

Information Security Identification and authentication

Advanced User Authentication II

2016-01-29

Amund Hunstad

Guest Lecturer, amund@foi.se

Agenda for lecture I within this part of the course

Background

Authentication✓

eID✓

Statistics in user authentication

ePassports✓

Biometric systems

Biometrics in general✓

Tokens

Fumy, W. and Paeschke, M. Handbook of eID Security

A. Jain, A. Ross and K. Nandakumar, Chapters 1 in "Introduction to Biometrics"

Agenda for lecture II within this part of the course

Background

Statistics in user authentication

Biometric systems

Statistics

Generic biometric system

Design cycle

(Multibiometrics, in lecture III)

Security threats

(Attacks, in lecture III)

Tokens

A. Jain, A. Ross and K. Nandakumar, Chapters 1, 6 & 7 in
"Introduction to Biometrics"

Biometrics, definition

"The automated use of physiological or behavioural characteristics to determine or verify identity"

Bio from Greek life

Metric from Greek measurement

In this case we measure

Physical properties of the user's body

Behaviour properties of the user

User authentication/identification

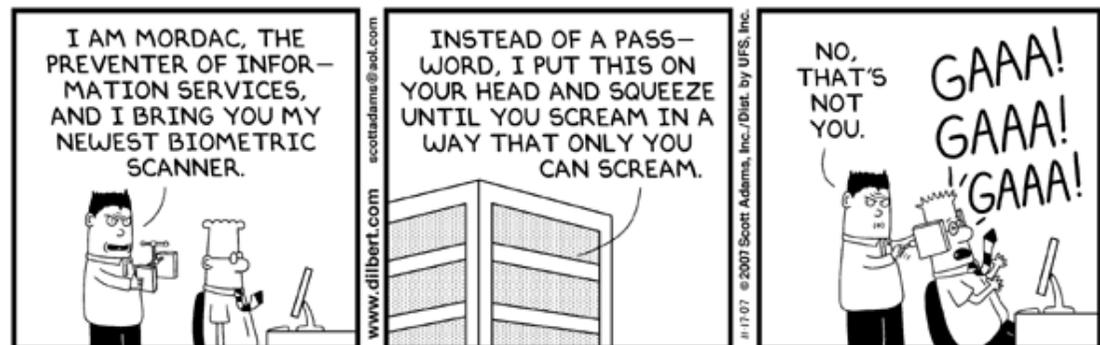
Can in an IT system be achieved via

What I know – passwords, PIN

What I have – ID-cards, smart-card, token

What I am/do – biometrics

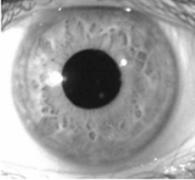
Identification Authentication

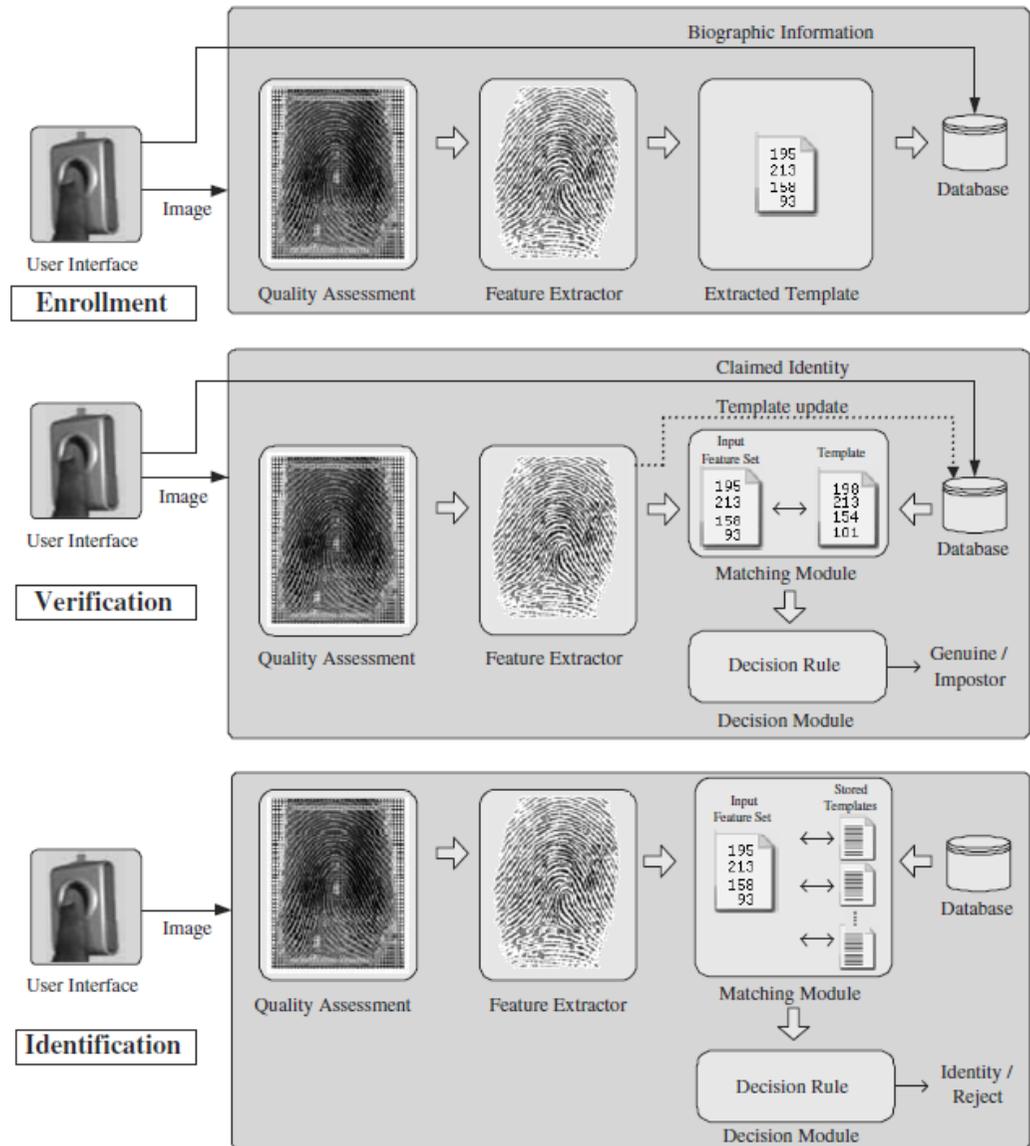
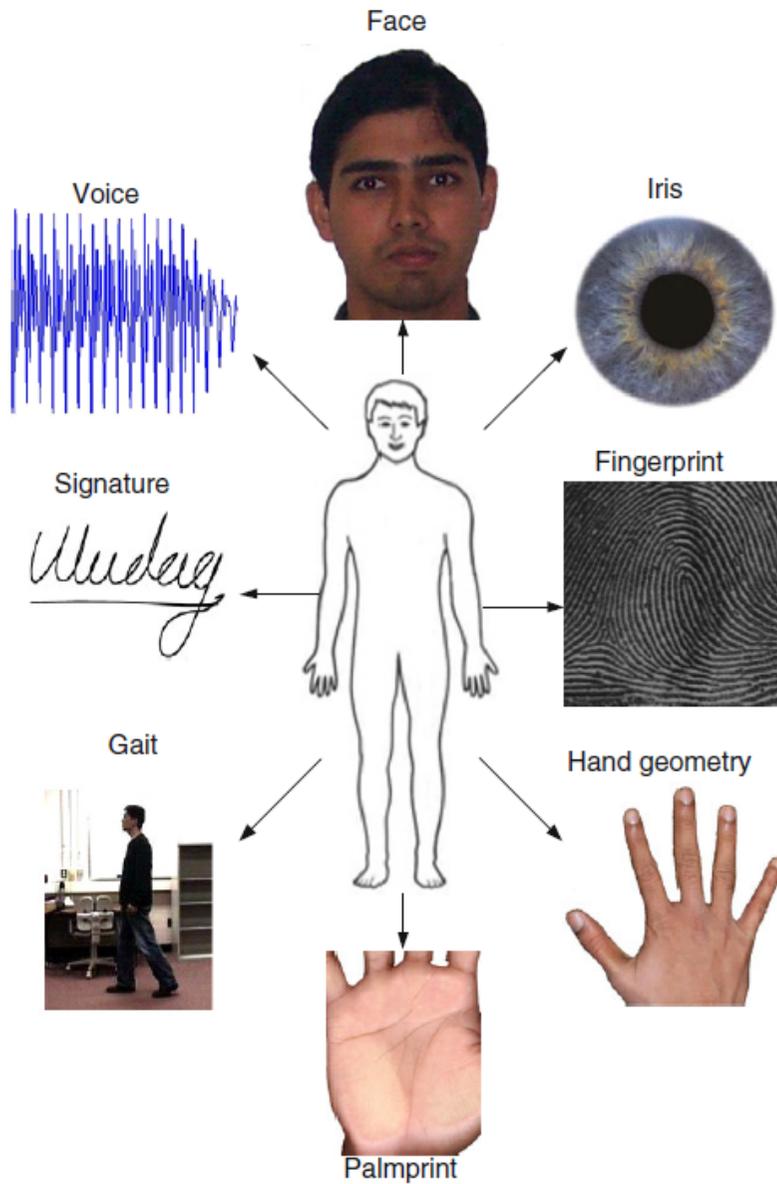


