UNIVERSITY OF AMSTERDAM

Jaap van Ginkel

Security of Systems and Networks

10 October 2024, Biometrics

Would you use Biometrics

Biometrics

Something You Are

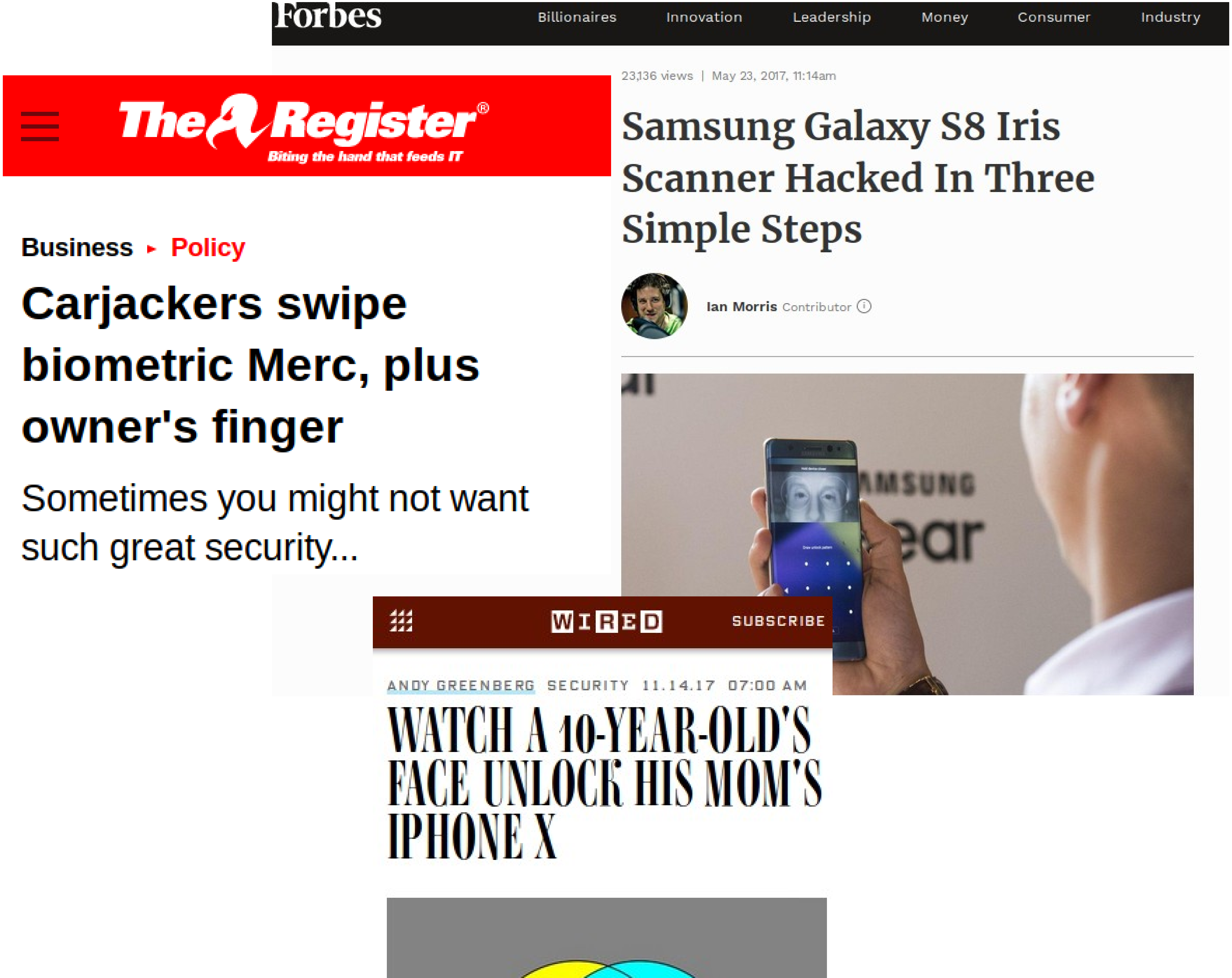
- Biometric
  - **"You are your key"** — Schneier
- Examples
  - Fingerprint
  - Handwritten signature
  - Facial recognition
  - Speech recognition
  - Gait (walking) recognition
  - "Digital doggie" (odor recognition)
  - Many more!

Are
Know
Have

Biometrics in Movies

Why Biometrics?

- Biometrics seen as desirable replacement for passwords
  - Cheap and reliable biometrics needed
  - Today, a very active area of research
- Biometrics are used in security today
  - Thumbprint mouse
  - Palm print for secure entry
  - Fingerprint to unlock car door, etc.
  - Face-ID on phone



Business ▸ Policy

Carjackers swipe biometric Merc, plus owner's finger

Sometimes you might not want such great security...

23,136 views | May 23, 2017, 11:14am

Samsung Galaxy S8 Iris Scanner Hacked In Three Simple Steps

Ian Morris Contributor

ANDY GREENBERG SECURITY 11.14.17 07:00 AM

WATCH A 10-YEAR-OLD'S FACE UNLOCK HIS MOM'S IPHONE X

Developments in face biometrics

Motive: General limited understanding of the processing of facial images by man and machine.

Goal: Improve the understanding of factors influencing the (im)possibilities of facial recognition and facial comparison by man and machine.

Content: Overview of different applications of face biometrics by man and machine depending on operational setting.

