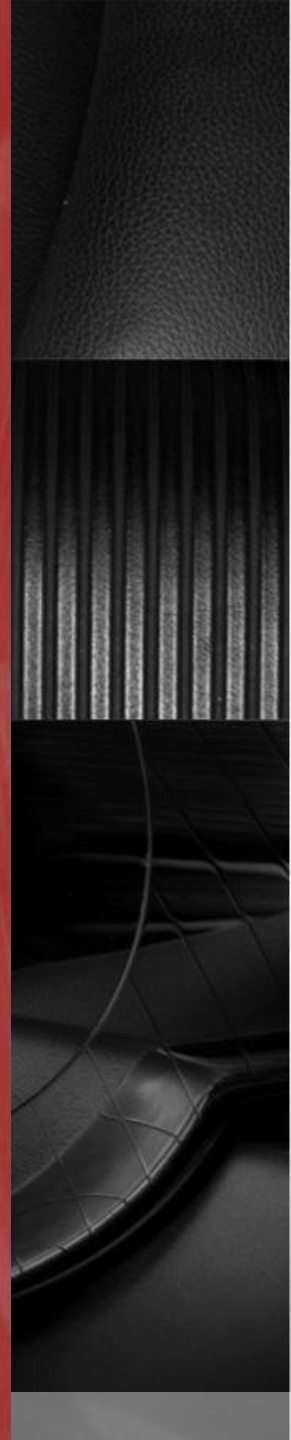
Chapter 15 - Biometrics

Alex Slutsky

Computer security seminar

Spring 2014

University of Haifa



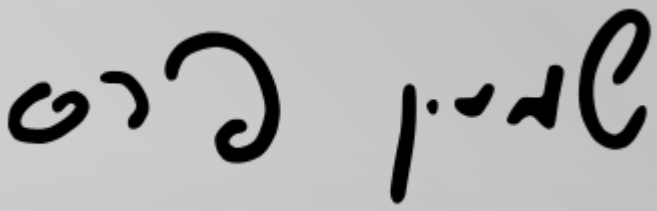
What is Biometrics?

Biometrics refers to the quantifiable data (or metrics) related to human characteristics and traits such as:

- Individual anatomy or physiology: hand geometry.
- Ingrained skill or behavior: handwritten signature.
- Combination of the two: your voice.

Handwritten Signatures

- Handwritten signatures are a very weak authentication mechanism by themselves but have worked well for centuries.



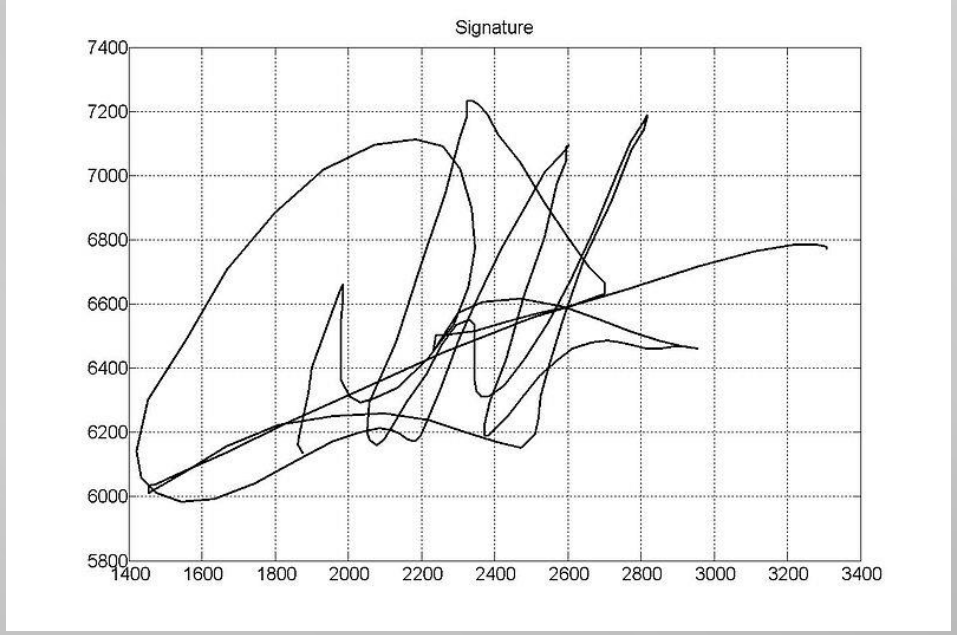
Signature of shimon Peres. Source: Wikipedia

Forged Signatures

- The law in Israel states that a forged document is null and void.
- Israeli banks are held accountable for accepting forged cheques.
- Bank tellers may struggle to authenticate a signature, as shown by the next experiment:
- An experiment showed that 105 professional document examiners, who each did 144 pairwise comparisons, misattributed 6.5% of documents.

