Basics II

CSE 40537/60537 Biometrics

Daniel Moreira

Spring 2022

UNIVERSITY OF NOTRE DAME

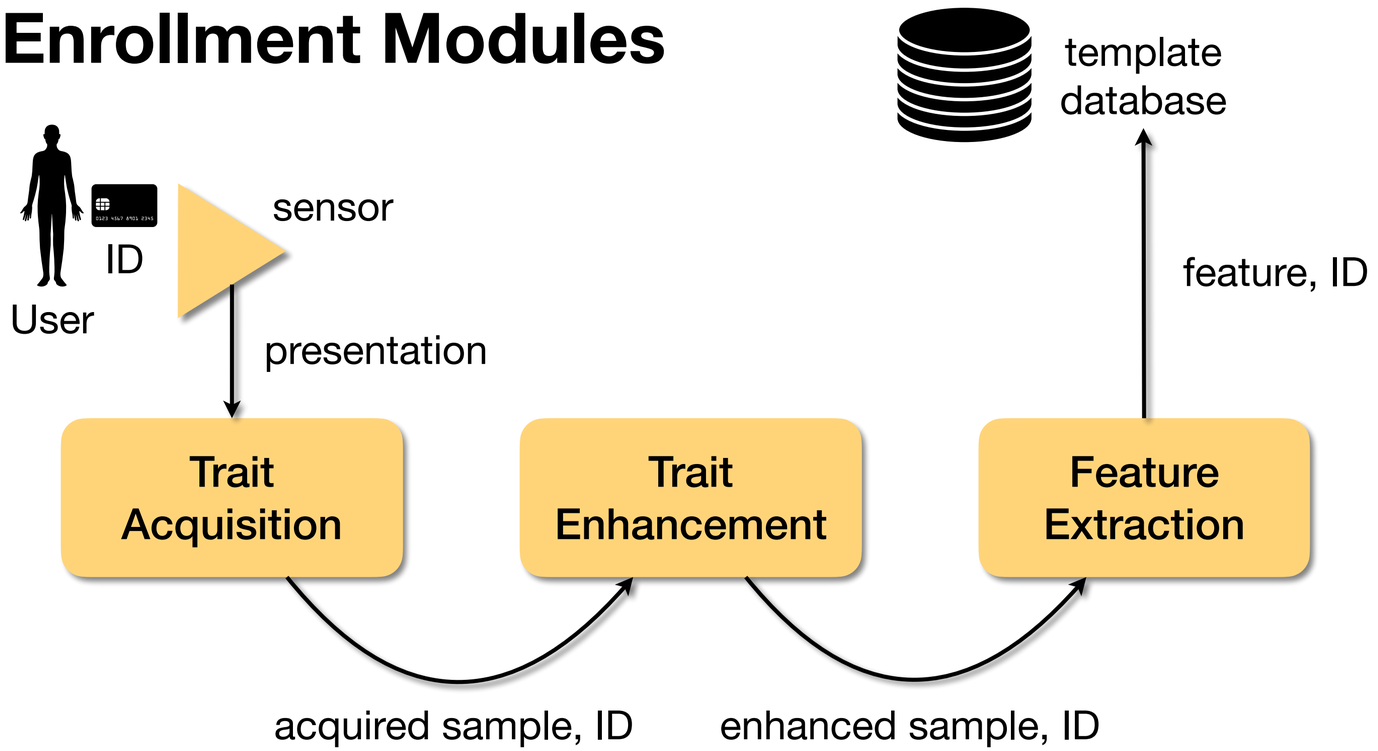
Today you will…

Get to know
Biometric system errors
Metrics to compare Biometric systems
Types of attacks to Biometric systems

Biometric Systems

RECAP

Enrollment Modules

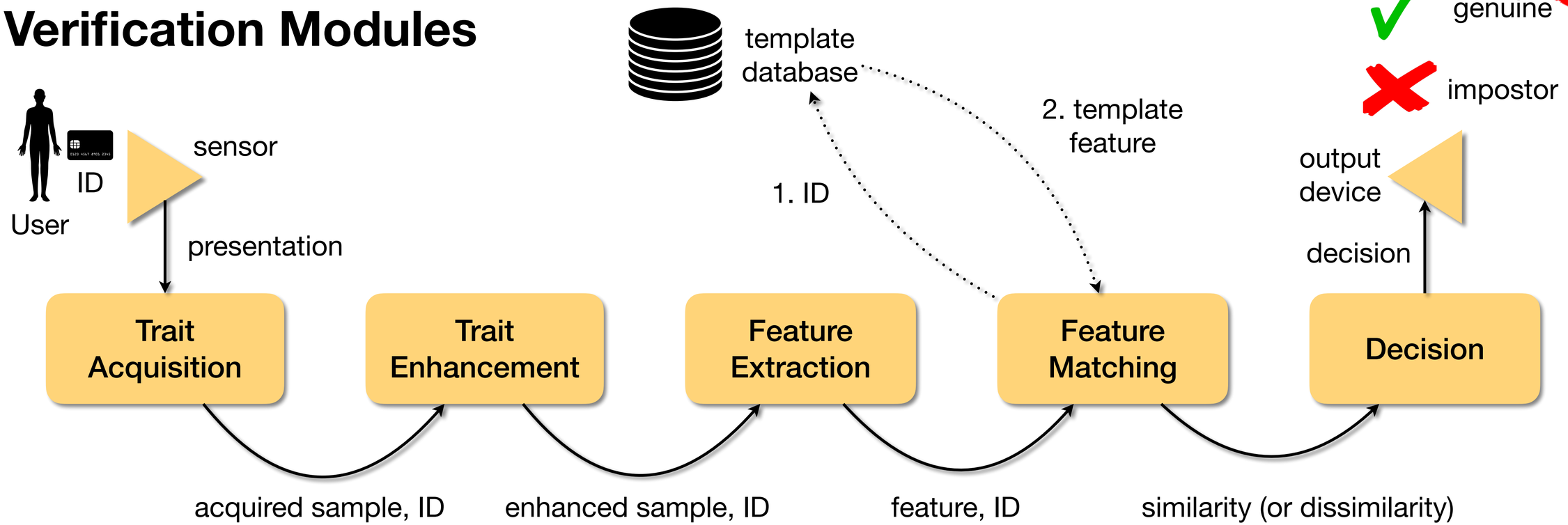


UNIVERSITY OF NOTRE DAME

Biometric Systems

RECAP

Verification Modules

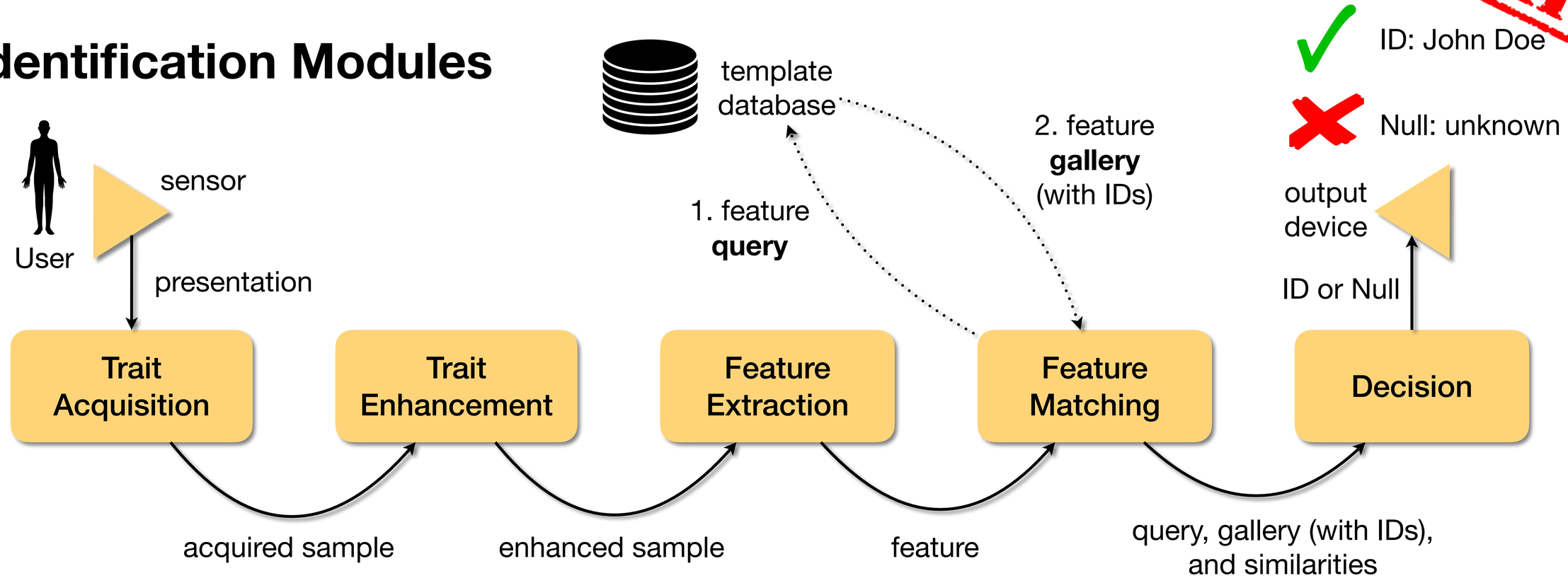


UNIVERSITY OF NOTRE DAME

Biometric Systems

RECAP

Identification Modules

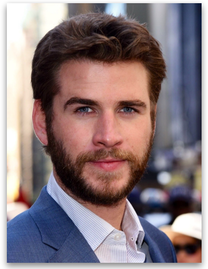


UNIVERSITY OF NOTRE DAME

Biometric Systems

RECAP

Open-set vs. Closed-set Identification



Query
(Liam Hemsworth)

Dataset

Robert Downey Jr.