Definitions

Biometric recognition:

“**Automated recognition of individuals** based on their biological and behavioral characteristics”

Biometric recognition encompasses **biometric verification** and **biometric identification.**

Biometric recognition allows to distinguish human beings and to recognize them to a certain degree depending on the:

Modality

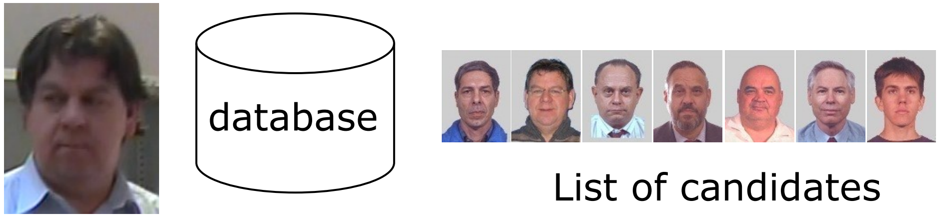
Application

Quality of the data

ISO, – Information technology — Vocabulary — Part 37: Biometrics, 2012, ISO/IEC: ISO/IEC 2382-37:2012(E).

Definitions

Definitions as used in this presentation:

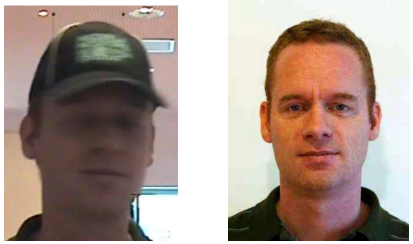


List of candidates

Facial recognition (1:N):

Man: Do I remember this person (as being person X)?

Machine: Biometric identification. Is a picture, similar to the picture of person X, in my database?



Facial comparison (1:1):

Man: Do these images depict the same person?

Machine: Biometric verification. Are these face images similar (to a pre-defined level)?

Facial comparison: man and machine

Machine:

+ Objective? Depending on training set!
+ Reproducible on conditioned material
- Poor performance in unconditioned circumstances
- Highly dependent on lighting, pose and position, facial expression, etc

Man:

+ Great (?) pattern recognition system
- Reproducibility/performance mostly unknown
- Bias/subjective

Modality: Face

Challenge: inter-person comparable (look-alikes)