Automatic Recognition of Handwritten Signatures

- This turns out to be a very difficult image processing task because of the variability between one genuine signature and another.
- The most popular method today is dynamic recognition, also known as “on-line”.



Example of dynamic signature. Source: Wikipedia

Errors Explained

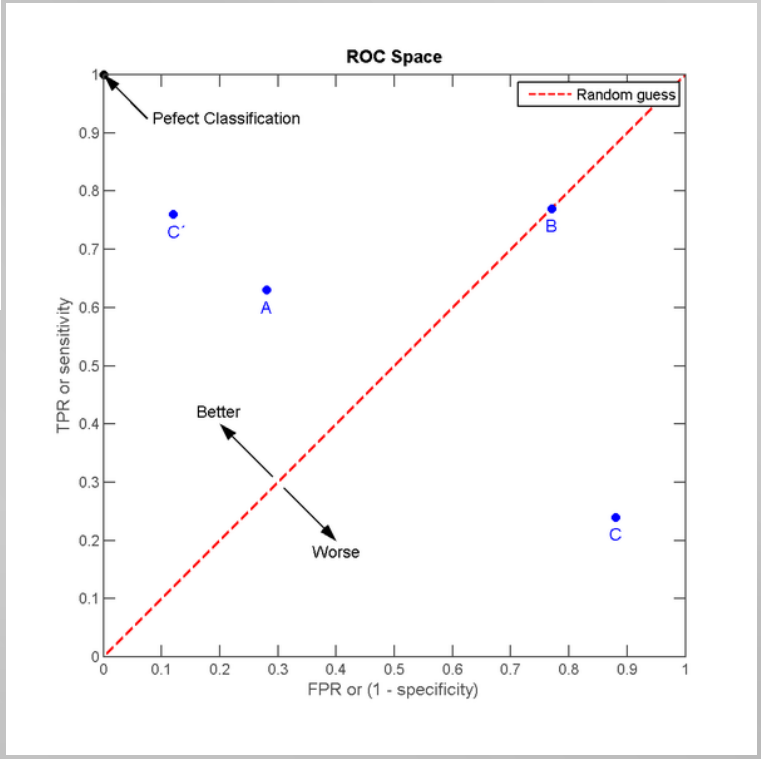
- Fraud (false acceptance rates) and insult (false rejection) rates.
- Equal error rate.
- UK banks set a target for biometrics of a fraud rate of 1% and an insult rate of 0.01%.

Receiver Operating Characteristic

		Condition (as determined by "Gold standard")	
		Condition positive	Condition negative
Test outcome	Test outcome positive	True positive	False positive (Type I error)
	Test outcome negative	False negative (Type II error)	True negative

Precision = Σ True positive / Σ Test outcome positive	Negative predictive value = Σ True negative / Σ Test outcome negative	
Sensitivity = Σ True positive / Σ Condition positive	Specificity = Σ True negative / Σ Condition negative	Accuracy

A			B			C			C′		
TP=63	FP=28	91	TP=77	FP=77	154	TP=24	FP=88	112	TP=76	FP=12	88
FN=37	TN=72	109	FN=23	TN=23	46	FN=76	TN=12	88	FN=24	TN=88	112
100	100	200	100	100	200	100	100	200	100	100	200
TPR = 0.63			TPR = 0.77			TPR = 0.24			TPR = 0.76		
FPR = 0.28			FPR = 0.77			FPR = 0.88			FPR = 0.12		
PPV = 0.69			PPV = 0.50			PPV = 0.21			PPV = 0.86		
F1 = 0.66			F1 = 0.61			F1 = 0.22			F1 = 0.81		
ACC = 0.68			ACC = 0.50			ACC = 0.18			ACC = 0.82		



All images taken from Wikipedia

Face Recognition

- Recognizing people by their facial features is the oldest identification mechanism of all, going back at least to our early primate ancestors.

Image taken from Wikipedia.

