

Computer security Lecture 3

Identification and Authentication
Biometrics

Ingo Hölscher

You will hear about:

- *ACL – access control list (extra)*
- Authentication vs authorization
- Biometrics
 - Basics / Characteristics
 - Difficulties with biometrics
 - Biometric techniques
 - Attacks on biometrics
 - Future – Present in biometrics

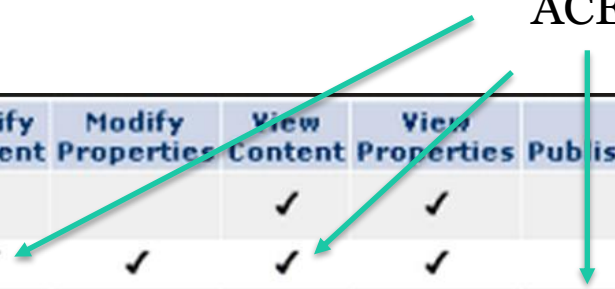
Access Control List (ACL)

- A table (list) that defines which access rights a user (group) has to a particular object
- Example: John Doe,
deny/read/write/full/execute/full/ ...
(-/r/rw/x)

	Title	Owner Control	Promote Version	Modify Content	Modify Properties	View Content	View Properties	Publish	Remove
	#AUTHENTICATED-USERS					✓	✓		☐
	HR_Managers		✓	✓	✓	✓	✓		
	QSAdmins	✓	✓	✓	✓	✓	✓	✓	☐
	PWDesigner					✓	✓		☐

Access Control List (ACL)

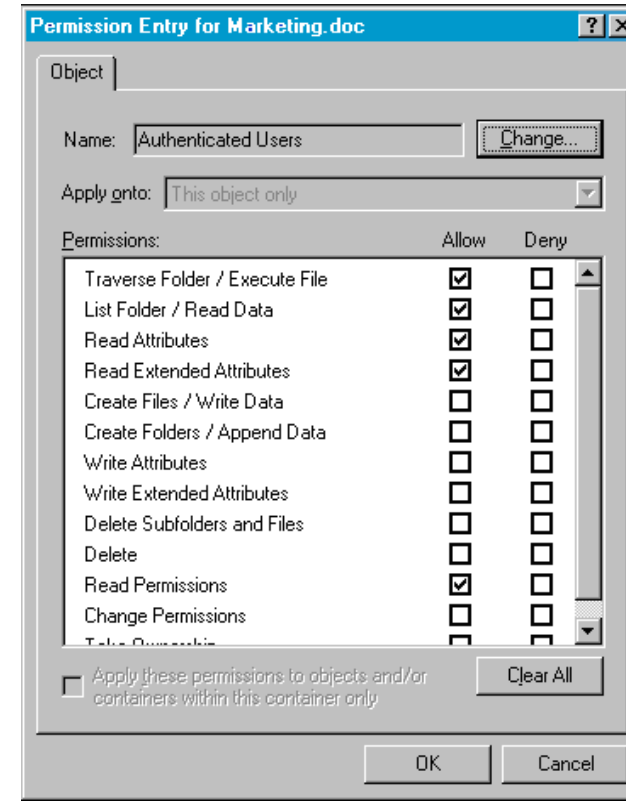
- A table (list) that defines which access rights a user (group) has to a particular object
- Example: John Doe,
deny/read/write/full/execute/full/ ...
(-/r/rw/x)



	Title	Owner Control	Promote Version	Modify Content	Modify Properties	View Content	View Properties	Publish	Remove
	#AUTHENTICATED-USERS					✓	✓		☐
	HR Managers		✓	✓	✓	✓	✓		
	QSAdmins	✓	✓	✓	✓	✓	✓	✓	☐
	PWDesigner					✓	✓		☐

Access Control List (ACL)

- Good control to check if user is authorized to a resource
- Difficult to manage



Authentication vs. Authorization

- Authentication
Verifying the **identity** of a user
- Authorization
controlling **what** resources a user has access to after authentication
- Authorization is **not** authentication

