Basics II

CSE 40537/60537 Biometrics

Daniel Moreira

Spring 2020

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 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/

UNIVERSITY OF NOTRE DAME

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

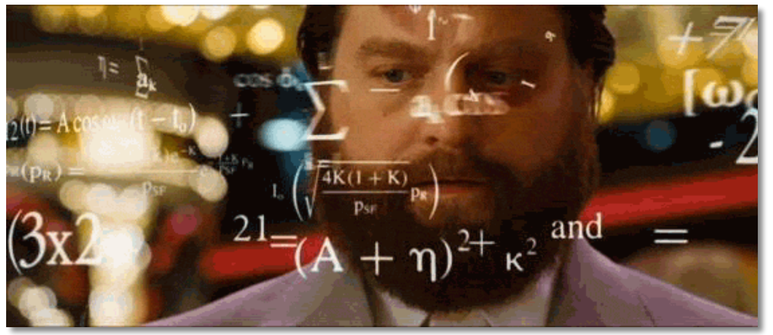
UNIVERSITY OF NOTRE DAME

Biometric System Errors

Math Model
Objective definition of 2 events:

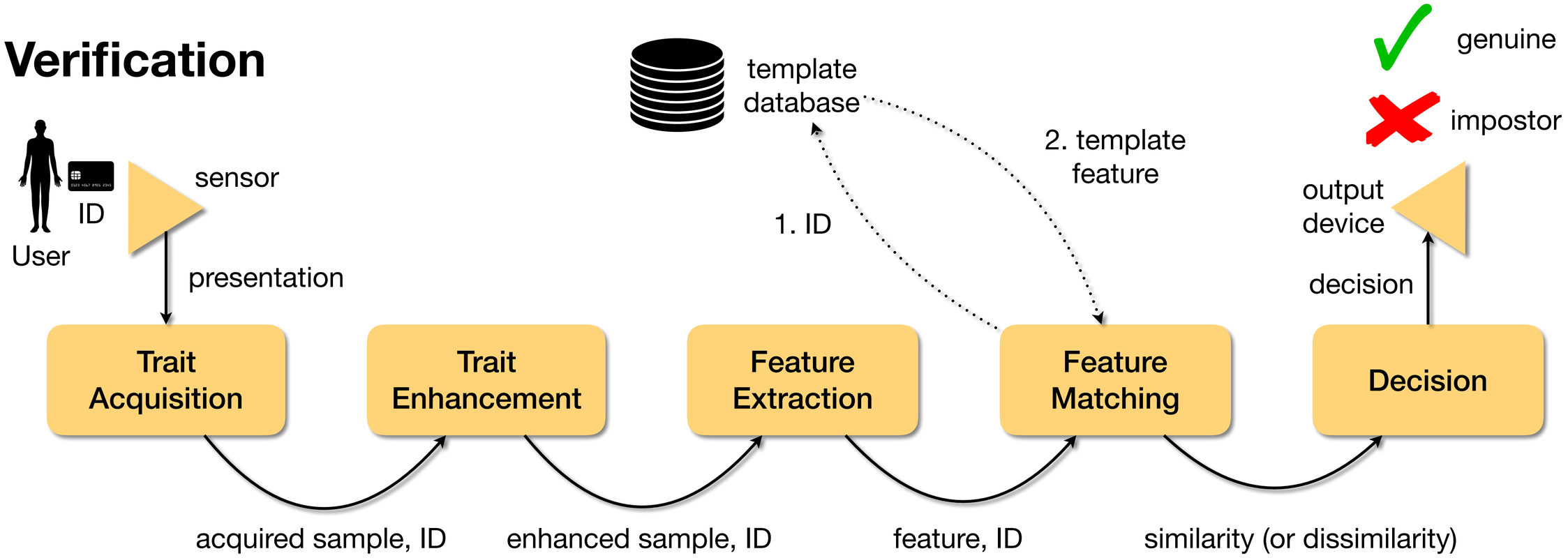
1. False Non-Match (FNM)
A comparison of two features of the same individual should lead to a match, but it led to a non-match.
It causes either a denial of access or helps repudiation.

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.

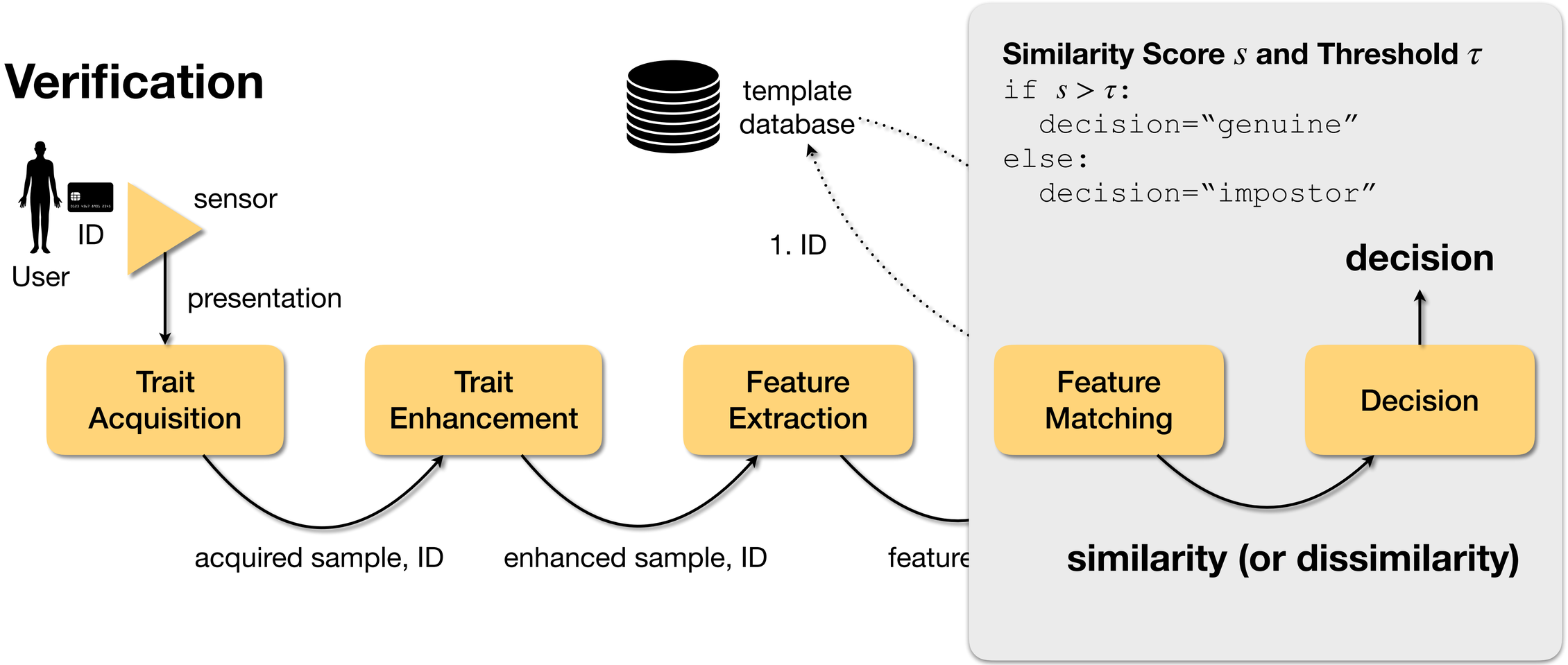


Let's see how to compute them!

