

Computer Security Seminar

Biometrics



Aviv Abramovich
Spring 2015
University of Haifa

Contents

- Section 1 – Introduction
- Section 2 – Systems
 1. Handwritten Signatures
 2. Face Recognition
 3. Bertillonage
 4. Fingerprints
 5. IRIS Code
 6. Voice Recognition
 7. Other Systems
- Section 3 – Comperasions
- Section 4 – What Goes Wrong? And Conclusions

"ד וַיִּקְבֹּץ יַפְתָּח אֶת-כָּל-אֲנָשֵׁי גִלְעָד, וַיִּלָּחֶם אֶת-אֶפְרָיִם;
וַיְכּוּ אֲנָשֵׁי גִלְעָד אֶת-אֶפְרָיִם, כִּי אָמְרוּ פְּלִיטֵי אֶפְרָיִם אֲתֵם-
גִלְעָד, בְּתוֹךְ אֶפְרָיִם בְּתוֹךְ מְנַשֶּׁה. ה וַיִּלְכֹּד גִלְעָד אֶת-
מַעְבְּרוֹת הַיַּרְדֵּן, לְאֶפְרָיִם; וְהָיָה כִּי יֹאמְרוּ פְּלִיטֵי אֶפְרָיִם,
אֲעֹבְרָהּ, וַיֹּאמְרוּ לוֹ אֲנָשֵׁי-גִלְעָד הַאֶפְרָתִי אַתָּה, וַיֹּאמֶר
לֹא. ו וַיֹּאמְרוּ לוֹ אֲמָר-נָא שְׂבַלְתָּ וַיֹּאמֶר סְבַלְתָּ, וְלֹא יָכִין
לְדַבֵּר כֵּן, וַיֹּאחֲזוּ אוֹתוֹ, וַיִּשְׁחַטְוּהוּ אֶל-מַעְבְּרוֹת הַיַּרְדֵּן;
וַיִּפֹּל בְּעֵת הַהִיא, מֵאֶפְרָיִם, אַרְבַּעַיִם וּשְׁנַיִם, אֶלְפֵי"

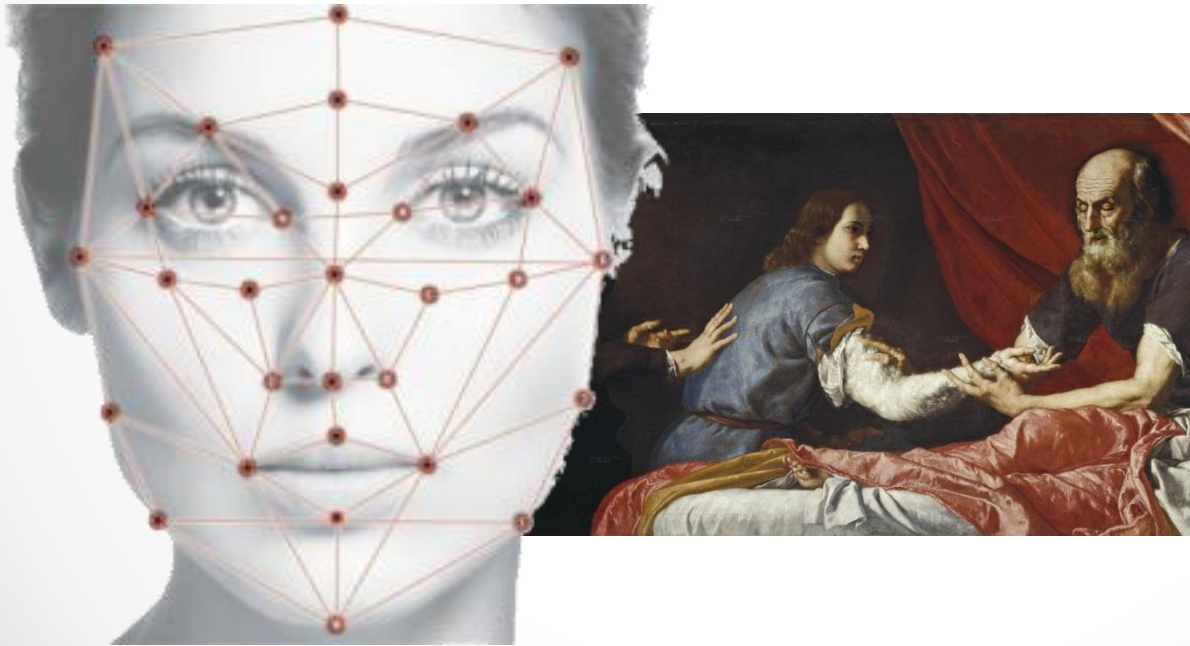
ספר שופטים, פרק י"ב, פסוקים ד'-ו'

What is “Biometrics”?

