Introduction to Biometric Technologies and Applications (I)

Fernando Alonso-Fernandez (F510)
ITE School

Email: feralo@hh.se

Course: Biometric Recognition
DI4025

Outline

Biometrics

- Intro & Definitions
- Biological/behavioural traits
- Requirements of a biometric trait
- How to choose a biometric trait

Application examples

- Sectors
- Market
- Mobile/ubiquitous biometrics

Outline

Biometrics

- Intro & Definitions
- Biological/behavioural traits
- Requirements of a biometric trait
- How to choose a biometric trait

Application examples

- Sectors
- Market
- Mobile/ubiquitous biometrics

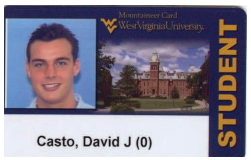
Questions About ”Identity”

- Who is this person?
- Have I interacted with this person before?
- Is this person authorized to enter the facility?
- Who is the owner of this smartphone?
- Am I communicating with Fernando?

Tokens of ”Identity”

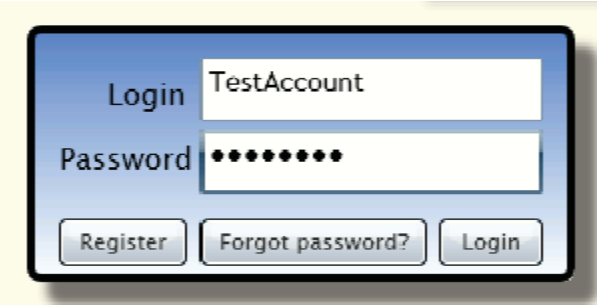
Something that I “**have**”

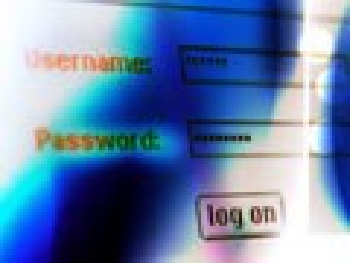
- Key
- Passport
- Driver’s License
- Birth Certificate



Something that I ”**know**”

- Password
- PIN code



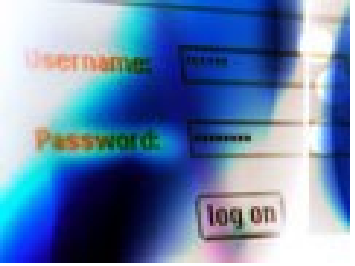


Problems with security systems based on tokens

They are easy and cheap to implement, but they are **not tied to a person**, so:

- Can be **copied**.
- Can be **Lost**.
- Can be **forgotten**.

- Worse! Can be **stolen** and used by a thief/intruder to access your data, bank accounts, car etc….



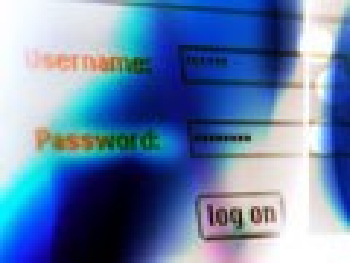
Problems with security systems based on tokens

Bank ATM

Input to ATM:

- Card
- PIN: 4 or 6 digits

Machine does not know who is inputting the card and PIN!



Problems with security systems based on tokens

Security Threats

- People can not be trusted based on ID documents
  - INTERPOL has data on 40M lost/stolen travel documents
  - Some of the 9/11 hijackers had multiple driver licenses

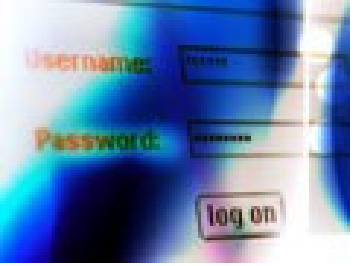
oblems with security
ems based on tokens

RANK	PASSWORD	CHANGE FROM 2015
1	123456	Unchanged
2	password	Unchanged
3	12345	2 ↗
4	12345678	1 ↘
5	football	2 ↗
6	qwerty	2 ↘
7	1234567890	5 ↗
8	1234567	1 ↗
9	princess	12 ↗
10	1234	2 ↘
11	login	9 ↗
12	welcome	1 ↘
13	solo	10 ↗
14	abc123	1 ↘
15	admin	NEW
16	121212	NEW
17	flower	NEW
18	password	6 ↗
19	dragon	3 ↘
20	sunshine	NEW
21	master	4 ↘
22	hottie	NEW
23	loveme	NEW
24	zaq1zaq1	NEW
25	password1	NEW

Almost **4% of people** use the worst password, **123456.**
Just over **10% of people** use one of the **25 worst passwords .**

https://www.teamsid.com/worst-passwords-2016/

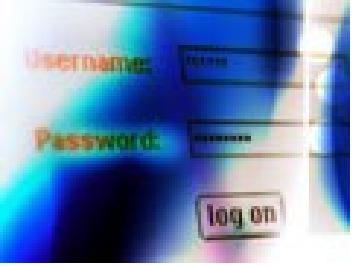
HALMSTAD UNIVERSITY



Problems with security systems based on tokens

- Increasing use of IT technology: **multiple accounts**
- **So many passwords**: we **end up** using things we know (birthdays, partner's name, dog, cat…)

- Weak passwords: easy to crack
- Strong passwords (meaningless): easy to forget



Problems with security systems based on tokens

Use complex passwords

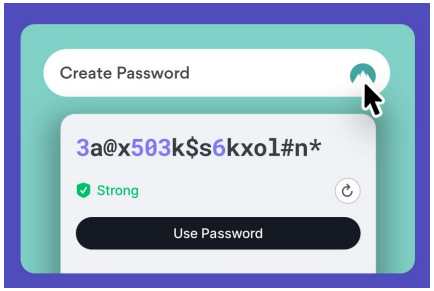
Your password should be at least 20 characters long and include a mix of uppercase and lowercase letters, numbers, and special symbols. Avoid using easily guessable information like birthdays, names, or common words.

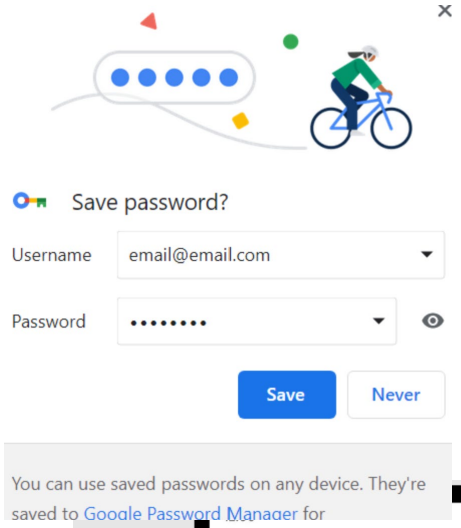
Never reuse passwords

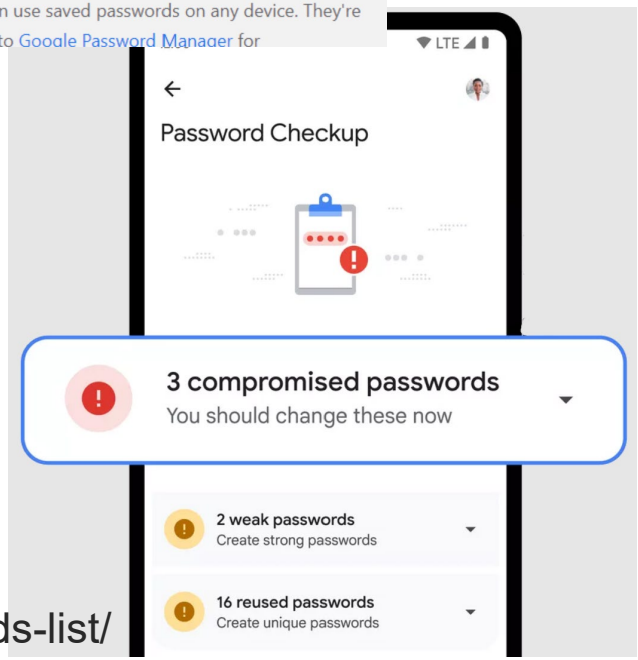
Never use the same password across multiple sites or services. If one account gets compromised, all your accounts could be at risk.

Check your passwords

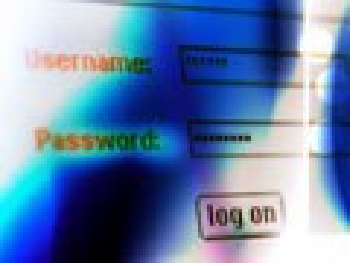
Take the time to regularly assess your password health. Identify weak, old, or reused passwords and improve with new and complex ones for a safer online experience.