© Scott Adams, Inc./Dist. by UFS, Inc.

Biometrics, examples

- Written signature
- Retinal scan
- DNA
- Vein pattern
- Thermal pattern of the face
- Keystroke dynamics
- Finger prints
- Face geometry
- Hand geometry
- Iris pattern
- Voice
- Ear shape
- Body motion patterns

 Fingerprint	 Face	 Iris	 Retina	 Ear
 Palm print	 Hand geometry	 Periocular	 Conjunctival vasculature	 Key stroke dynamics
 Anthropometry	 Signature	 Facial thermogram	 Hand thermogram	 Gait



Matching, decision regions, hypothesis testing

A typical system has a threshold parameter which determines the allowed variance

Statistical theory for hypothesis testing enables analysis

It is necessary to balance user population statistics against intended use

More about this ...

Statistics in user authentication

Problems and unexpected effects

Statistics in user authentication

For identification, you must consider the probabilities that two persons ever have matching authentication data

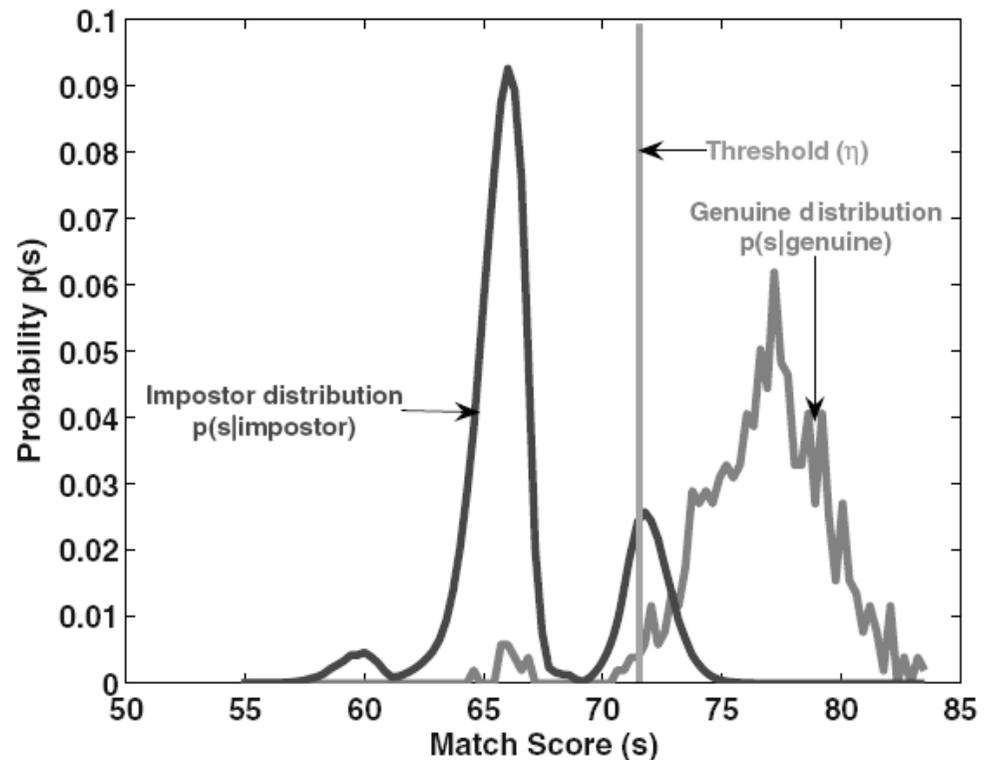
For verification, you must estimate the probability that an impostor can guess a victim's parameter value and imitate it

Statistics in biometrics

A typical system has a threshold parameter which determines the allowed variance

Use statistical theory for hypothesis testing

Balance user population statistics against intended use plus importance of each of the CIA criteria, and set thresholds accordingly



Failure rates

Admitting a person under the wrong identity

FAR – False Acceptance Rate, also called

FMR – False Match Rate

Rejecting a person claiming correct identity

FRR – False Rejection Rate, also called

FNMR – False Non-Match Rate

Failure rate effects

Remember:

Admitting a person under the wrong identity
means damaged Confidentiality and/or
Integrity

Rejecting a person claiming correct identity
means damaged Availability

Identification effects

Hypothesis testing answers “True” or “False”

Hypothesis can be “this is person X”

Highly unbalanced in the sense that most subjects are not person X

Creates effects that surprise some

Identity testing problems

Suppose there are 10,000 persons on a “no fly” list

An airport uses identification devices with $FAR=0,1\%$ and $FRR=5\%$. Reasonable values?