Biometrics is a name for a bunch of methods to identify or authenticate people by unique features

What is “Biometrics”? (Cont.)

1. Identify by measuring some aspect of individual anatomy or physiology (Fingerprints, face-Recognition, hand-Geometry, etc..)



What is “Biometrics”? (Cont.)

2. Some deeply ingrained skills or behavior
(Accent, language, signature...)

Language ភាសា Linguaggio ЯЗЫК
Γλώσσα Język ភាសា لسان بولی
भाषा ភាសា 言語 Language
Langage ভাষা 言語
भाषा భాష 鮫 言語
Linguagem Wika ភាសា اللغة
Sprache 语言 𑌕𑌗𑌕 Bahasa 언어



3. Combinations of these two

Some background...

The biometrics exists for thousands of years (the Jacob and Isaack story) but were not enough reliable and advanced.

Since the 9/11 terror attacks, the market has significantly taken off.

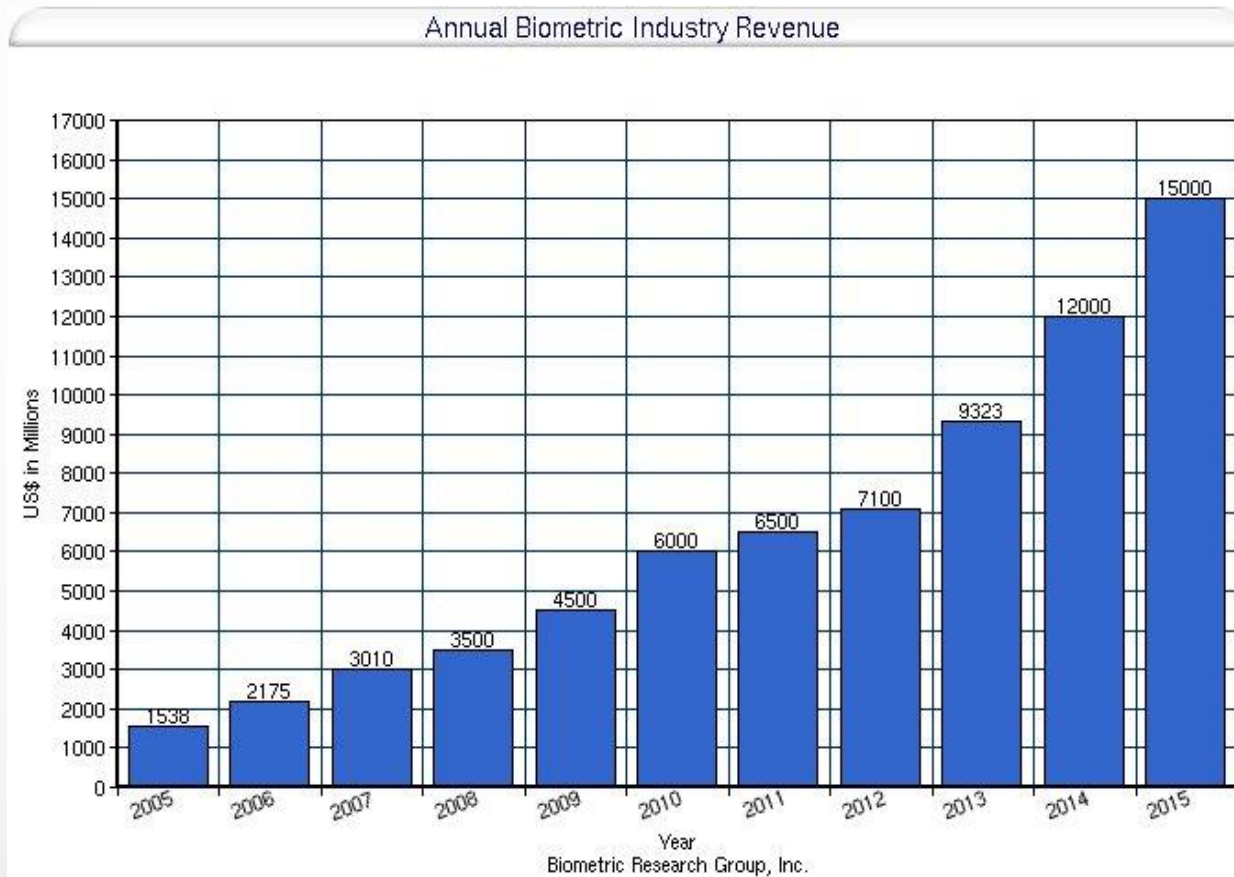
US-VISIT program which fingerprints visitors to the USA and the FBI's fingerprint database.