Scarlet Johansson

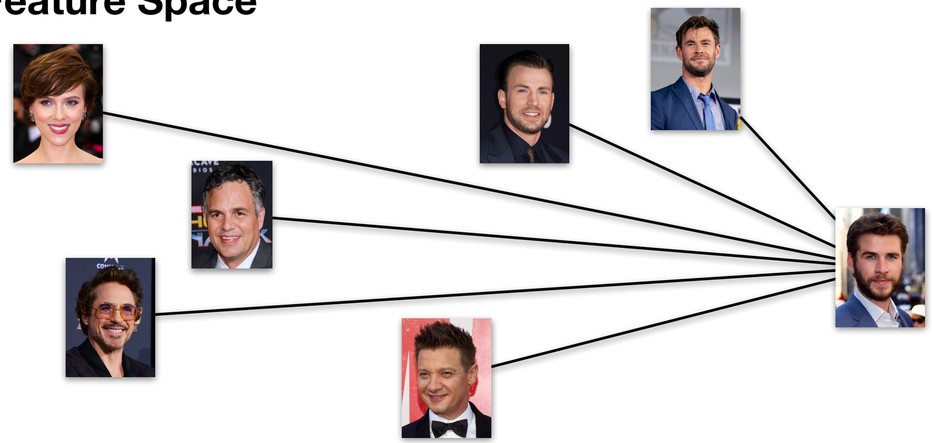
Chris Evans

Mark Ruffalo

Chris Hemsworth

Jeremy Renner

Feature Space



Closed Set

Output
This is Chris Hemsworth! ✗

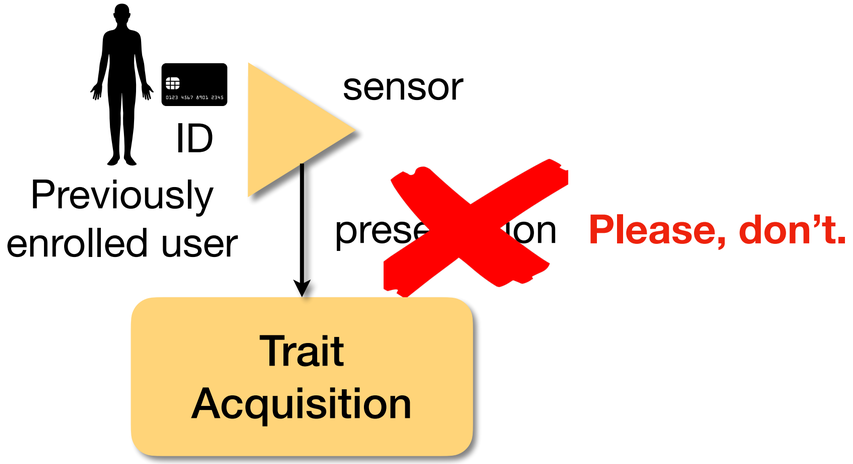
Open Set

Output
I don't know this person! ✓

UNIVERSITY OF NOTRE DAME

Biometric Systems

Enrollment Revision

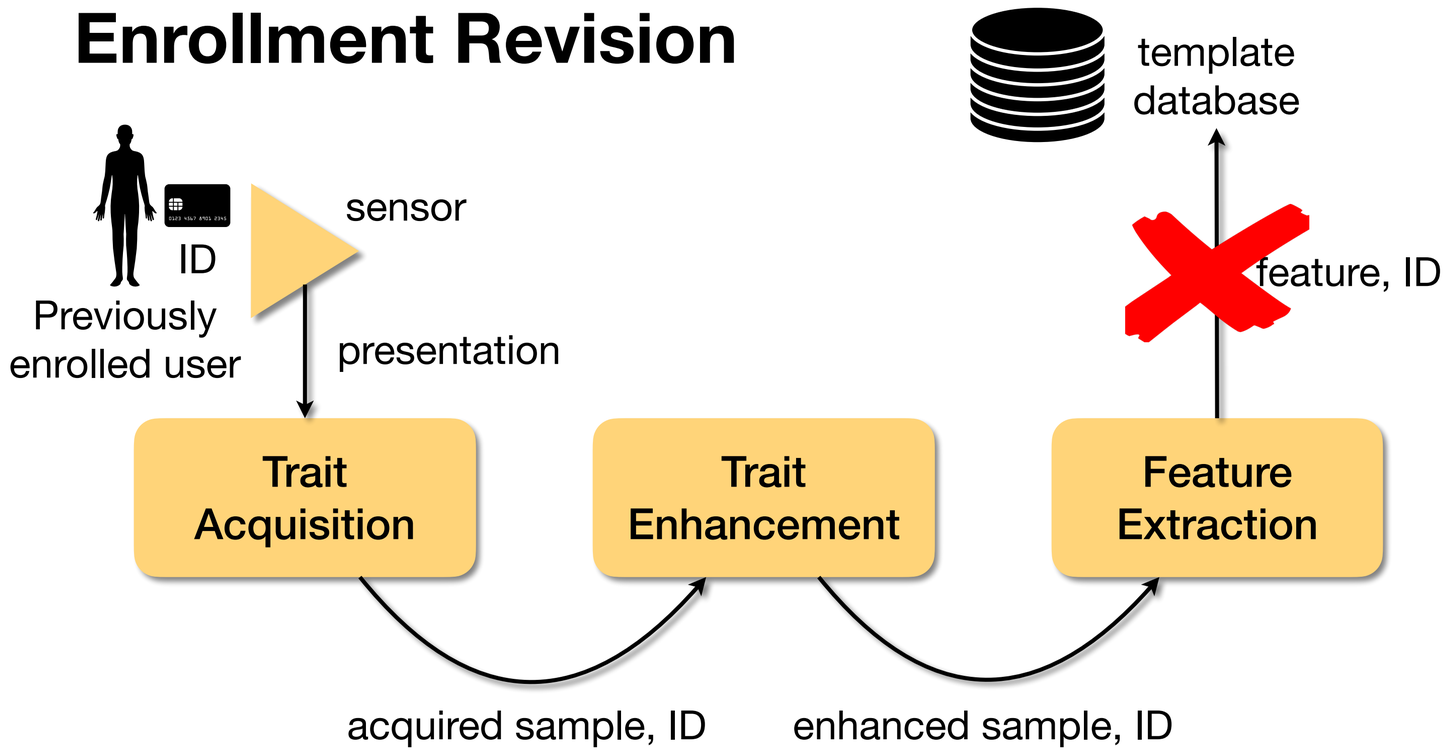


Attended operation?
"I'm seeing here in my notes that you are already enrolled."

UNIVERSITY OF NOTRE DAME

Biometric Systems

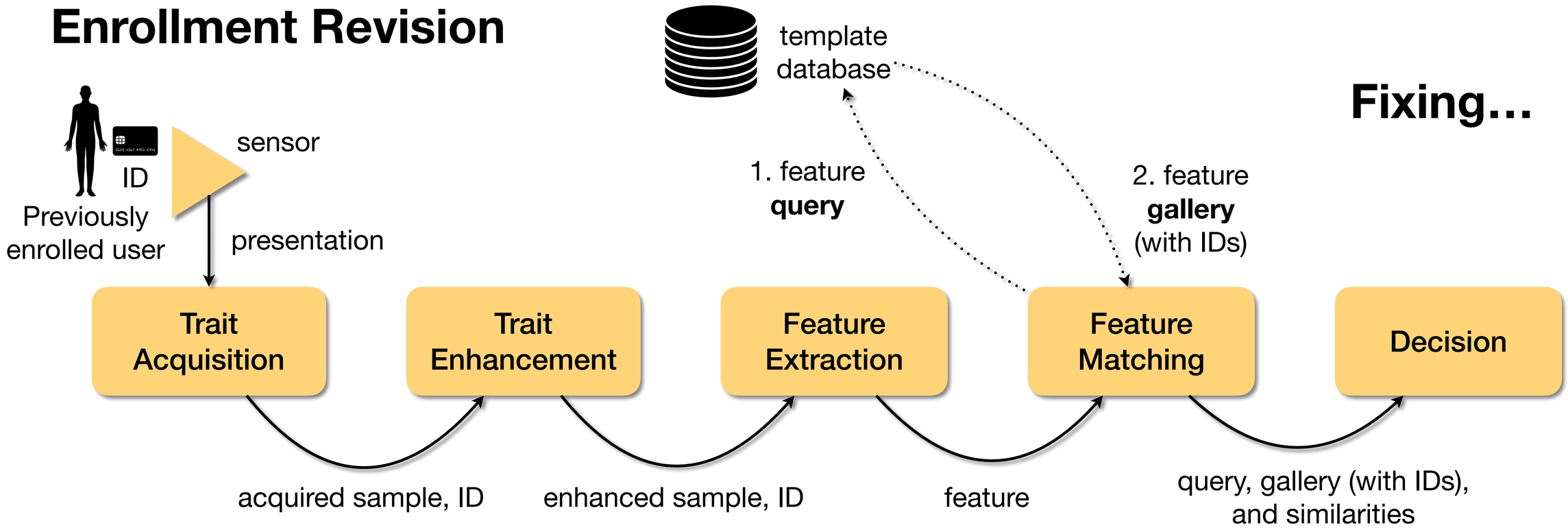
Enrollment Revision



Unattended operation?
The system must deal with re-enrollment attempts.