A terrorist has a 5% chance of getting aboard. Send 20 and one will succeed

A typical airport like Arlanda ($\approx 50\,000$ passengers per day) will detain 50 innocent people each day

Traps in using FRR

False Rejection Rate is a mean value over a trial population

It does not (necessarily) give the general probability that a given user is rejected

Usually there is a subset of users who get most of the rejections

It is not valid for users deliberately trying not to be recognised

Conditional v mean values

If the correct user is often rejected due to anomalies, attempts at false acceptance as that user may fail often and vice versa. This distorts “true” values

If the attacker knows the statistics of single users, the most likely victim can be chosen

Example 1

A user population has two sets of users, X with excellent characteristics for the biometric system and Y with bad characteristics. 1% belong to Y

A user from X has FAR 0.5%

A user from Y has FAR 50%

Total FAR \approx 1%

An attack deliberately at a Y person still has 50% probability of succeeding

Example 2

A user population has two sets of users, X with good characteristics for the biometric system and Y with bad characteristics. 1% belong to Y

A user from X has FRR 0.5%

A user from Y has FRR 50%

Total FRR \approx 1% (looks good, you must re-authenticate only once for every 100 attempts on the average)

Users from Y must re-authenticate every other time when using the system. And they must make three attempts one out of four times etc.

General statistics

How large is the set of possible values?

Are some more likely than others?

How large is the user population?

How many guessing attempts can be made per time unit?

Are there restrictions on the possible number of attempts against the same user?

Are there general restrictions on the number of attempts?

Illustration example, card PIN

A card PIN has 10,000 possible values

The probability to guess a PIN in the usually allowed three consecutive attempts is thus only one in more than 3000

If 3500 cards are stolen each year, at least one misuse through correctly guessed PIN should be expected per year

With 5000 stolen cards, it is more likely that one of them gets its PIN guessed in the first attempt, than that none gets that effect

Remember

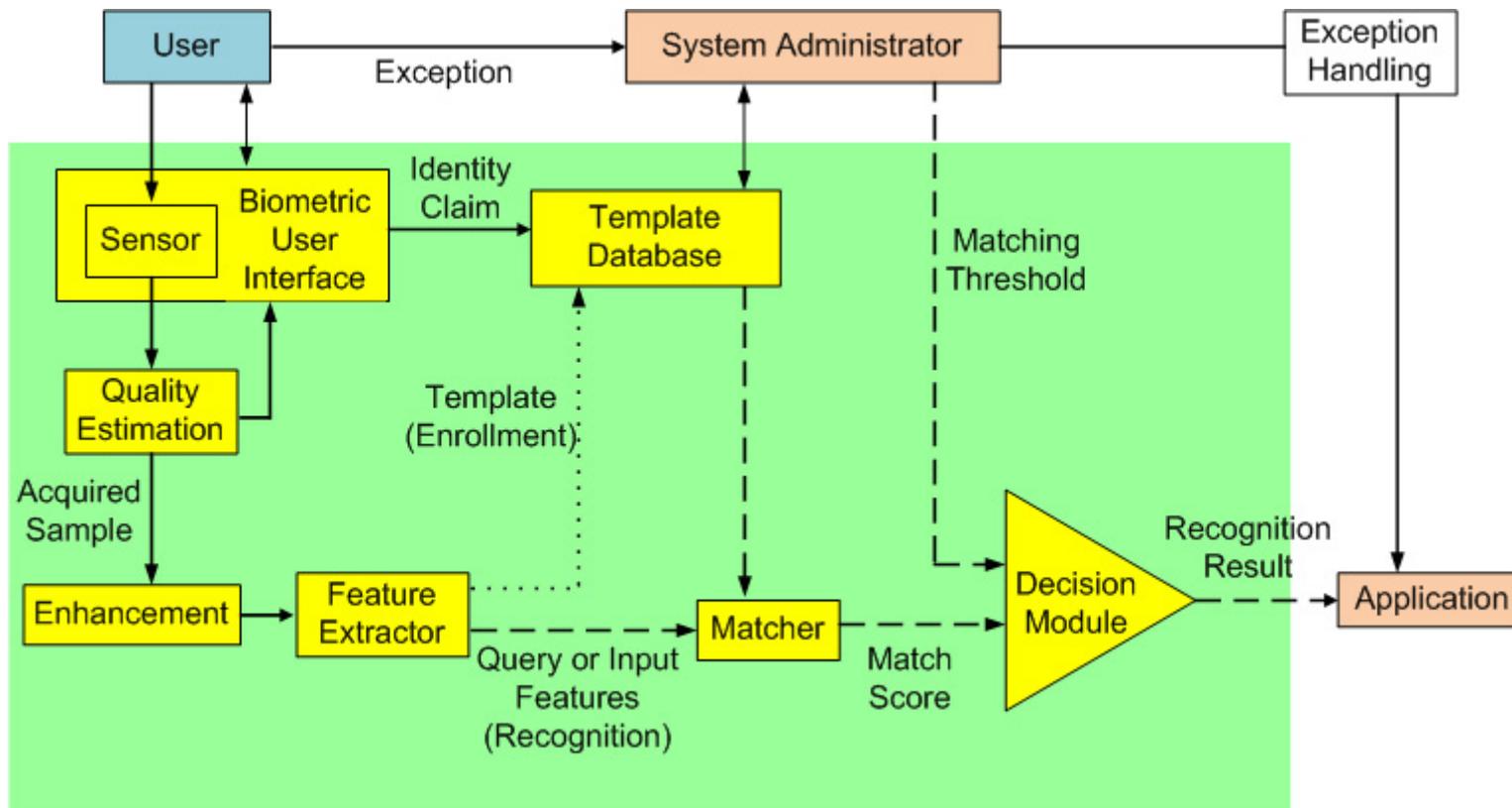
Balance risks against population characteristics, like size but not only size

Average risks can be much higher for subsets of users than for the total population

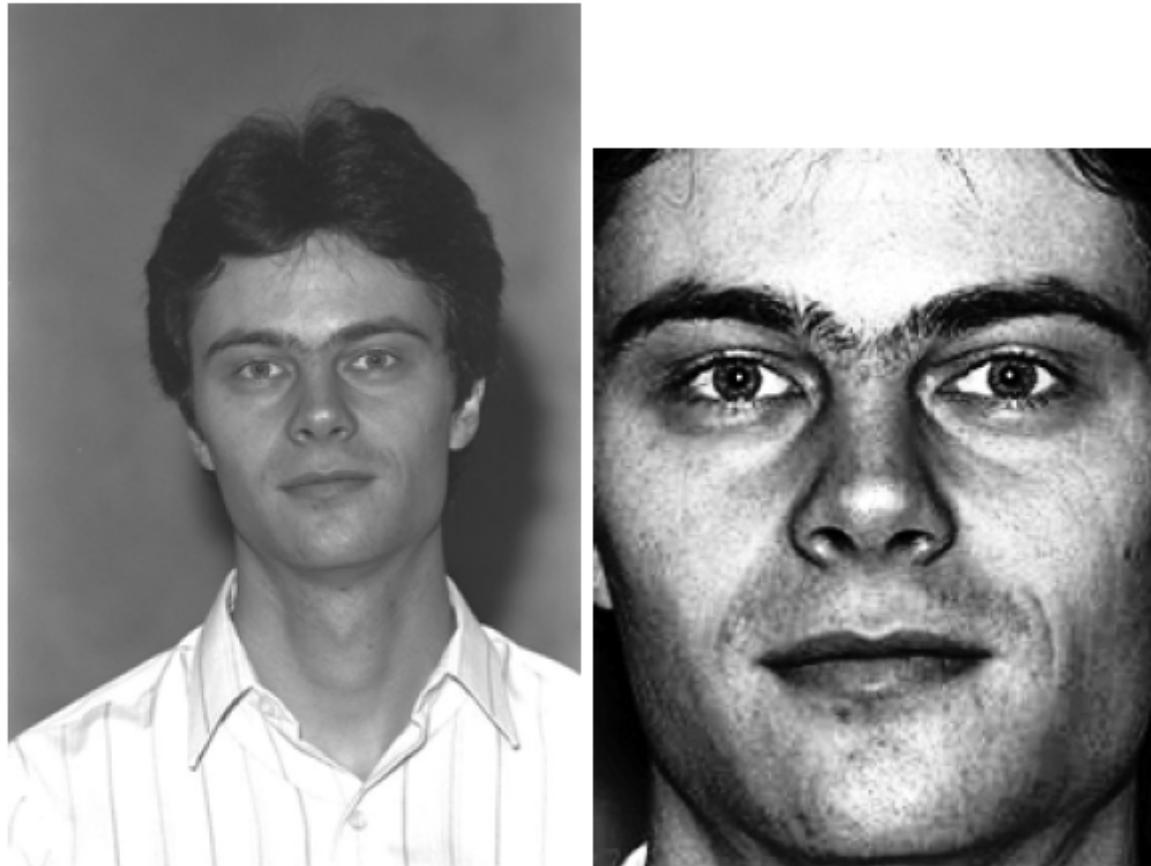
If one single customer is hit, it does not matter to that customer that the average risk per customer was very low