Market Worth

1998: market worth: 50 millions \$

2005: market worth 1.5 billion \$ (30,000% in less than a decade!!!)

By 2020: **34 billion \$** (estimation, MarketsAndMarkets.com)



Biometric and Data Security?

- Authentication system
- Security
- Access Control

Access Control - בקרת גישה - פרק 4 בספר "Security Engineering" של רוס אנדרסון

סמינר באבטחת מחשבים עם פרופ' אור דונקלמן
מוצג ע"י מוסטפא מחאמיד

19.04.2015

MULTILEVEL SECURITY
CHAPTER 8 IN SECURITY ENGINEERING
AMIR SHWARTZ

https://www.centos.org/docs/5/html/Deployment_Guide-en-US/sec-mls-ov.html

MULTILATERAL SECURITY

Based on chapter 9 of "Security Engineering" by Ross Anderson

Presenter: Omer Paparo – עומר פפרו

Handwritten Signatures

Origin: Classical China, carved seals.
considered higher status.

In Europe start around the medieval times, but used mainly to write the people names.

Very weak authentication mechanism (Very easy to forge) but have worked well for centuries...



Carved seals

(Source: Google images)

A handwritten signature in black ink that reads "Steve Jobs". The signature is written in a cursive, flowing style with a long, sweeping tail on the final letter.

Steve Jobs' Signature
(Source: Wikipedia)

Handwritten Signatures (cont.)

Who's to blame when signature is forged?



Fraud and insult rates (More about it in the next slides)

It's difficult to automatically check if a handwritten signature is authentic.

Signature tablets

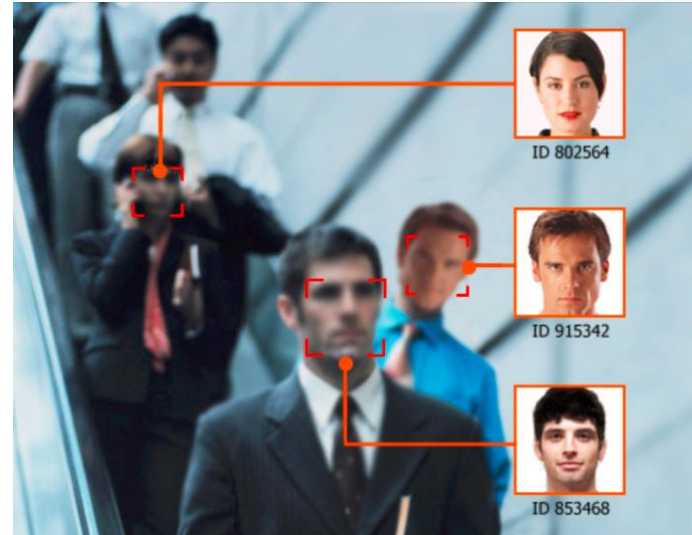
Face Recognition

The ability to identify people by their faces

Deterrence

How good we
are with strangers?

20% of witnesses making
mistakes in identity parades



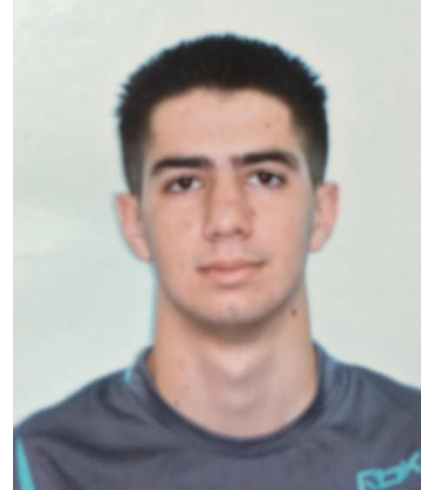
Face Recognition (Cont.)

The west-minster supermarket's experiment:

good,good



bad,good



good,bad



bad,bad



Face Recognition (Cont.)

Photo-ID doesn't seem to work, and this is one of the reasons for trying to automate the process

By 2003, the technology had improved somewhat, with one vendor recognizing 64% of subjects against a database of over 30,000.