Metrics

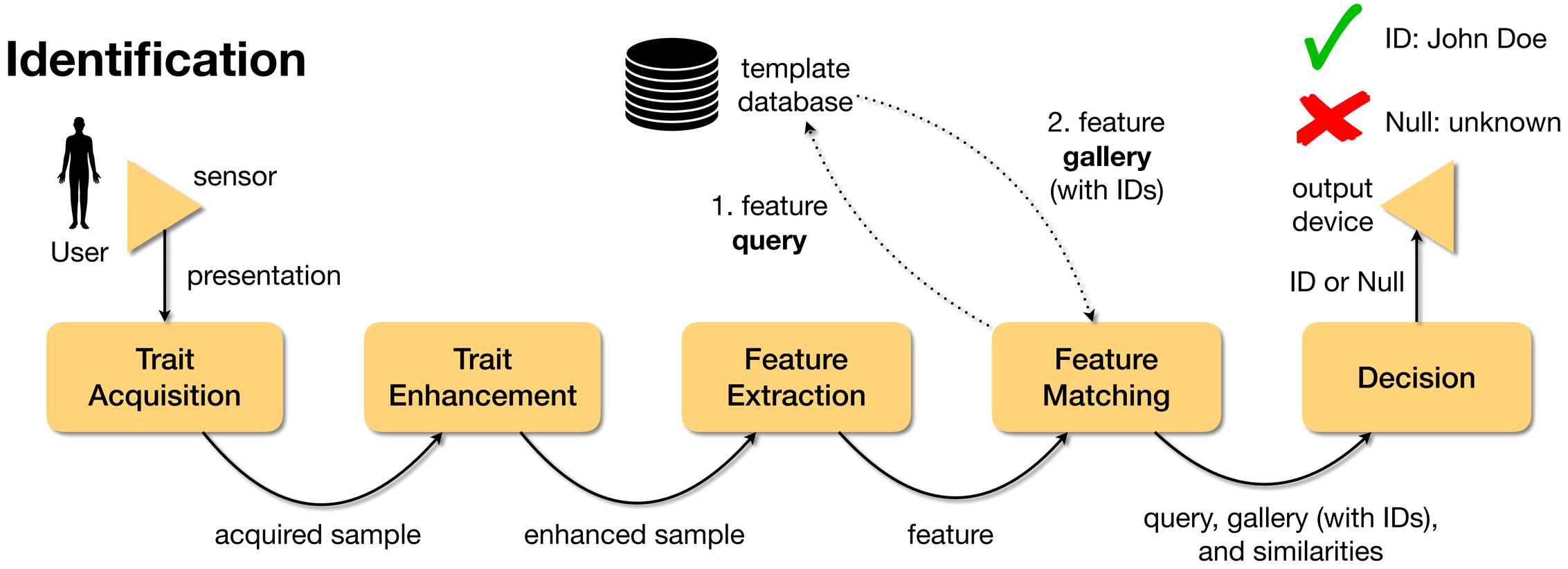


Metrics

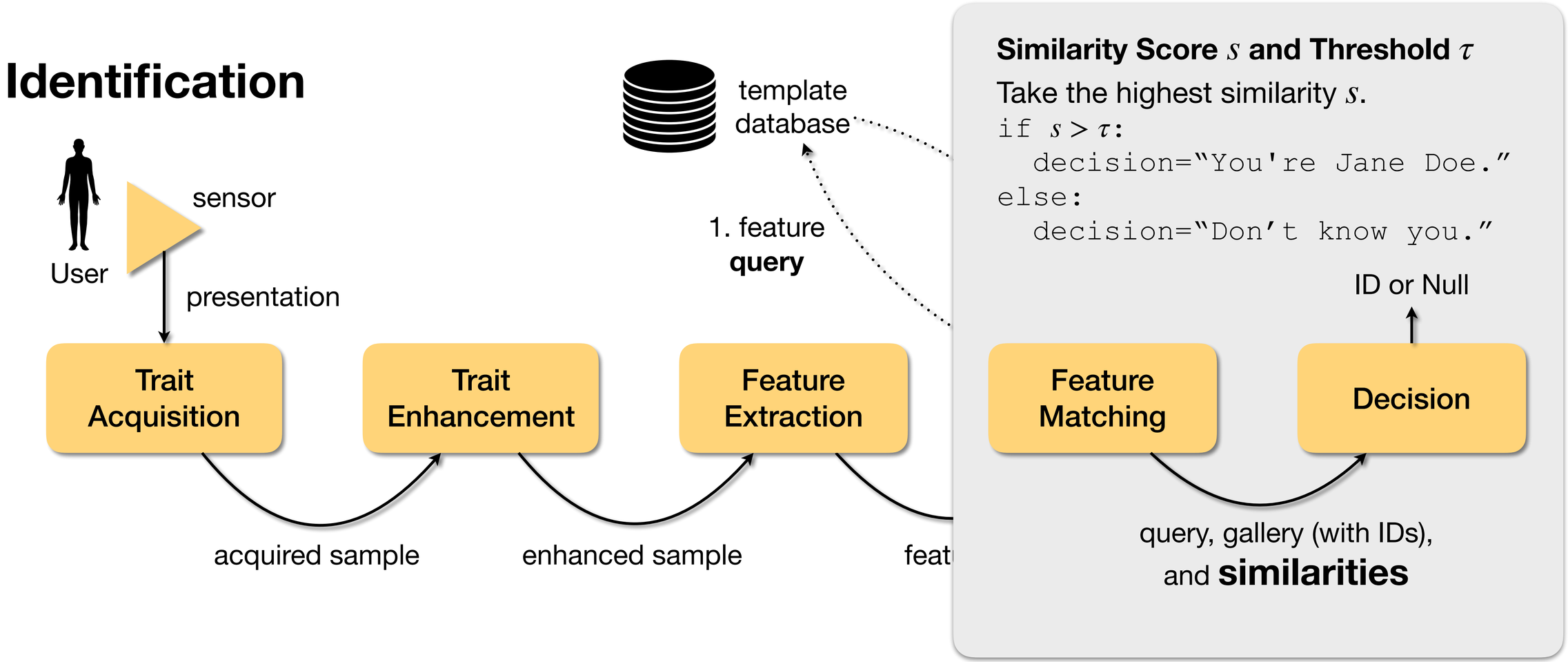


UNIVERSITY OF NOTRE DAME

Metrics

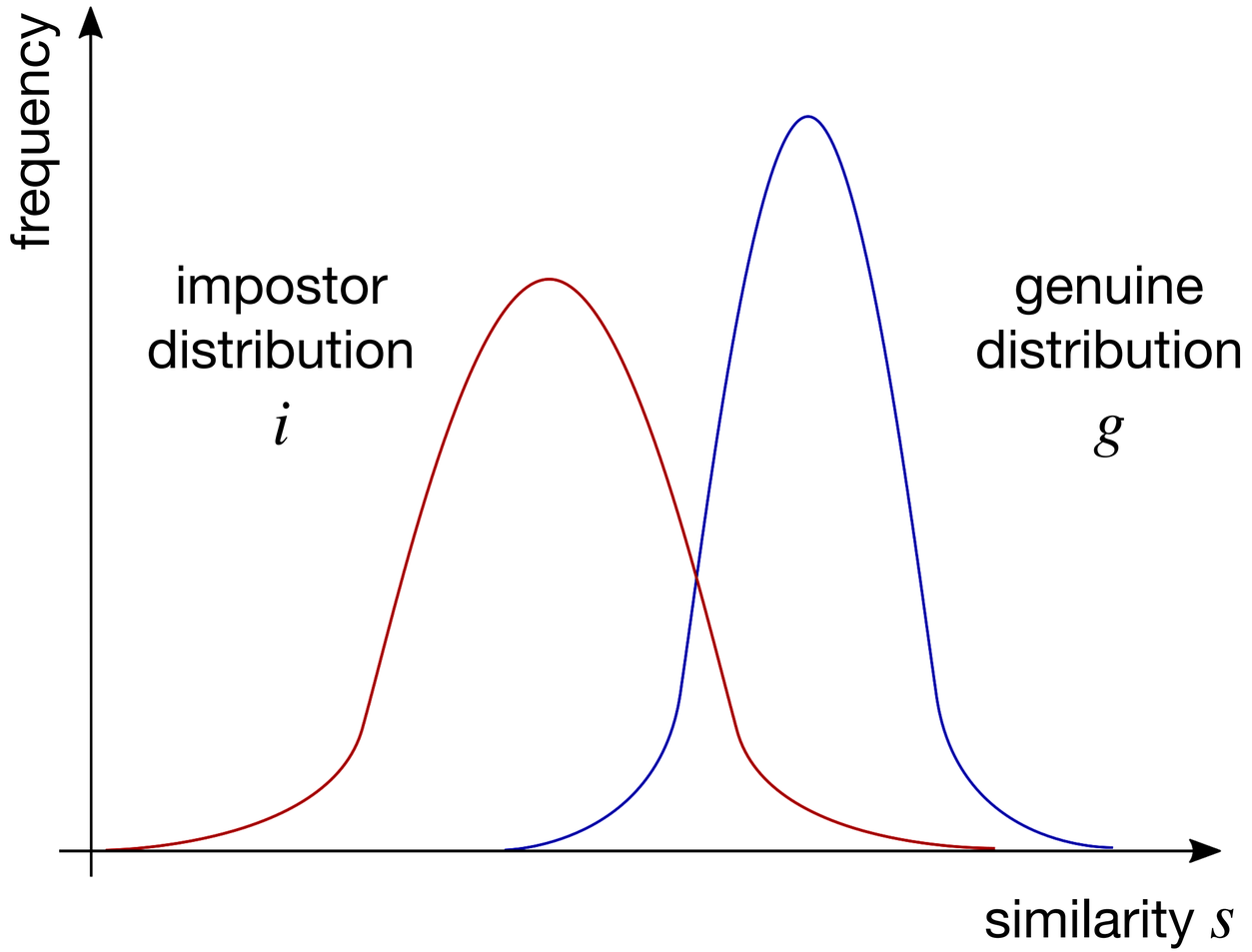


Metrics

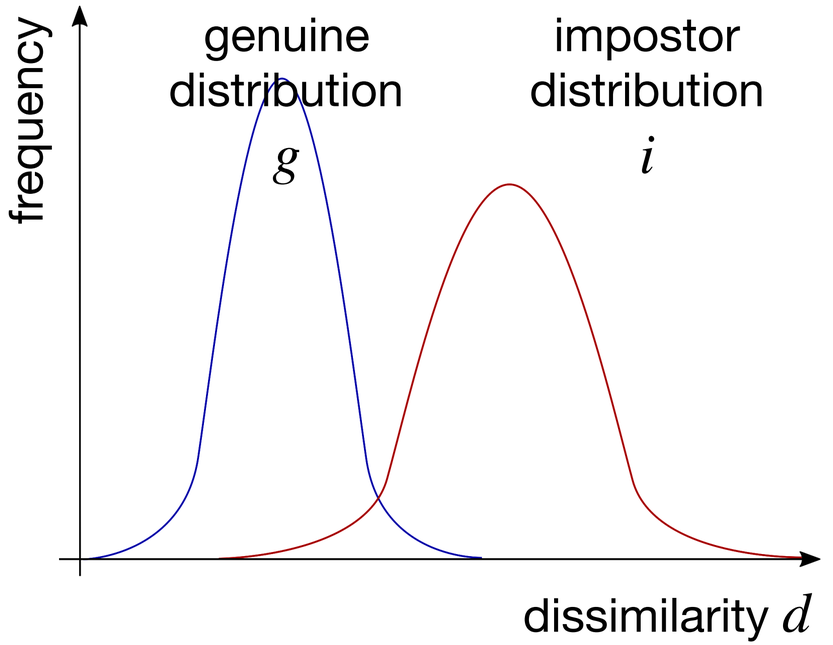


UNIVERSITY OF NOTRE DAME

Metrics

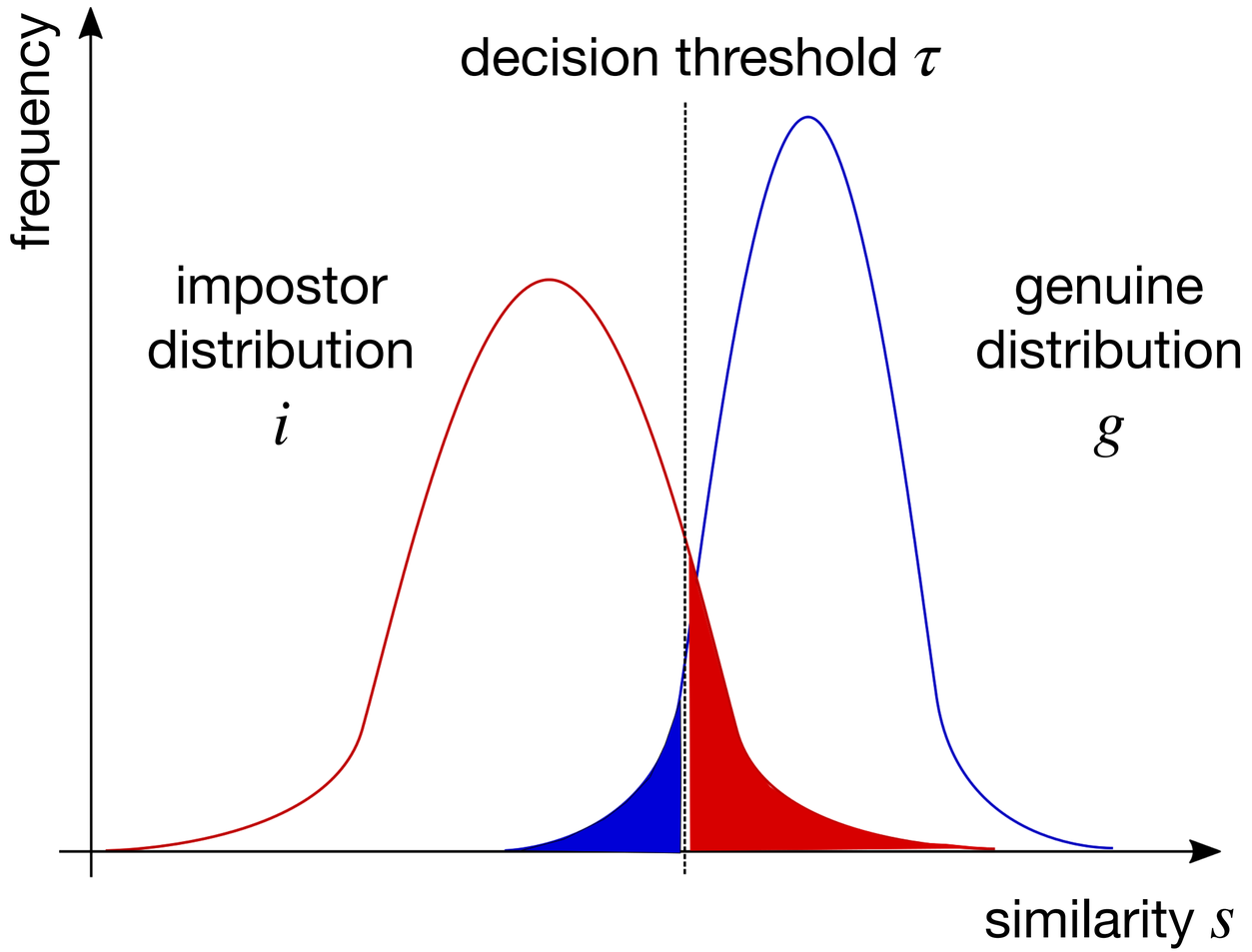


In case of dissimilarities…



UNIVERSITY OF NOTRE DAME

Metrics