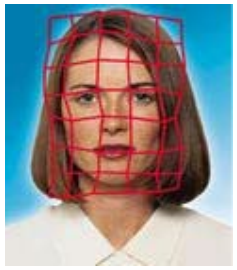
https://nordpass.com/most-common-passwords-list/

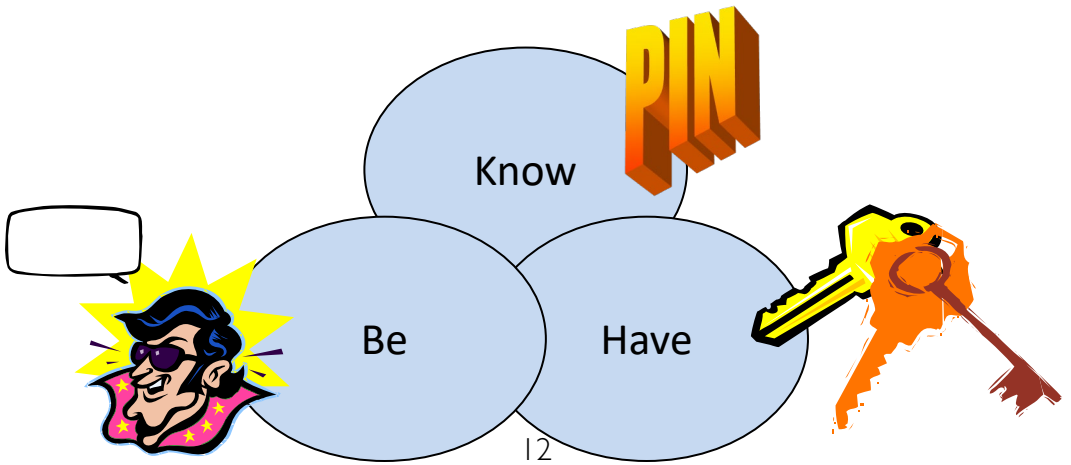


Many problems with token-based security systems…

ANSWER: BIOMETRIC TECHNOLOGY

Recognize a person based on body traits, not ID card or PIN





Biometric Recognition

- The term "biometrics" is derived from the Greek words bio (life) and metric (to measure).

- For our use, biometrics refers to technologies for:
  - **automatic recognition** of individuals
  - by measuring **biometric characteristics**
    - ✓ Physical/biological property
    - ✓ Physiological/behavioral process

  …from which:
  - **distinguishing** (~unique), and
  - **repeatable**

  features can be extracted

Tokens vs. Biometrics

(+) good
(-) bad

	Security	Traceability	Complexity
Tokens (card, passwords)	(-) • **Can be**: copied, lost, forgotten, stolen	(-) • **Not tied** to a person (anyone with the token has the same ”privilege”)	(+) • **Cheap**, **easy** to implement
Biometrics	(+) • **Cannot be**: lost, forgotten • **More difficult** to copy or steal • **Avoids**: too complex or too simple password, ”post-it” passwords	(+) • **Tied** to a person (need that the person be physically present) • More **convenient** (no need to ”carry” or ”remember”) • Allows to detect **multiple identities**	(-) • More **complex** and **expensive** • Additional **hardware and software**

- Multifactor authentication

MFA: Multifactor authentication

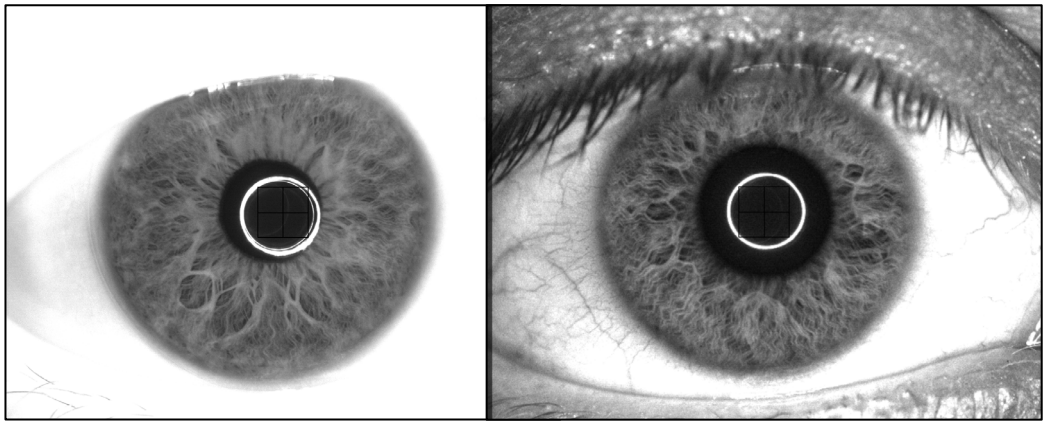
- Multi-step account login process that requires users to enter **more information than just a password**, e.g. code to email or phone, answer secret question, or scan a biometrics

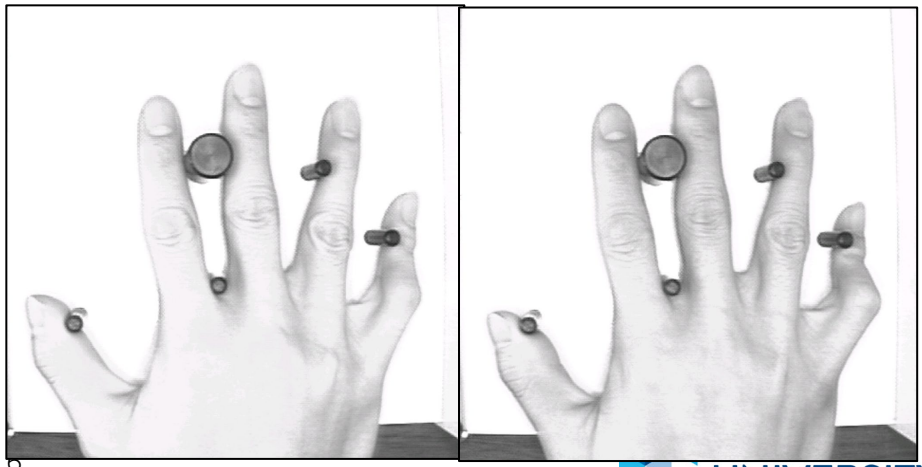
➢ EU Revised Payment Services Directive (PSD2), where MFA is mandatory since 2019 for banking/ payment services and 2021 for e-commerce, requiring at least two of the following:

- Something the user knows (e.g., password or PIN)
- Something the user has (e.g., mobile device, card reader, token)
- Something the user is (e.g., biometrics).

Biometric Recognition

- Given two biometric samples, estimate if they are from the **same person or not**





Identity vs. Recognition

- We **do not** necessarily want to elicit **identity**
- We **want** to **recognize** a person

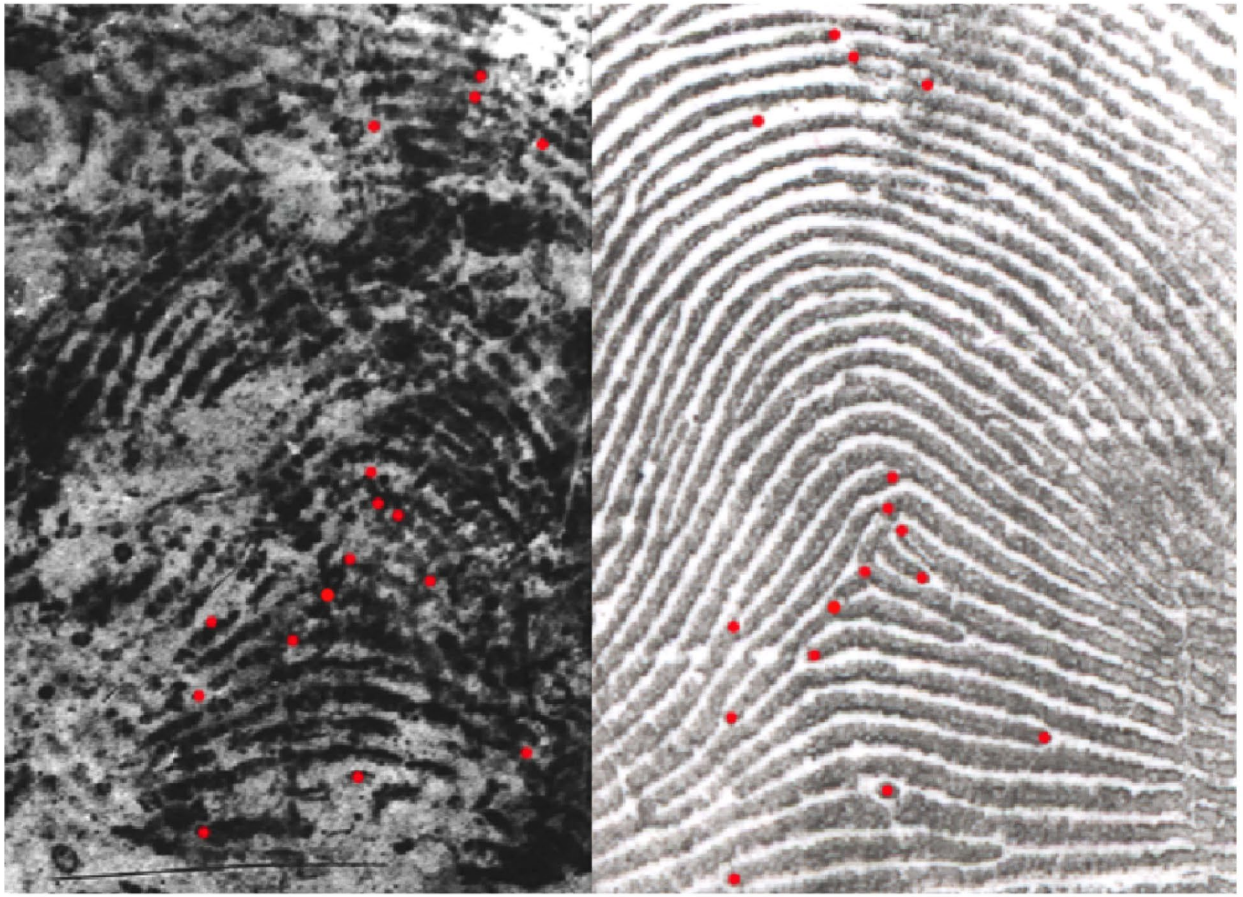
Based on a **single** fingerprint image, we cannot say this belongs to *Isaac Newton*