If some customers are at high risk, the organisation is bound to get hit eventually

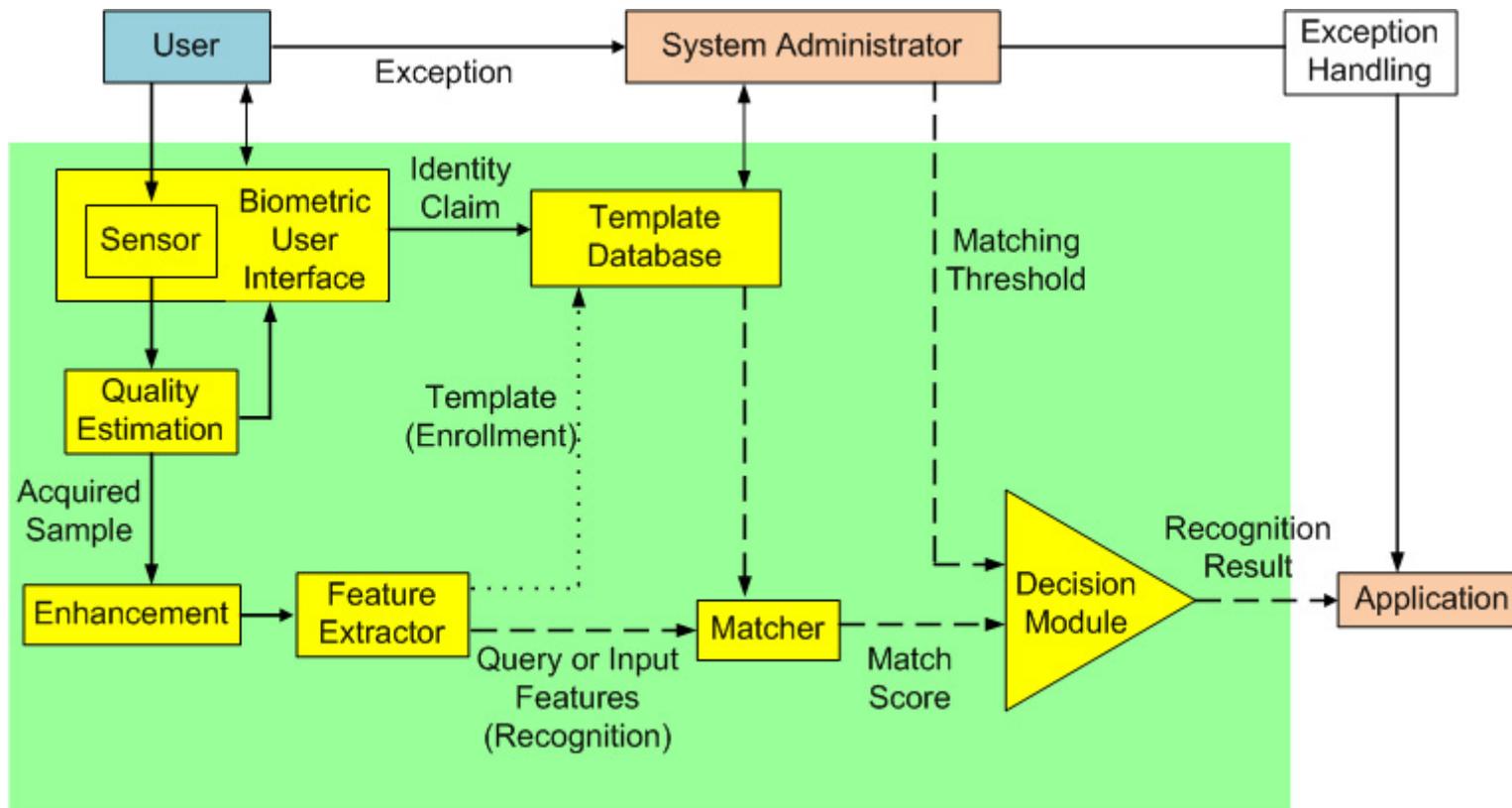
Generic biometric system: Building blocks