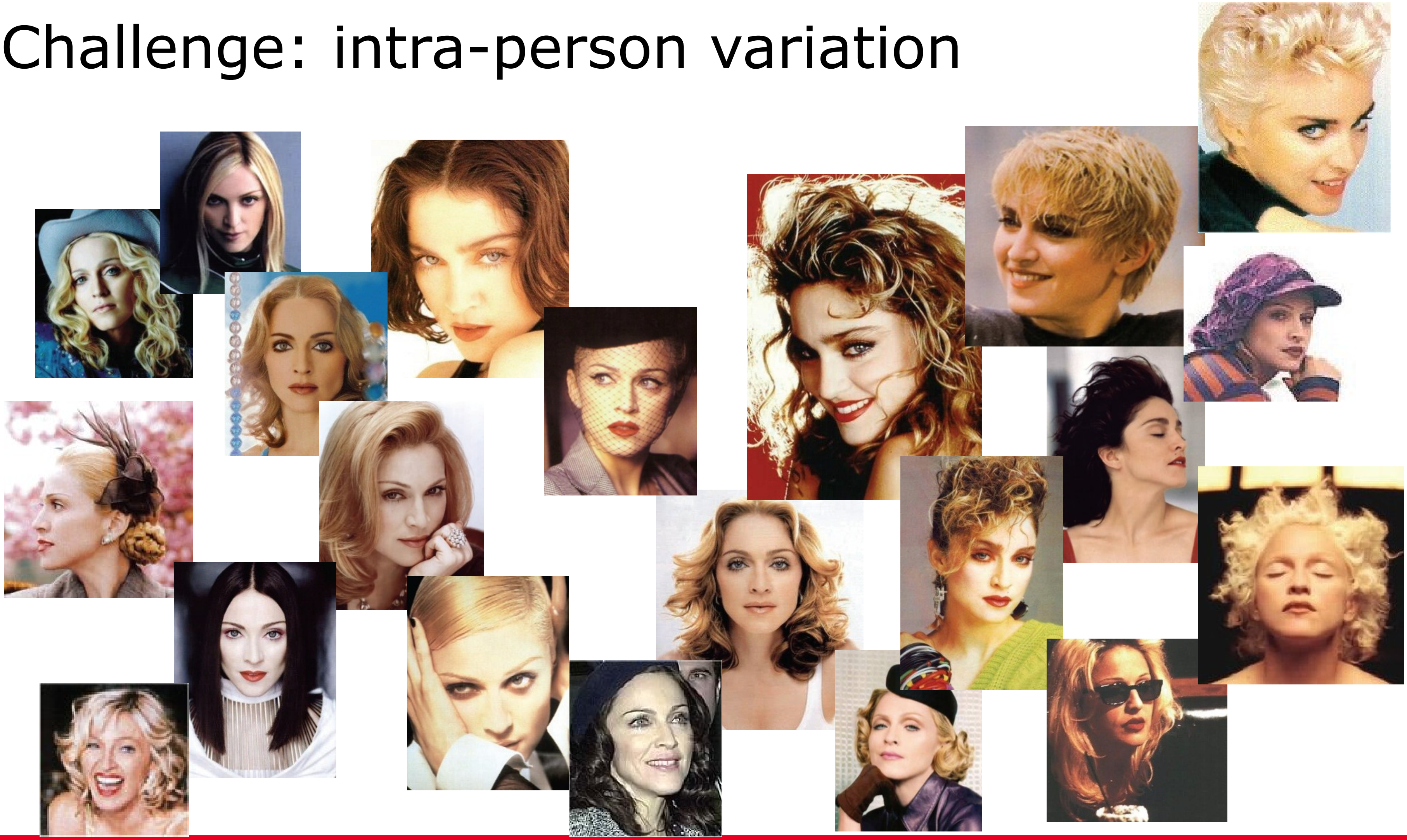
http://multiples.about.com

http://www.nypost.com

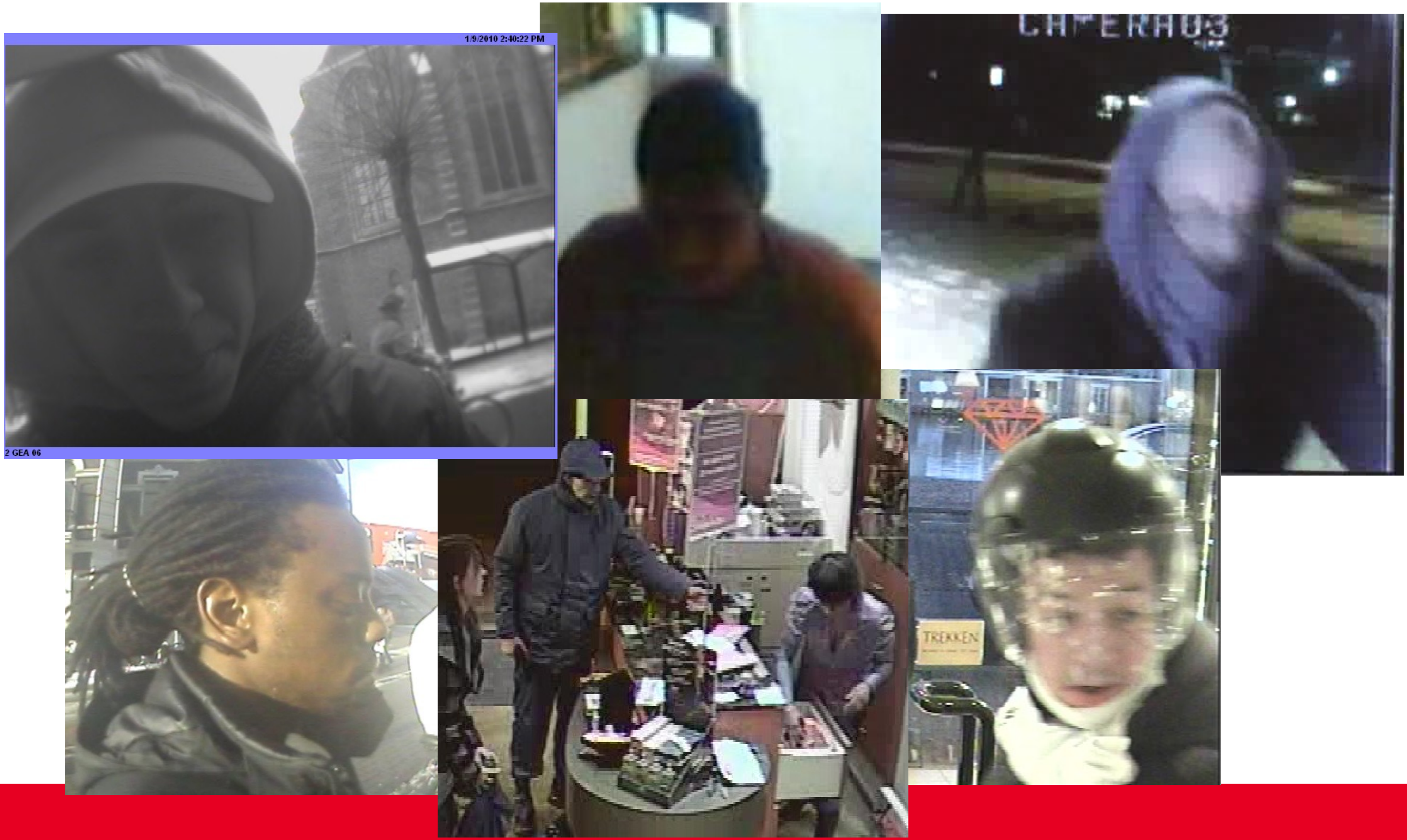
http:// www.tujefetevigila.com

Modality: Face

Challenge: intra-person variation



Case material: Unconditioned images



Confounding factors: subject

- Pose
- Occlusion
- Expression
- Ageing
- Weight change
- Makeup
- Hair
- Jewelry
- Clothing
- ………

Confounding factors: imaging

- Camera position
- Lighting
- Distortion
    - Distance
    - Lens
- Dynamic range
- Sharpness
- Resolution
- Compression
- Noise
- Artifacts
- ……..

Central questions security and safety

Is this the person we are looking for?
Is this the person he/she says to be?

Challenges:

1. Controlled/un controlled environment
2. Distortion image, fingerprint, speech, ….
3. Modalities
4. Level of proof
5. Person & identity

Applications

Face Biometrics applications:

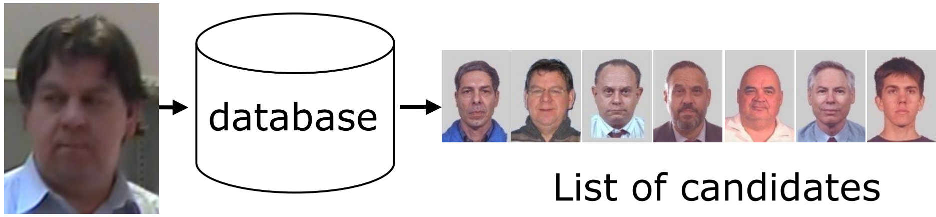
1) Intelligence Gathering for Identity Management

Case A

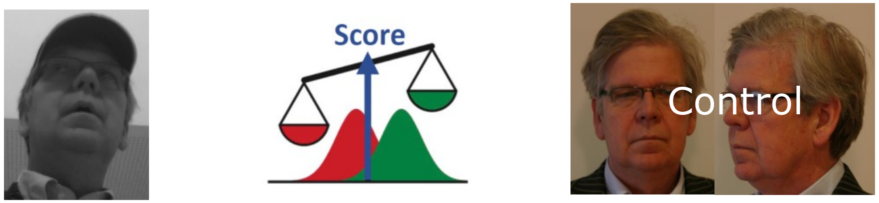
Case B

2) Screening and Access Control

3) Investigative and Operational Tool



4) Forensic Biometrics: Evidence



Ideal Biometric

- **Universal** — applies to (almost) everyone
  - In reality, no biometric applies to everyone
- **Distinguishing** — distinguish with certainty
  - In reality, cannot hope for 100% certainty
- **Permanent** — physical characteristic being measured never changes
  - In reality, want it to remain valid for a long time
- **Collectable** — easy to collect required data
  - Depends on whether subjects are cooperative
- Safe, easy to use, etc., etc.