Recognizing People

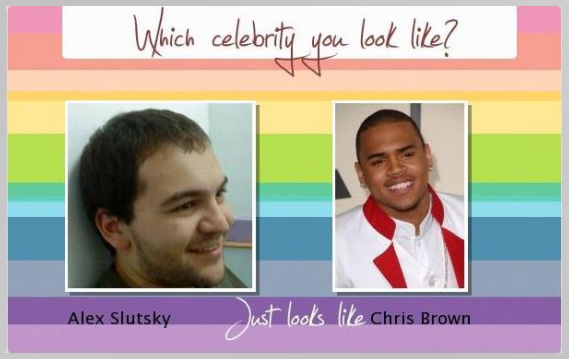
- But even if we are good at recognizing friends in the flesh, how good are we at identifying strangers by photo ID?

Facial Recognition Experiment

- 44 students, each with 4 different photographs:
  - 1. Good, Good:

  - 2. Bad, Good:

  - 3. Good, Bad:



  - 4. Bad, Bad:

Facial Recognition

- Even picking out faces from an image of a crowd is a non-trivial computational task.
- Error rates were up to 20%.

Bertillonage

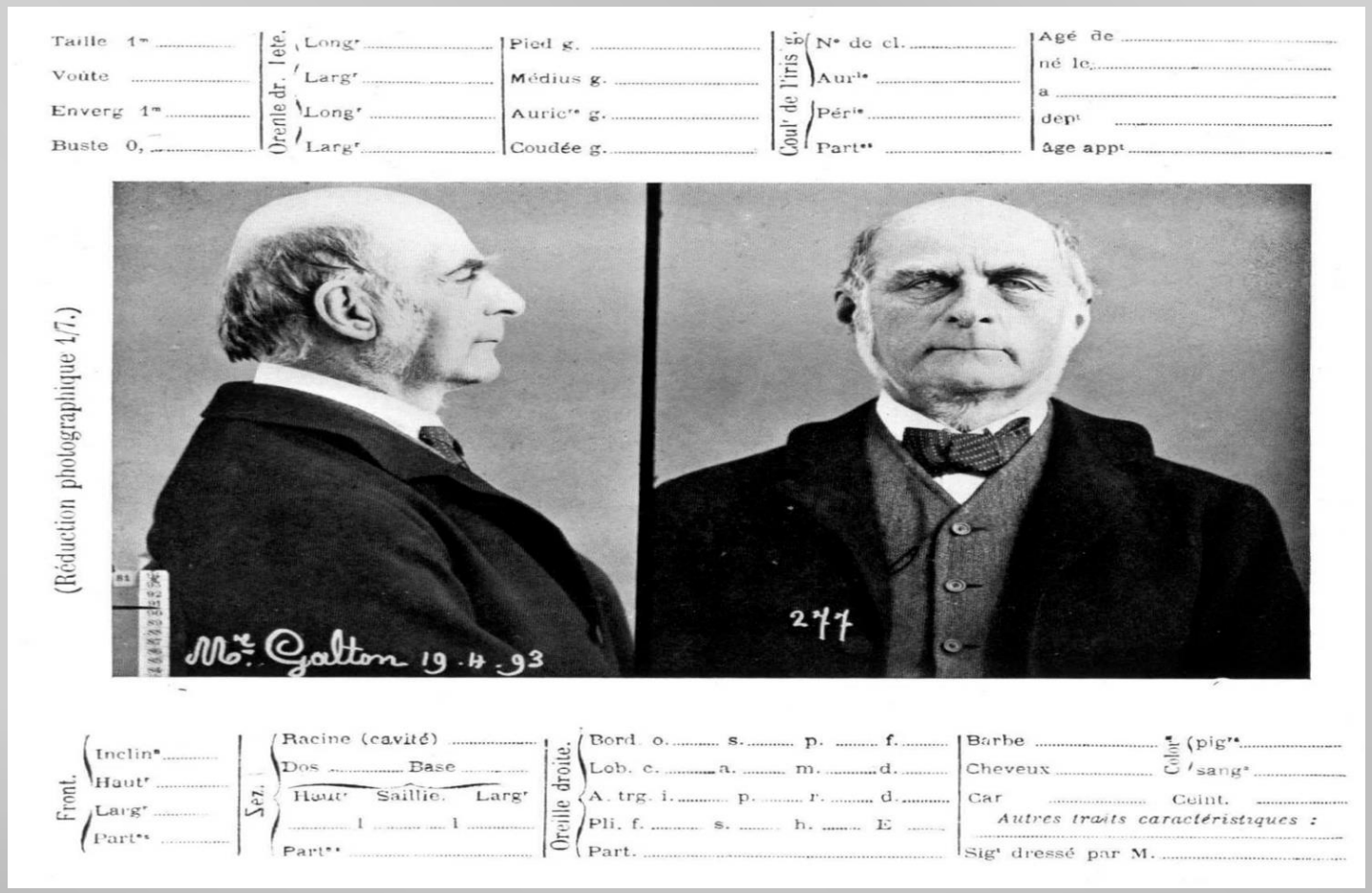


Image taken from Wikipedia.