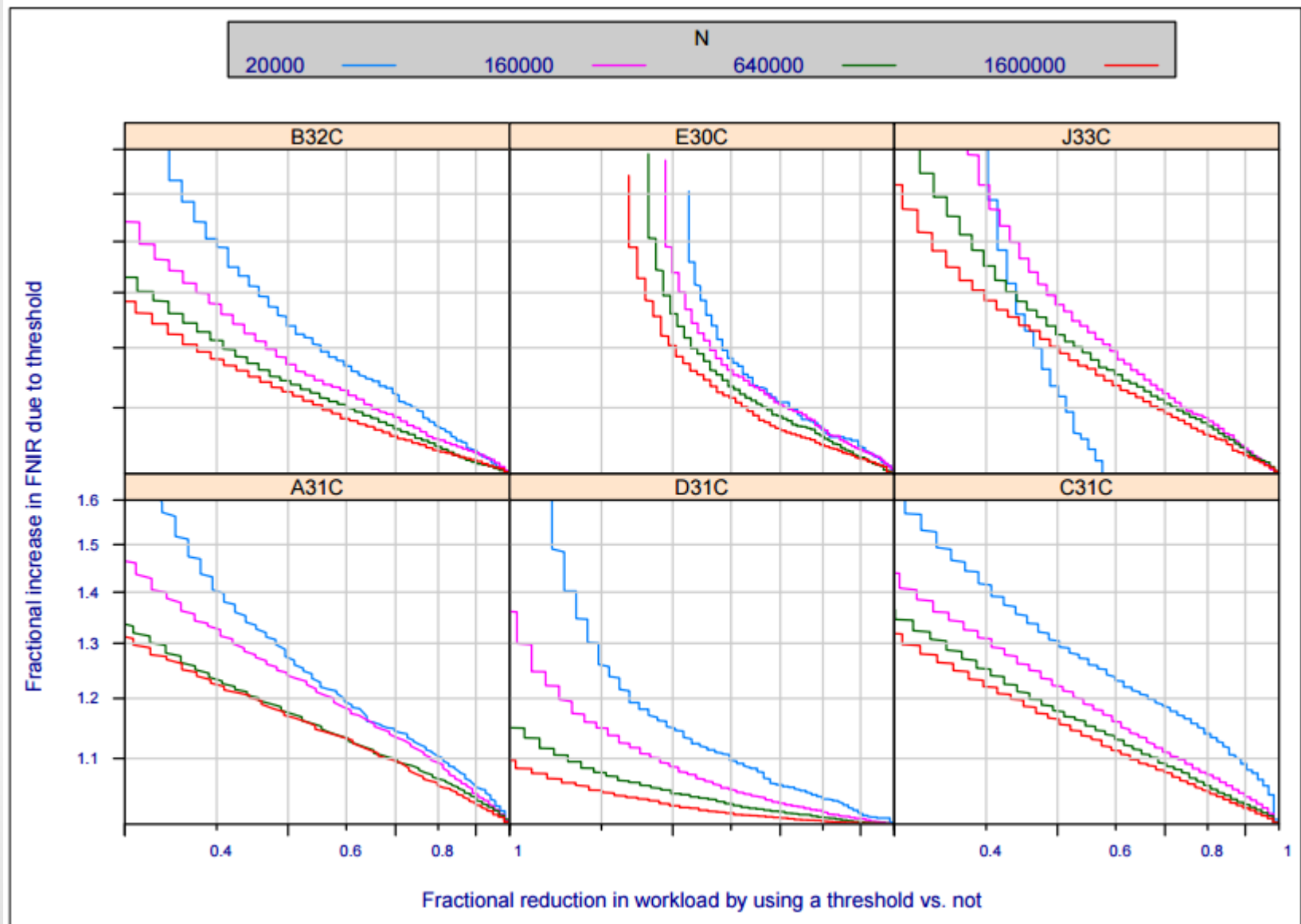
NIST's FRVT

Error rates were up to 20%

Yet facial recognition is already the second largest-selling biometric with a nominal 19% of the market