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

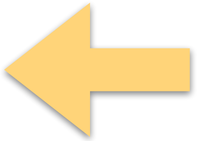
$$FM(\tau) = \int_{\tau}^{\infty} i(s)\ ds$$

Metrics

In Practice

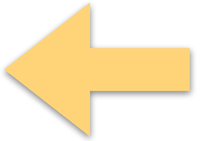
False Non-Match Rate (FNMR) and False Match Rate (FMR)

$$FNMR(\tau) = \frac{\#(false\ non-matches\ for\ \tau)}{\#(genuine\ comparisons)}$$



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

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



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

Metrics

In Practice

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

$$FNMR(\tau) = \frac{\#(false\ non-matches\ for\ \tau)}{\#(genuine\ comparisons)}$$

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

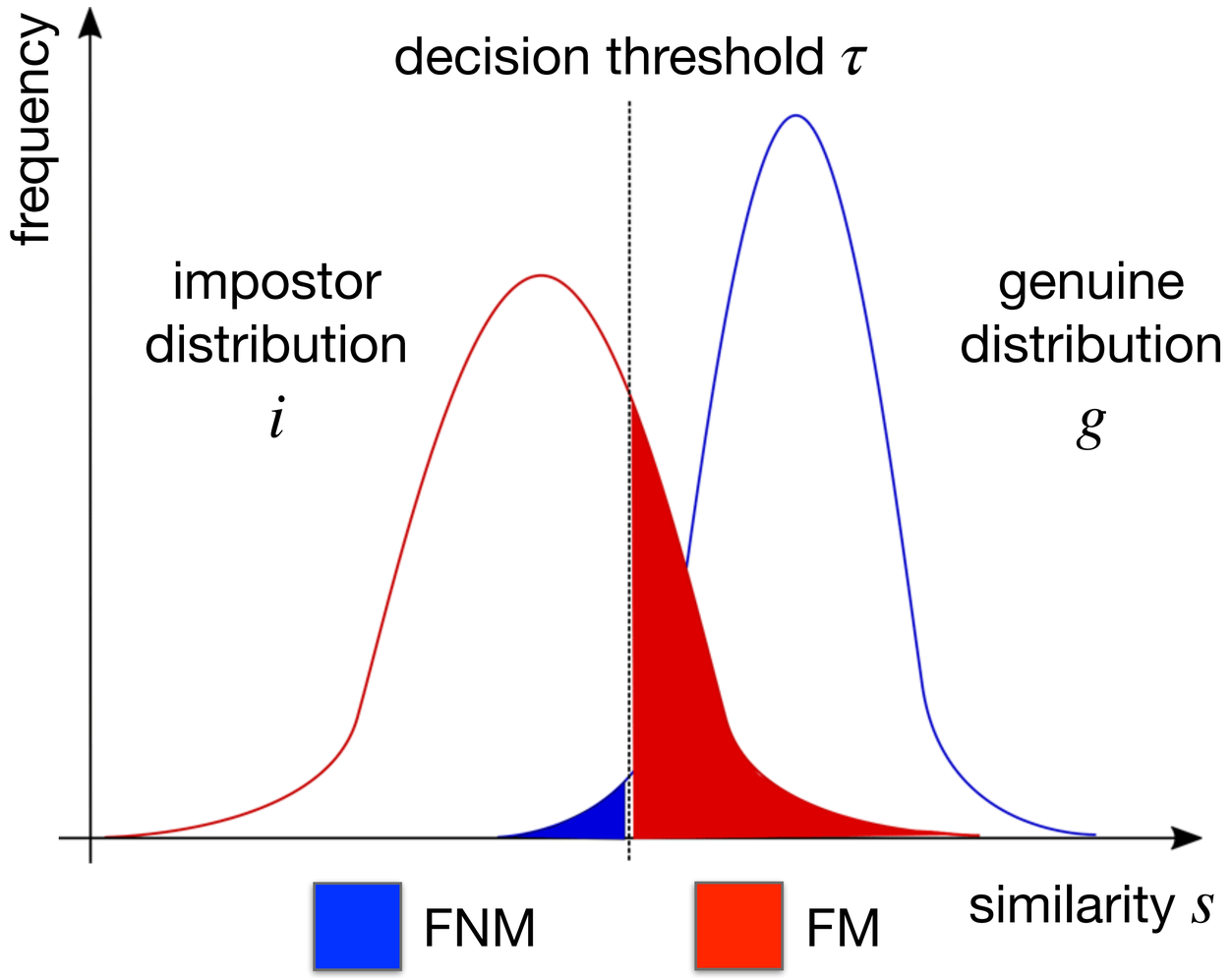
In Practice
Interpretation of *R values.