Bertillonage

- System based on bodily measurements, such as height standing and sitting, the length and width of the face, and the size and angle of the ear.
- This technique has made a comeback in the form of hand-geometry readers.

Fingerprints

The use of fingerprints to identify people was discovered independently a number of times:

- In the Spanish version of history, they were first used in Argentina where they secured a murder conviction in 1892; while Cuba, which set up its fingerprint bureau in 1907, beat the USA whose first conviction was in Illinois in 1911.
- The Croatian version notes that the Argentinian system was developed by one Juan Vucetich, who had emigrated from Dalmatia.
- The German version refers to Professor Purkinje of Breslau, who wrote about fingerprints in 1828. Success truly has many fathers!

Verifying Positive or Negative Identity Claims

American police forces have historically used fingerprints to:

- Identify arrested suspects to determine whether they are currently wanted by other agencies.
- Whether they have criminal records.
- Whether they have previously come to attention under other names.

Vulnerability

- An old trick was for a crook to distract (or bribe) the officer fingerprinting him.
- Fingerprints could be molded and cloned quickly and cheaply using cooking gelatin.
- Breathing on a finger scanner to reactivate a latent print left there by a previous, authorized, user.

Crime Scene Forensics

- 16-point fingerprint match was considered to be incontrovertible evidence.
- In Israel 12-point, 9-point and even 7-point fingerprint is mentioned in court.
- But then came Shirley McKie.

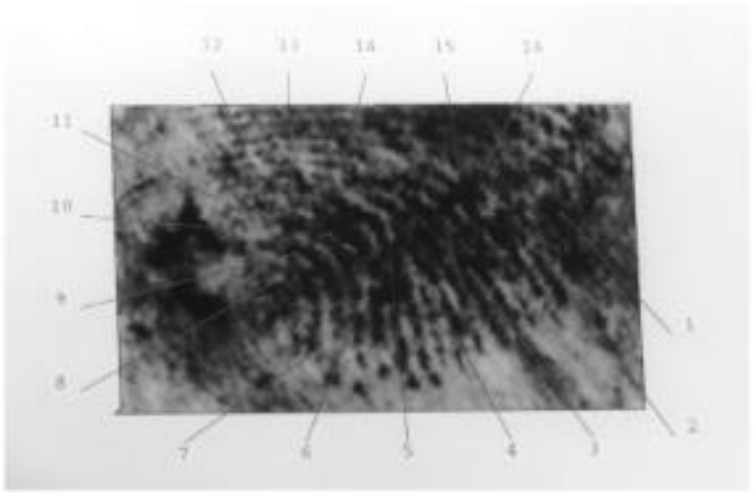


Figure 15.1: Crime scene print

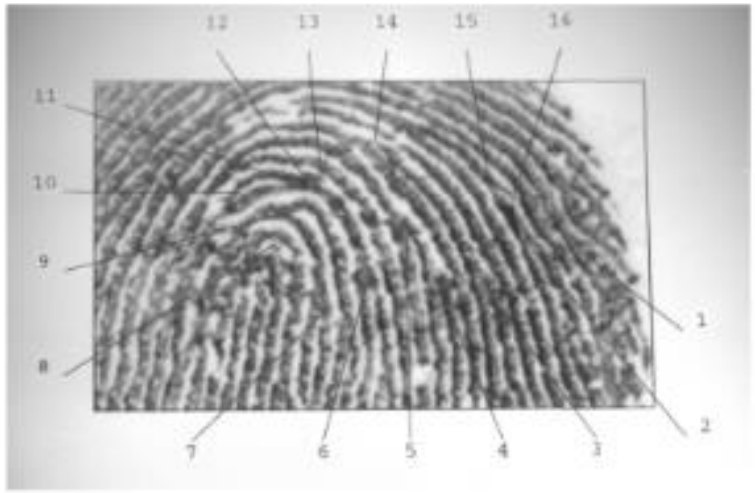


Figure 15.2: Inked print

Image taken from Ross Andresson's book ``Security Engineering''

Are Fingerprints Reliable?