Authentication vs. Authorization

Step 1

Authentication by/via

- login user/pwd
- ID-token/PIN
- certificates
- Other authentication methods



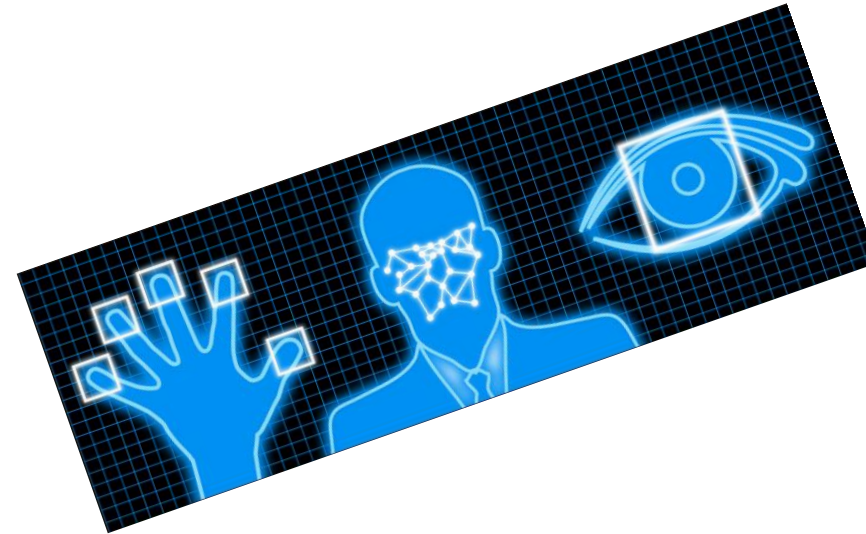
Step 2

Authorization

Decision about permission
to access a certain resource.
ACL

Authentication modes

- **Something you know**
(passwords, PIN, ...)
- **Something you have**
(keys, badges, tokens, smart card, ...)
- **Something you are**
biometrics (handwriting, fingerprints, retina patterns, ...)



Biometrics

The science of using biological properties to identify individuals

www.lexias.com/html/glossary1.html

Identification of people by measuring some aspect of individual anatomy or physiology, some deeply ingrained skill, or other behavioral characteristic, or something that is a combination of the two

www.primode.com/glossary.html

Characteristics for biometrics

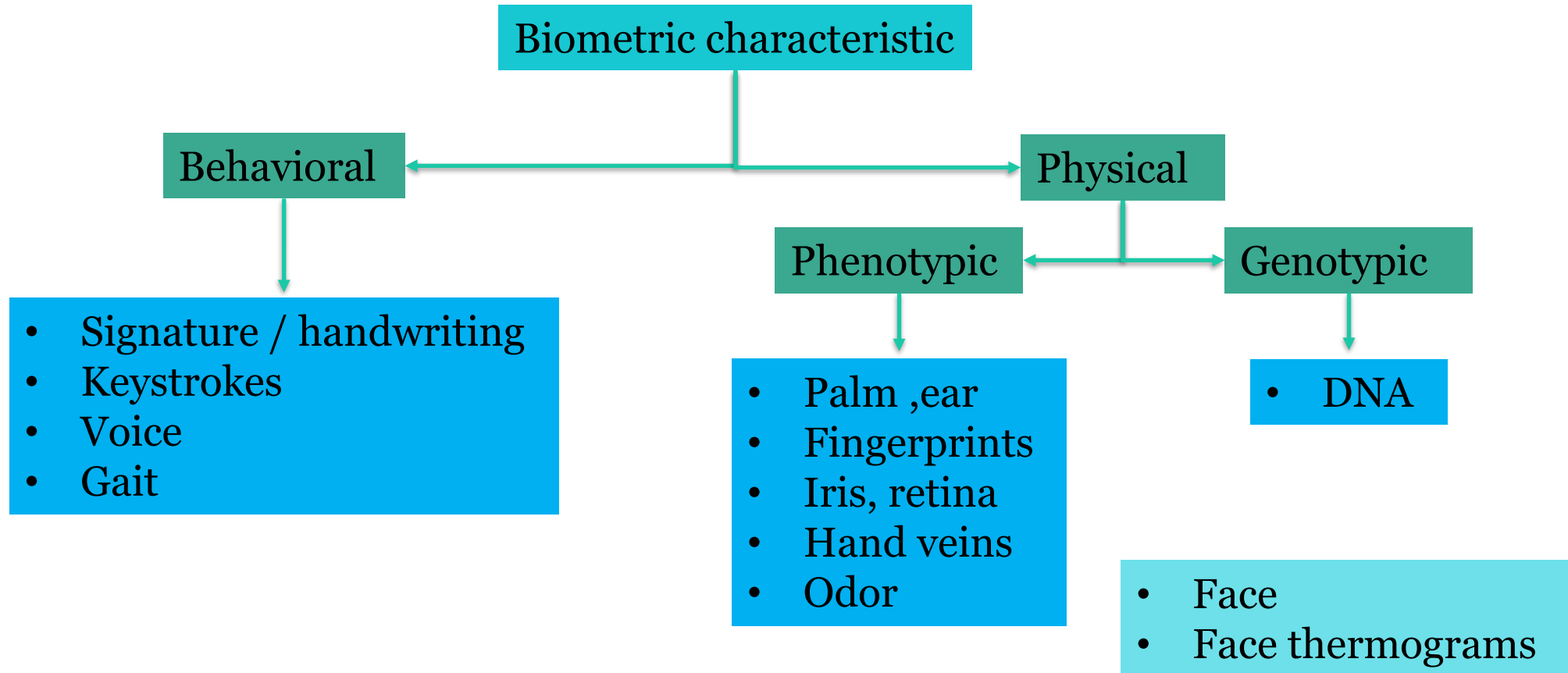
➤ Basic requirements

- **Uniqueness** - a property must be distinct for different individuals (not a blood group etc.)
- **Permanence** - a property cannot change over time
- **Universality** - everyone (almost) must possess such a property
- **Collectability** - it has to be possible to measure (easily) a property
- **Immunity to circumvention** - it has to be hard to fool the system