Biometric Modes

- **Identification** — Who goes there?
  - Compare one to many
  - Example: The FBI fingerprint database
- **Authentication** — Is that really you?
  - Compare one to one
  - Example: Thumbprint mouse
- Identification problem more difficult
  - More “random” matches since more comparisons
- We are interested in authentication

Enrollment vs Recognition

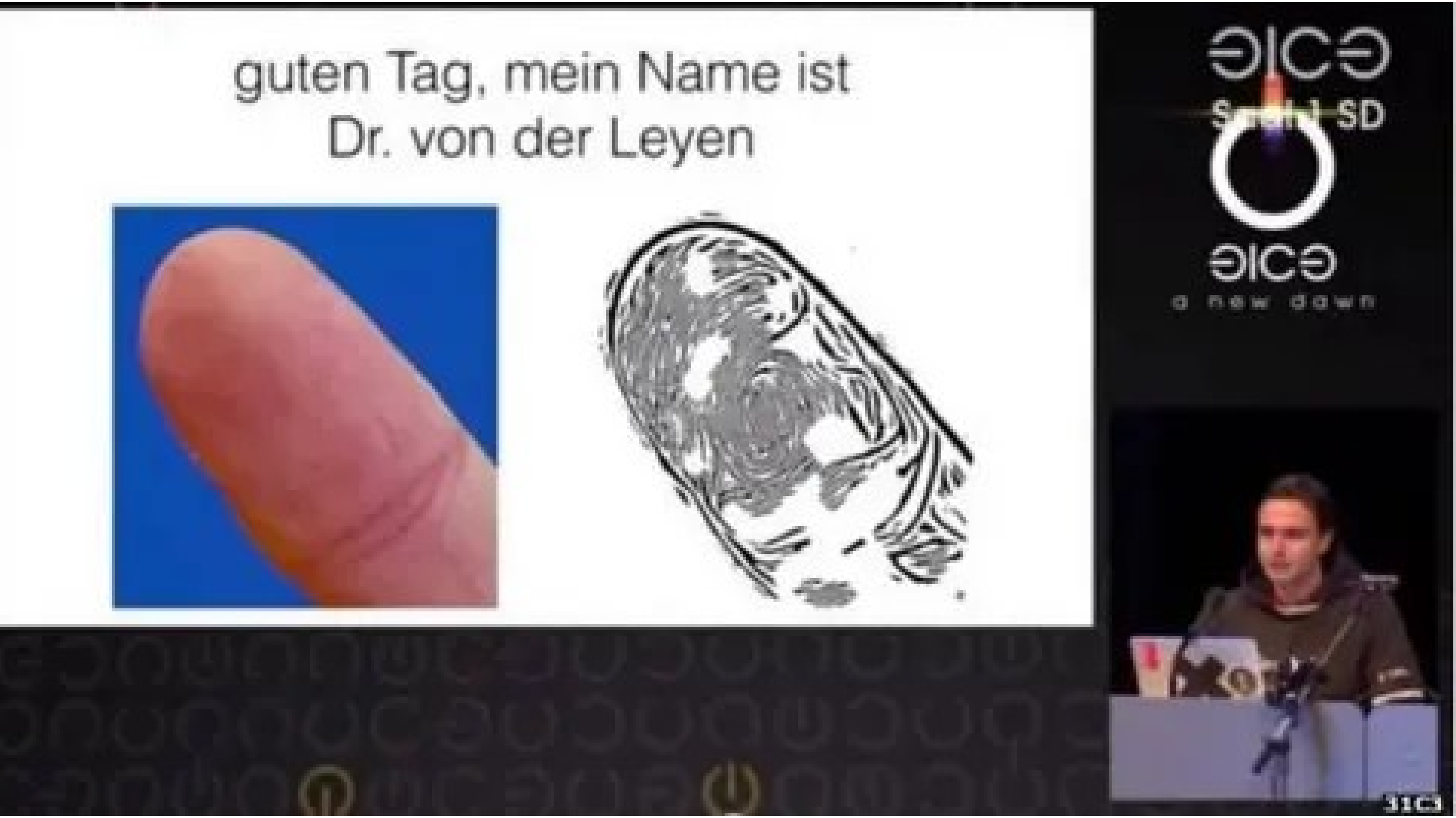
- Enrollment phase
  - Subject’s biometric info put into database
  - Must carefully measure the required info
  - OK if slow and repeated measurement needed
  - Must be very precise for good recognition
  - A weak point of many biometric schemes
- Recognition phase
  - Biometric detection when used in practice
  - Must be quick and simple
  - But must be reasonably accurate

Cooperative Subjects

- We are assuming cooperative subjects
- In identification problem often have uncooperative subjects
- For example, facial recognition
  - Proposed for use in Las Vegas casinos to detect known cheaters
  - Also as way to detect terrorists in airports, etc.
  - Probably do not have ideal enrollment conditions
  - Subject will try to confuse recognition phase
- Cooperative subject makes it much easier!
  - In authentication, subjects are cooperative