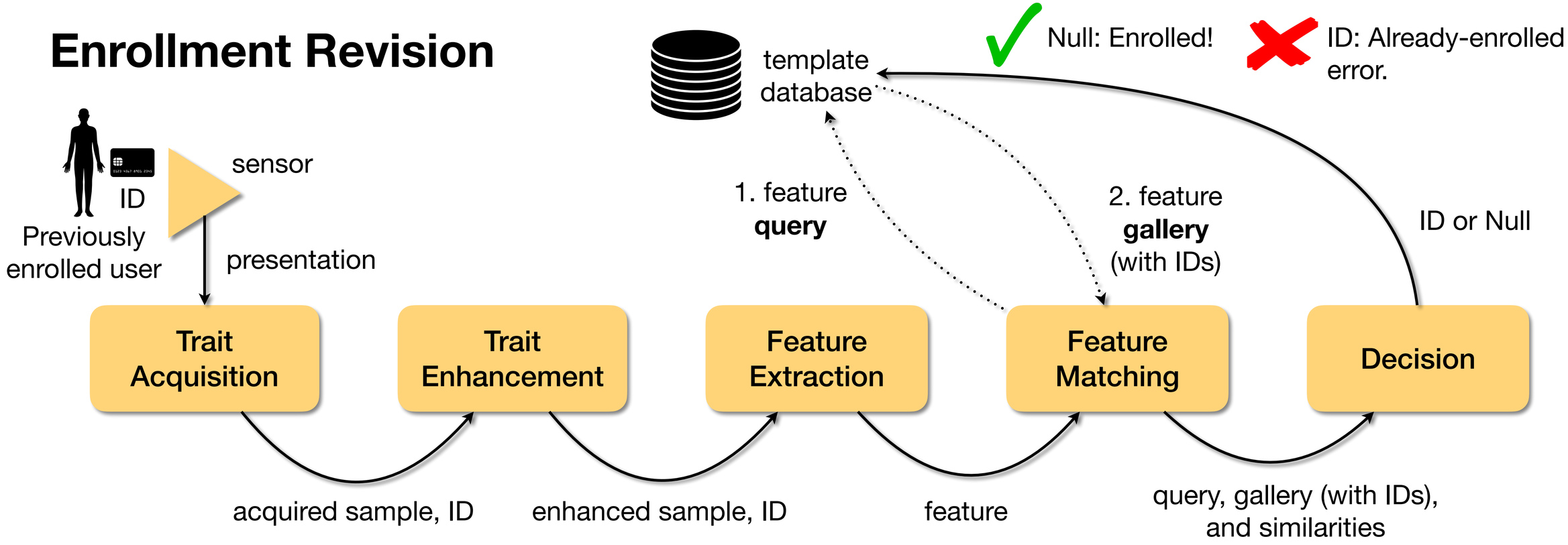
UNIVERSITY OF NOTRE DAME

Biometric Systems



Biometric Systems

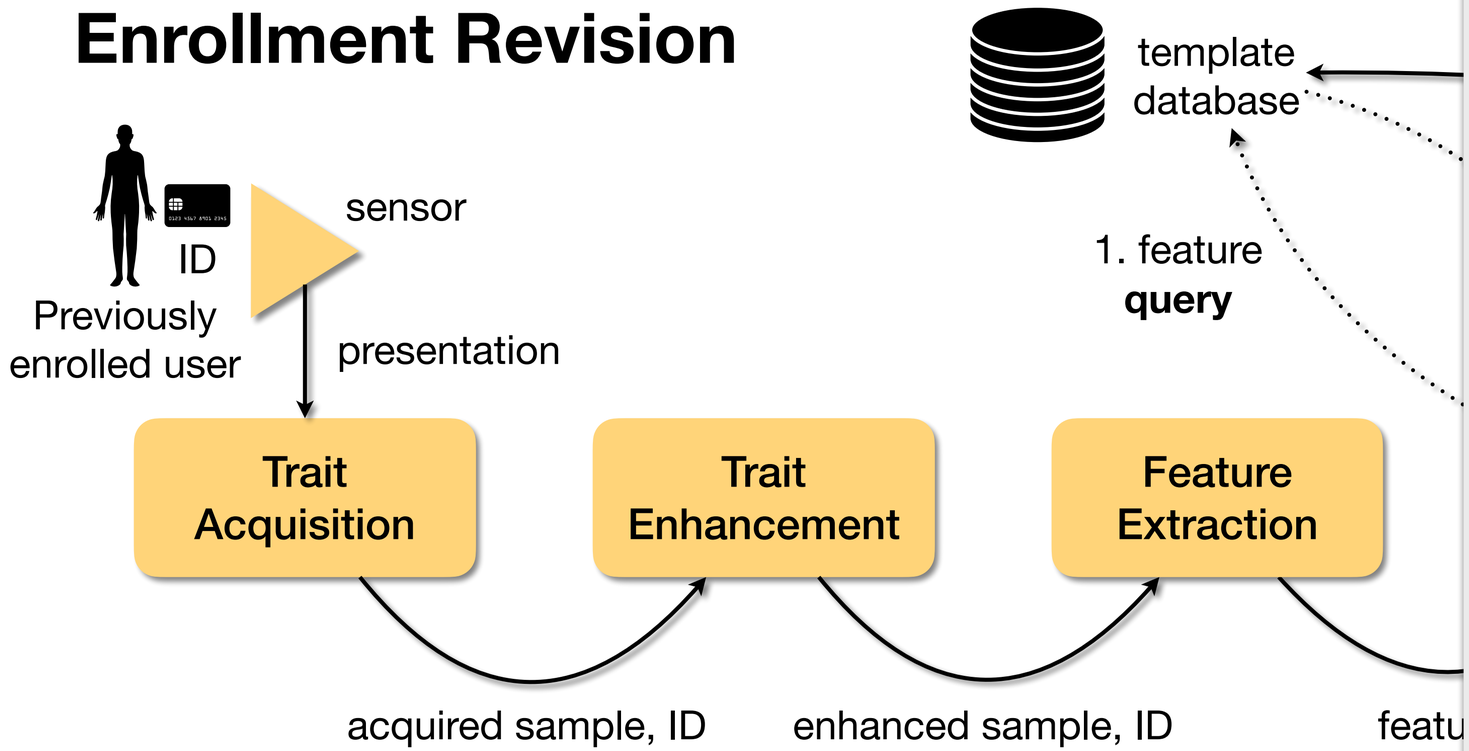
Enrollment Revision



UNIVERSITY OF NOTRE DAME

Biometric Systems

Enrollment Revision



Fast Enrollment
There might not be time to process these 2 modules. E.g., if you have millions of enrolled users, or a distributed template database.

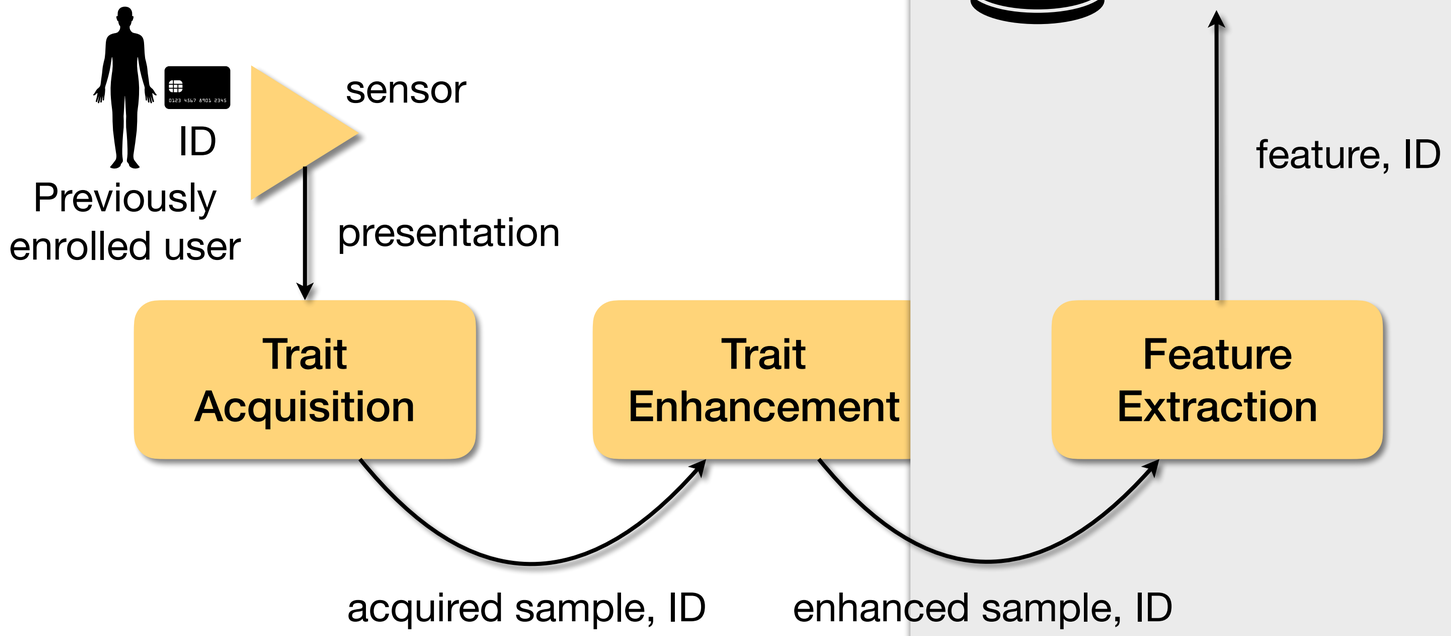
Feature Matching

Decision

UNIVERSITY OF NOTRE DAME

Biometric Systems

Enrollment Revision



Fast Enrollment
Possible solution: conclude enrollment after *Feature Extraction*.

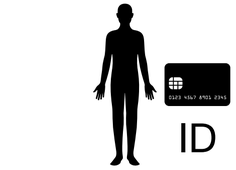
Feature Matching

Decision

Proceed to *Feature Matching* and *Decision* and take the needed time.

Biometric Systems

Enrollment Revision



Previously enrolled user

sensor

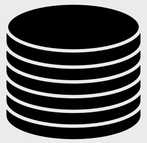
presentation

Trait Acquisition

Trait Enhancement

acquired sample, ID

enhanc



template database

De-duplication

Once the system has finally found a duplication, remove it, and take other necessary actions.

ID: Already-enrolled error. Remove duplication.

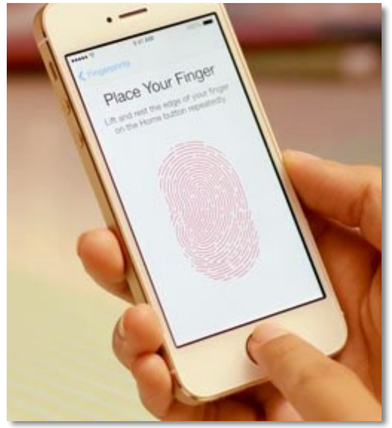
Feature Matching

Decision

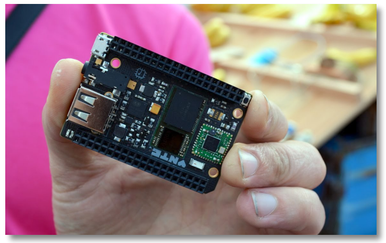
UNIVERSITY OF NOTRE DAME

Biometric Systems

Deployment



From all modules integrated within single chips…



To disperse modules independently deployed in diverse platforms.

UNIVERSITY OF NOTRE DAME

Biometric Systems

What do we want to consider?
Things to consider when designing a Biometrics system, besides trait.

Cooperative or non-cooperative users? (1/5)
Do users want to be identified?

Don’t appeal to covert deployment.

Biometric Systems

What do we want to consider?
Things to consider when designing a Biometrics system, besides trait.

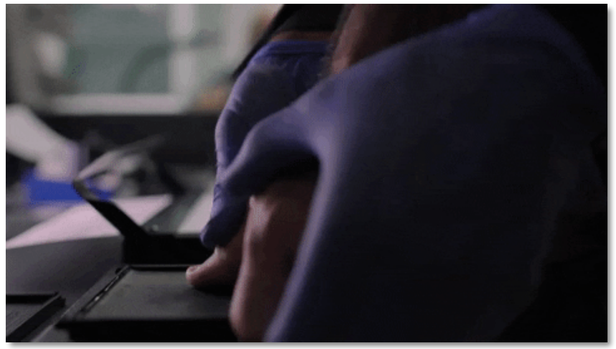
Habituated or non-habituated users? (2/5)
Do users interact with the system frequently or sporadically?

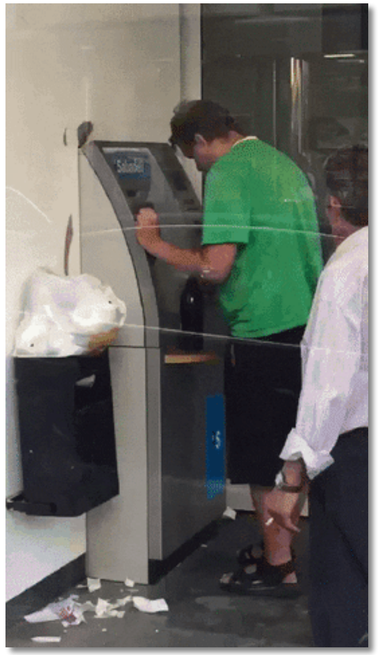
UNIVERSITY OF NOTRE DAME

Biometric Systems

What do we want to consider?
Things to consider when designing a Biometrics system, besides trait.

Attended or unattended operation? (3/5)
Will somebody be helping users?



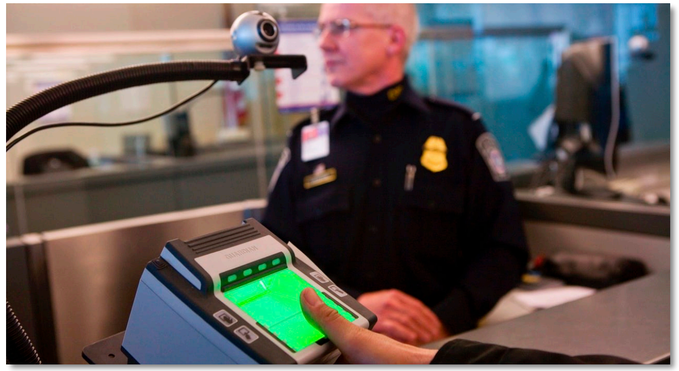


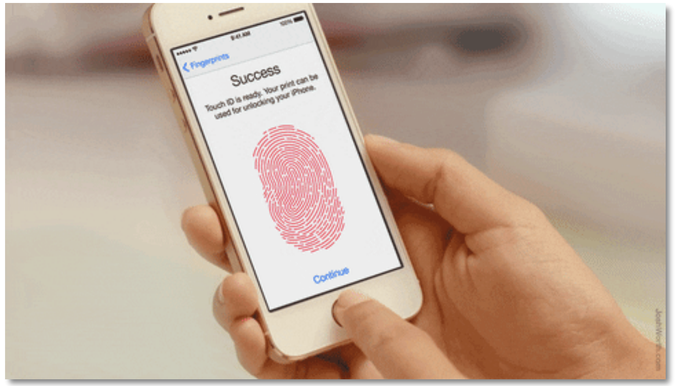
UNIVERSITY OF NOTRE DAME

Biometric Systems

What do we want to consider?
Things to consider when designing a Biometrics system, besides trait.