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.

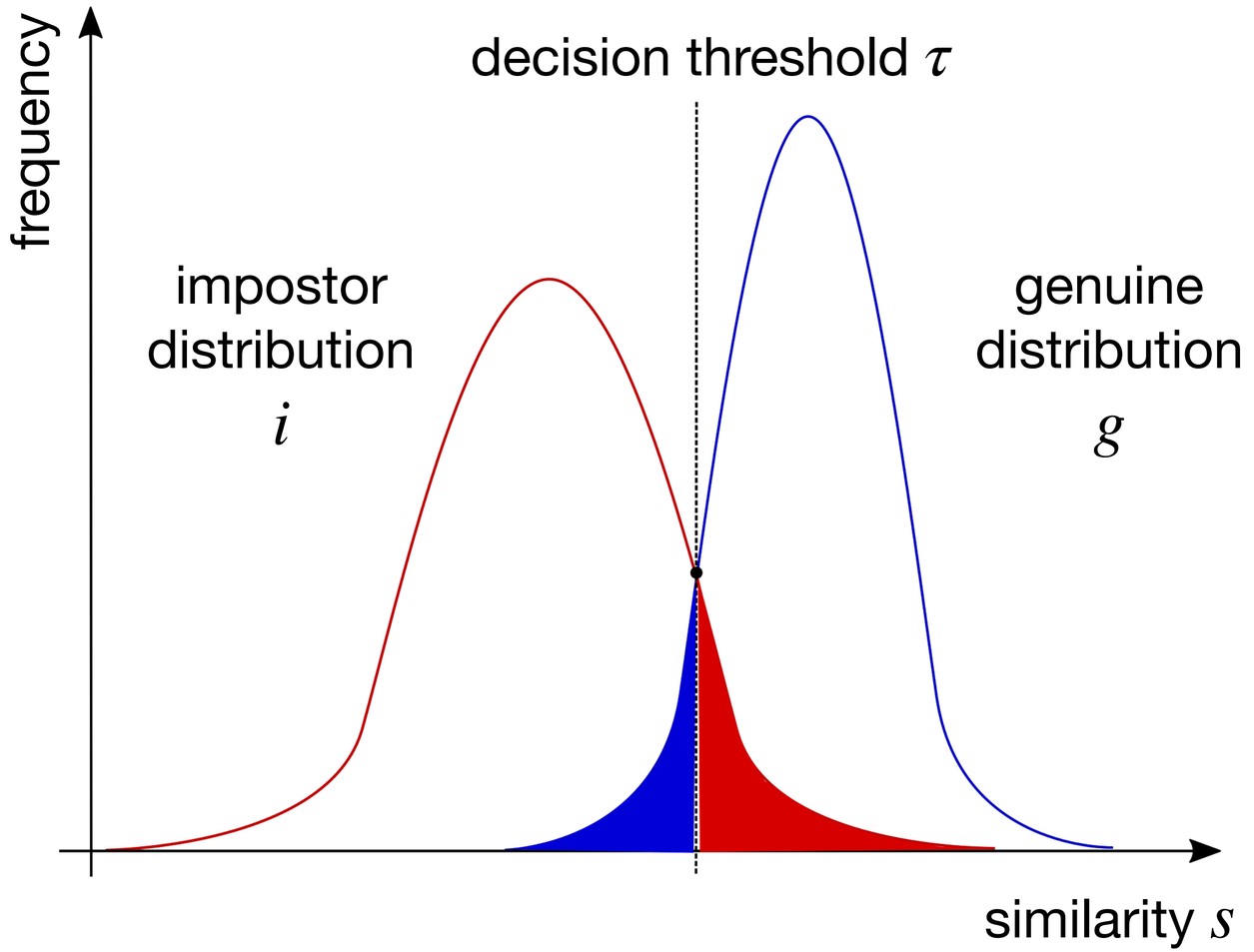
Metrics

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?

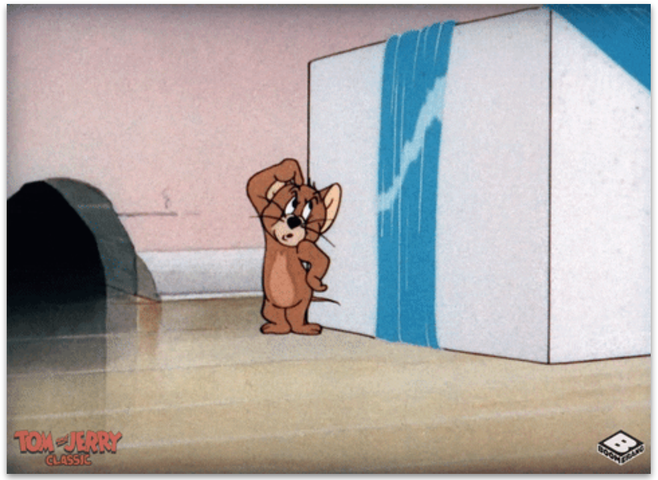
Equal Error Rate (EER)
Common practice.
Pick the threshold where FNMR = FMR.

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)?