We need a **reference** fingerprint image that is known to belong to *Isaac Newton* in order to make this assessment

Criminal Investigation

Are These The Same?

- Are these two prints from the same finger?



Search operation

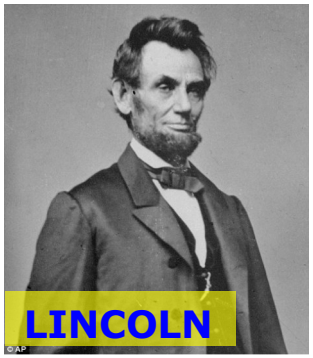
Is He There?

- Are any of the Boston Bombers in this scene?

History

Is This Really Him?

- Is this really a photograph of Abraham Lincoln?

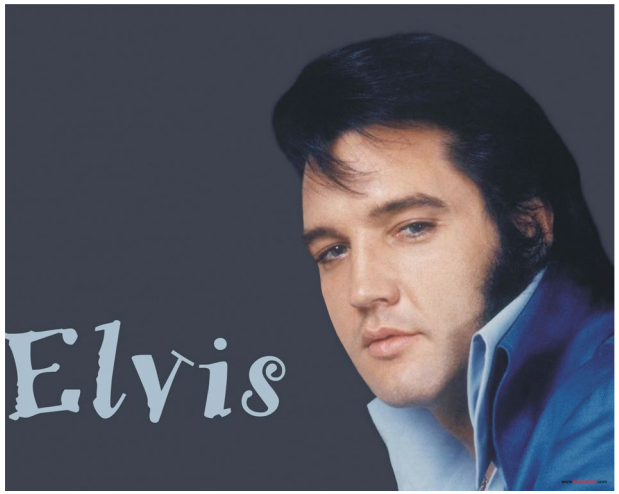


?

Authenti cation

Who is Singing?

- Is this really Elvis Presley's voice? (And if so, is he still alive?!)



https://www.youtube.com/watch?v=HGsssVWiu54

Retrieval

Where is She?

- Find all video frames in which Odette appears

Why Biometrics?

- **Security**: Does the person have a prior criminal record?
- **Convenience**: No need to carry credentials (pw, ID)
- **Audit trail**: Who accessed this bank account?
- **Fraud detection**: Is this person the rightful owner of the credit card?
- **De-duplication**: One person, one identity

Palm vein scanners used for patient registration in Houston hospital system; 2,488 patients are named Maria Garcia and 231 of them have the same birth date

Biometric System

BIOMETRIC TRAIT

HUMAN MACHINE INTERFACE

PERSON

Biometric Characteristics

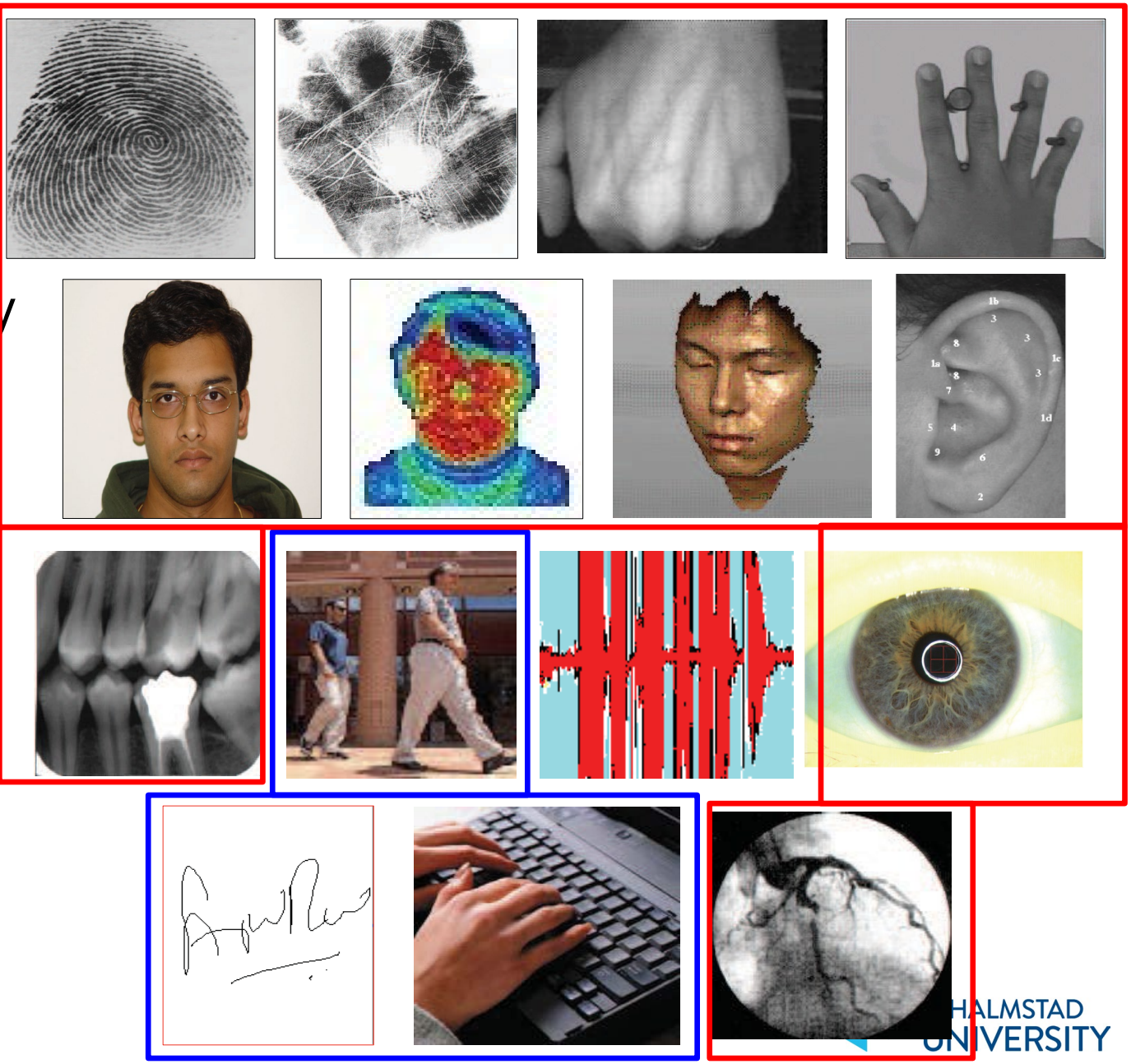
Physical

- DNA
- Fingerprint
- Palmprint
- Vein pattern
- Hand geometry
- Face
- Iris
- Retina Scan

Behavioral

- Signature
- Gait
- Keystroke

- Voice



Biometric Characteristics

Physical

- DNA
- Fingerprint
- Palmprint
- Vein pattern
- Hand geometry
- Face
- Iris
- Retina Scan

- Always “present”
- The biometric characteristic itself has high stability
- BUT: other factors may alter our capability to capture a stable sample

Behavioral

- Signature
- Gait
- Keystroke

- Needs “execution”
- The biometric characteristic itself is variable, even in the short-term

- Voice

Attributes of a Biometric Trait

Any human characteristic can be used as a biometric characteristic as long as it **satisfies**:

- **Universality** (Does every user have it?)
- **Uniqueness/distinctiveness**
  (Is sufficiently distinctive across users?)
- **Permanence** (Does it change over time?)
- **Collectability** (Can it be measured quantitatively?)