Feature extraction: Segmentation and enhancement



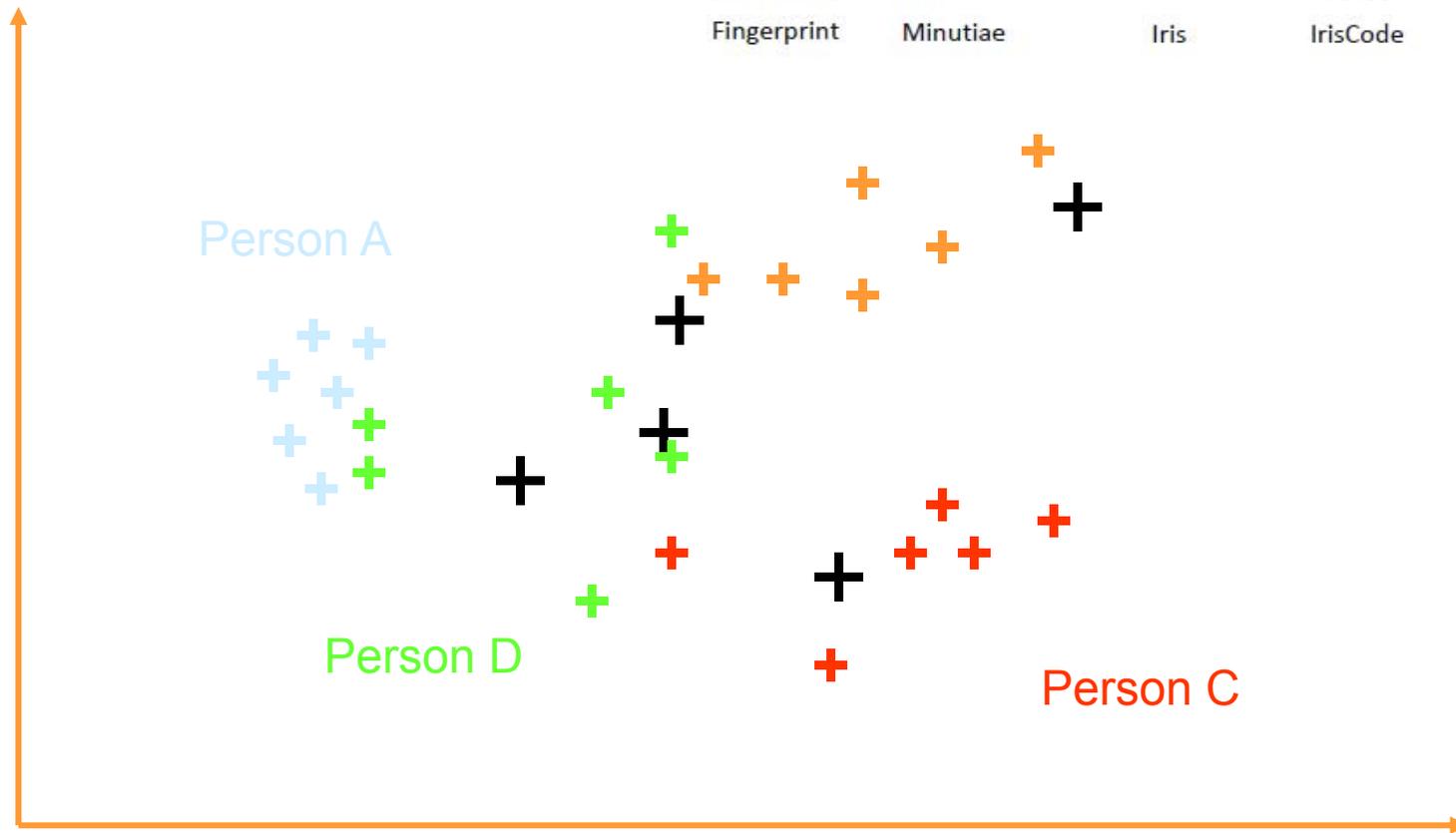
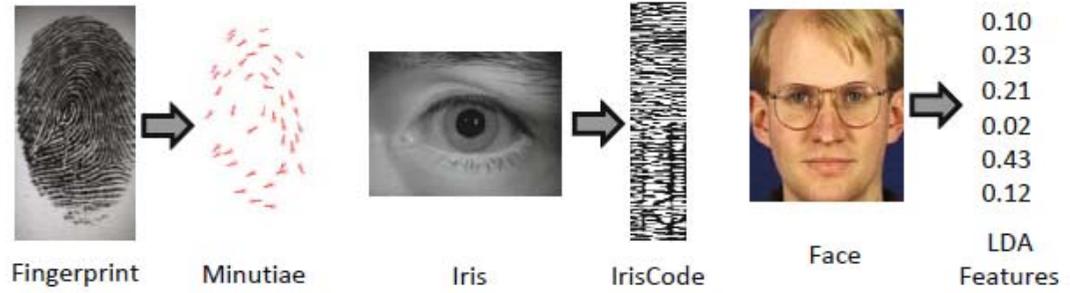
Generic biometric system: Building blocks



