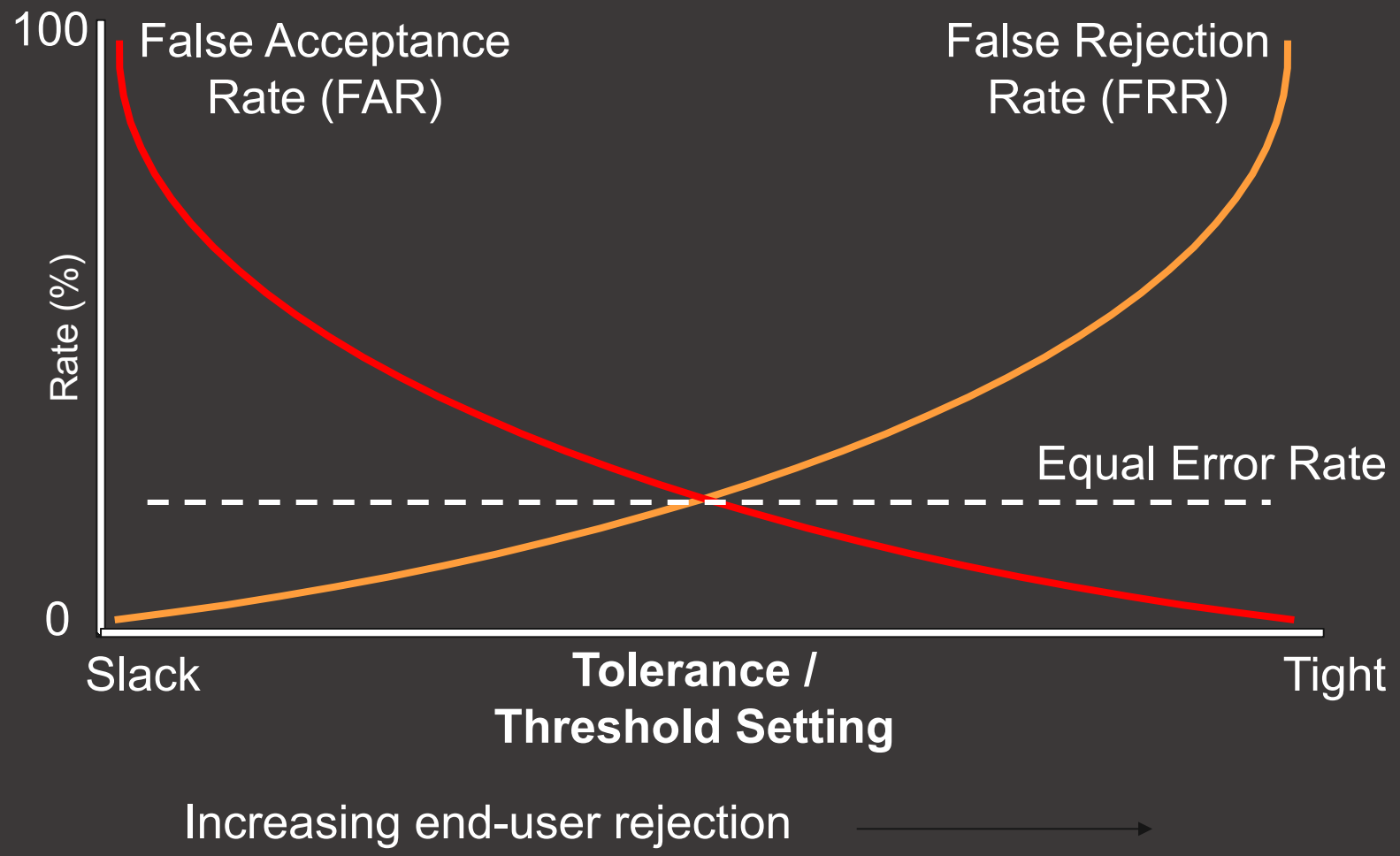
The biometric scores are based upon the feature vectors of each of the modalities – iris, fingerprint, facial recognition etc.

Comparison of those features through decision boundaries are used to distinguish between different inputs and either classify input as a ‘match’ or ‘no-match.’

These decision boundaries exist in mobile phone biometrics - to unlock or in passports for international travel.

What score is likely to be sufficient for a match?