In **practical** systems, other issues must be considered too:

- **Performance**
  (Does it meet error rate, speed, resources required..?)
- **Acceptability** (Is it acceptable to the users?)
- **Vulnerability/circumvention** (Can it be easily spoofed?)

No biometric trait is “optimal”, but many are “admissible”

Attributes of a Biometric Trait

(Subjective) comparison. Many cases subject to “IF”

Biometric Type	Accuracy	Ease of Use	User Acceptance
Fingerprint	High	Medium	Low (Medium?)
Hand Geometry	Medium	High	Medium
Voice	Medium	High	High
Retina	High	Low	Low
Iris	High	Low	Medium
Signature	Medium	Medium	High
Face	Low (*)	High	High

How to Choose a Biometric Trait?

Accuracy: often the primary criterion (but not the only one)
Other factors to consider as well

Attributes of the **Interface/Environment**

- **Overt vs Covert** (Is the subject aware?) (surveillance?)
- **Attended vs Unattended** (Is there operator involvement?)
- **Cost of operation**

Attributes of the **Person**

- **Non- vs. Cooperative** (conceal own identity?)
- **Non- vs. Habituated** (subject adapted to the system?)
- **Age, Gender, Ethnicity, Pathological state** (What is the Biological, Physical, Psychological state of the individual?)

Outline

Biometrics

- Intro & Definitions
- Biological/behavioural traits
- Requirements of a biometric trait
- How to choose a biometric trait

Application examples

- Sectors
- Market
- Mobile/ubiquitous biometrics

Applications of Biometric Systems

Commercial:

- Computer login
- Electronic payment
- E-commerce
- ATMs
- Physical access
- Record management

Government:

- Passport control
- National ID
- Social security
- Welfare benefits

Forensic:

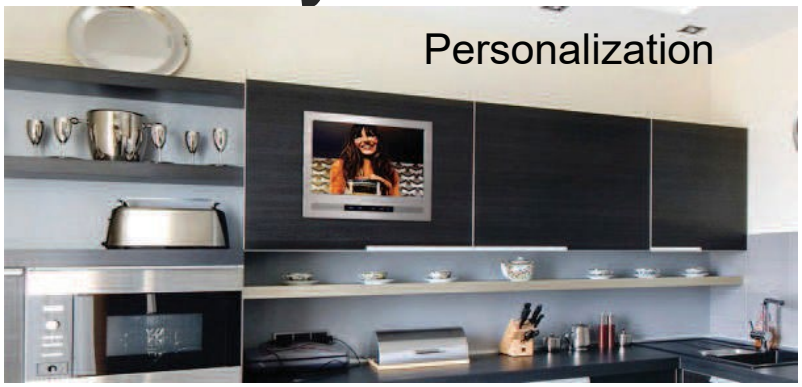
- Missing persons
- Corpse identification
- Parenthoood
- Criminal investigation

Applications of Biometric Systems

Commercial

Verification

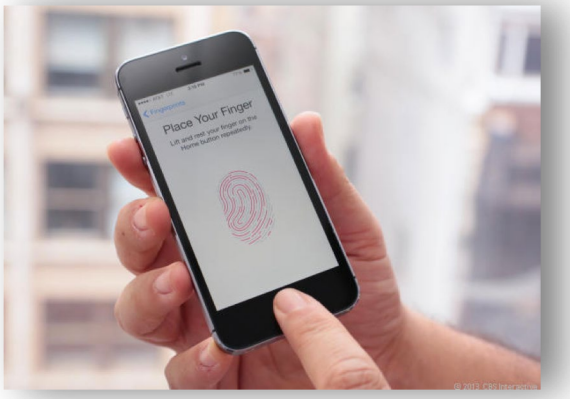
Transactions: finger vein ATM



Personalization

Fingerprint: Privaris Key Fob

Convenience



Fingerprint: Apple Touch ID

Safety

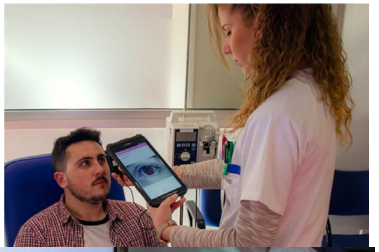
Applications of Biometric Systems

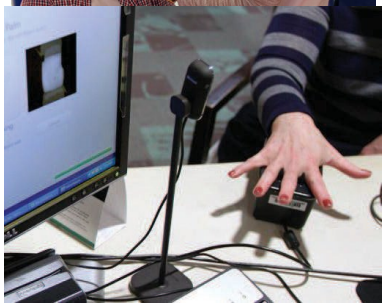
Government

Iris: Frankfurt Airport

Fingerprint: US-VISIT program

Healthcare



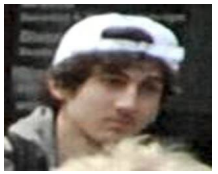


Travel

Applications of Biometric Systems

Forensic

Boston marathon bombing, April 15, 2013

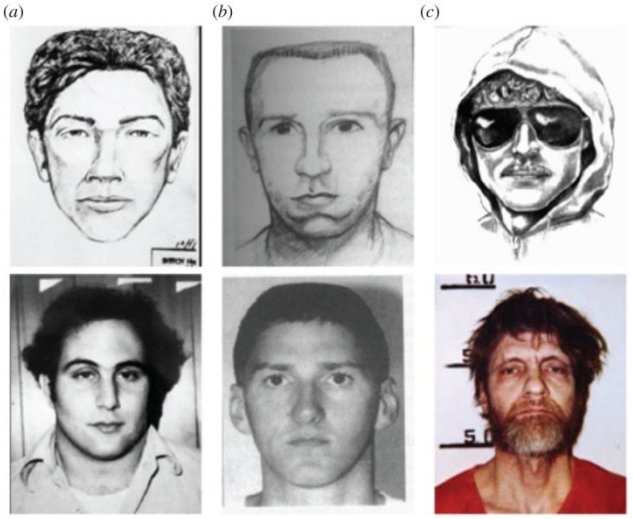


Suspects

Photo in database

Automated tattoo image matching

Latent fingerprint



Sketch-to-photo face comparison

Applications of Biometric Systems

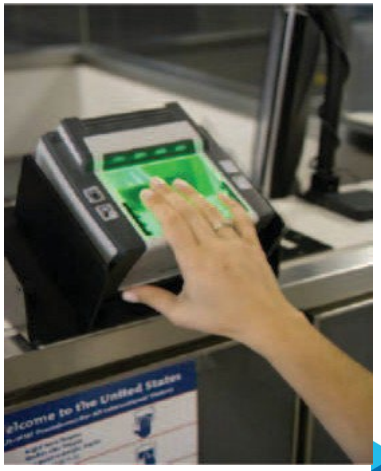
	Commercial	Government	Forensic
Purpose	Convenience and/or security	Security, prevent duplicates	Security, avoid missing someone
Cooperativity	High	Depends	Low
Control in the acquisition	Depends	High	None

Popular Biometric Traits

Fingerprint, face, iris: The three most popular

- Fingerprint, face: Availability of large databases collected by public agencies (driver/ID licenses, immigration)
  (*) and today by big tech companies like Facebook or Google
- Iris: adopted for large-scale systems (e.g. border crossing) due to its high accuracy

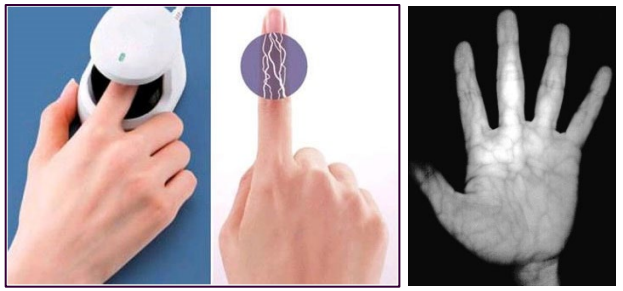
➢ Plenty of research devoted to these modalities



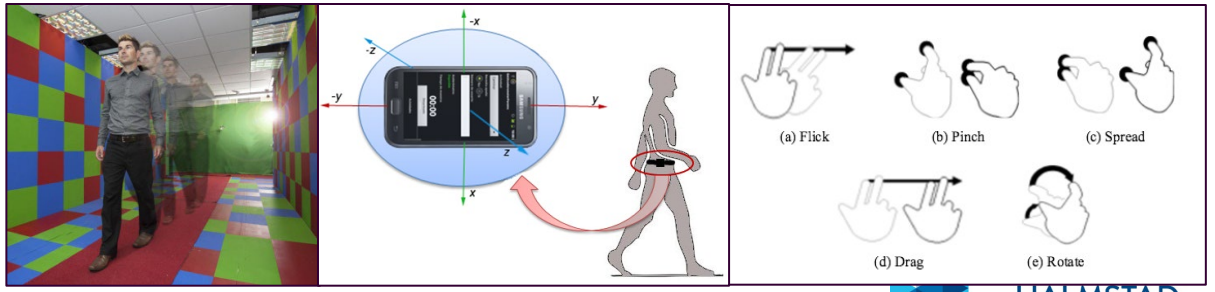
Popular Biometric Traits

Other proposed in the literature

- DNA, palmprint: often the only trace at crime scenes
- Voice, signature, hand geometry, vascular patterns: commercial applications deployed, but use yet limited