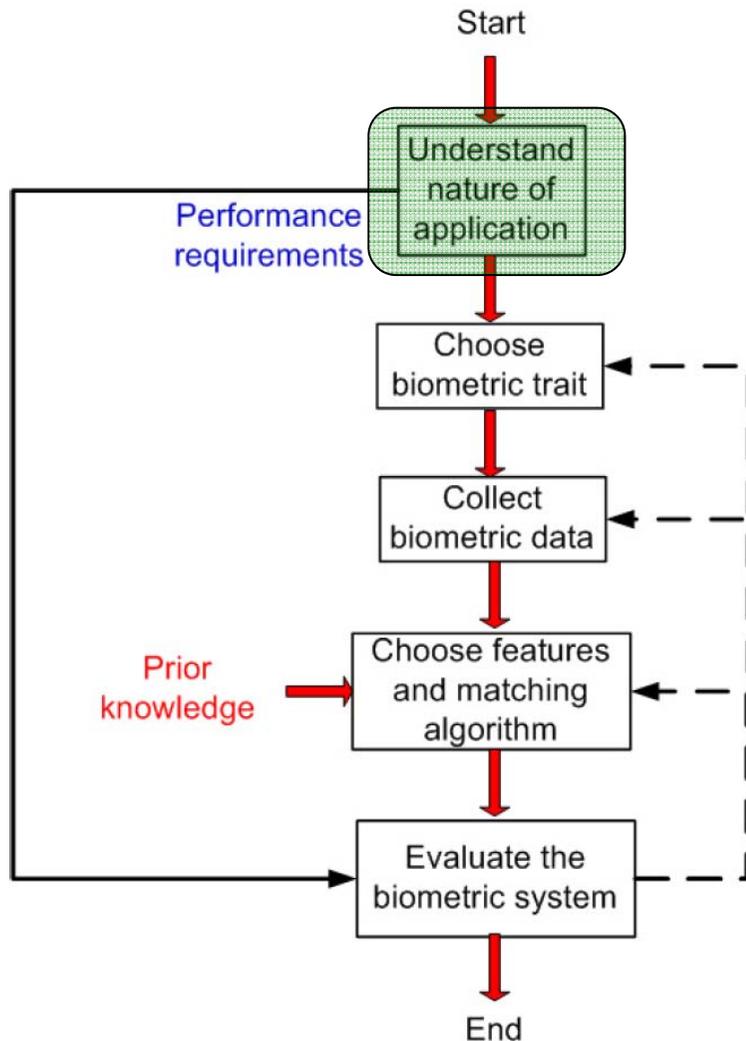
A generic biometric system



Classification



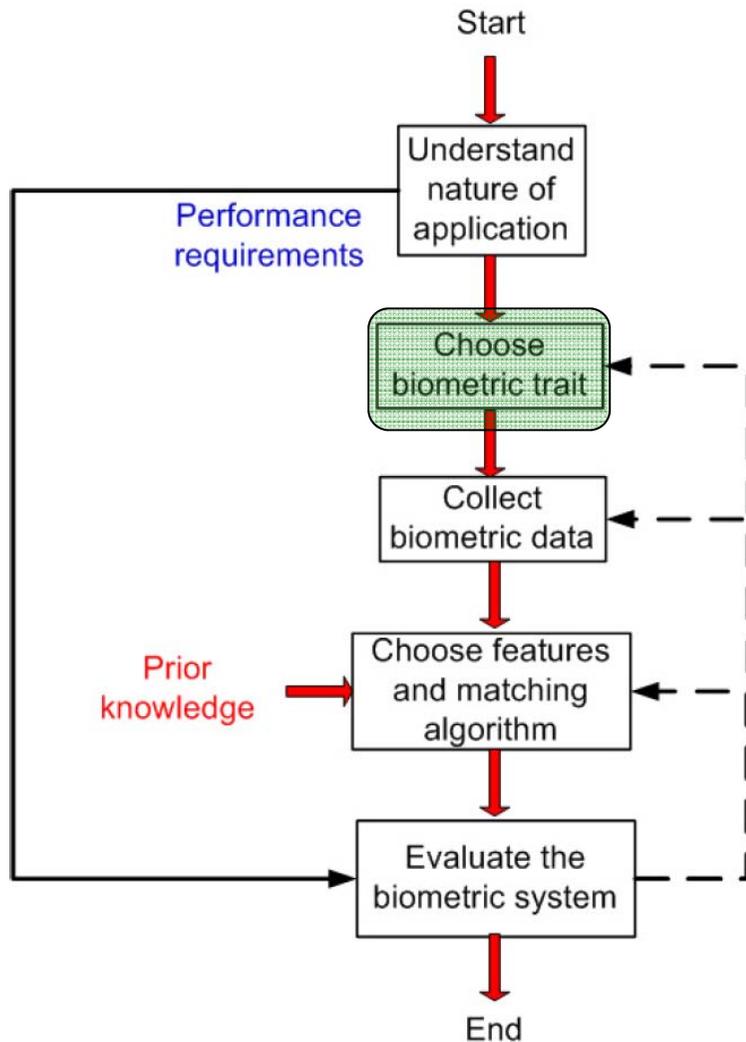
Design cycle of biometric systems



Nature of application

- Cooperative users
- Overt/covert deployment
- Habituated/Non-habituated users
- Attended/Unattended operation
- Controlled/Uncontrolled operation
- Open/Closed system

Design cycle of biometric systems



Choice of biometric trait

- Universality
- Uniqueness
- Permanence
- Measurability (Collectability)
- Performance
- Acceptability
- Circumvention

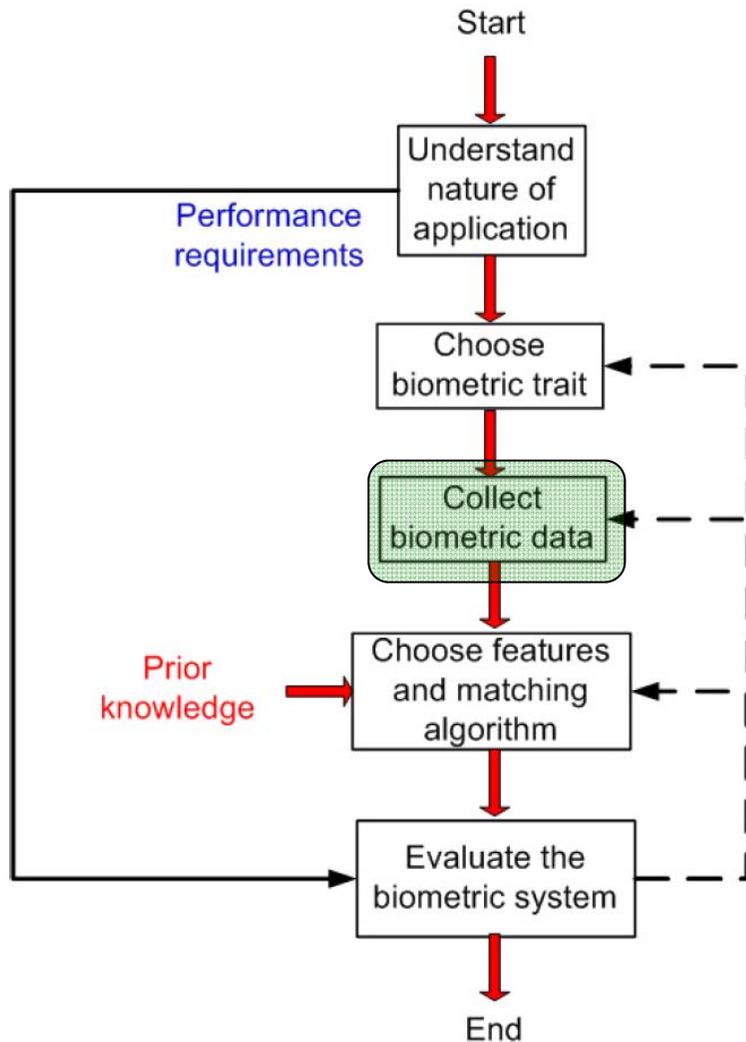
Requirements on biometric traits

Biometrics	Univer- sality	Unique- ness	Perma- nence	Collect- ability	Perfor- mance	Accept- ability	Circum- vention
Face	H	L	M	H	L	H	L
Fingerprint	M	H	H	M	H	M	H
Hand Geometry	M	M	M	H	M	M	M
Keystroke Dynamics	L	L	L	M	L	M	M
Hand vein	M	M	M	M	M	M	H
Iris	H	H	H	M	H	L	H
Retina	H	H	M	L	H	L	H
Signature	L	L	L	H	L	H	L
Voice	M	L	L	M	L	H	L
Facial Thermogram	H	H	L	H	M	H	H
DNA	H	H	H	L	H	L	L

H=High, M=Medium, L=Low

Attempt to classify methods according to how they meet all seven criteria. Valid today? Do you agree in general? Look closely and make your own assessment! There is no “correct” answer...

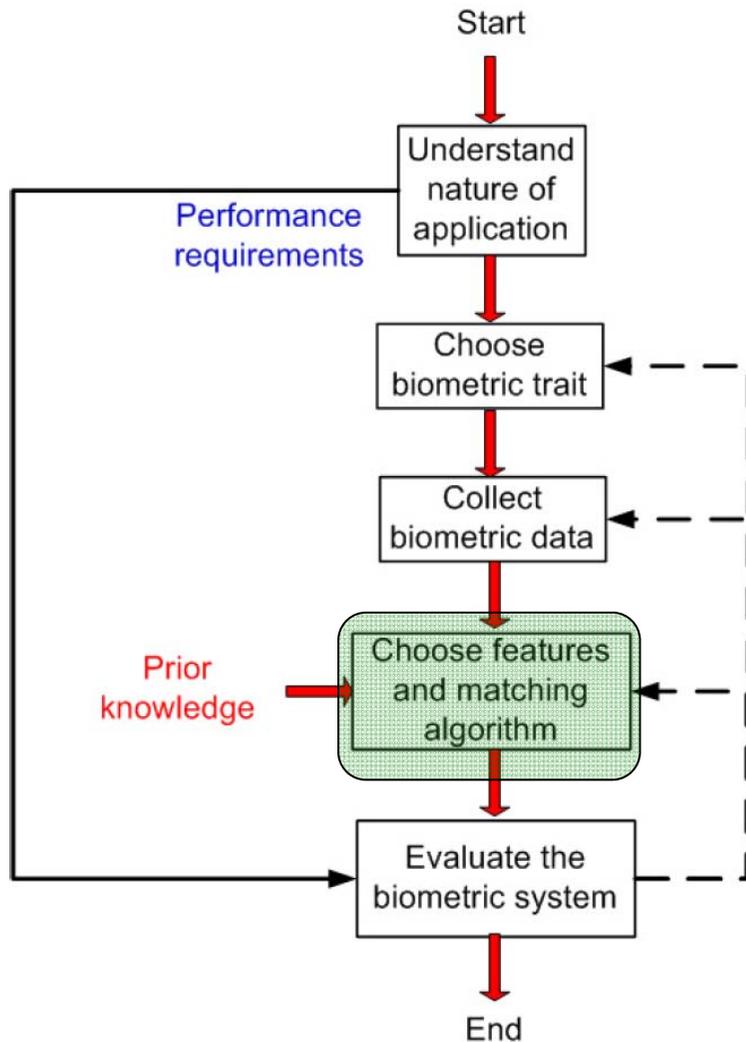
Design cycle of biometric systems



Collecting biometric data

- Appropriate sensors
 - Size, cost, ruggedness, high quality biometric samples
- Collection environment
- Sample population
 - Representative of the population
 - Exhibit realistic intra-class variations
- User habituation
- Legal, privacy & ethical issues