Biometric Errors

- **Fraud rate** versus **insult rate**
  - Fraud — user A mis-authenticated as user B
  - Insult — user A not authenticate as user A
- For any biometric, can decrease fraud or insult, but other will increase
- For example
  - 99% voiceprint match ⇒ low fraud, high insult
  - 30% voiceprint match ⇒ high fraud, low insult
- **Equal error rate:** rate where fraud == insult
  - The best measure for comparing biometrics



guten Tag, mein Name ist
Dr. von der Leyen

Fingerprint History

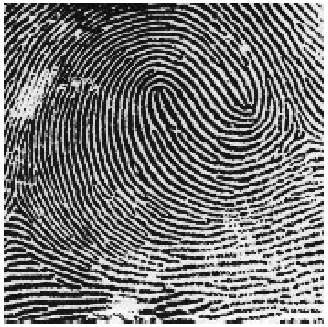
- 1823 — Professor Johannes Evangelist Purkinje discussed 9 fingerprint patterns
- 1856 — Sir William Hershel used fingerprint (in India) on contracts
- 1880 — Dr. Henry Faulds article in *Nature* about fingerprints for ID
- 1883 — Mark Twain's *Life on the Mississippi* a murderer ID'ed by fingerprint

Fingerprint History

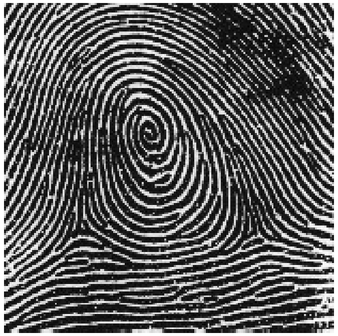
- 1888 — Sir Francis Galton (cousin of Darwin) developed classification system
  - His system of “minutia” is still in use today
  - Also verified that fingerprints do not change
- Some countries require a number of points (i.e., minutia) to match in criminal cases
  - In Britain, 15 points
  - In US, no fixed number of points required

Fingerprint Comparison

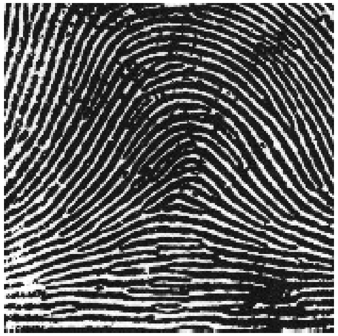
- Examples of loops, whorls and arches
- Minutia extracted from these features



Loop (double)