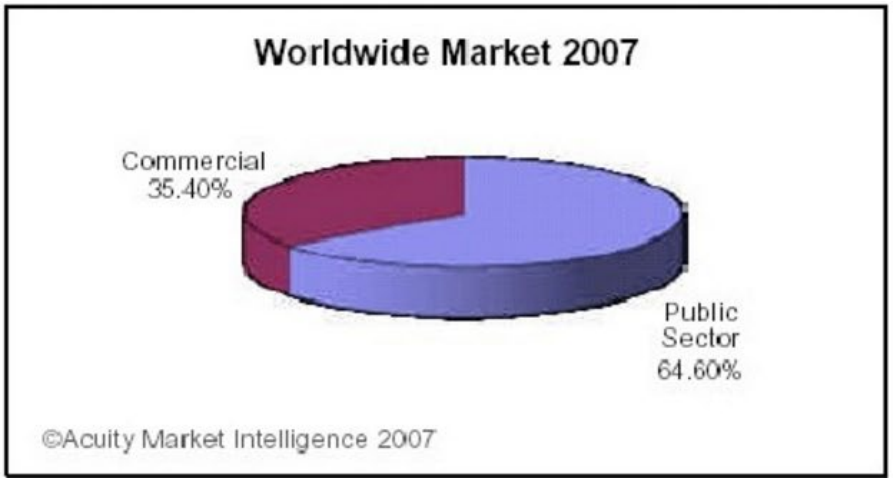


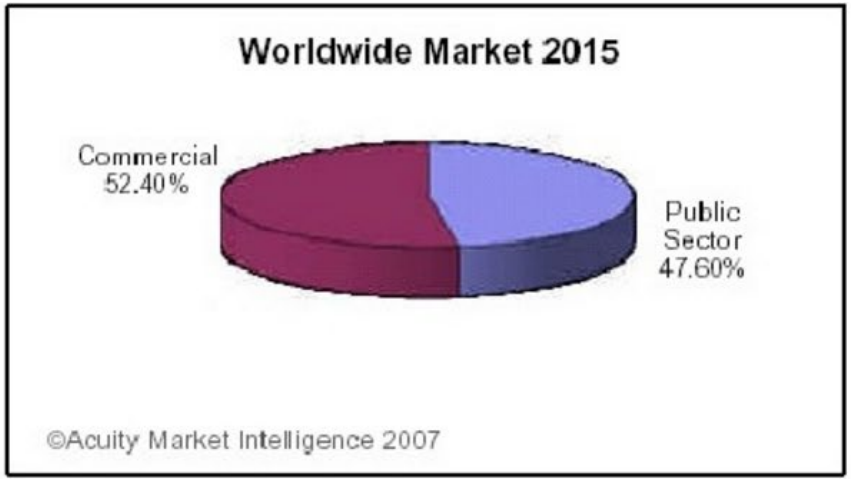
- Gait, ear, keystroke/screen dynamics, ECG, EEG: niche research, yet to attain maturity and acceptance