UNIVERSITY OF NOTRE DAME

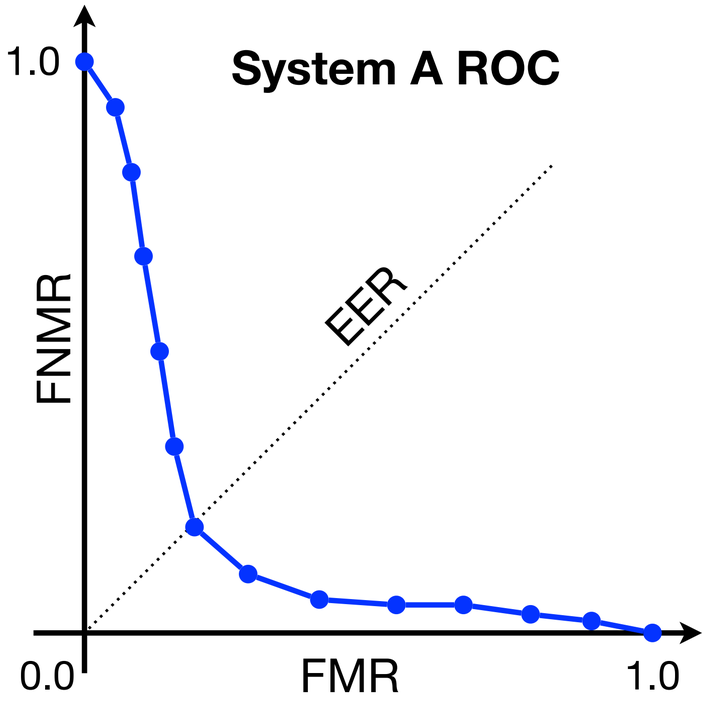
Metrics

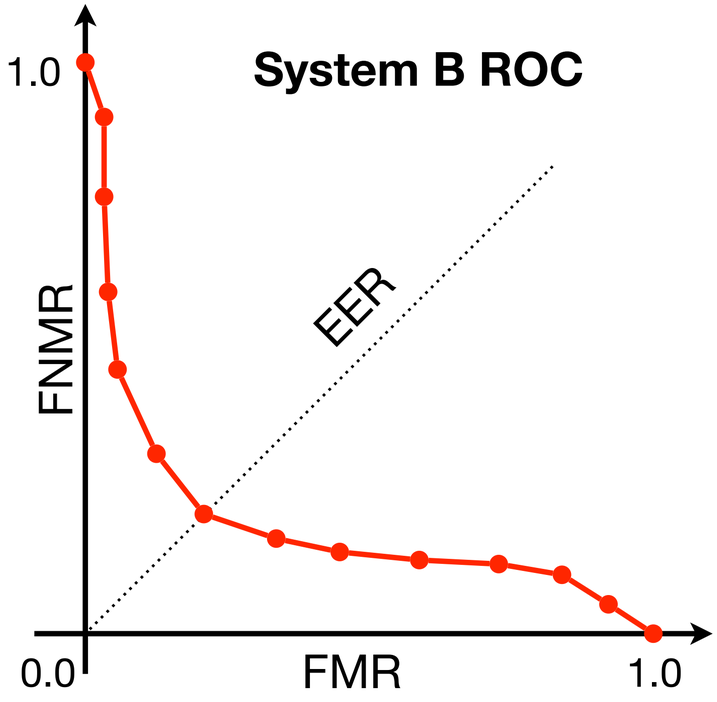
How to compare two different systems?
Biometric systems *A* and *B.*

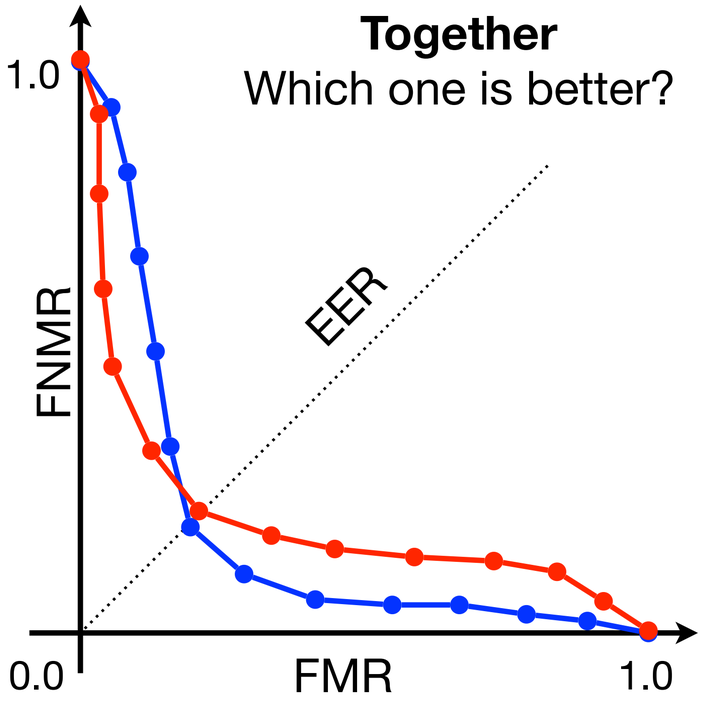
Use a Receiver Operating Characteristic (ROC) curve (2/3)