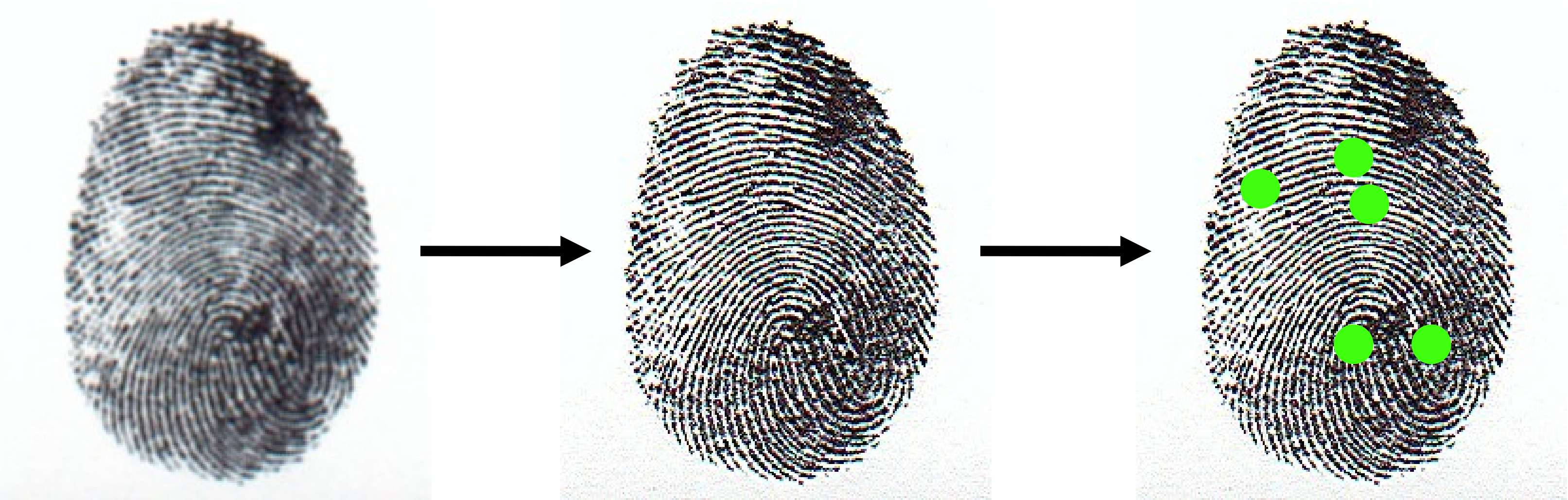


Whorl



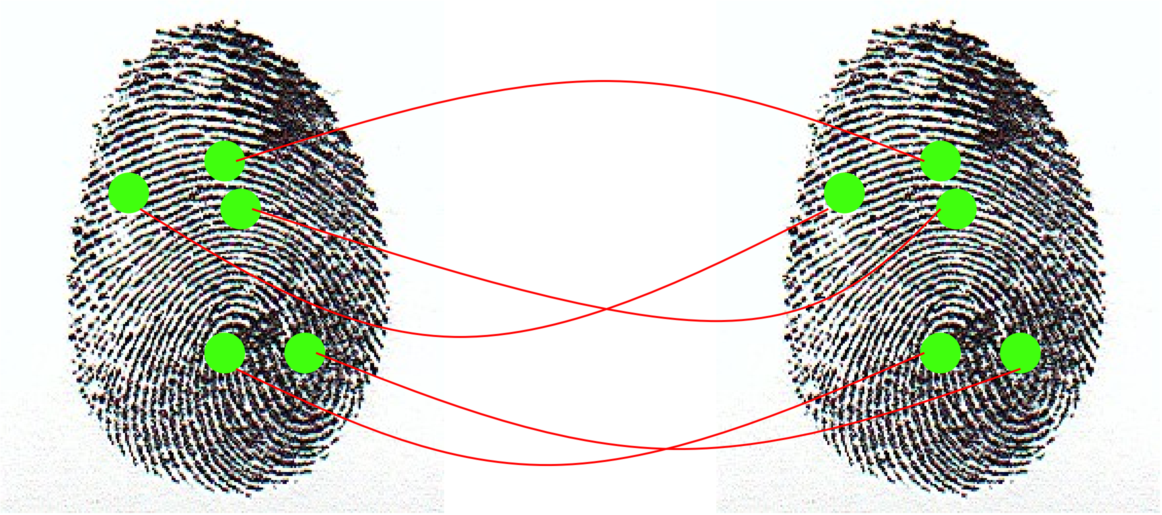
Arch

Fingerprint Biometric



- Capture image of fingerprint
- Enhance image
- Identify minutia

Fingerprint Biometric



- Extracted minutia are compared with user's minutia stored in a database
- Is it a statistical match?

Hand Geometry

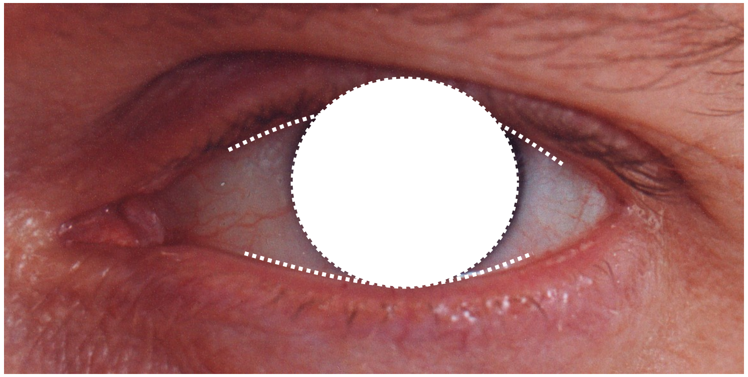
- Popular form of biometric
- Measures shape of hand
  - Width of hand, fingers
  - Length of fingers, etc.
- Human hands not unique
- Hand geometry sufficient for many situations
- Suitable for authentication
- Not useful for ID problem

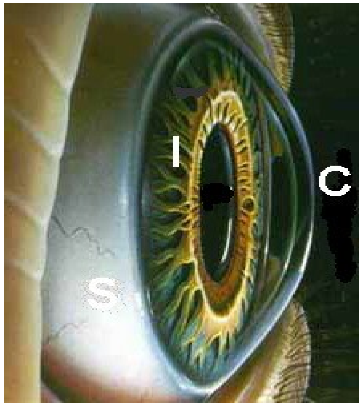
INSTRUCTIONS
PRÉSENTER VOTRE CARTE AU CENTRE DU LECTEUR
ATTENDRE QUE L'AFFICHAGE INDIQUE "POSER MAIN"
INSÉRER VOTRE MAIN DANS LE LECTEUR DE MAIN
ATTENDRE L'ACCEPTATION DU LECTEUR DE MAIN
ATTENDRE LA LUMIÈRE VERTE SUR LE TOURNIQUET
TRAVERSER LE TOURNIQUET
101/1
RSI 101/1

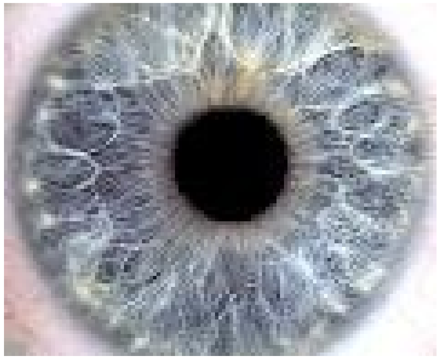
Hand Geometry

- Advantages
  - Quick
  - 1 minute for enrollment
  - 5 seconds for recognition
  - Hands symmetric (use other hand backwards)
- Disadvantages
  - Cannot use on very young or very old
  - Relatively high equal error rate

Iris Patterns







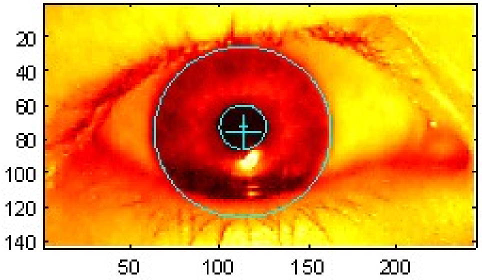
- Iris pattern development is “chaotic”
- Little or no genetic influence
- Different even for identical twins
- Pattern is stable through lifetime

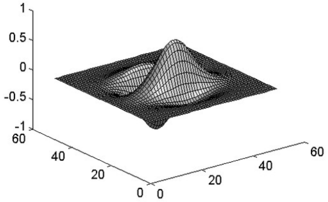
Iris Recognition: History

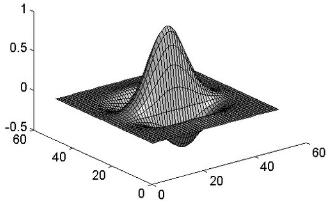
- 1936 — suggested by Frank Burch
- 1980s — James Bond films
- 1986 — first patent appeared
- 1994 — John Daugman patented best current approach
  - Patent owned by Iridian Technologies