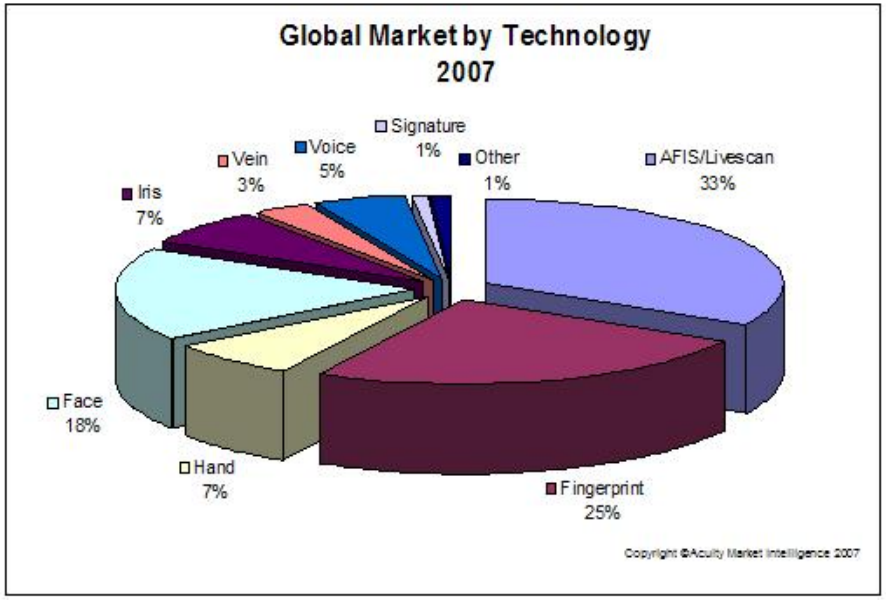
Market Share of Biometrics

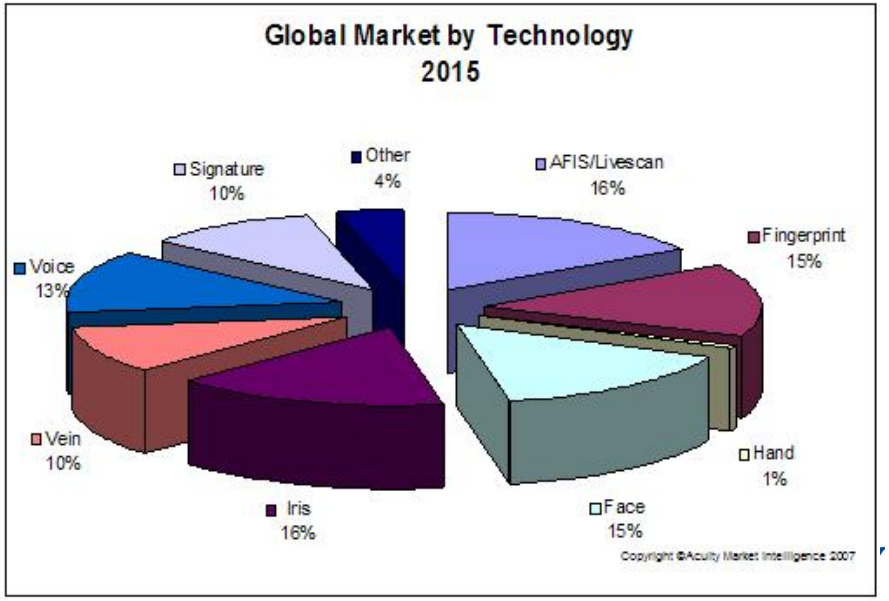
By sector





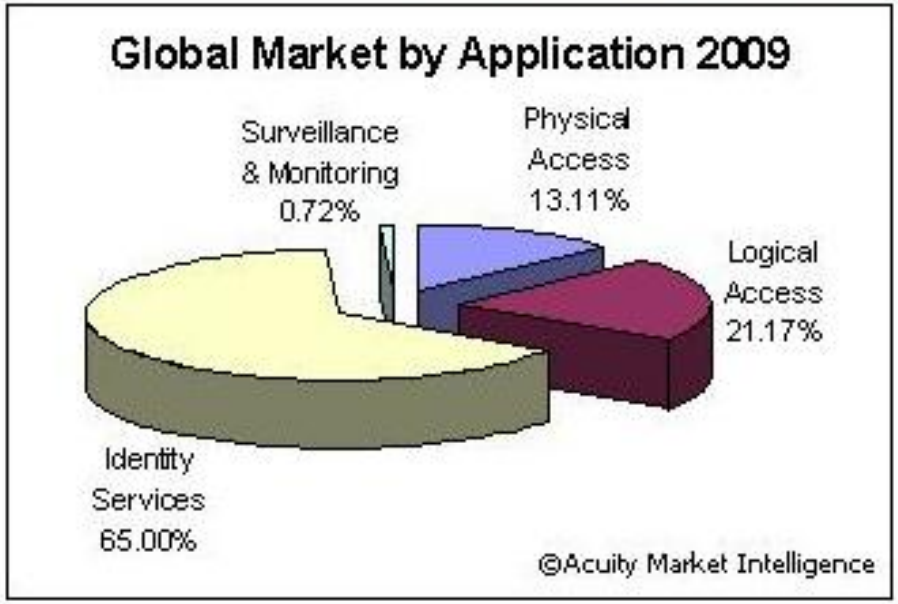
By modality

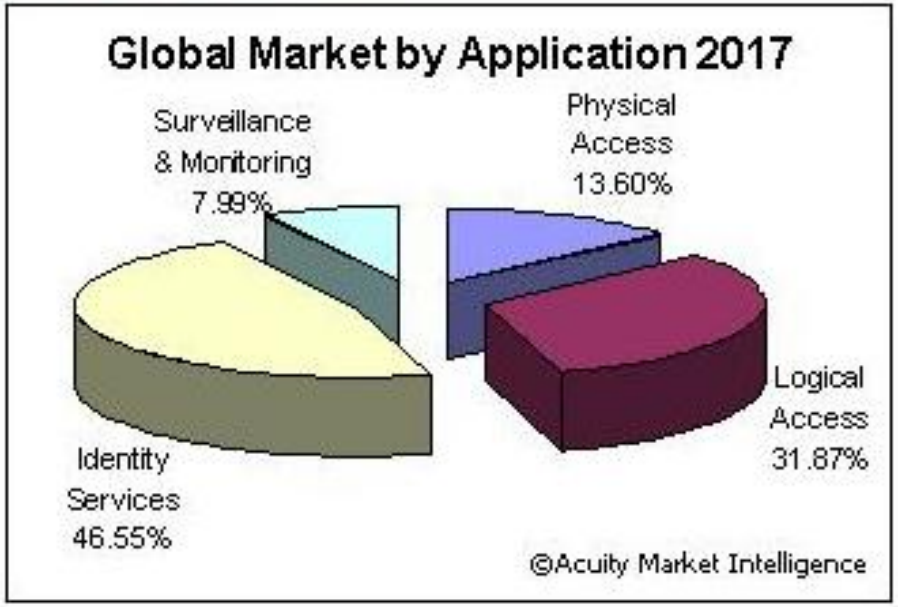




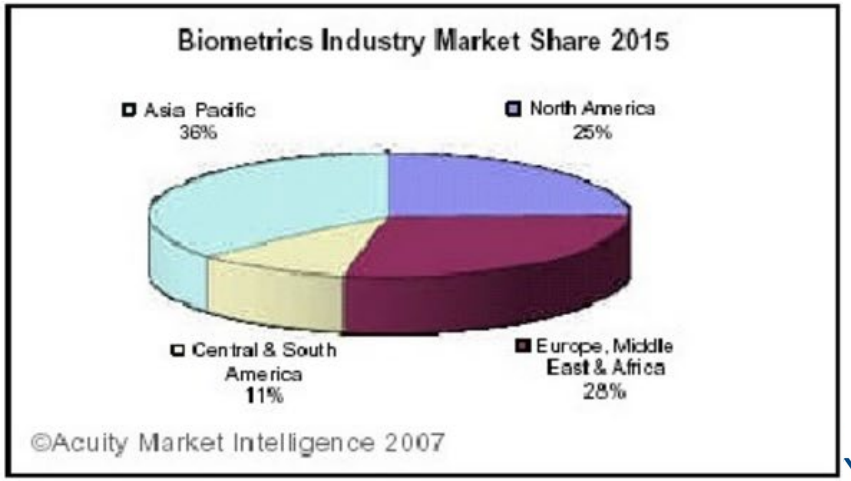
Market Share of Biometrics

By application



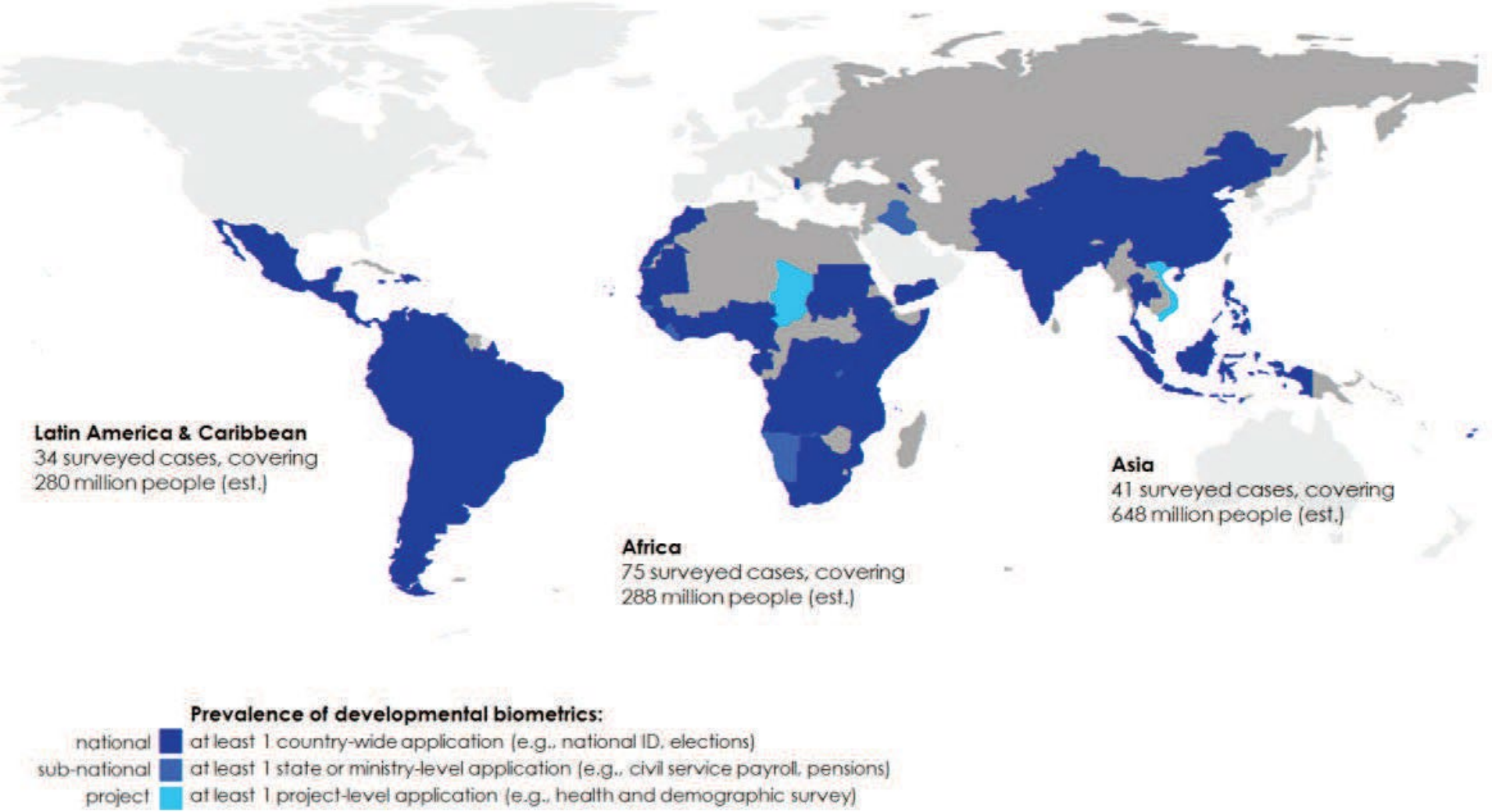


By region



The Biometrics Revolution

Over 1 billion people have been covered by biometric identification programs in the Low Middle Income Countries

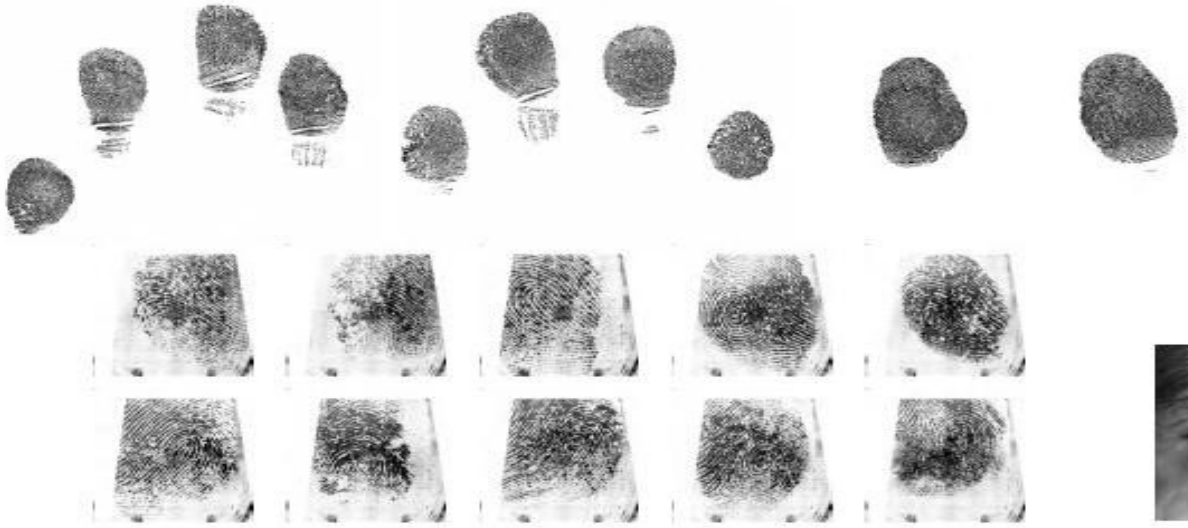


The Biometrics Revolution

- "Rich countries have long used biometrics for **forensics** and **security** but fewer have incorporated them into their national identity systems or used them to underpin public service delivery."
- "In contrast, we have seen a proliferation of **non-security applications** in low- and middle-income countries, from civil registries to voter rolls, health records to social transfers, public payrolls to pension payments and beyond."
- "This divergence in purpose partly reflects the different identification baselines in rich and poor countries—the **identity gap**."