Psychologist Itiel Dror conducted an experiment:

- Six experts who each looked at eight prints, all of which they had examined for real in the previous few years.
- Only two of the experts remained consistent.
- The other four experts made six inconsistent decisions between them.
- The prints had a range of difficulty, and in only half of the cases was misleading contextual information supplied.

Important points

- Dror's work confirmed that the cases in which misidentifications occur tend to be the difficult ones.
- It was inevitable that sooner or later, in a large enough database a 16-point mismatch would be found.
- The belief that any security mechanism is infallible creates the complacency and carelessness needed to undermine its proper use.
- A belief of infallibility ensures that the consequences of the eventual failure will be severe.

Iris Codes

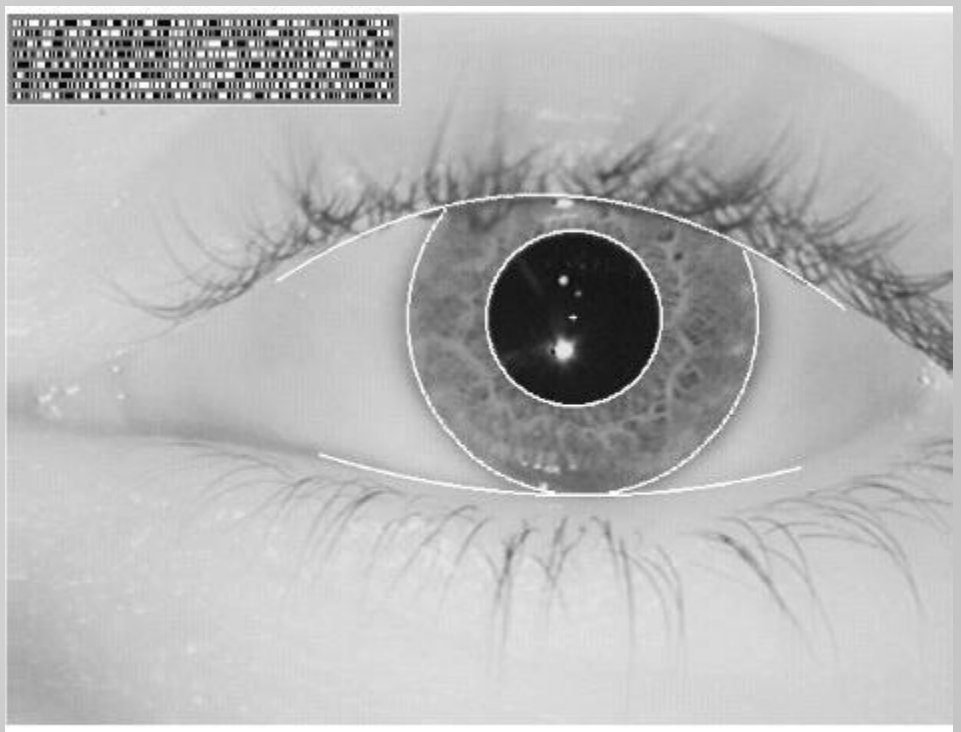


Figure 15.3: An iris with iris code (courtesy John Daugman)

Image taken from Ross Andresson's book “Security Engineering”.

Iris Codes

- Iris codes provide the lowest false accept rates of any known verification system — zero.
- So far as is known, every human iris is measurably unique.
- The iris pattern contains a large amount of randomness, and appears to have many times the number of degrees of freedom of a fingerprint.

Iris Codes - Problems

- Many things, from eyelashes to hangovers, can cause the camera to not see enough of the iris.
- Failure to enroll certain people.
- Getting the picture cheaply without being too intrusive.

Voice Recognition

- Voice recognition is the attempt to authenticate a person using recordings of his/hers voice.
- There are some interesting attacks on these systems.

Other Biometrics

- Typing patterns.
- Vein patterns.
- Literary analysis.
- Facial thermograms.
- DNA typing.

What Goes Wrong?

- Forensic biometrics often do not tell as much as one might assume.
- Another aspect of freshness is that most biometric systems can, at least in theory, be attacked using suitable recordings.
- Most biometrics are not as accurate for all people, and some of the population can not be identified as reliably as the rest (or even at all).

What Goes Wrong? continued

- A point that follows from this is that systems may be vulnerable to collusion.
- The statistics are often not understood by system designers, and the birthday paradox is particularly poorly appreciated.
- Another aspect of statistics comes into play when designers assume that by combining biometrics they can get a lower error rate.