Metrics

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



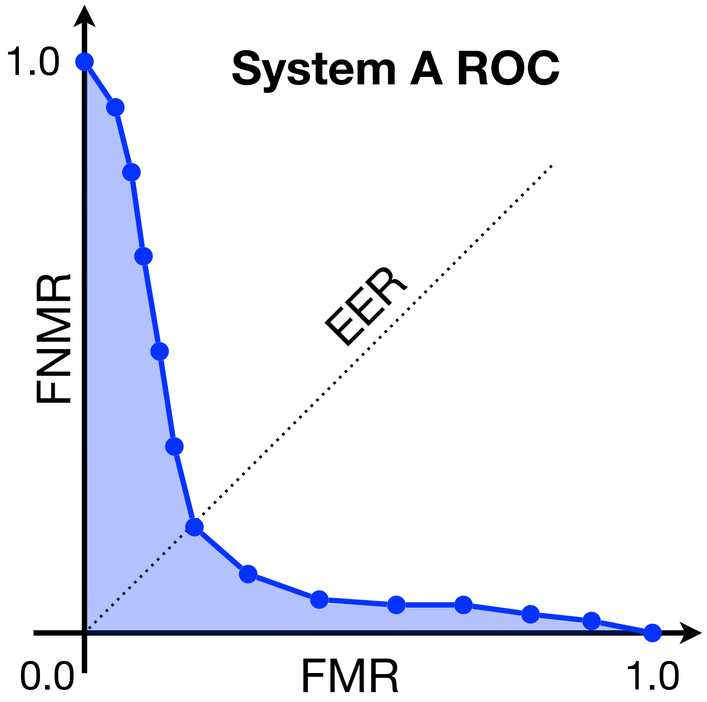


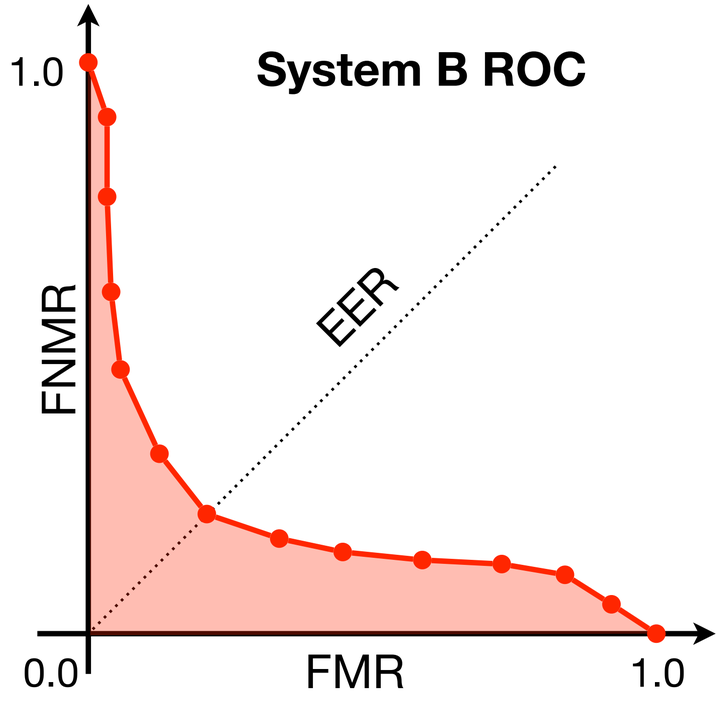


Compute FMR and FNMR for a variety of thresholds.

Metrics

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





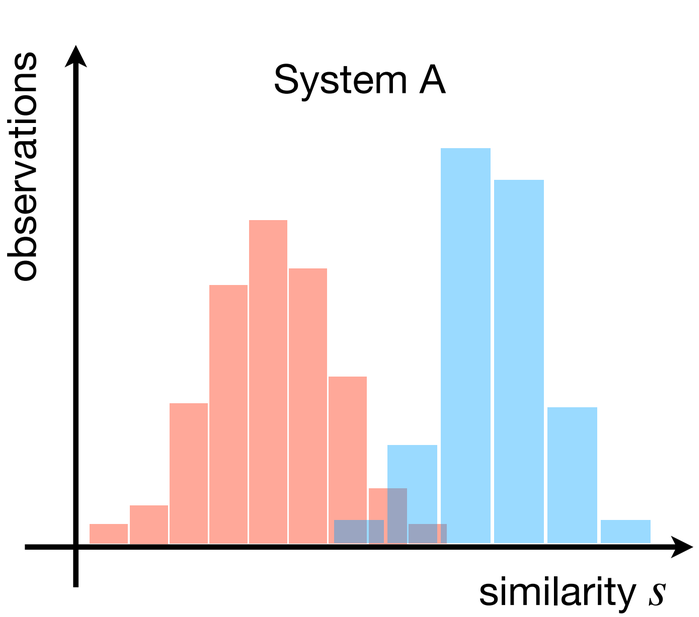
Which one is better?
Compute the
Area Under The Curve
(AUC).
The best solution
presents smaller AUC.

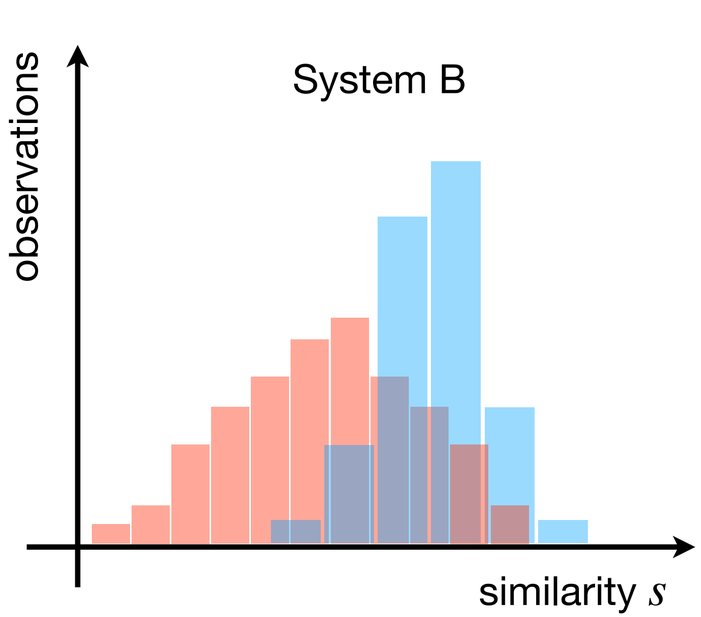
UNIVERSITY OF NOTRE DAME

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)





impostor genuine

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

It is System A!
How do we compute it?

UNIVERSITY OF NOTRE DAME

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).

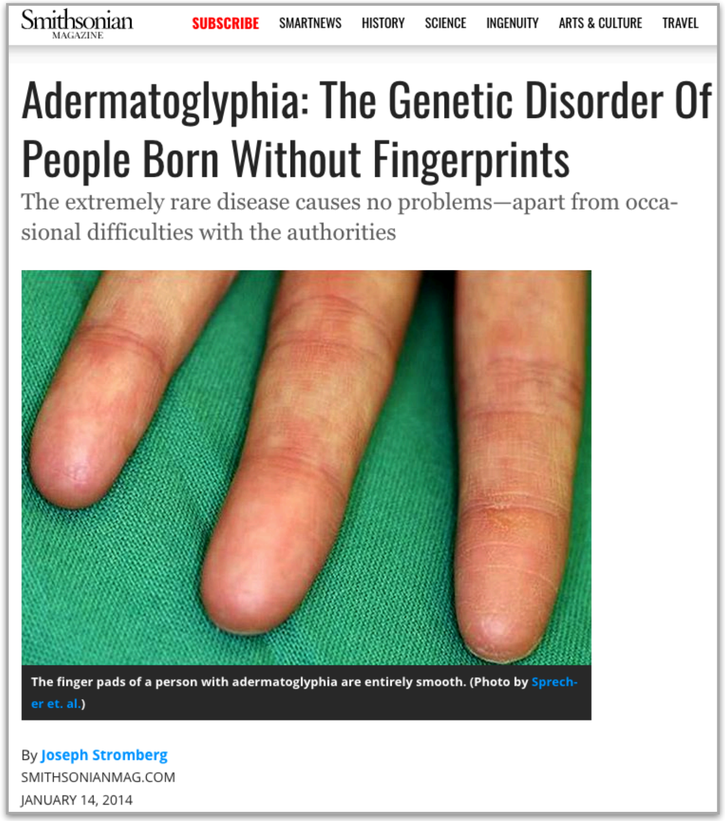
The larger the separation between the distributions, the larger the value of d-prime.