Characteristics for biometrics

- Additional requirements
 - **Acceptability** - physical contact considerations, privacy considerations, religious issues, ...
 - **Efficiency** - of acquisition, recognition, storage

Characteristics for biometrics



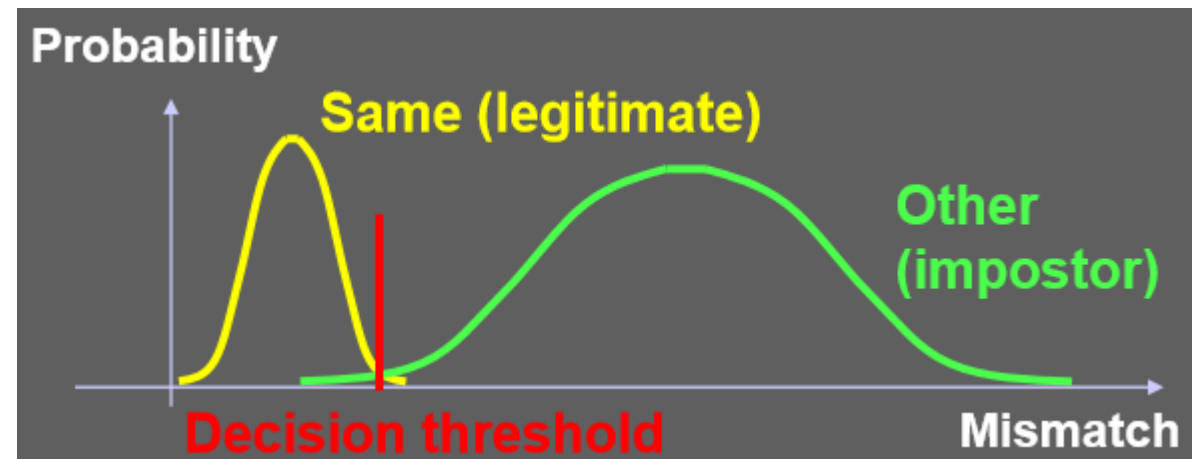
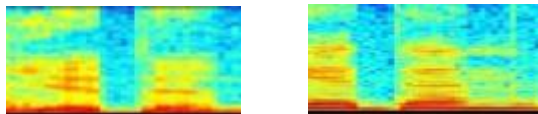
Difficulties with biometrics

- Expectations – fast and reliable recognition
- Reality
 - Samples are never exactly the same

Same face?



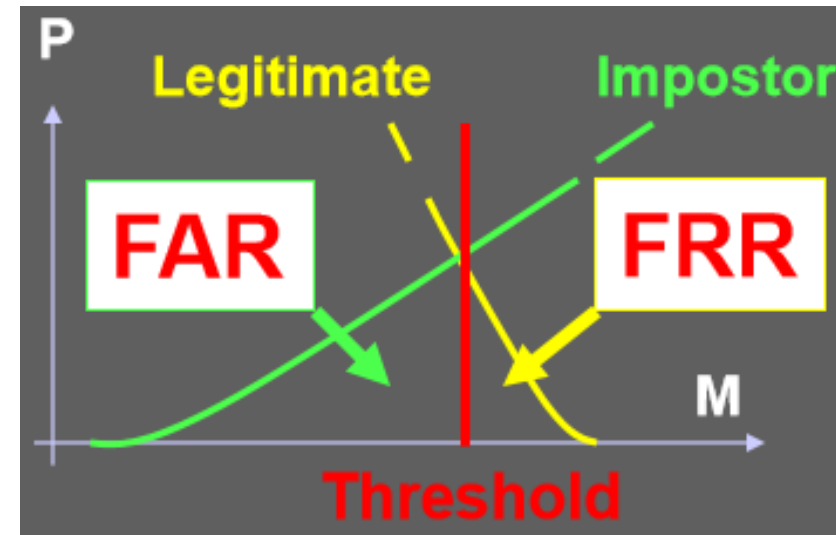
Same speaker?