FAR / FRR relationship

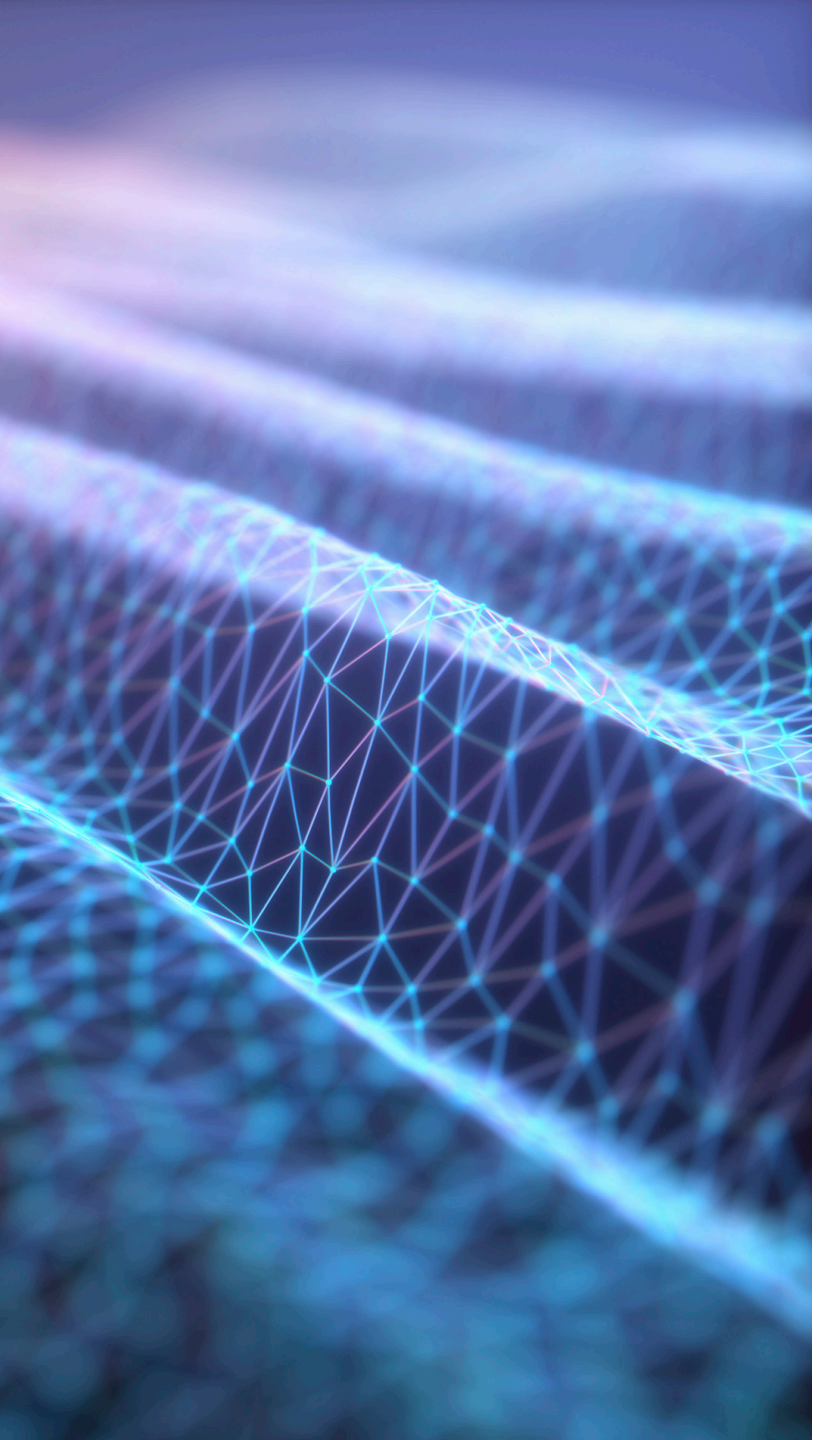


False rejection and false acceptance

False rejection - When a legitimate user who should be confirmed as a ‘match’ by the biometric system is incorrectly confirmed as ‘no-match’ and denied authentication.

False acceptance – When an illegitimate user or a threat actor is incorrectly confirmed as a ‘match’ by the system when a decision should have classified them as ‘no-match.’