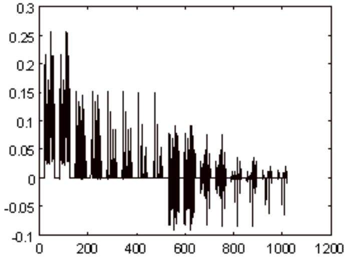
Iris Scan

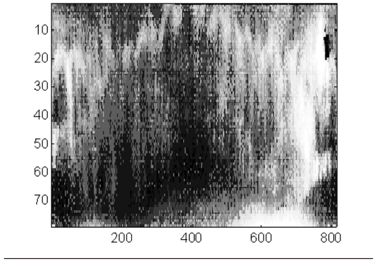
- Scanner locates iris
- Take b/w photo
- Use polar coordinates…
- Find 2-D wavelet trans
- Get 256 byte iris code











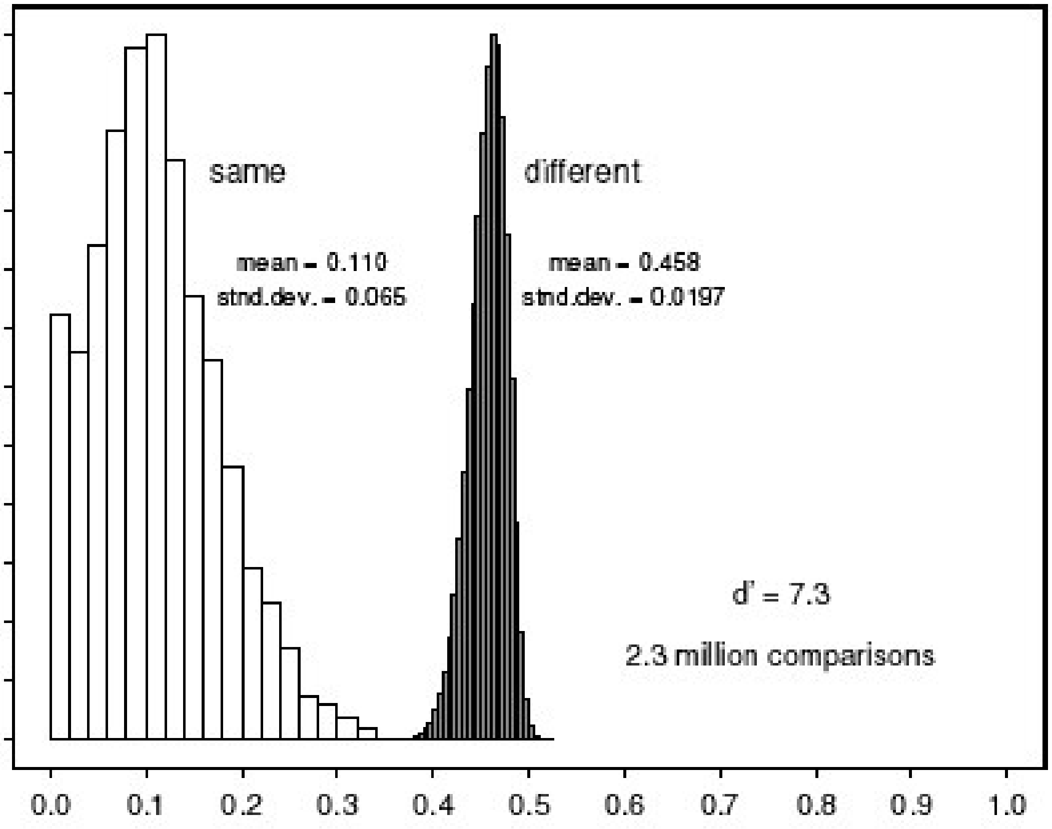
Measuring Iris Similarity

- Based on Hamming distance
- Define d(x,y) to be
  - # of non-match bits / # of bits compared
  - d(0010,0101) = 3/4 and d(101111,101001) = 1/3
- Compute d(x,y) on 2048-bit iris code
  - Perfect match is d(x,y) = 0
  - For same iris, expected distance is 0.08
  - At random, expect distance of 0.50
  - Accept iris scan as match if distance < 0.32

Iris Scan Error Rate

distance	Fraud rate
0.29	1 in $1.3 \ast 10^{10}$
0.30	1 in $1.5 \ast 10^{9}$
0.31	1 in $1.8 \ast 10^{8}$
0.32	1 in $2.6 \ast 10^{7}$
0.33	1 in $4.0 \ast 10^{6}$
✶ 0.34	1 in $6.9 \ast 10^{5}$
0.35	1 in $1.3 \ast 10^{5}$

✶ : equal error rate



ROC Curve

receiver operating characteristic

Attack on Iris Scan

- Good **photo** of eye can be scanned
- And attacker can use photo of eye
- Afghan woman was authenticated by iris scan of old photo
  - Story is here
- To prevent photo attack, scanner could use light to be sure it is a “live” iris