Difficulties with biometrics

False rejection / False acceptance

- Denying access to legitimate users is called false rejection
- Allowing access to illegitimate users is called false acceptance
- The probabilities of these two failures decide the quality of the biometric system



FAR = False Acceptance Rate
FRR = False Rejection Rate

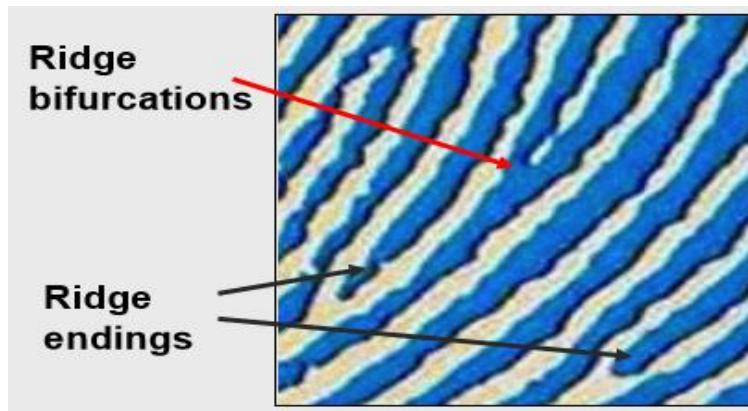
Difficulties with biometrics

- Enrolment not accepted or too complicated
- People without index fingers
- Injury makes authentication impossible
- Human iris change with age
- ...

An overview of biometric techniques

Fingerprint based recognition

- Major current technology
- Earliest records - authentication imprints on clay tables - Babylon, 1700 B.C
- Approved to be a forensic method in Great Britain in 1901



Minutiae features



- No identical fingerprints found among recorded hundreds of millions – uniqueness
- Completely forms in early natal period and remains unaltered permanence
- Most of us have it – universality
- Easy to collect in an acceptable way (subject's cooperation)

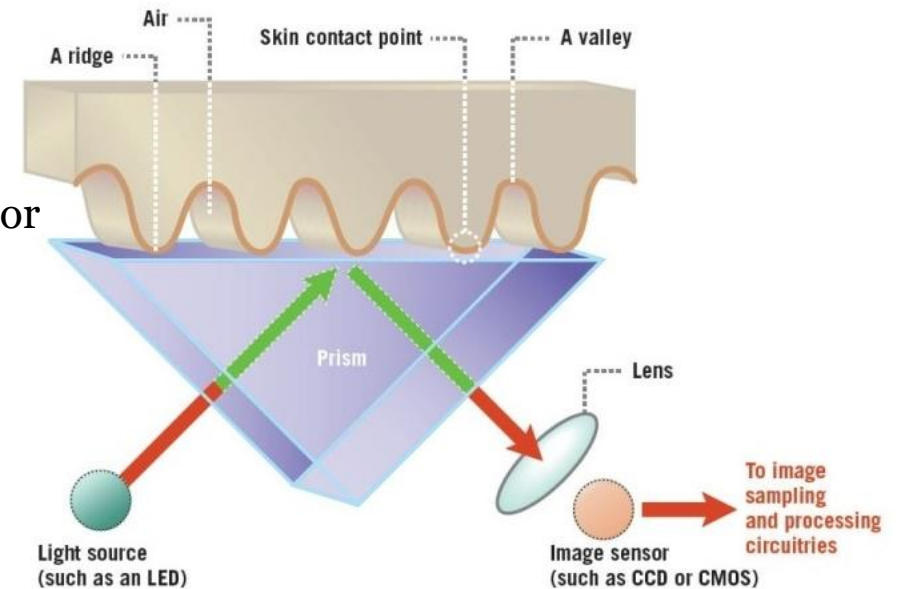
Fingerprint acquisition

➤ Optical readers

- Inexpensive
- Easy to fool (not all types) – photos etc
- Image quality can become low due to dirt (reader or finger), residual imprints etc
- Low-cost, low security systems – PC access



An optical sensor.