Controlled or uncontrolled environment? (4/5)
How do the environmental conditions change?
(temperature, illumination, etc.)





UNIVERSITY OF NOTRE DAME

Biometric Systems

What do we want to consider?
Things to consider when designing a Biometrics system, besides trait.

What are the computational requirements? (5/5)
Consider memory footprint, processing time, response time, and system availability.

UNIVERSITY OF NOTRE DAME

Biometric Systems

What do we want to avoid?

Covert deployment
Users must be aware of the Biometric system collecting their data.
Respect their privacy.

No data confidentiality
Collected data must be confidential. Avoid function creep.

Unsafe system
We will get to know threats (attacks) that may harm a system's integrity.

UNIVERSITY OF NOTRE DAME

Biometric System Errors

Denial of Access (1/3)

Verification
Jane Doe: Here, I'm Jane Doe.
System: No, you're not.

Identification
Jane Doe: Here, my fingerprints.
System: I don't know you.

UNIVERSITY OF NOTRE DAME

Biometric System Errors

Denial of Access (1/3)

Possible Causes
Intrinsic failure: intra-user trait variation,
due to different sensors, hardware malfunction, pose, illumination, make-up, aging, illness, cosmetic surgeries, etc.

Adversarial attack: malicious alteration of
template database, etc.

Biometric System Errors

Intrusion (2/3)

Verification
Jane Doe: Here, I'm Jane Fonda.
System: Welcome, Jane Fonda!

Identification
Jane Doe: Here, my fingerprints.
System: Welcome, Jane Fonda!

https://www.wired.com/story/10-year-old-face-id-unlocks-mothers-iphone-x/

Biometric System Errors

Intrusion (2/3)

Possible Causes
Intrinsic failure: inter-user high similarity,
due to low trait uniqueness,
poor trait capture, etc.

Adversarial attack:
impersonation, spoofing, etc.

impersonation

spoofing

Biometric System Errors

Repudiation (3/3)

Verification
Jane Doe: See, I'm not Jane Doe.
System: Yeah, you're right.

Identification
Jane Doe: Here, my fingerprints.
System: Yeah, I don't know you.

Biometric System Errors

Repudiation (3/3)

Possible Causes
Intrinsic failure: hardware malfunction, intra-user trait variation.

Adversarial attack: obfuscation.

obfuscation

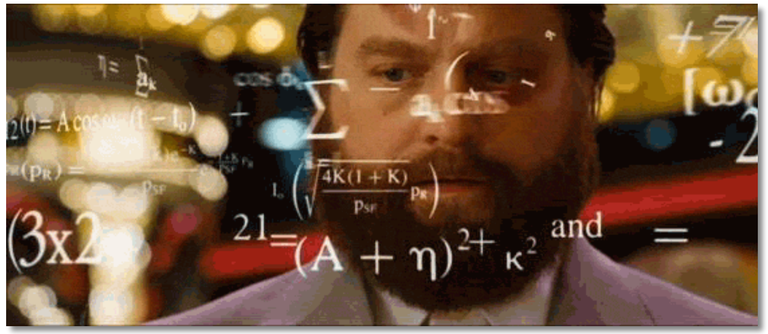
UNIVERSITY OF NOTRE DAME

Biometric System Errors

Math Model
Objective definition of 2 events:

1. False Non-Match (FNM)
A comparison of two features of the same individual should lead to a match, but it led to a non-match.
It causes either a denial of access or helps repudiation.

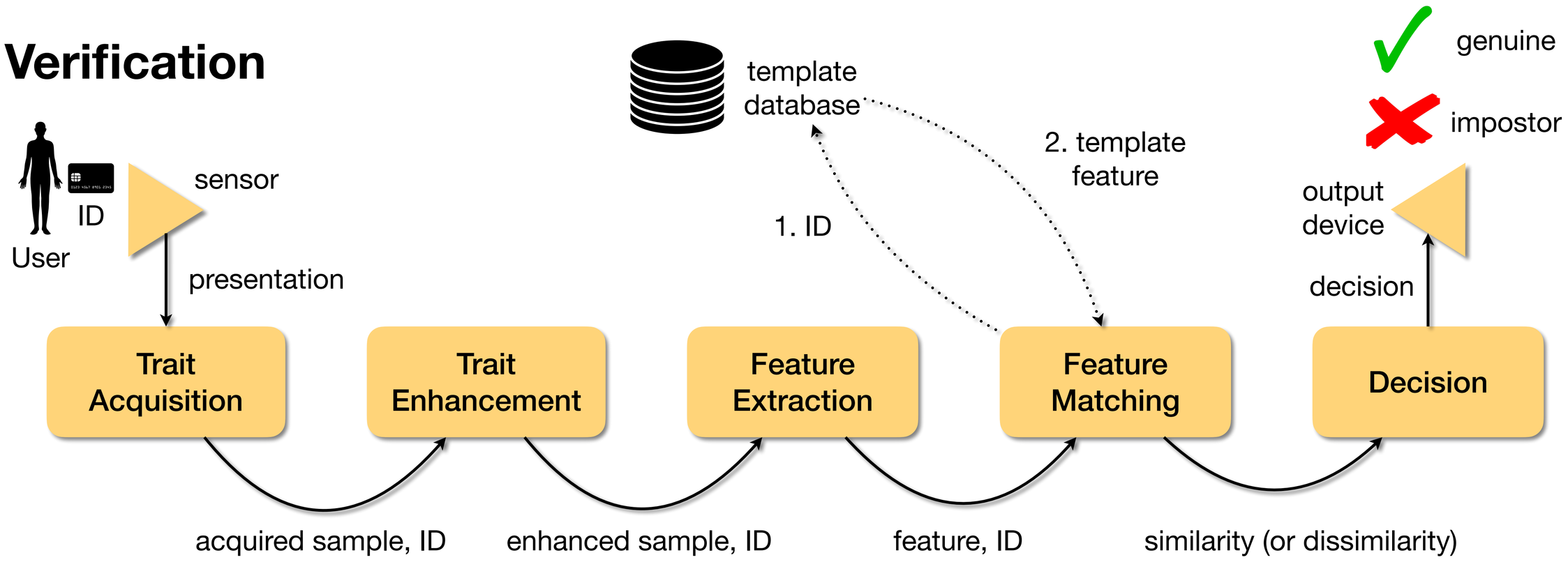
2. False Match (FM)
A comparison of two features from different individuals should lead to a non-match, but it led to a match.
It helps an intrusion.



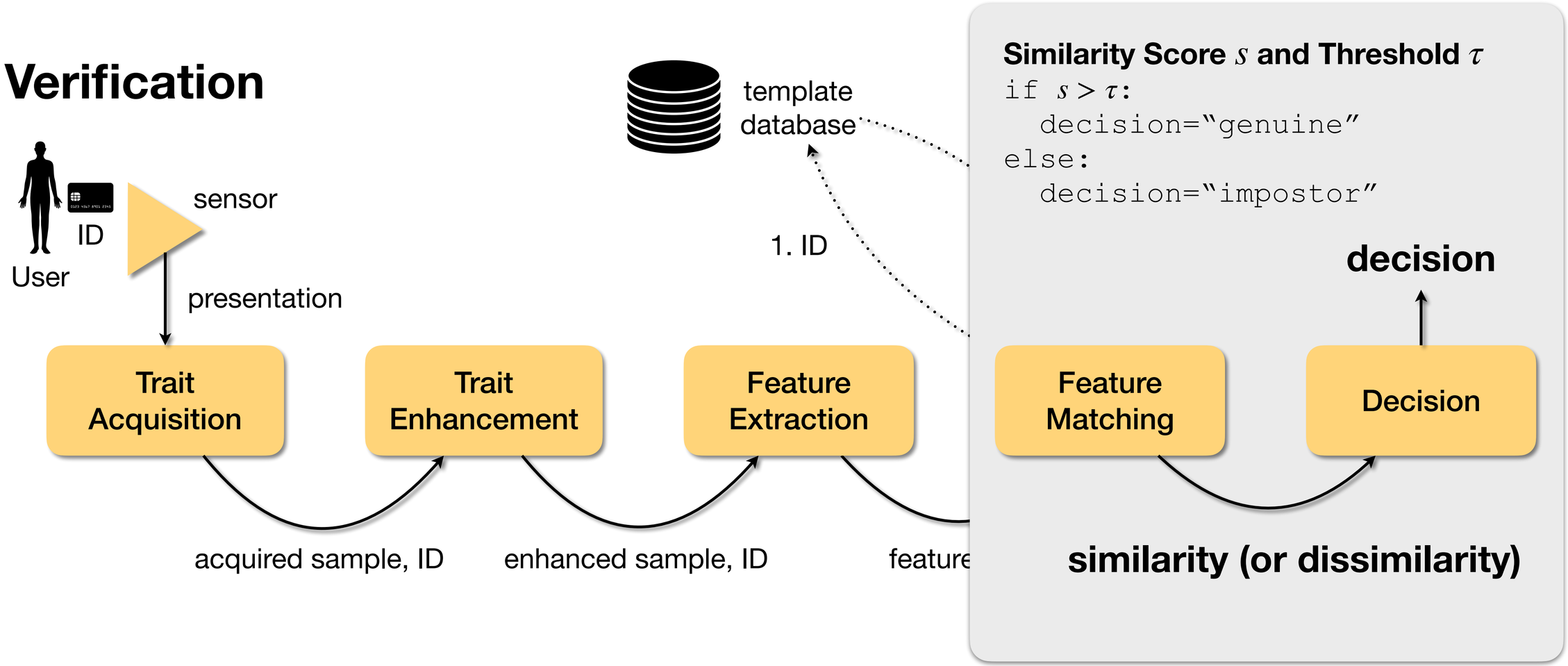
Let's see how to compute them!