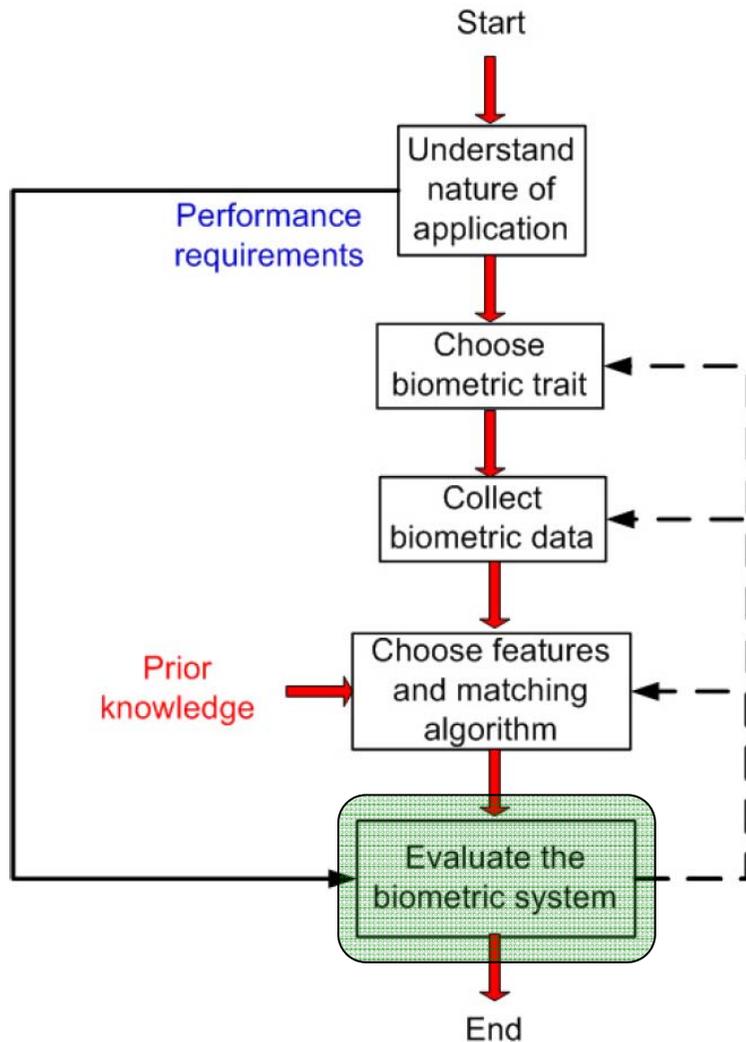
Design cycle of biometric systems



Choice of features/matching algorithm

- Prior knowledge of the biometric trait
 - Uniqueness
- Mimic human ability to discriminate
- Interoperability between biometric systems
- Common data exchange formats ...

Design cycle of biometric systems



Evaluation of biometric systems

- Technology evaluation
- Scenario evaluation
- Operational evaluation

- Error rates
- System reliability, availability, maintainability
- Vulnerabilities
- User acceptability
- Cost, throughput, benefits
- Return on investment

How to cheat a biometric system?

Cheat the sensor

Picture of another persons face

Voice recordings

...

Cheat the system

False user permission

Intrude/manipulate communication

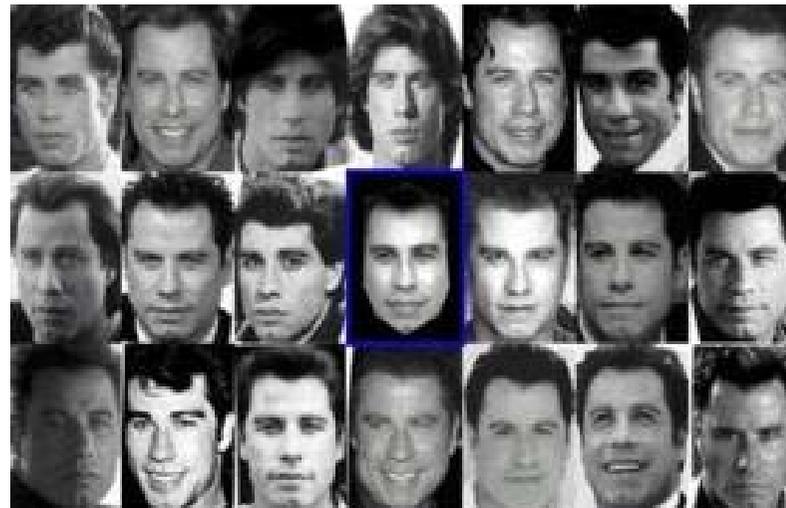
...

What are the disadvantages of biometric systems

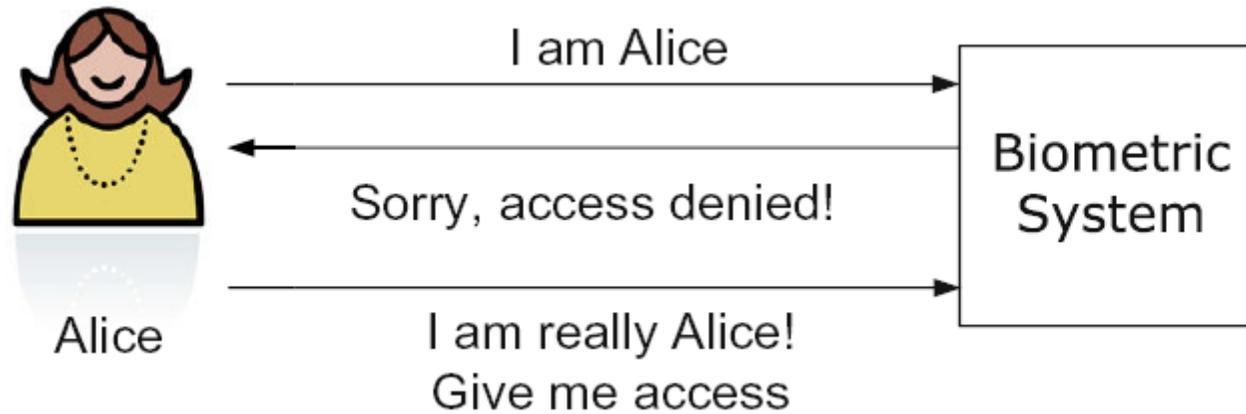
Sensors of low quality and sensitive to noise