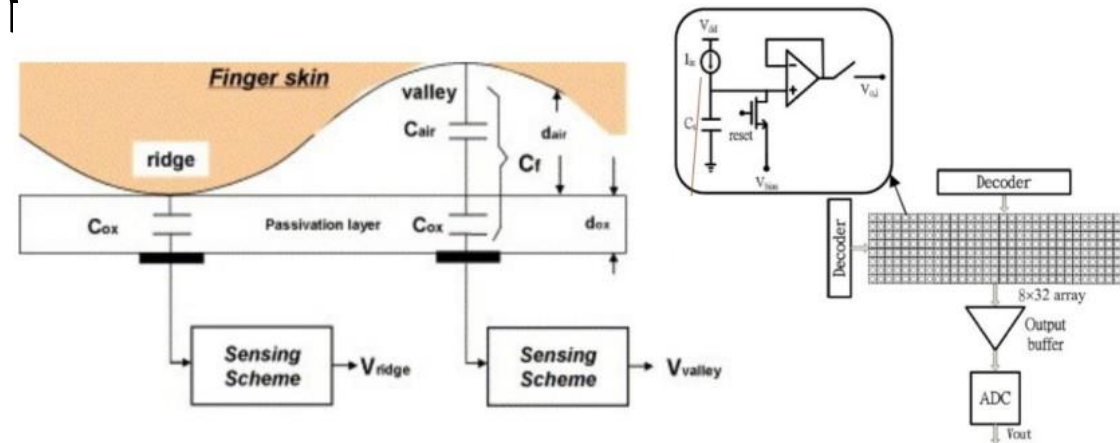
Fingerprint acquisition

➤ Capacitive readers

- Skin surface - a capacitor's electrode
- Quality - usually good
- Rather inexpensive
- Hard to fool

➤ Thermal readers

- A difference in a temperature of ridges (warmer) and valleys (colder) or the air inbetween
- Rather inexpensive, hard to circumvent
- Quality depends on ambient temperature (finger temperature)



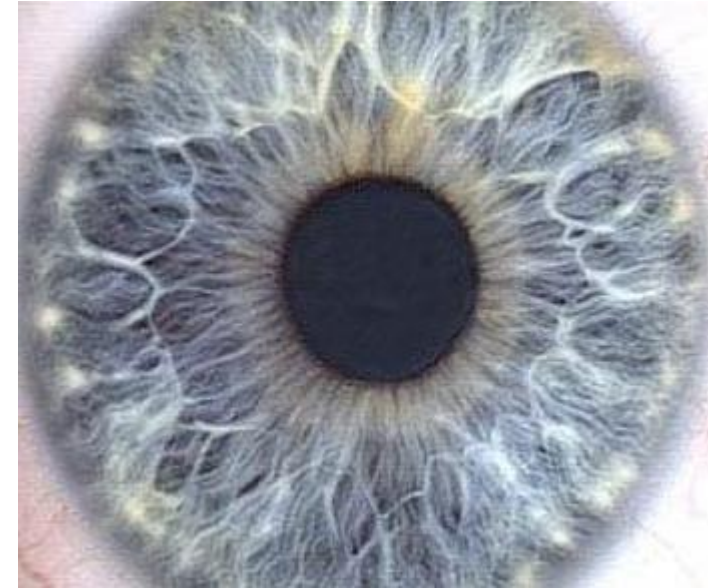
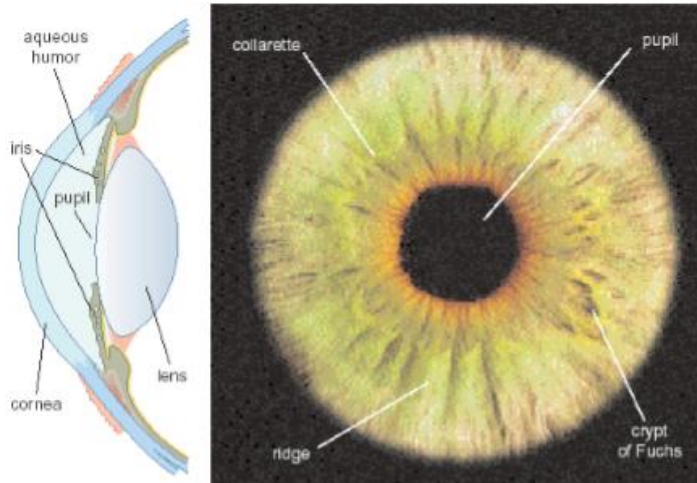
Fingerprint acquisition

➤ **Ultrasound readers**

- Inner layers of skin are subject to scanning by ultrasound
- Expensive
- Considered to be the most difficult (impossible) to circumvent Inner layers of skin are subject to scanning

Iris-based recognition

- **Major prospective technology**
- No identical irises found among recorded hundreds of millions – **uniqueness**
- Completely forms in early natal period - **permanence**



- Most of us have it – **universality**
- Easy to get – **collectability**
- No physical contact nor cooperation required - **acceptability**
- Hard to circumvent

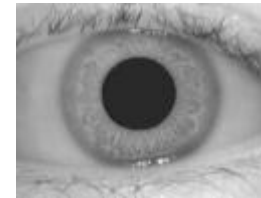
Iris-based recognition

Iris analysis

Visible light



Near infrared



J. Daugman's algorithm (the IrisCode)

Retina-based recognition

- Considered to be the most credible
 - No identical retinas found so far - **uniqueness**
 - Completely forms in early childhood (later changes possible) - **permanence**
 - Most of us have it - **universality**
 - Possible to scan – **collectability**
... but: physical contact required
 - **low acceptability**
 - Objects of interest: veins