UNIVERSITY OF NOTRE DAME

Metrics

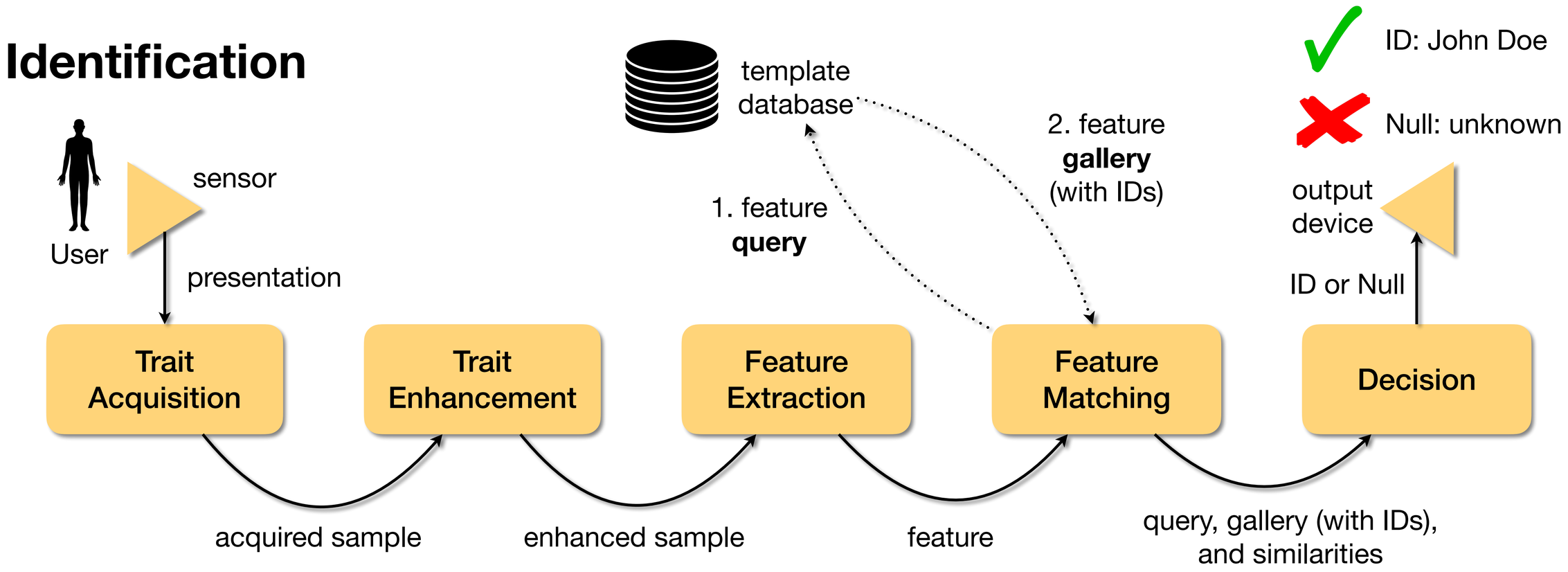


Metrics


Verification
User
ID
sensor
presentation
template database
1. ID
Trait Acquisition
Trait Enhancement
Feature Extraction
Feature Matching
Decision
acquired sample, ID
enhanced sample, ID
feature
similarity (or dissimilarity)
decision
Similarity Score s and Threshold τ
if $s > \tau$:
decision="genuine"
else:
decision="impostor"

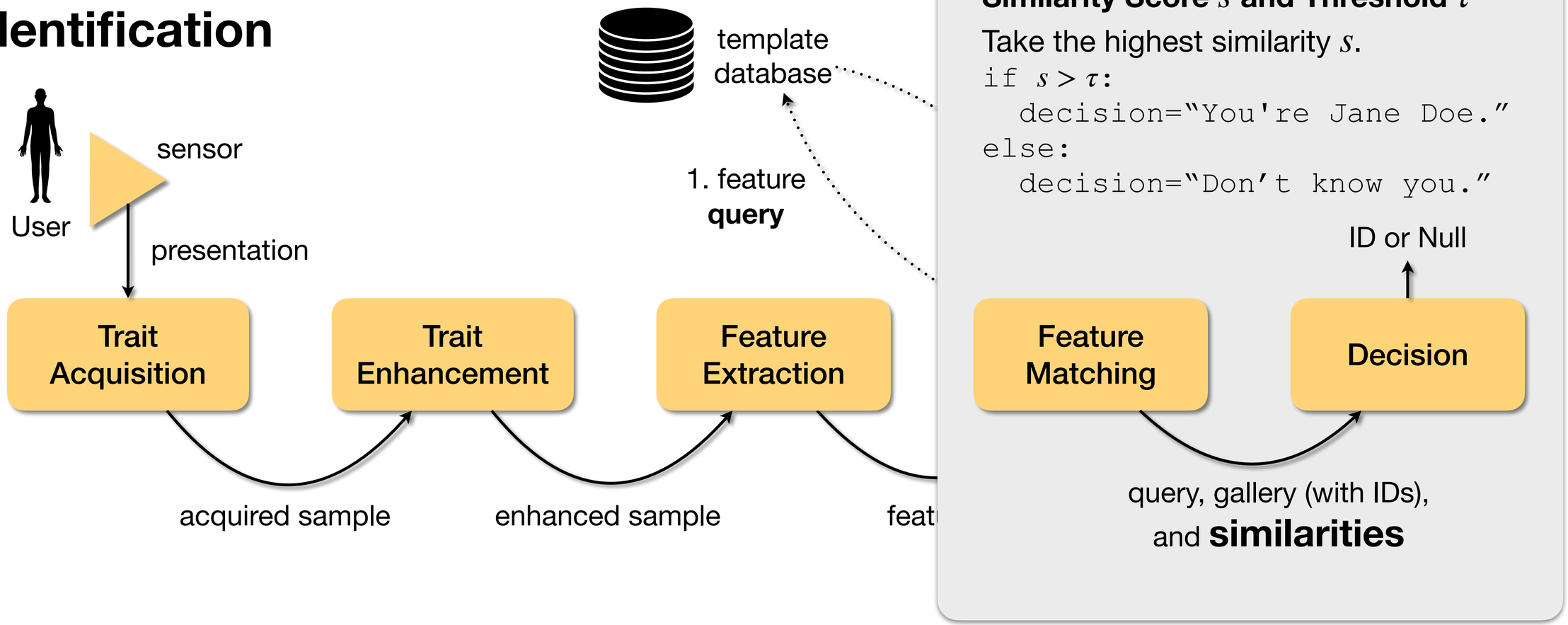
Metrics

Identification



Metrics

Identification

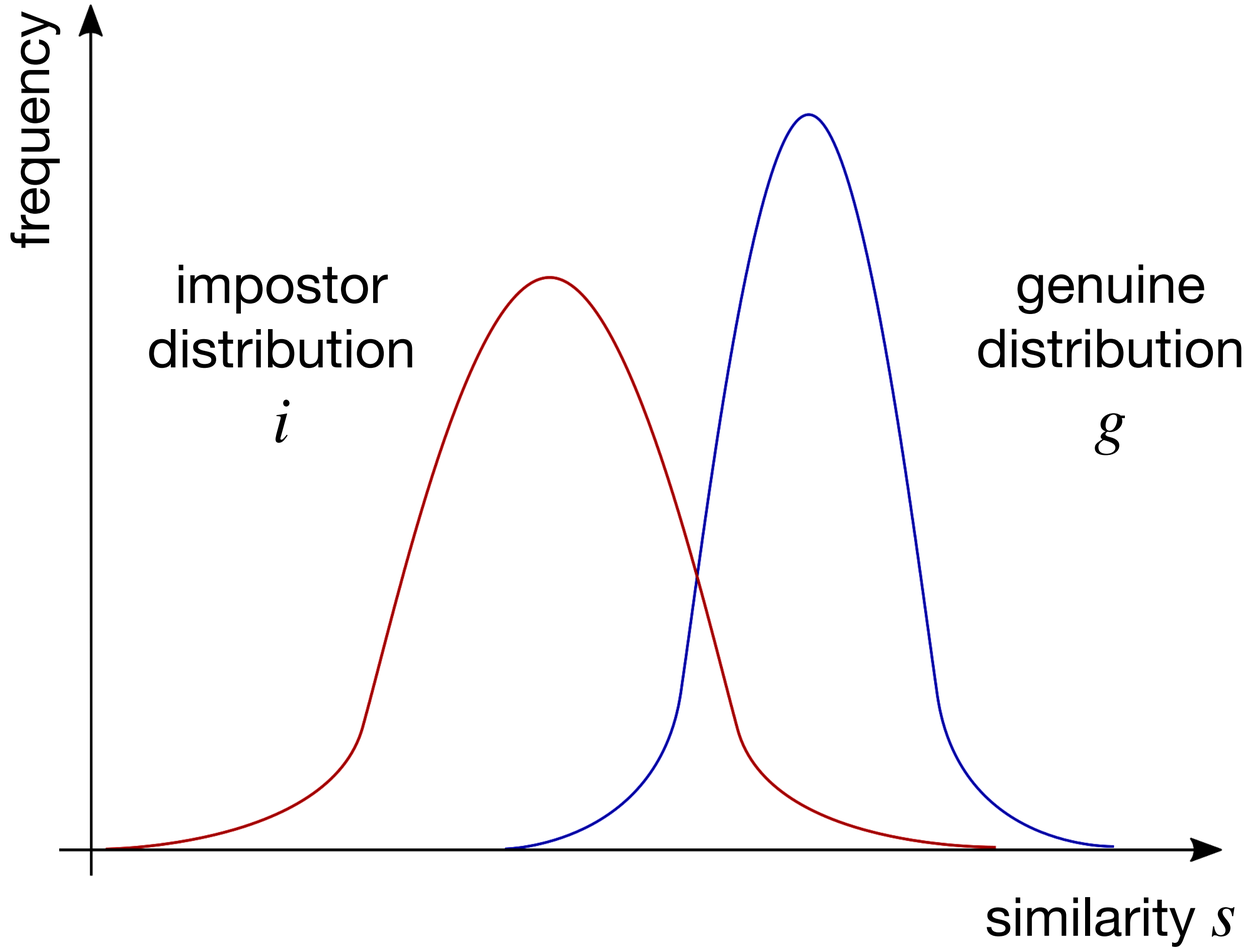


Similarity Score s and Threshold τ

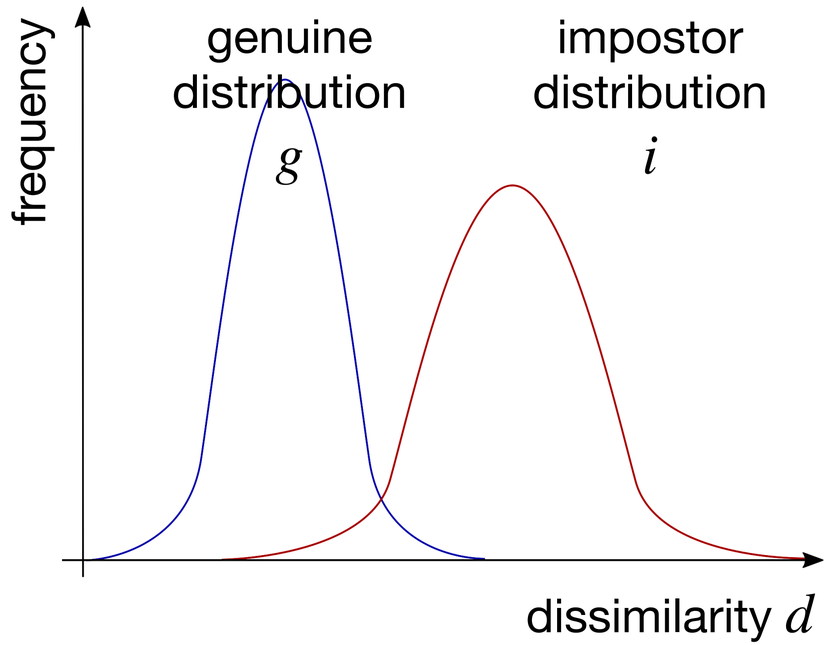
Take the highest similarity s.

```
if s > τ:
  decision="You're Jane Doe."
else:
  decision="Don't know you."
```