It's all about the threshold

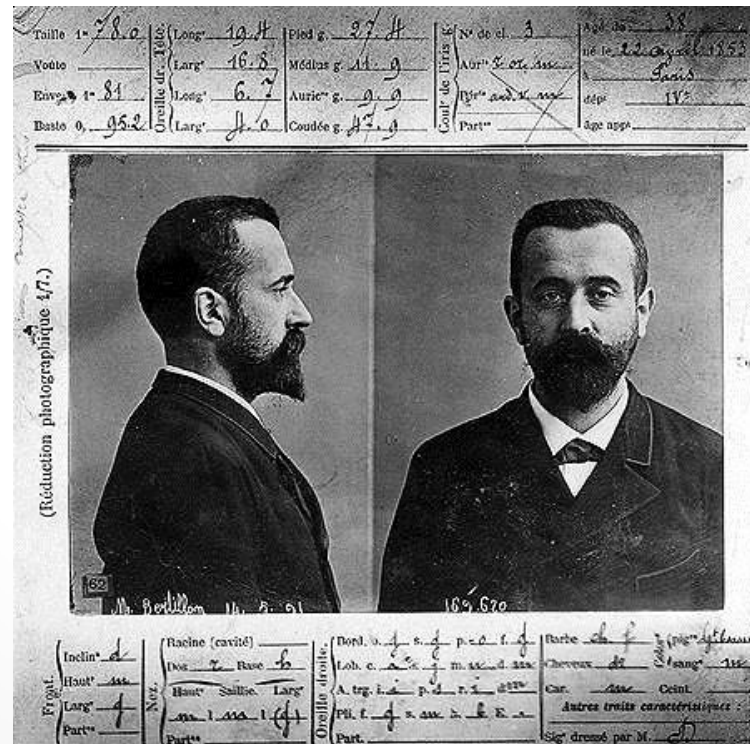


Source: FRVT 2014 report

Bertillonage

Identify people by their bodily measurements.

Eventually it fell out of favour, once police forces understood how to index and search for...



Fingerprints

Automatic fingerprint identification systems (AFIS) are by far the biggest single technology

Classify patterns of minutiae such as branches and end points of the ridges.

What purposes?



Fingerprints (cont.)

Fingerprints are now used by the world's police forces for essentially two different purposes:

1. Identifying people
(the main use in the USA)
2. Crime scene forensics
(their main use in Europe).



Verifying Positive or Negative Identity Claims

Who's in the USA fingerprints data base?

1. Criminals and Arrested
2. Anyone wanting a U.S. government.
3. The US-VISIT program:
Since 9/11, fingerprints are also used in immigration and visitor.



Verifying Positive or Negative Identity Claims (Cont.)

So how good are automatic fingerprint identification systems?

2004: from DB of 6m bad guys, 0.31% false match and 4% miss match

This is all about the trade-off between **false negatives** and **false positives** (“false alarm”)

by now, the better ones have an equal error rate of slightly below 1% per finger



Fingerprints Disadvantages

10-print verification took over a minute. This will come down with **time** (For example: Airport with 300 arrivals every 15 minutes...)

A number of people such as manual workers and pipe smokers **damage their fingerprints** frequently

Scars or distorted fingerprints

Amputees (קטועי גפיים)

Extra/less fingers

Tricking the Scanners

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

The more expensive thermal scanners could still be defeated by rubber molded fingers



Stage 1: The liquid gel is poured into a wax mold



Stage 2: The gel hardens into a removable gel mold



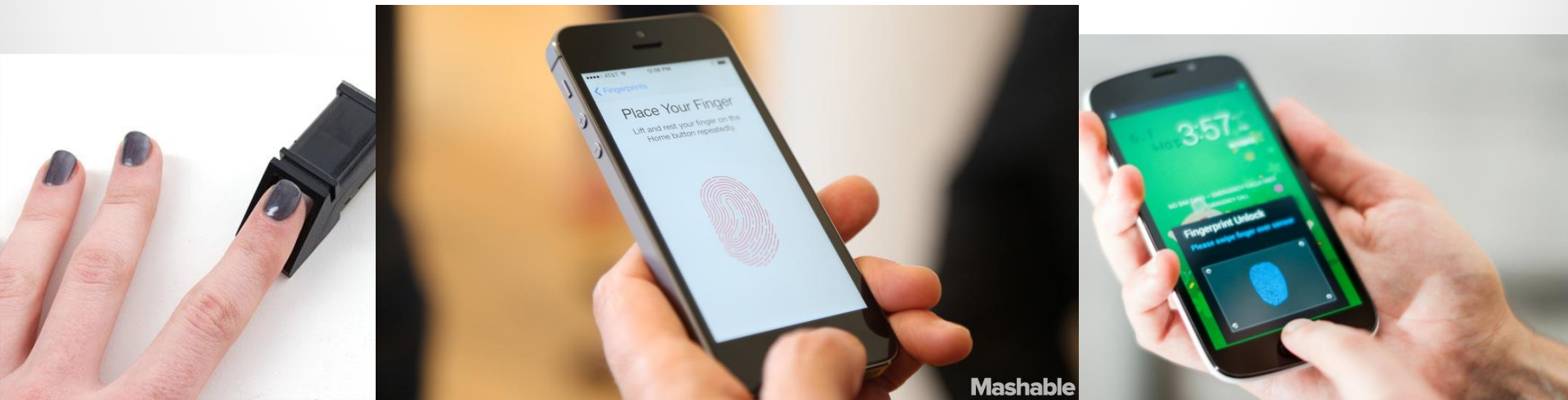
Stage 3: A fake fingerprint is produced
note: This allows body heat to pass through the hackers finger