Retina-based recognition

➤ Considered to be the most credible

- No identical retinas found so far -

uniqueness

- Completely forms in early childhood (later changes possible)

- Most of us have it - unique

- Possible to scan – collection ... but: physical contact - low acceptability

- Objects of interest: vein patterns



Performance in access-control systems

- Very good
- Natural liveness tests - considered impossible to circumvent
- High-security facilities



Face-based recognition

(facial recognition)

➤ **The most acceptable**

- Surveillance and monitoring systems
- Permanence: **aging, diseases**

➤ **Other challenges**

- Face localization (detection)
- Acquisition errors – illumination, background
- Uniqueness: twins, beard, facial expressions, make-up ...

Sharbat Gula, 1985 : 2002

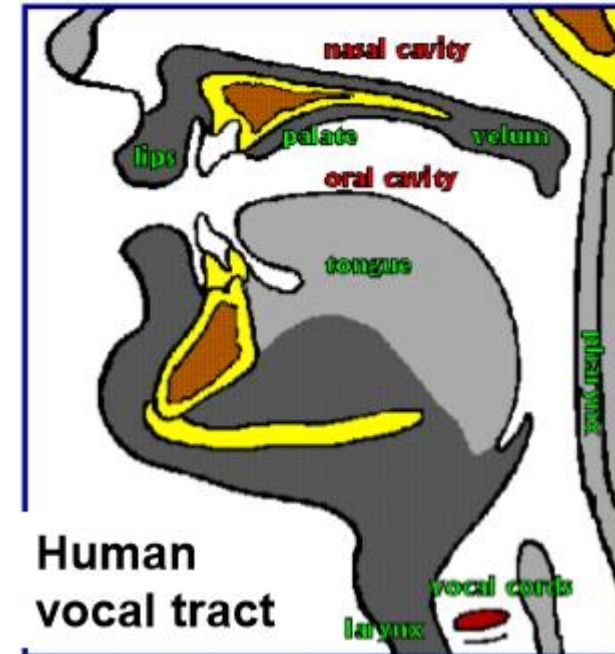
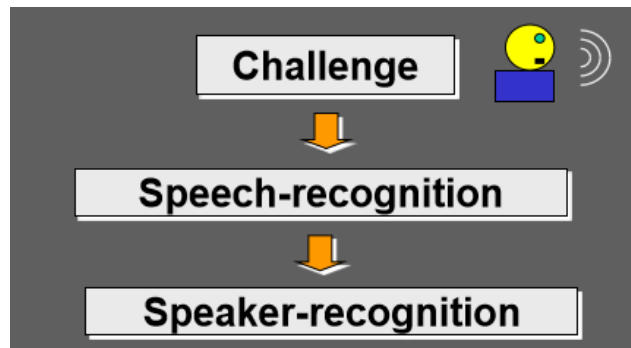
➤ **Huge security market (CCTV)**

- Massive deployments in airports after 9/11

Voice-based recognition

➤ Highlights

- Most of us have it - **universality**
- Easy to acquire (no cooperation)
- Gets changed (**aging**, **health**...)
- Uniqueness **hard** to be proved
- Combination of individual physical properties and learned elements



- The only means for remote applications
- Successive increase in recognition confidence level

Voice-based recognition

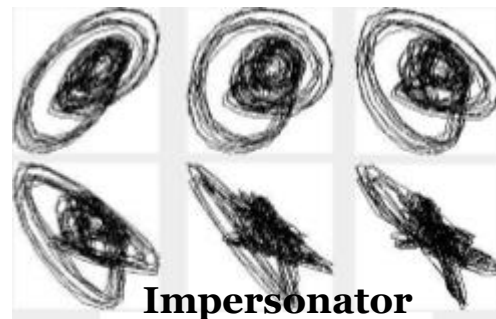
➤ Other challenges

- Deliberate imitation
- Noise

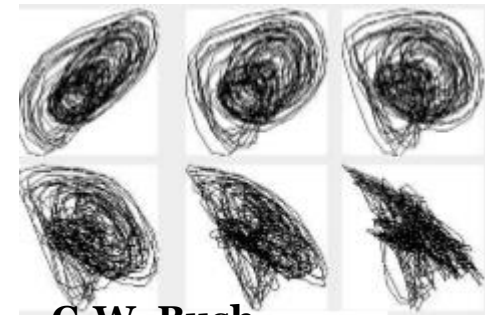
➤ Features

- Adopted from speech recognition (LPC; linear predictive coding)
- Pronunciation
- ...