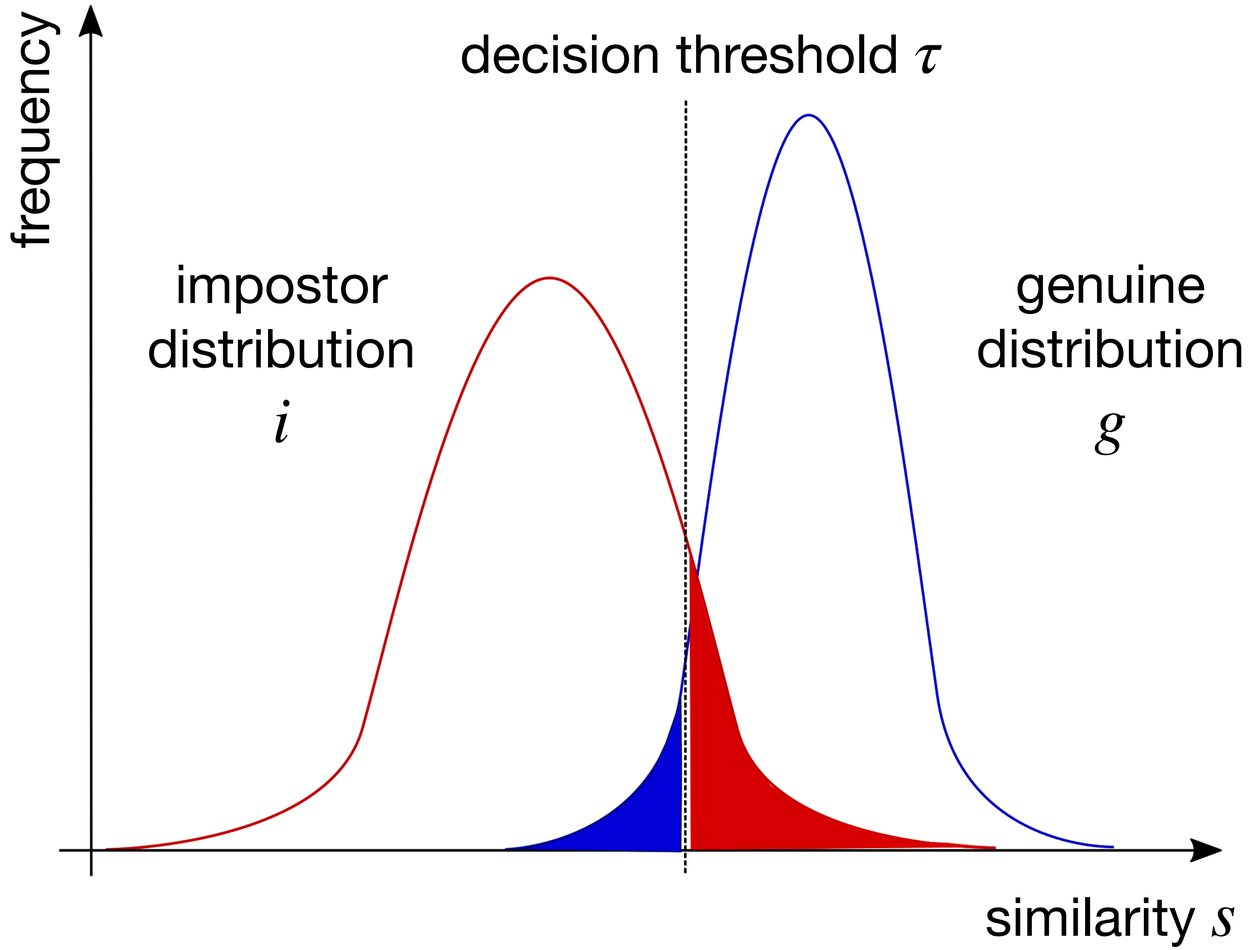
Metrics



In case of distances…



Metrics



$$FNM(\tau) = \int_{-\infty}^{\tau} g(s)\ ds$$

$$FM(\tau) = \int_{\tau}^{\infty} i(s)\ ds$$

Metrics

In Practice

False Non-Match Rate (FNMR) and False Match Rate (FMR)

$$FNMR(\tau) = \frac{\#(false\ nonmatches\ for\ \tau)}{\#(genuine\ comparisons)}$$

$$FNM(\tau) = \int_{-\infty}^{\tau} g(s)\ ds$$

$$FMR(\tau) = \frac{\#(false\ matches\ for\ \tau)}{\#(impostor\ comparisons)}$$

$$FM(\tau) = \int_{\tau}^{\infty} i(s)\ ds$$

Metrics

In Practice

False Non-Match Rate (FNMR) and False Match Rate (FMR)

$$FNMR(\tau) = \frac{\#(false\ nonmatches\ for\ \tau)}{\#(genuine\ comparisons)}$$

How many of the genuine comparisons are wrongly computed by the system?

$$FMR(\tau) = \frac{\#(false\ matches\ for\ \tau)}{\#(impostor\ comparisons)}$$

How many of the impostor comparisons are wrongly computed by the system?

Metrics

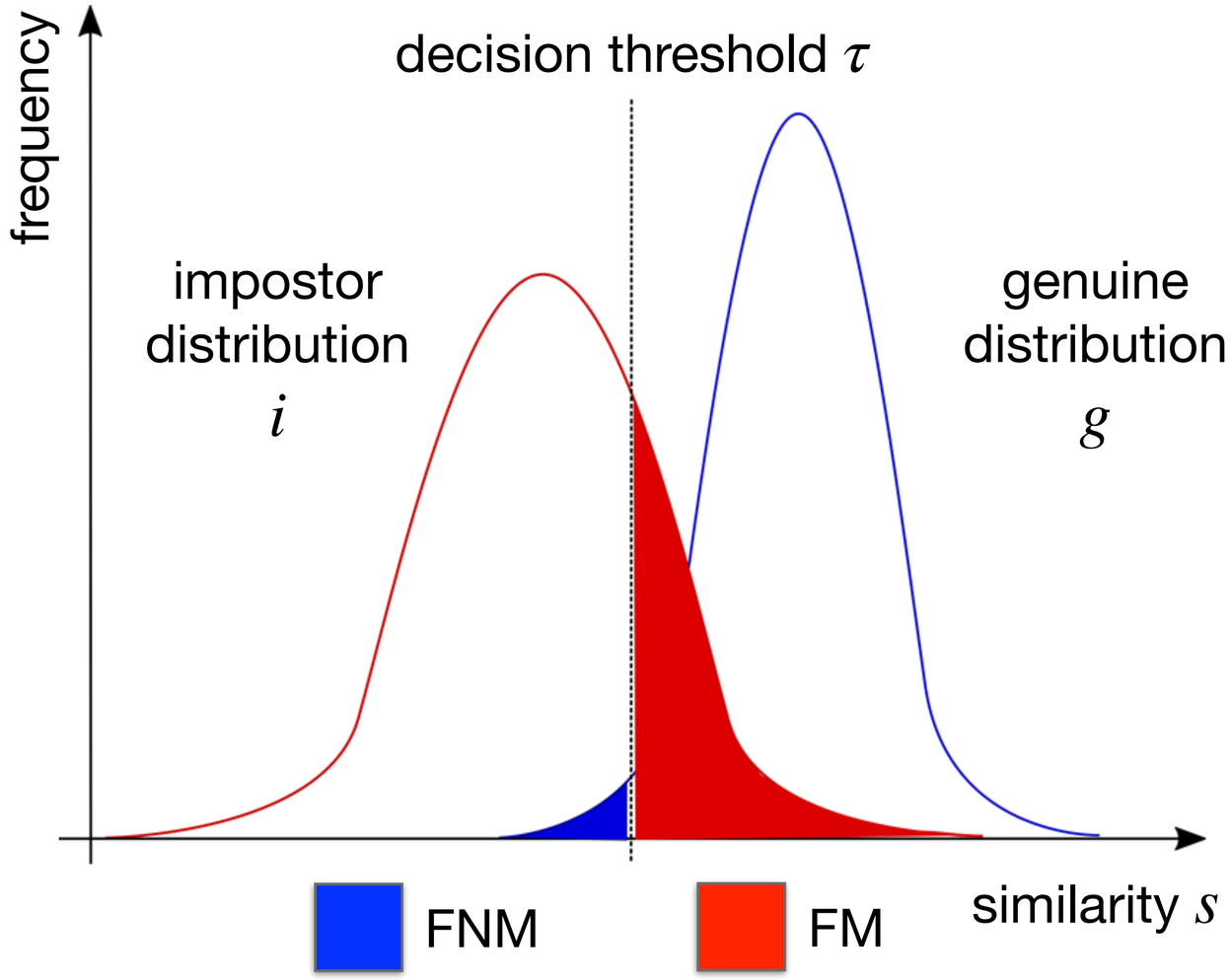
In Practice
Interpretation of *R values.

Suppose a face recognition system with FMR=0.1%
FMR=0.001, one error in every 1K comparisons.
Is it good?

Suppose the Newark airport
5K people per hour, 14h per day (70K people per day)
Suppose a suspect watch list with 100K people: 7 billion comparisons per day.
Average number of false matches per day: 7 million people to double check every day.

Terrorist watch list in 2016: 1,8 million people

Metrics



What is the impact of changing the decision threshold?

The larger the value of τ:
The larger the value of FNM;
The smaller the value of FM.

FNM and FM are inversely proportional.