Fingerprints - Conclusions

However, fingerprint systems still **dominate the biometric market**, and are rapidly expanding into relatively low-assurance applications

1998: 78% of biometric technology market

2005: 43% of biometric technology market



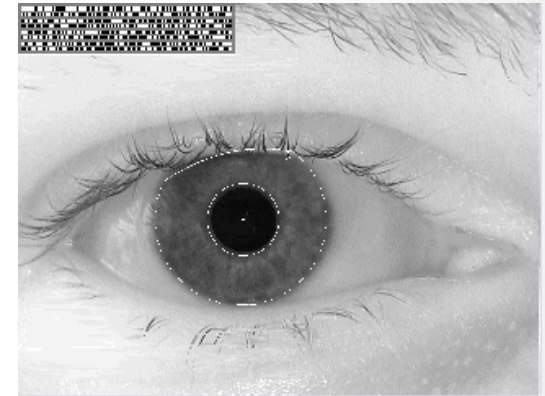
Iris Code

Recognizing people by the patterns in the irises of their eyes.

best error rates of automated systems when measured under lab conditions.

So far as is known, every human iris is measurably unique

John Daugman found signal processing techniques that extract the information from an image of the iris into a 256 byte iris code.



Speed and accurate

Lowest false accept rates of any known verification system — **zero**

Voice Recognition

Identifying a speaker from a short utterance.

Villain might somehow manage to train himself to imitate your voice in a manner that the equipment finds acceptable.

Easy to record someone and than use his voice to manipulate the System.



Other Systems

- Typing patterns/dynamics
- Vein patterns
- Writing styles
- Shape of the ear, gait, lip prints and the patterns of veins in the hand
- DNA

False Positive (Accept) vs False Negative (Reject)

Biometric	FAR	FRR	Subjects	Comments
Face Recognition	1%	10%	37437	Varied light, indoor/outdoor
Fingerprints	2%	2%	25000	Rotation and exaggerated skin distortion
Hand Geometry	2%	2%	129	With rings and improper placement
IRIS	0.94%	0.99%	1224	Indoor environment
Keystrokes	7%	0.1%	15	During 6 months period
Voice Recognition	2%	10%	30	Text dependent and multilingual

(Taken from Noha Hesham and Moataz Mahmoud from “slideshare”)

Techniques Comparison

Characteristics	Fingerprints	Hand Geometry	Retina	IRIS	Face Recognition	Signature	Voice Recognition
Ease of Use	High	High	Low	Medium	Medium	High	High
Error Incidence	Dryness, dirt, age	Hand injury, age	Glasses	Light	Lighting, age, glasses, hair	Changing Signature	Noise, colds
Accuracy	High	High	Very High	Very High	High	Low	Low
User Acceptance	Medium	Medium	Medium	Medium	Medium	High	High
Long Term Stability	High	Medium	High	High	Medium	Medium	Medium

(Taken from Noha Hesham and Moataz Mahmoud from "slideshare")

What Goes Wrong?

- *“if it’s probably secure, it probably isn’t”* (Lars Knudsen)
- Environmental conditions can cause havoc. Noise, dirt, vibration and unreliable lighting conditions all take their toll.
- There are a number of interesting attacks that are more specific to biometric systems and that apply to more than one type of biometric

Conclusions

- There is always a trade-off between the false accept rate and insult rate.
- If any biometric becomes very widely used, there is increased risk of forgery in unattended operation

- *“if it’s probably secure, it probably isn’t”*
The challenge of keeping all that sensitive data.



- *If passwords database is hacked, the users can change their passwords. What about biometric “passwords” ?*