<https://youtu.be/u5DpKjlgoP4>



Impersonator



G.W. Bush

Other biometric techniques

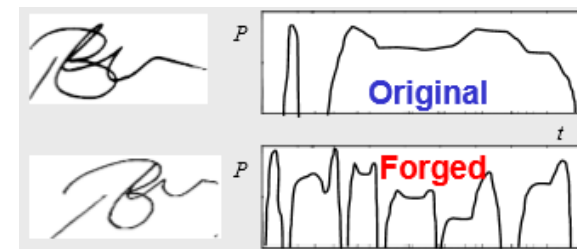
➤ Palm

- Popular access control technique
- Acquisition of frontal and side view
- Cooperation required (can be hard for persons with arthritis - system of pegs)
- unique but not applicable for large-scale systems

➤ Signature

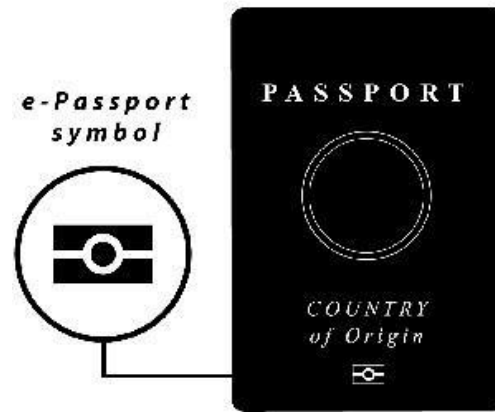
- Significant variations for the same individual
- Static and dynamic verification
- Forgery of signature dynamics is almost impossible

➤ Ears, gait, odor, DNA ...



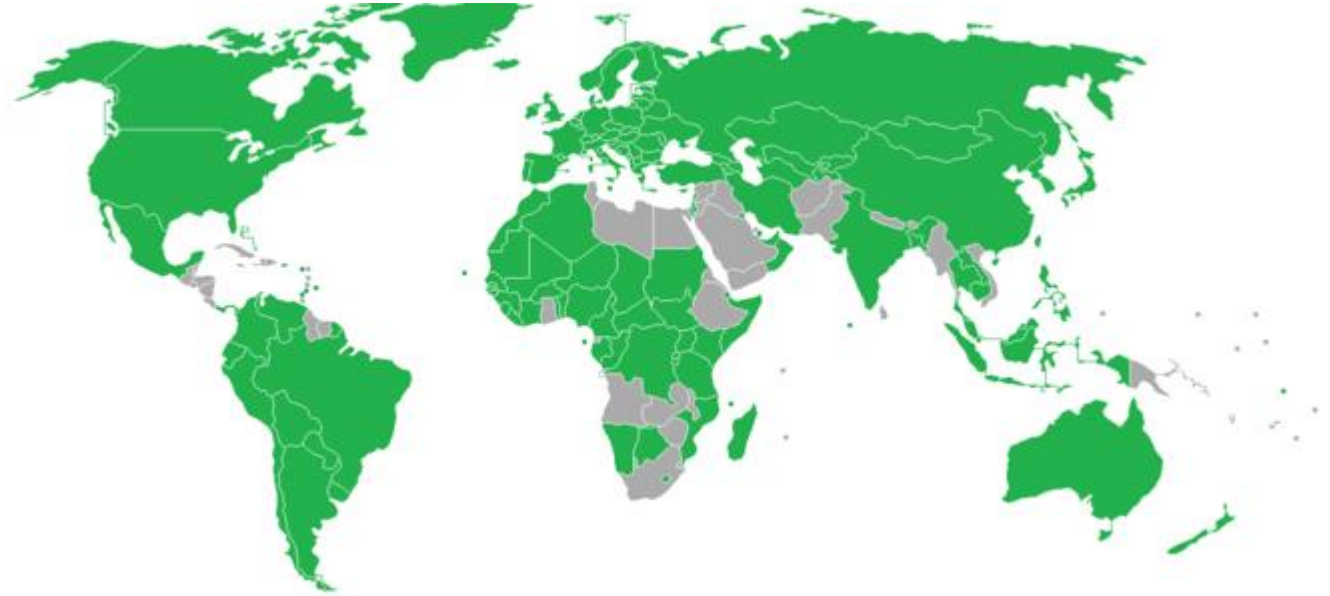
Biometrics irl

- Biometric passports



Biometrics irl

- Biometric passports
- Combined paper and electronic passport
- Contactless smart card
- PKI for authentication of stored data
- Standards for face, iris, fingerprint recognition
- ICAO – Int. Civil Aviation Org. (Doc. 9303)



Availability of biometric passports by the end of 2021

NOTE: Some countries only issue e-passports to diplomatic employees abroad

Biometrics irl

- CCTV – closed circuit television



Attacks on biometrics

➤ **Fingerprints copies by**

- Gelatin or tape and even Wine gum
<https://youtu.be/Fxdhb65iciM>
- high res photos
<https://www.bbc.com/news/technology-30623611>