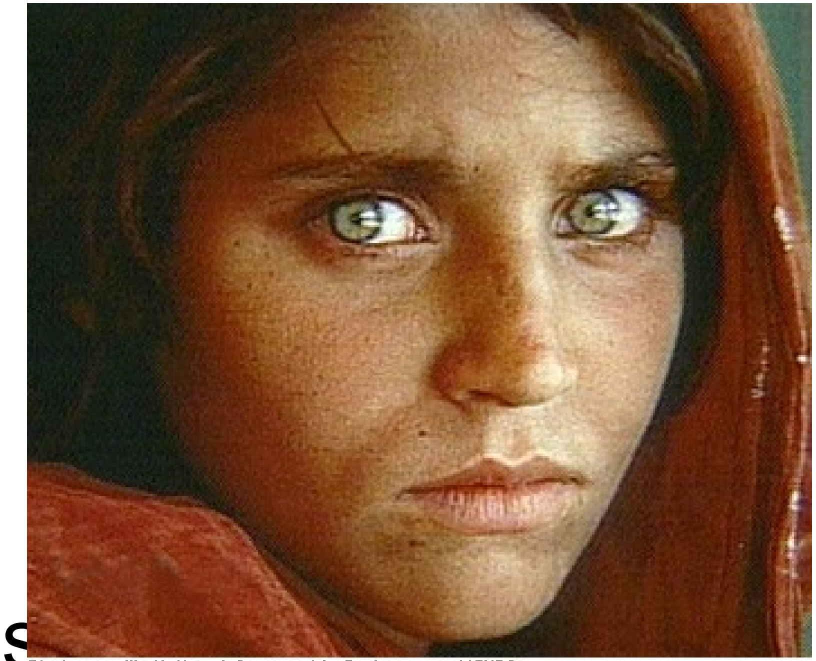


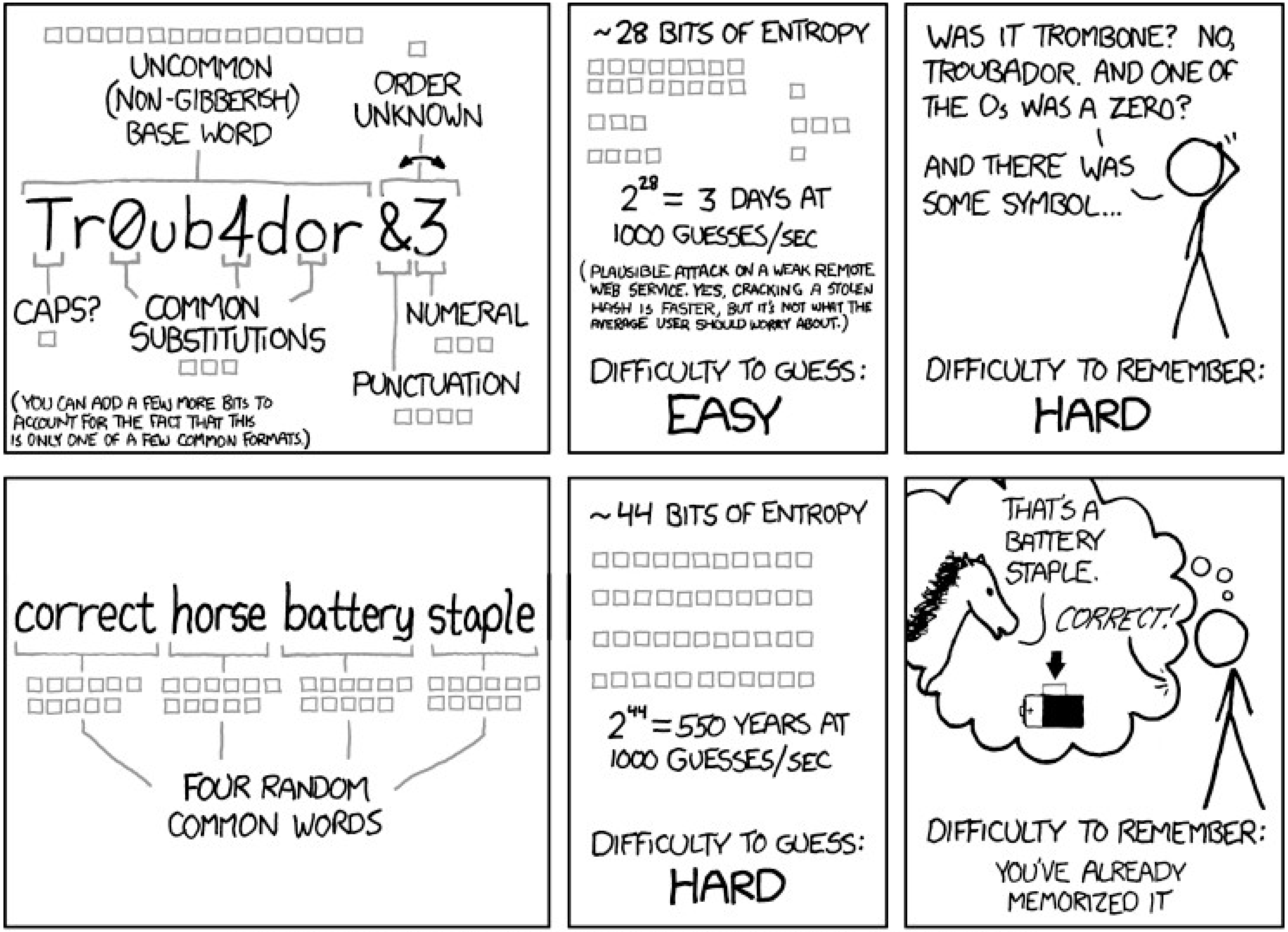
Photo credit: National Geographic Explorer on MSNBC

Equal Error Rate Comparison

- Equal error rate (EER): fraud == insult rate
- **Fingerprint** biometric has EER of about 5%
- **Hand geometry** has EER of about 10^{-3}
- In theory, **iris scan** has EER of about 10^{-6}
  - But in practice, hard to achieve
  - Enrollment phase must be extremely accurate
- Most biometrics much worse than fingerprint!
- Biometrics useful for authentication…
- But ID biometrics are almost useless today

Biometrics: The Bottom Line

- Biometrics are hard to forge
- But attacker could
  - Steal Alice’s thumb
  - Photocopy Bob’s fingerprint, eye, etc.
  - Subvert software, database, “trusted path”, …
- Also, how to revoke a “broken” biometric?
- **Biometrics are not foolproof!**
- Biometric use is limited today
- That should change in the future…


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor&3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Mind effectiveness