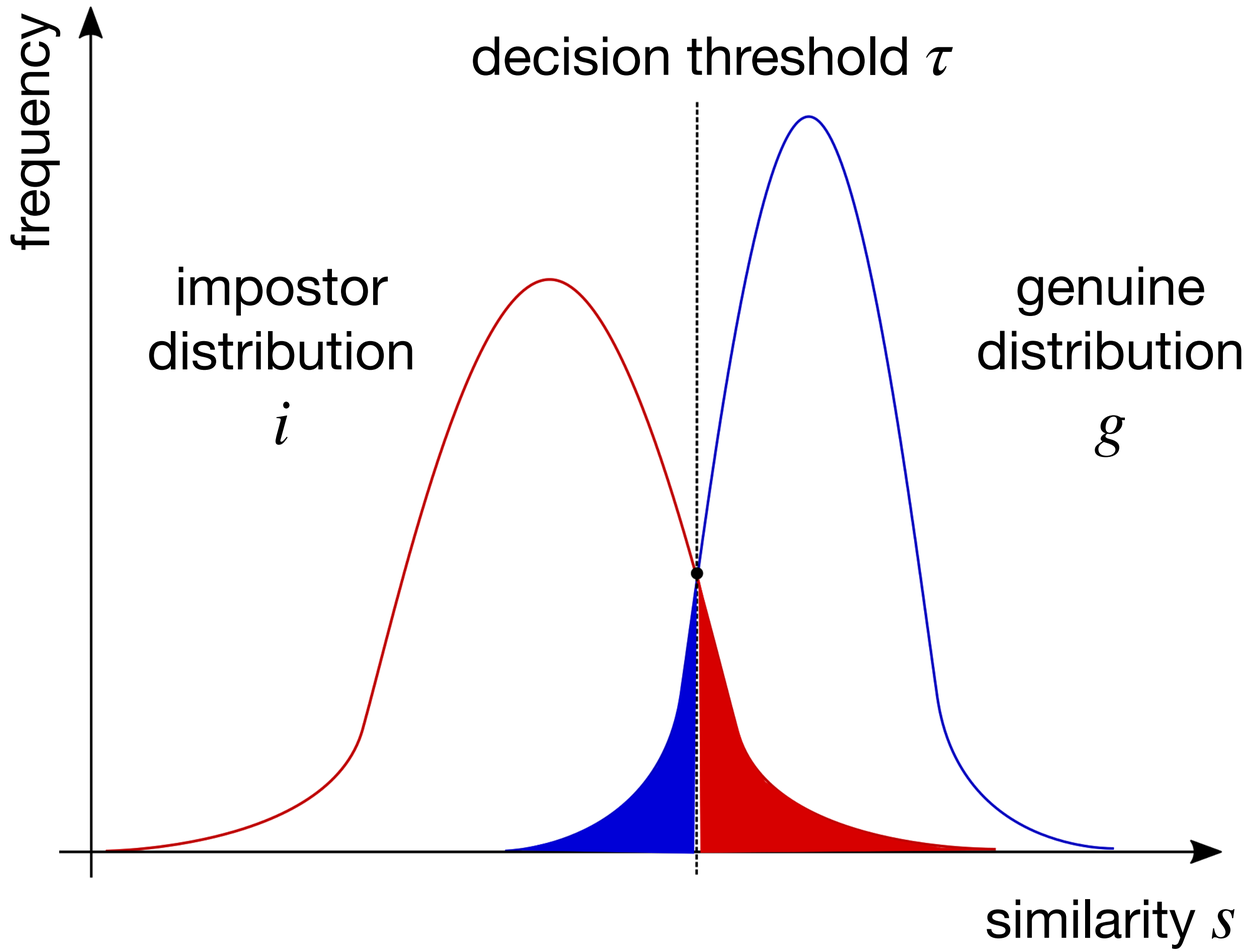
Metrics

What to choose?

Small FNMR
Suitable to avoid denial of access
and repudiation.
Increases intrusion probability, though.

Small FMR
Suitable to avoid intrusion.
Increases denial of service and
repudiation probability, though.

Metrics



What to choose?

Equal Error Rate (EER)
Common practice.
Pick the threshold where FNMR = FMR.

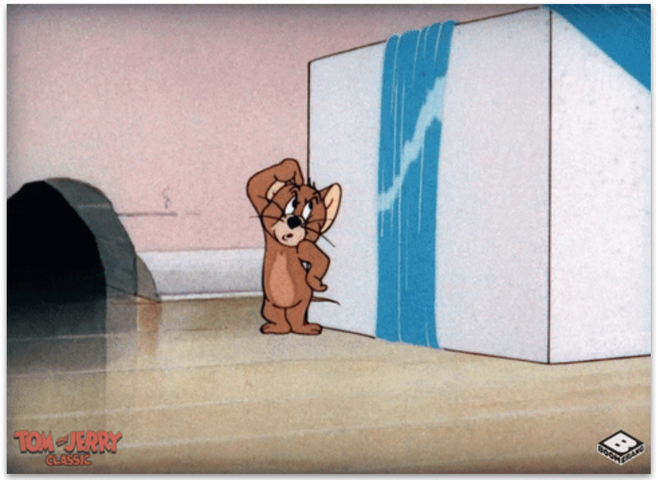
UNIVERSITY OF NOTRE DAME

Metrics

How to compare two different systems?
Biometric systems *A* and *B.*

Compare both systems' FNMR and FMR at EER (1/3)
Take the one with smaller FNMR and FMR values.

What to do when system A has smaller FNMR than system B, but larger FMR (or vice-versa)?



Metrics

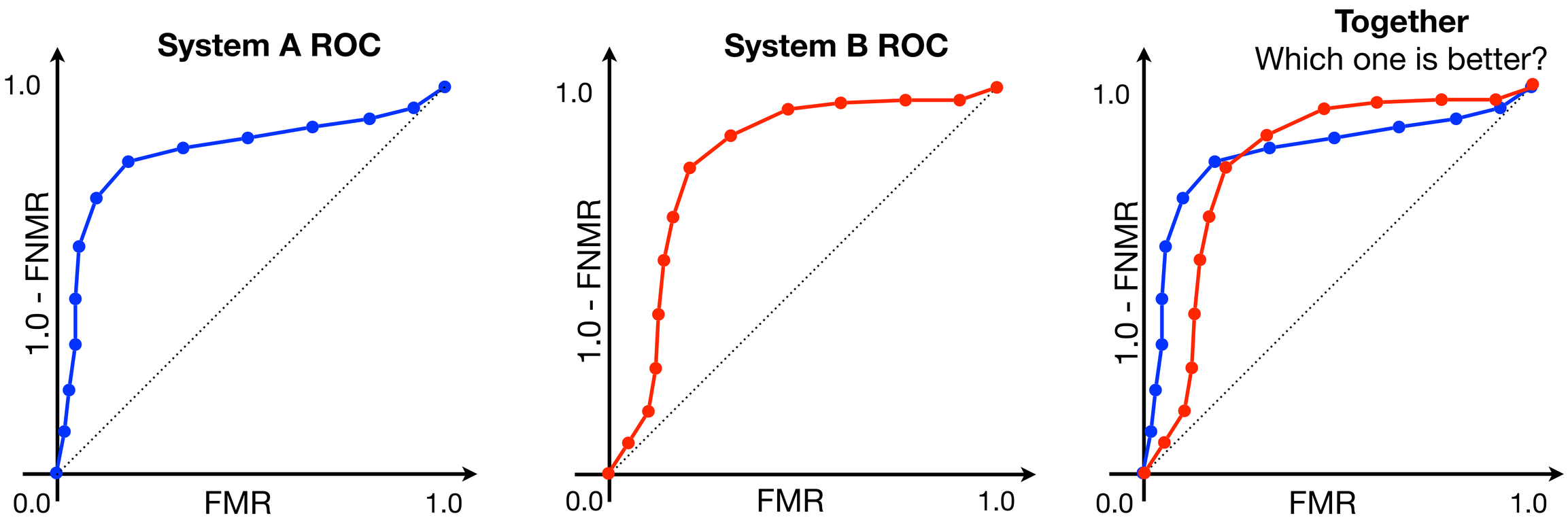
How to compare two different systems?
Biometric systems *A* and *B.*

Use a Receiver Operating Characteristic (ROC) curve (2/3)

Metrics

How to compare two different systems?
Biometric systems *A* and *B.*

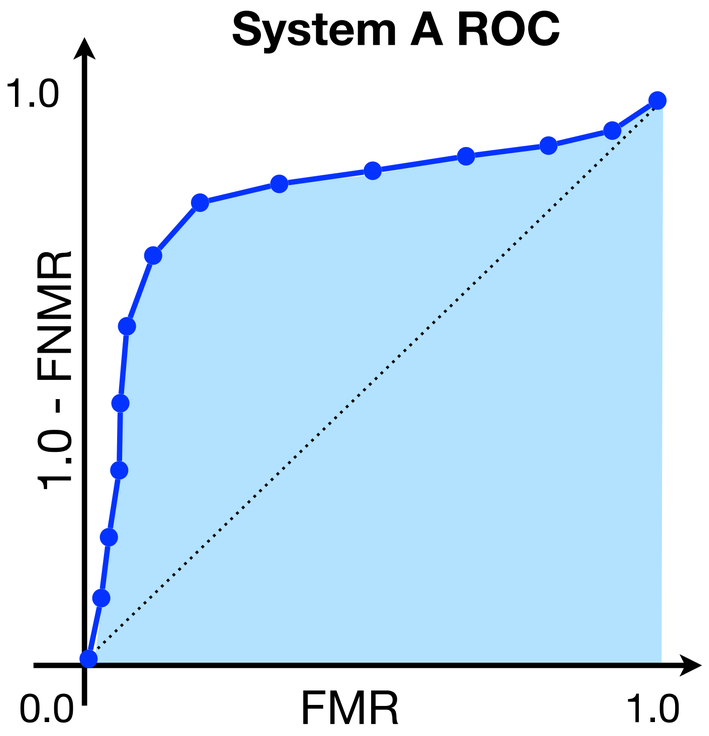
Compute FMR and FNMR for a variety of thresholds.

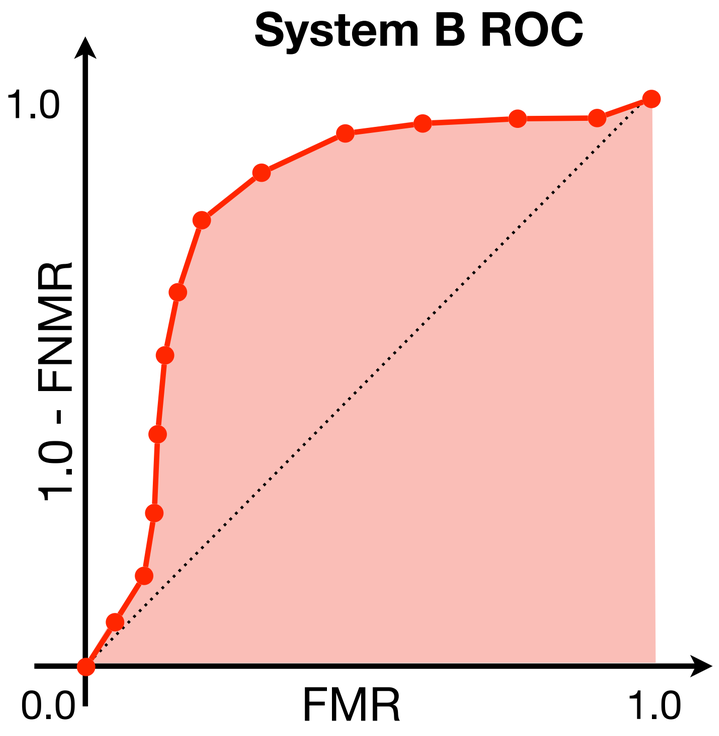


UNIVERSITY OF NOTRE DAME

Metrics

How to compare two different systems?
Biometric systems *A* and *B.*



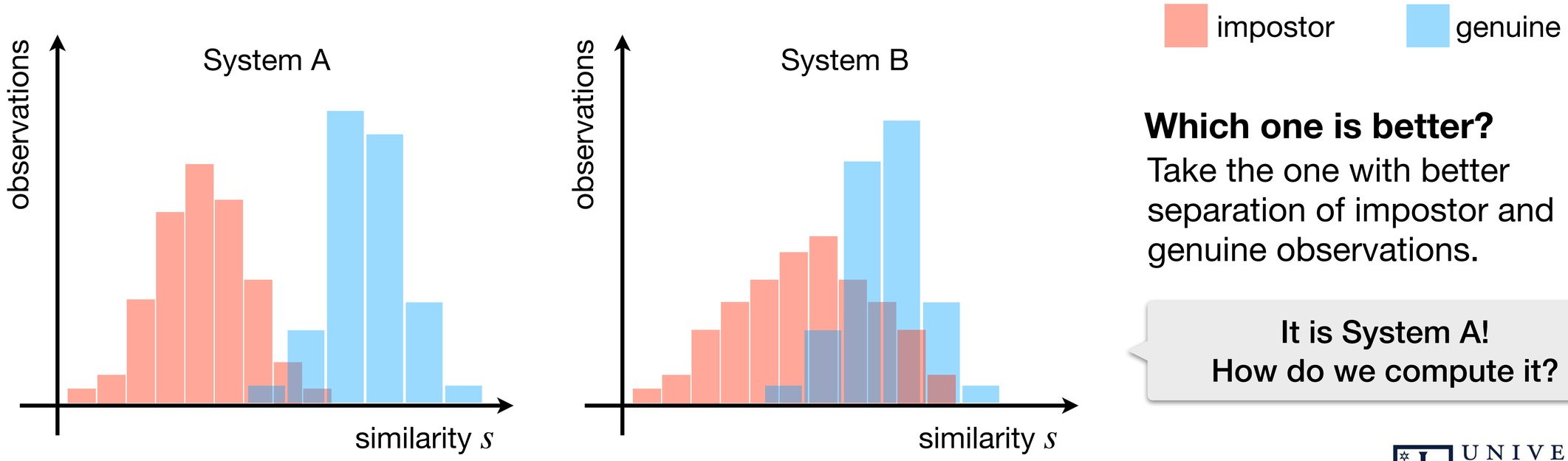


Which one is better?
Compute the
Area Under The Curve
(AUC).
The best solution
presents larger AUC.