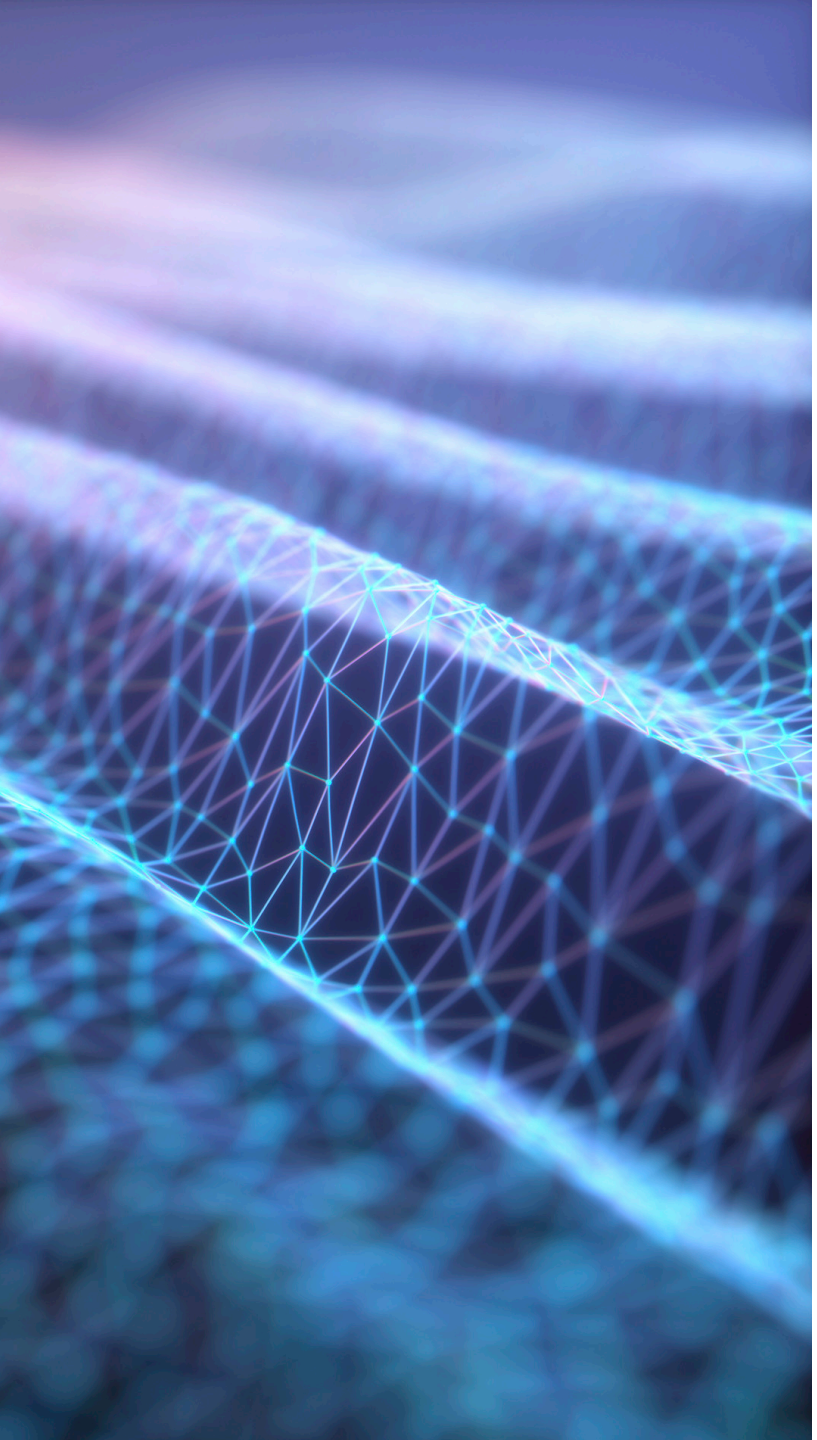
When Google first introduced facial recognition on their mobiles – a photograph of an individual could result in a ‘match.’



Activity: Varying inputs

Enroll on the biometric systems again, but this time try providing your biometric input in different ways.

- With your fingers, try your fingertips or the sides of your fingers.
- With your face, try from further away or with other people in view, use a photograph (from a mobile phone).
- With your eye, try looking to the side, or slightly closing your eye.



Discuss:
Issues with variance

What did you notice, what issues came up when you tried to enroll this time?

Liveliness tests

Liveliness tests help a biometric system determine whether an input sample is authentic – such as a real person rather than a photograph.