➤ **But**

- Modern security devices check for liveness,

Attacks on biometrics

➤ **Biometric passport hacks**

- Early years (2005 – 2008)

Several successful attacks on chip

https://en.wikipedia.org/wiki/Biometric_passport

Attacks on biometrics

➤ **Deepfake**

Deepfake = Deep Learning + Fake (machine learning)

- **Fake photos**
 - **Fake videos**
 - **Even fake audio**
-
- **Attacks peoples digital identities**
 - **Used as cyber weapon**
 - **politicians, celebrities but even more and more private people are victims**

Attacks on biometrics

➤ **Deepfake**

Deepfake = Deep Learning + Fake (machine learning)

- **Fake photos**
- **Fake videos**
- **Even fake audio**

- <https://www.forskning.se/2022/06/02/avslojar-deepfake#>
- <https://www.creativebloq.com/features/deepfake-examples>
- <https://www.tiktok.com/@deeptomcruise?lang=en>
- <https://deepfakesweb.com/>

Attacks on biometrics

➤ **Deepfake**

Deepfake = Deep Learning + Fake (machine learning)

- **Fake photos**
- **Fake videos**
- **Even fake audio**

➤ **How to detect a Deepfake (indications of deepfake)**

- **Facial transformation**
facial expressions and contours do not match
- **Body poses**
poses and posture are out of line, blurring and or misalignment on edges
- **Digital "fingerprint" of source**
source and creation can reveal fake. Use of blockchain verification can help verify authenticity of content

Biometrics – future or present?

➤ Camera technology

- Blade Runner 1982
- Iris Scan
- Minority Report 2002
- Retinal Scan
- ...

Biometrics – future or present?

- Camera technology
 - Iris/retina scan
 - Behavior analysis
 - Thermoanalytics scan

Biometrics – future or present?

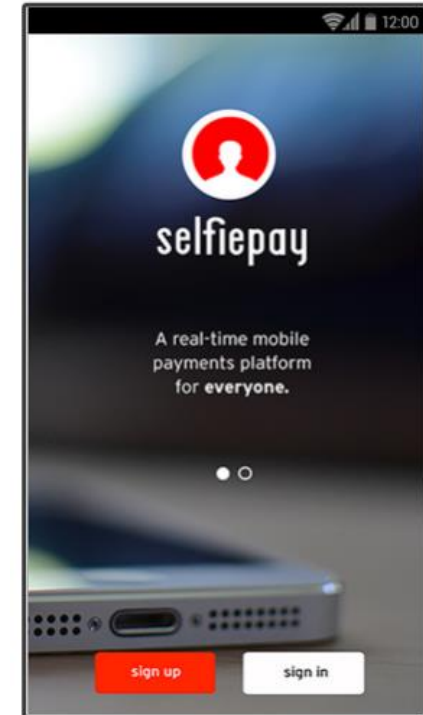


➤ Ear scan

- Outer ear scan
- Capacitative screen
- Inner ear
- Sound/ultrasound echo

Biometrics – future or present?

- Pay with fingerprint, facial, PayPal, Samsung Pay, Apple pay, Google Pay, ...
- Visa card biometrics at ATM
- MasterCard selfie pay
- US Colleges and universities move to biometric in access control



Recap: something you are

- Vary each time you measure them
- Scheme must allow variation
- Can deny access to legitimate users
- Can allow access to illegitimate users
- Can be copied
- Can be obtained by others quite easily
- Cannot be changed if compromised
- Cannot be handed over in duress

Final thoughts

- Biometrics are not secret
 - Biometrics are (ideally) unique to each individual
 - Increasing number of successful attacks against biometric identification
-> rethink before replacing password
- Recommendation: Biometric should be used
for 2FA (the 2nd factor)
- Or**
- In combination with password

Link collection:

- [Biometrics passport - Wikipedia](#)
- [Mobile Accessories | FLIR Systems](#) Thermal camera for mobil devices
- [Hacker fakes German minister's fingerprints using photos of her hands | Technology | The Guardian](#)
- [Asia Times | Israeli spyware: WhatsApp hack raises global fears | Article](#)
- [The Xerox character-substitution bug is worse than first thought | Computerworld](#)
- [Ryska hackare tar över Chrome och Firefox med trojan – TechWorld](#)
- [Hacking an ATM, as easy as using Windows XP](#)
- [Password Cracking - Computerphile – YouTube](#) old but still viable
- [FireEye confirmss that APT14 Group hacked TeamViewer](#)
- [WiGLE: Wireless Network Mapping](#) One of many sites that tracks Wifi and Bluetooth networks (legally and not invasive)

Ingo Hölscher
ingo.holscher@liu.se
IT-avdelningen APP

www.liu.se