Alan Gelb and Julia Clark. 2013. "Identification for Development: The Biometrics Revolution." CGD Working Paper 315. Washington, DC: Center for Global Development. http://www.cgdev.org/content/publications/detail/1426862

India's Aadhar Program



The largest biometric system in the world!

- Provide a 12-digit unique ID number (UID) to all Indian residents
- **De-duplication** (one person, one UID) using 10 fingers & 2 iris
- ~1.21B residents enrolled (May 2018), ~99% aged 18 and above

Mobile Phone-based Vaccination Registry

Use fingerprint scans to track children who have received immunizations. The goal is to reduce redundant doses and increase coverage levels in developing countries (Mark Thomas, VaxTrak)

UAE Border Control System

- The United Arab Emirates (UAE) Ministry of Interior requires iris recognition tests on **foreigners entering UAE** from 35 air, land, and sea ports.
- Via internet links each traveller is compared against each of **1,000,000 expellees** (foreign nationals expelled for various violations), whose IrisCodes were registered in a central database upon expulsion.

- The time required for an exhaustive search through the database is about **1 second**.
- On an average day, 12,000 arriving passengers are compared against the entire watch list of 1,000,000 in the database; this is about **12 billion comparisons per day.**

Biometrics For Lifetime

Fingerprint capture of a baby at a health clinic in Cotonou, Benin

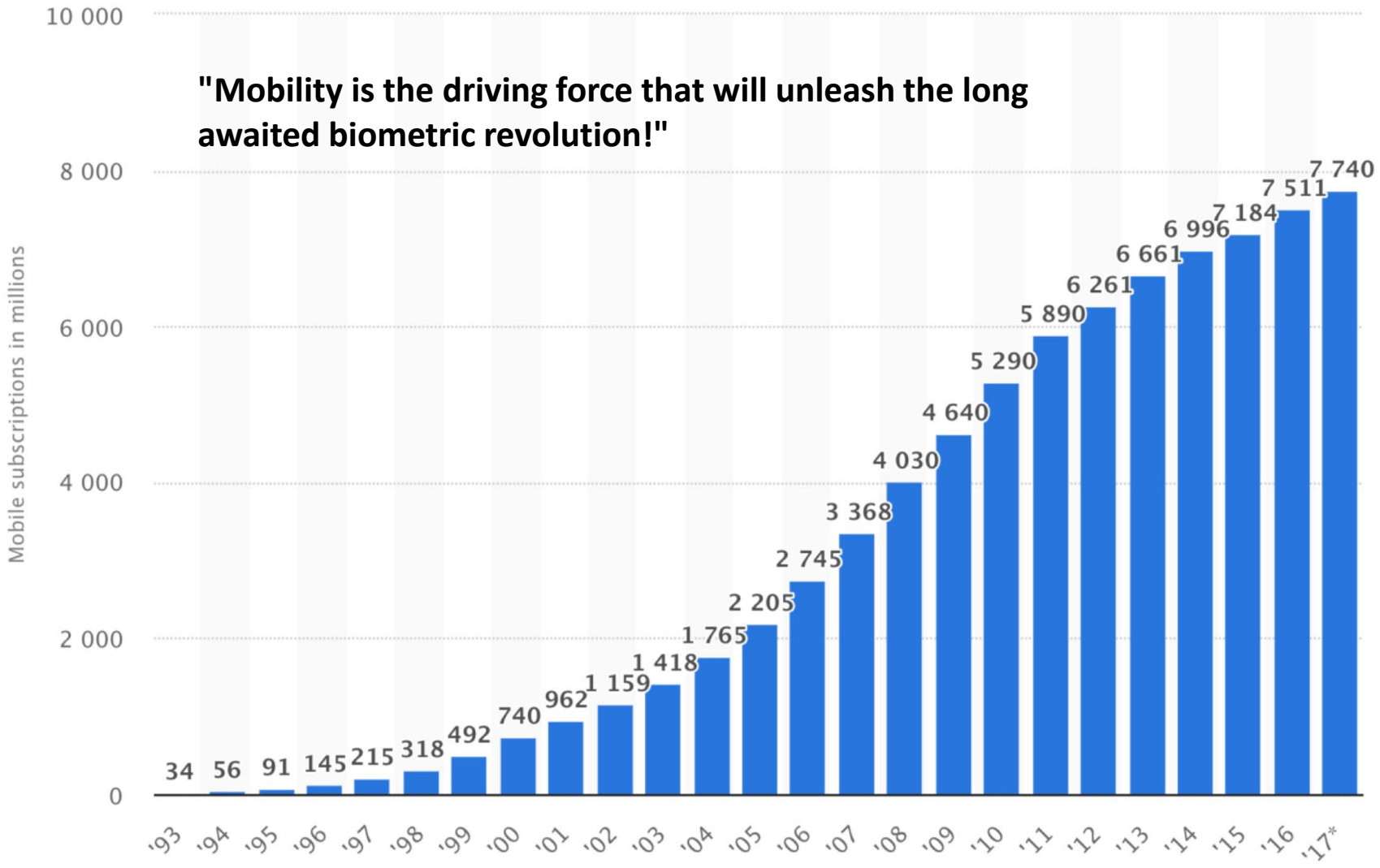
Inked finger of an Afghan woman after voting in Bamiyan, Afghanistan

Tattoos to Distinguish Identical Twins

Haircuts help to avoid confusion among the four identical six-year-old twins

http://www.cbsnews.com/8301-503543_162-57508537-503543/chinese-mom-shaves-numbers-on-quadruplets-heads/