Biometrical features needs to be unique

Temporal variations (ageing, beards, weight etc...) complicates the use



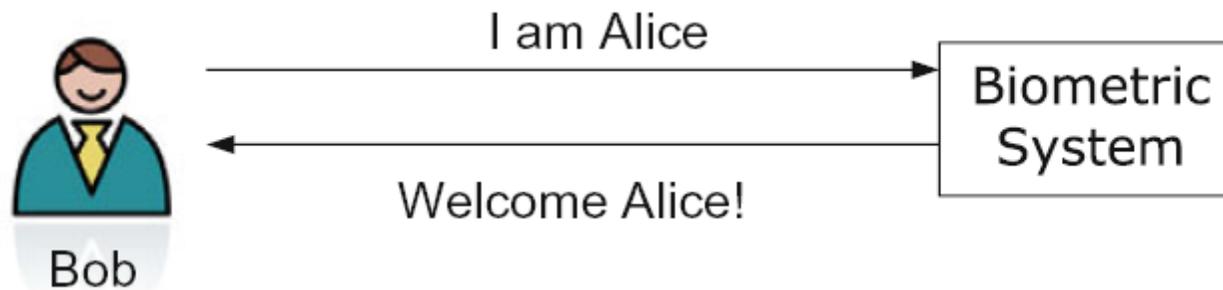
Security threats: Denial-of-service (DoS)



Legitimate users are prevented from obtaining access to the system or resource that they are entitled to

Violates availability

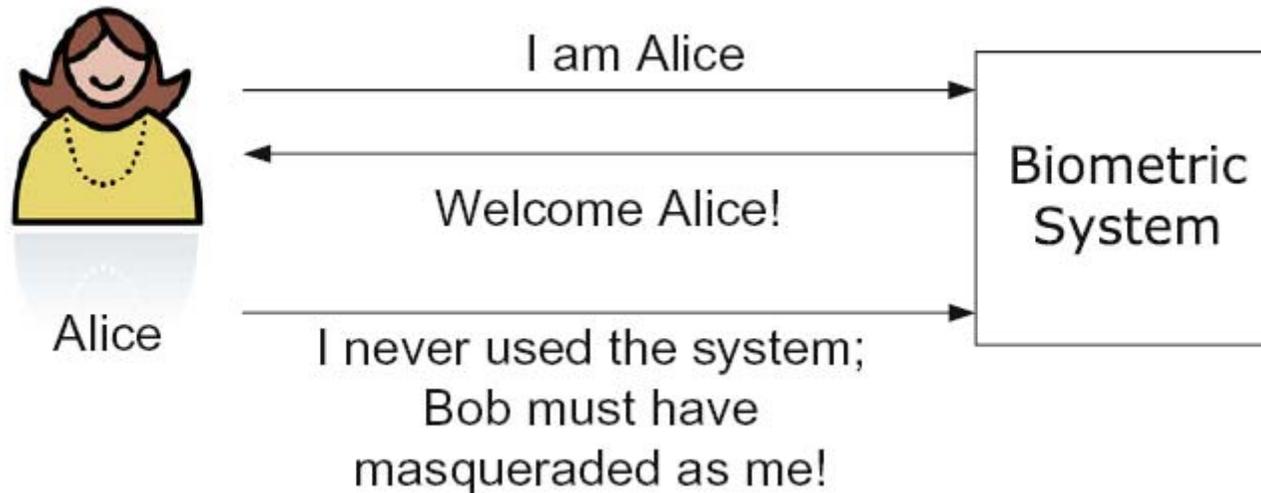
Security threats: Intrusion



An unauthorized user gains illegitimate access to the system

Affects integrity of the biometric system

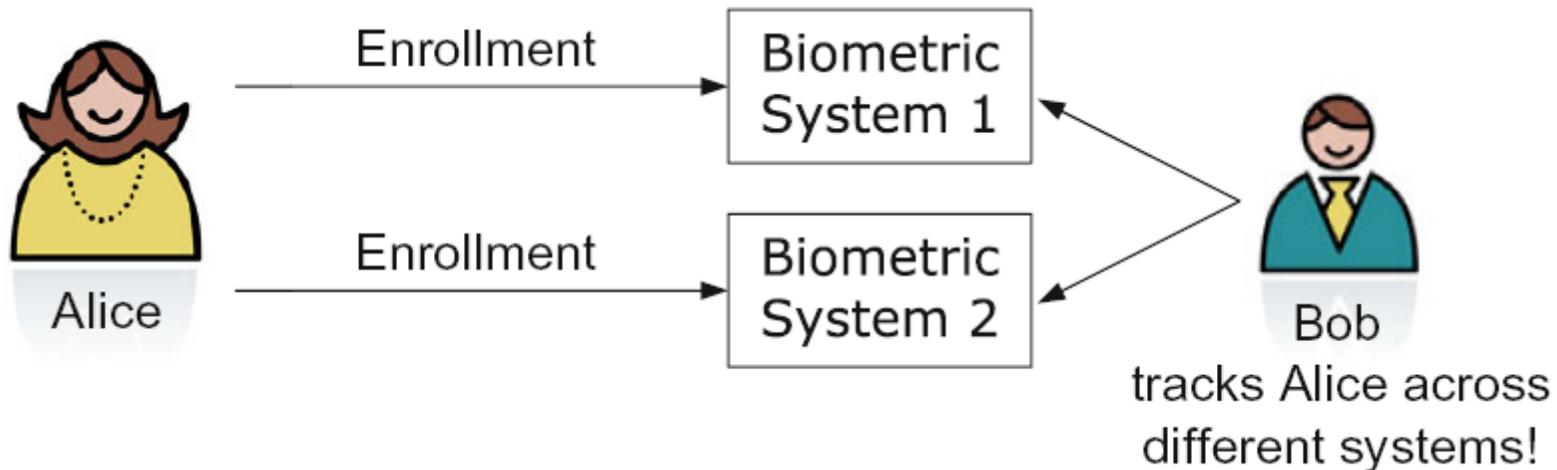
Security threats: Repudiation



A legitimate user denies using the system after having accessed it.

Corrupt users may deny their actions by claiming that illegitimate users could have intruded the system using their identity

Security threats: Function creep



An adversary exploits the biometric system designed to provide access control to a certain resource to serve another application, for example, a fingerprint template obtained from a bank's database may be used to search for that person's health records in a medical database

Violates confidentiality and privacy.



I'VE DISCOVERED A WAY TO GET COMPUTER
SCIENTISTS TO LISTEN TO ANY BORING STORY.

... but is really the story boring?

- Possible security threats
 - Threat agents
- Public confidence and acceptance
- What if the application is
 - Border control
 - Management of welfare schemes
 - ...

Agenda for lecture II within this part of the course

Background

Statistics in user authentication

Biometric systems

Statistics✓

Generic biometric system✓

Design cycle✓

Multibiometrics

Security threats✓

Attacks

Tokens

A. Jain, A. Ross and K. Nandakumar, Chapters 1, 6 & 7 in
"Introduction to Biometrics"



Linköping University

expanding reality

www.liu.se