Metrics

How to compare two different systems?
Biometric systems *A* and *B.*

Compute the difference between impostor and genuine distributions for each system (3/3)



Which one is better?
Take the one with better separation of impostor and genuine observations.

It is System A!
How do we compute it?

Metrics

How to compare two different systems?
Biometric systems *A* and *B.*

Compute the difference between impostor and genuine distributions for each system (3/3)

Which one is better?
Take the system with
larger **d-prime**:

$$d' = \frac{\sqrt{2} \times |\mu_{genuine} - \mu_{impostor}|}{\sqrt{\sigma^2_{genuine} + \sigma^2_{impostor}}}$$

Hypothesis: the distributions are Gaussians (with mean μ and standard deviation σ).

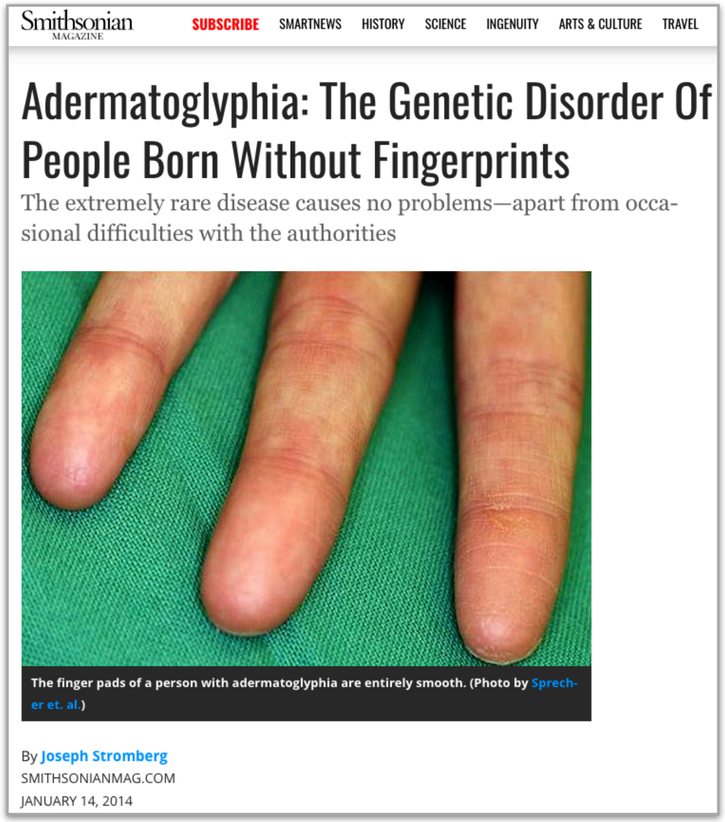
The larger the separation between the distributions, the larger the value of d-prime.

Metrics

Other Metrics (1/4, 2/4)

Failure to Acquire (FTA)
Rate of falsely rejected biometric samples due to problems in acquisition.

Failure to Enroll (FTE)
The same as FTA, but during enrollment.


Smithsonian MAGAZINE SUBSCRIBE SMARTNEWS HISTORY SCIENCE INGENUITY ARTS & CULTURE TRAVEL

Adermatoglyphia: The Genetic Disorder Of People Born Without Fingerprints

The extremely rare disease causes no problems—apart from occasional difficulties with the authorities

The finger pads of a person with adermatoglyphia are entirely smooth. (Photo by Sprecher et. al.)

By Joseph Stromberg
SMITHSONIANMAG.COM
JANUARY 14, 2014

https://www.smithsonianmag.com/science-nature/adermatoglyphia-genetic-disorder-people-born-without-fingerprints-180949338/

UNIVERSITY OF NOTRE DAME

Metrics

Other Metrics (3/4, 4/4)

Positive Metrics
True Non-Match Rate (TNMR)
TNMR = 1.0 - FMR

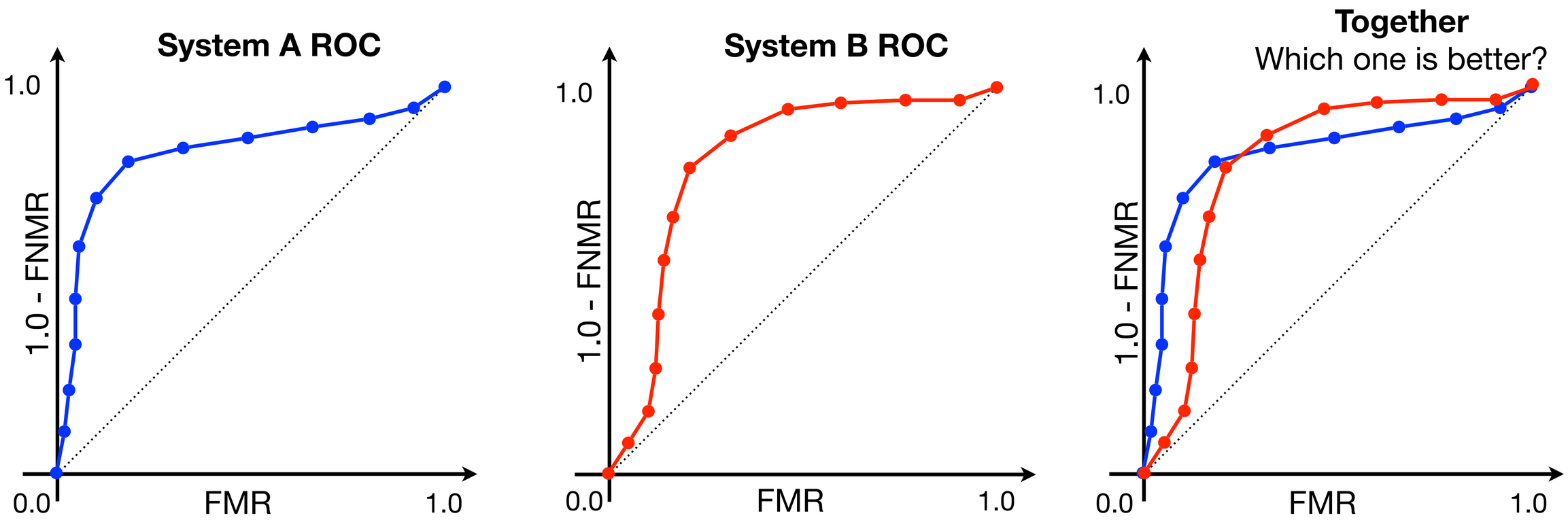
True Match Rate (TMR)
TMR = 1.0 - FNMR

You want to maximize these instead of minimizing.

Metrics

How to compare two different systems?
Biometric systems *A* and *B.*

Compute FMR and FNMR for a variety of thresholds.

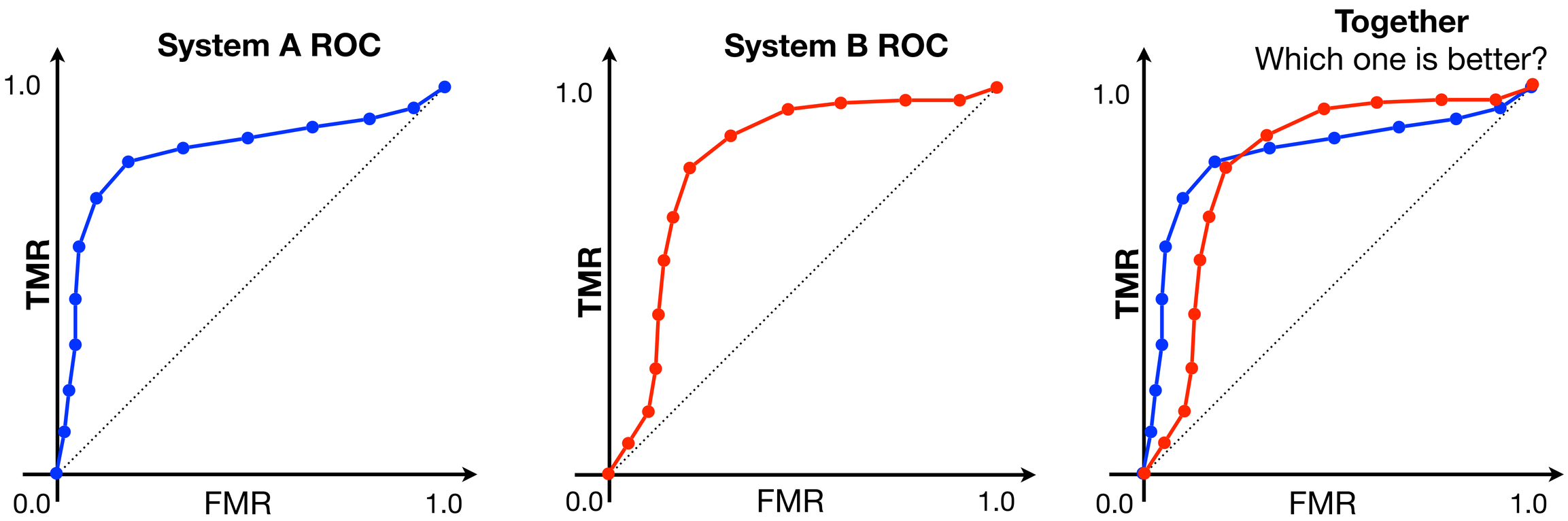


UNIVERSITY OF NOTRE DAME

Metrics

How to compare two different systems?
Biometric systems *A* and *B.*

Compute FMR and FNMR for a variety of thresholds.



S’up Next?

First Coding Day
Implementation of metrics.

Bring your computers
Don’t have one?
Please let me know ASAP.

Be ready! :)
Tools: Python 3 (important), PyCharm IDE (optional).