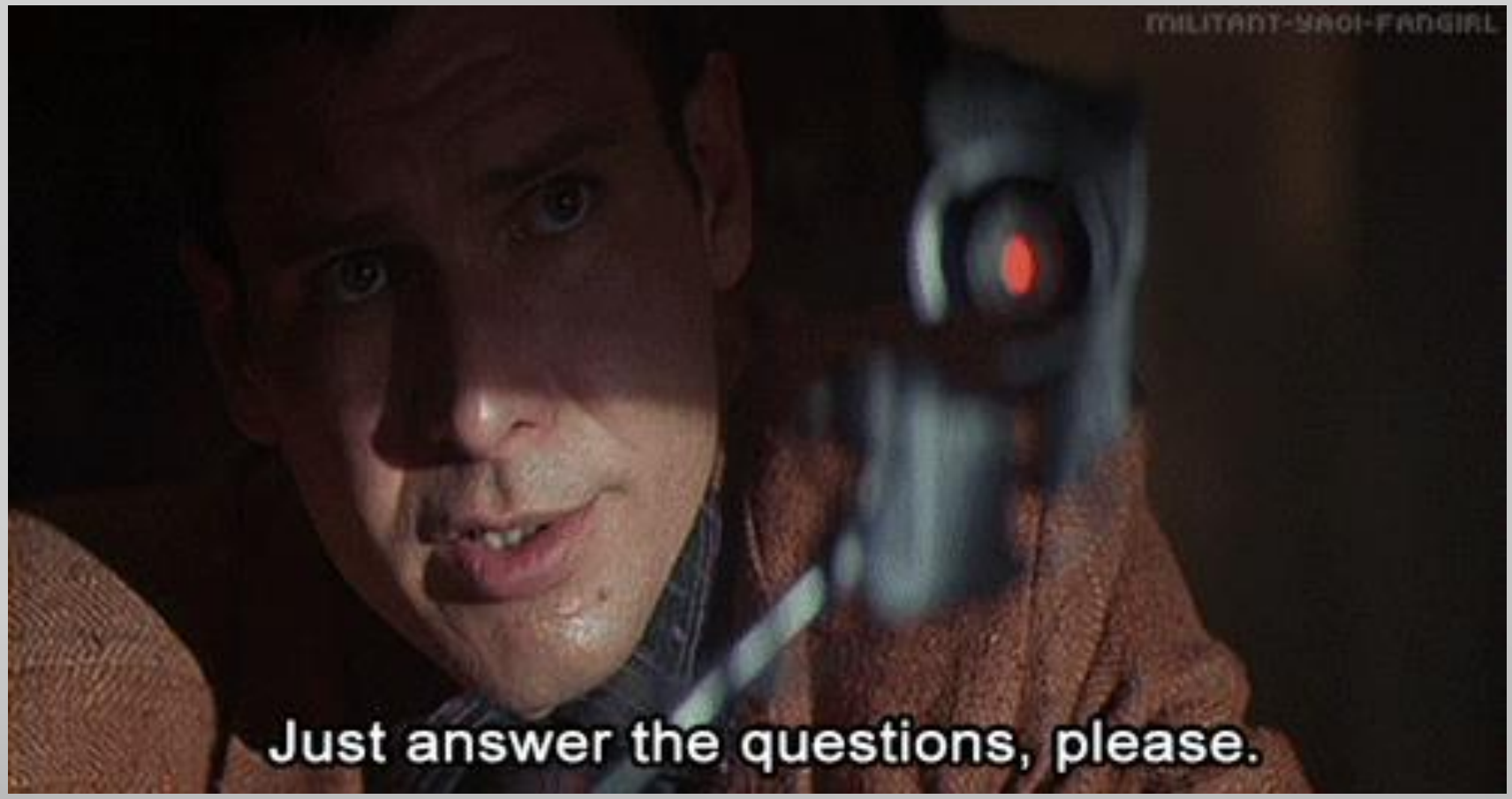
What Goes Wrong? continued

- Many vendors have claimed that their products protect privacy.
- Automating biometrics can subtly change the way in which security protocols work, so that stuff that used to work now does not.
- It is worth thinking what happens when humans and computers disagree.

Research Problems

- Is it possible to build a system — other than iris scanning— which will meet the banks' goal of a 1% fraud rate and a 0.01% insult rate?
- Is it possible to build a static signature verification system which has a good enough error rate?
- Are there any completely new biometrics that might be useful in some circumstances?

Question?



Applause