Fingerprint liveliness detection:

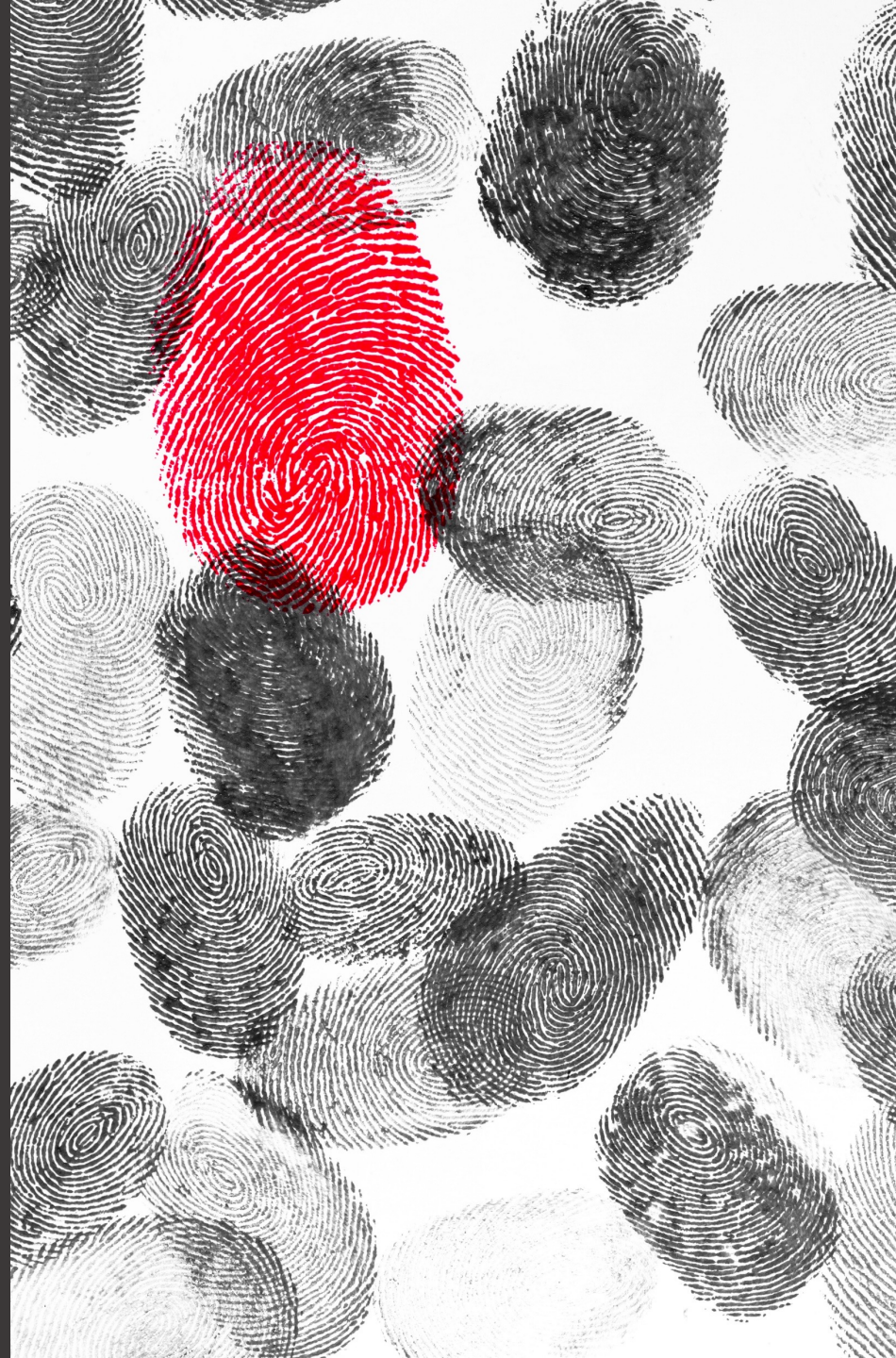
- Analysing Sskin distortion, blood flow, sweat pores

Facial Liveliness Detection:

- Analysing blinking, eye movement, or subtle facial muscle movements.

Iris Liveliness Detection:

- Analysing pupil dilation, eye movement, or the response to light stimuli.



Implementation effectiveness

Compared to passwords and tokens, biometrics offer a much more robust method for authentication.

However, the effectiveness of biometric systems depends on how comprehensive the system is and how well it is implemented.

A poorly implemented biometric system will be able to be bypassed with the aid of fingerprint moulds or high-resolution photographs.


Any Questions?
Thank You