Mobile Biometrics



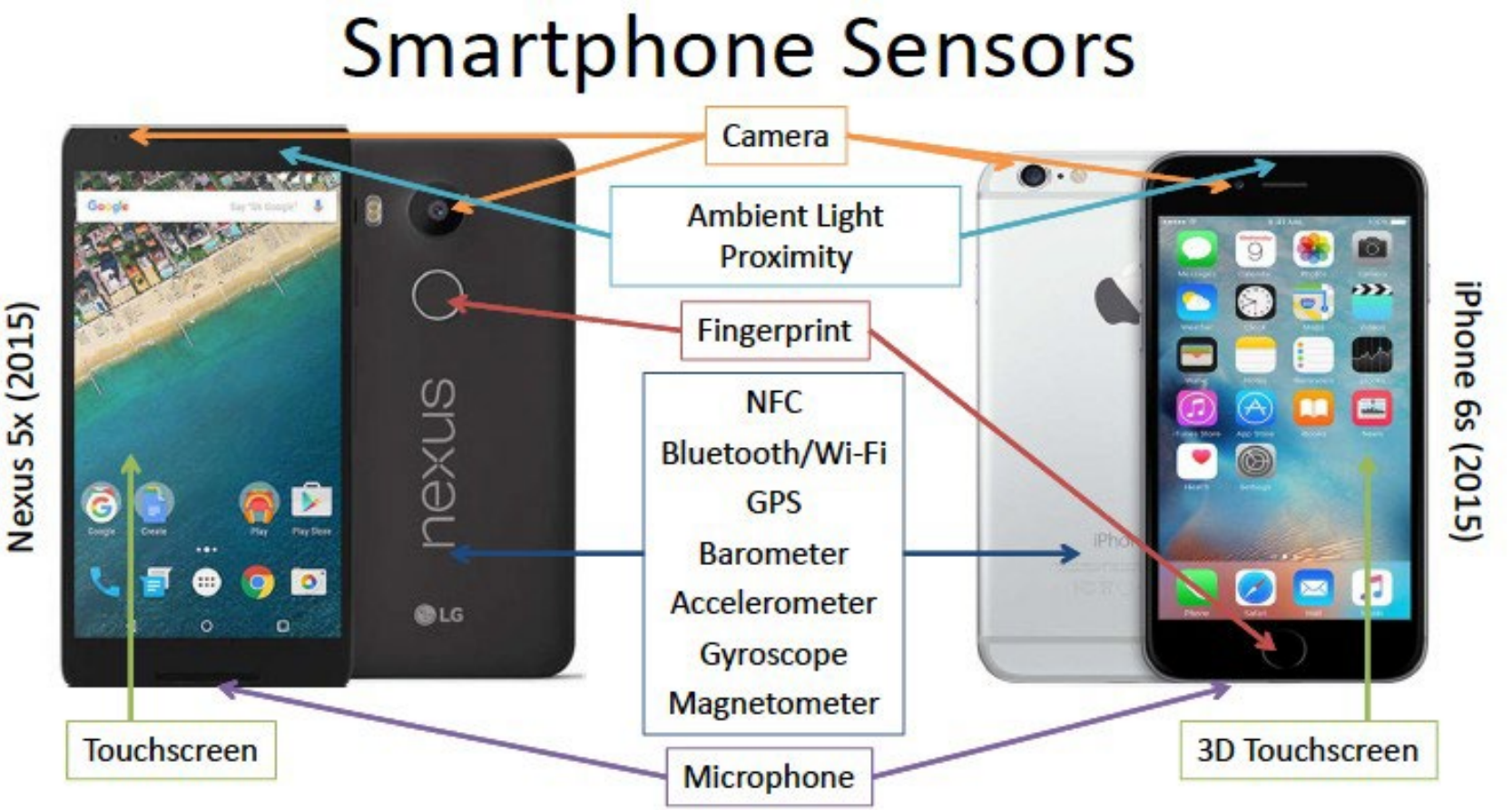
Data visualized by tableau

Mobile Biometrics

Global subscription penetration in Q1 2018 was 104%
Joseph Van Os/Getty Images

M-Pesa allows deposit, withdraw & transfer money with a mobile; $882M USD/month

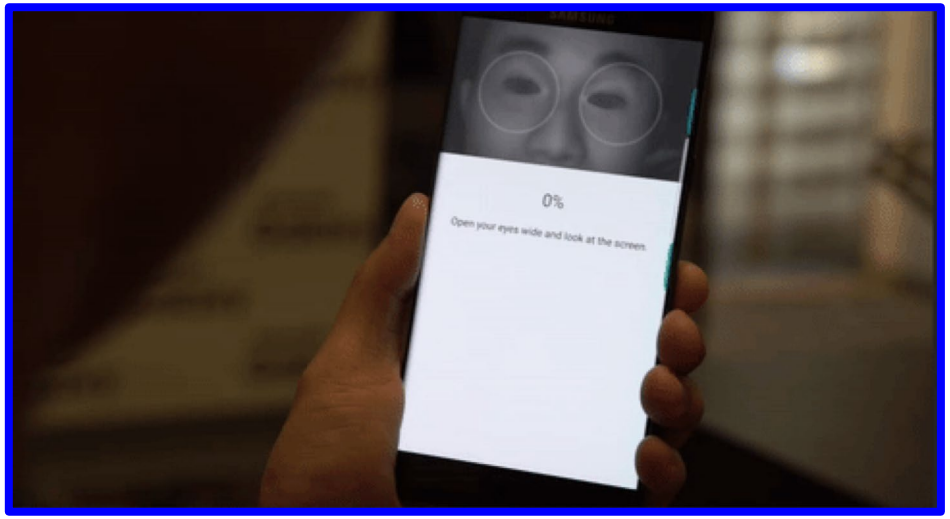
Mobile (Ubiquitous, Continuous) Biometrics



Mobile Biometrics

FINGERPRINT

https://media.giphy.com/



IRIS

© Mashable

In-display Fingerprint Sensor

© pinoy techno guide

Synaptics + Vivo

© gizmodo

Smartphone Payment Systems

Accepted at 1 million+ stores

Supported by 300+ Banks

Millions of Capable Devices

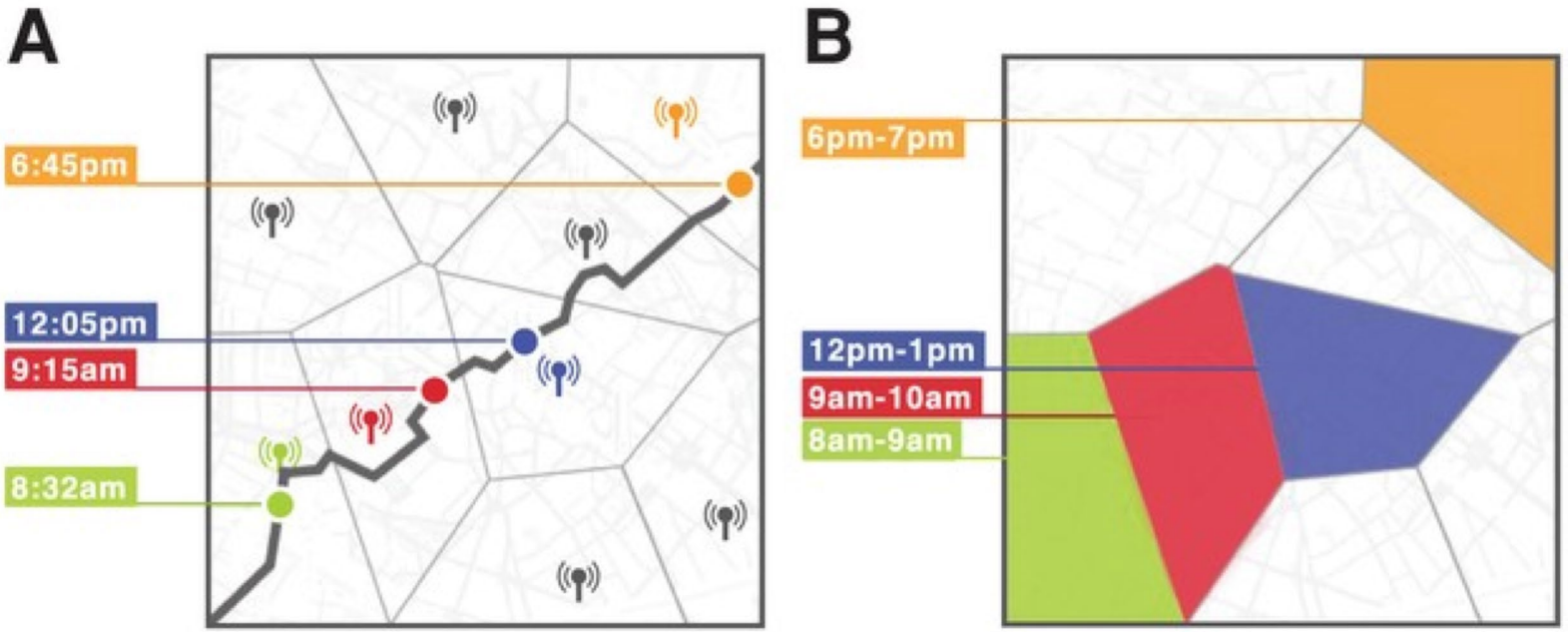
BankID

swish®

Obtrusive versus Non-obtrusive

Identification Without Biometric Data!

De Montjoye, Hidalgo, Verleysen & Blondel, "Unique in the Crowd: The Privacy Bounds of Human Mobility", Scientific Reports, vol. 3, 2013



With just anonymous location data, it is possible to figure out "who you are" by tracking your smartphone

- 15 months of mobility data for 1.5 million individuals and found that human mobility traces are highly unique.
- 4 spatio-temporal points are enough to uniquely identify 95% of the individuals

Take-home messages

- Welcome to this course!

- Biometrics does not necessarily supplant passwords or tokens, but (in combination), they can provide a **better approach** to security
  - Multifactor authentication

- No biometric trait is ”the best”, it depends on the requirements of **each specific application**
  - Interplay of several factors
  - Performance, user interaction, interface, ergonomics, environment, operation…

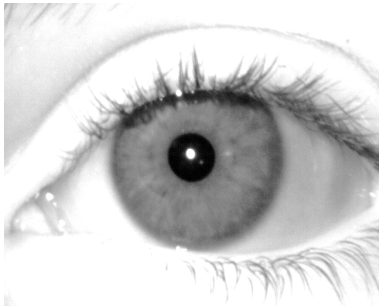
Take-home messages

- Face, fingerprint, iris: the most popular (due to public agencies)
- Other modalities with commercial deployments or at laboratory stage
- Will mobiles dominate the world?

Take-home messages

- Information from a single sample

- Gender: Male
- Age: 25
- Health: Very good
- Eye Sight: Wears glasses
- Ethnicity: Asian Indian
- **Name?**



- Gender: Male
- Age: 34
- Health: Good
- Ethnicity: White
- Constricted pupil suggests strong ambient illumination
- **Name?**

- We need a reference sample that is known to belong to that person in order to say who s/he is

Philosophical Musings

- What constitutes the identity of an individual?
- What are the societal implications of machines identifying humans?
- What are the moral and ethical implications of a biometric system misidentifying an individual in high-risk environments such as a combat zone?

Introduction to Biometric Technologies and Applications (I)

Fernando Alonso-Fernandez (F510)
ITE School

Email: feralo@hh.se

Course: Biometric Recognition
DI4025