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.



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)

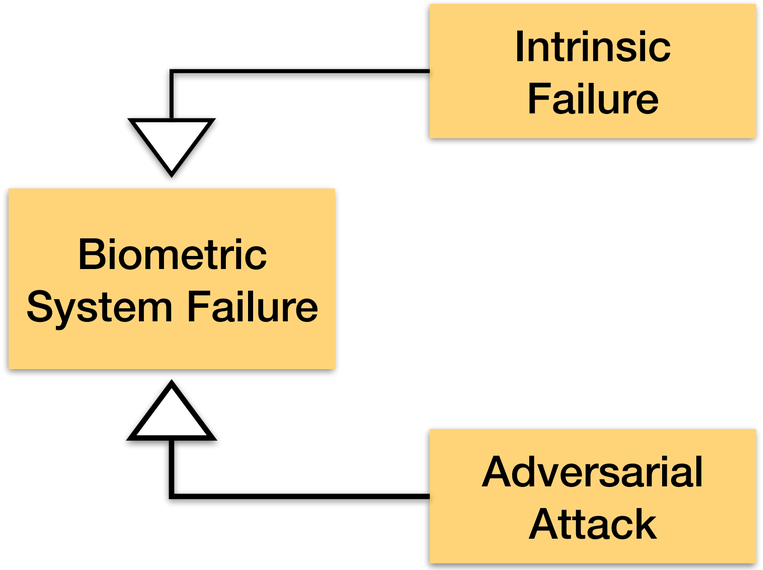
Positive Metrics
True Non-Match Rate (TNMR)
TNMR = 1.0 - FNMR

True Match Rate (TMR)
TMR = 1.0 - FMR

You want to maximize these instead of minimizing.

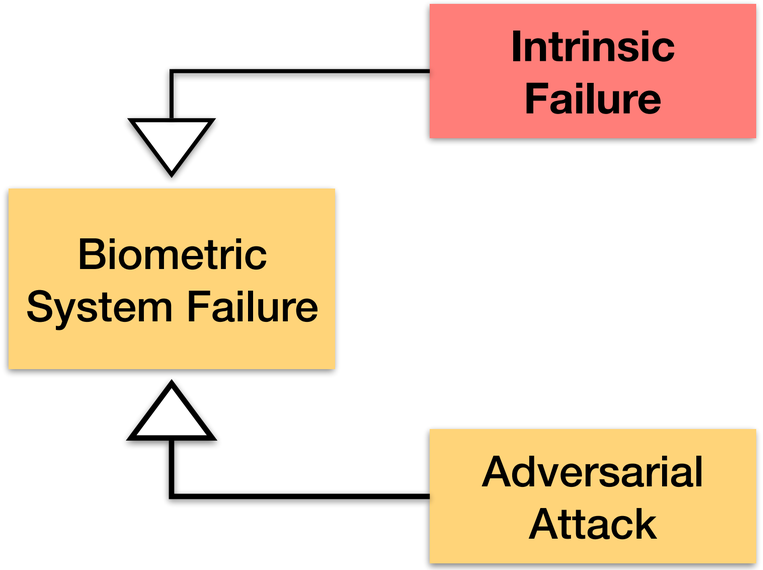
Attacks

Threat Model



Attacks

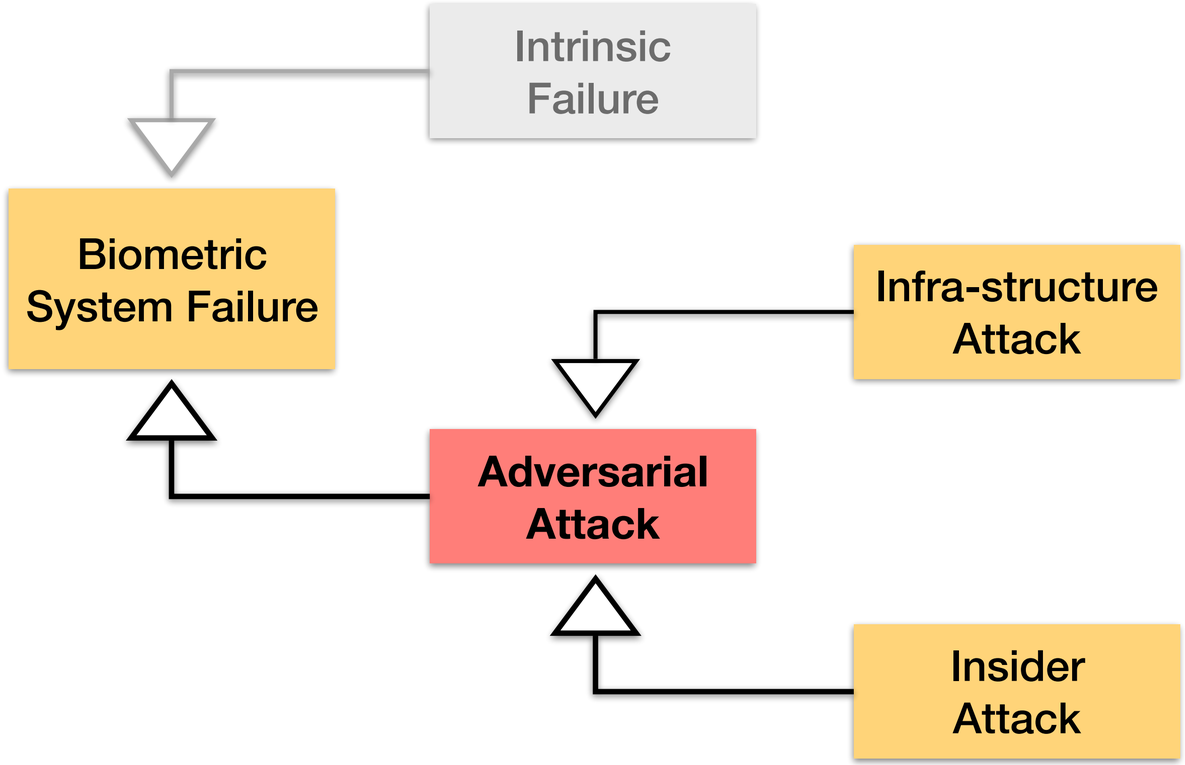
Threat Model



Not attacks
Errors due to the limitation of the solutions and due to hardware stress.

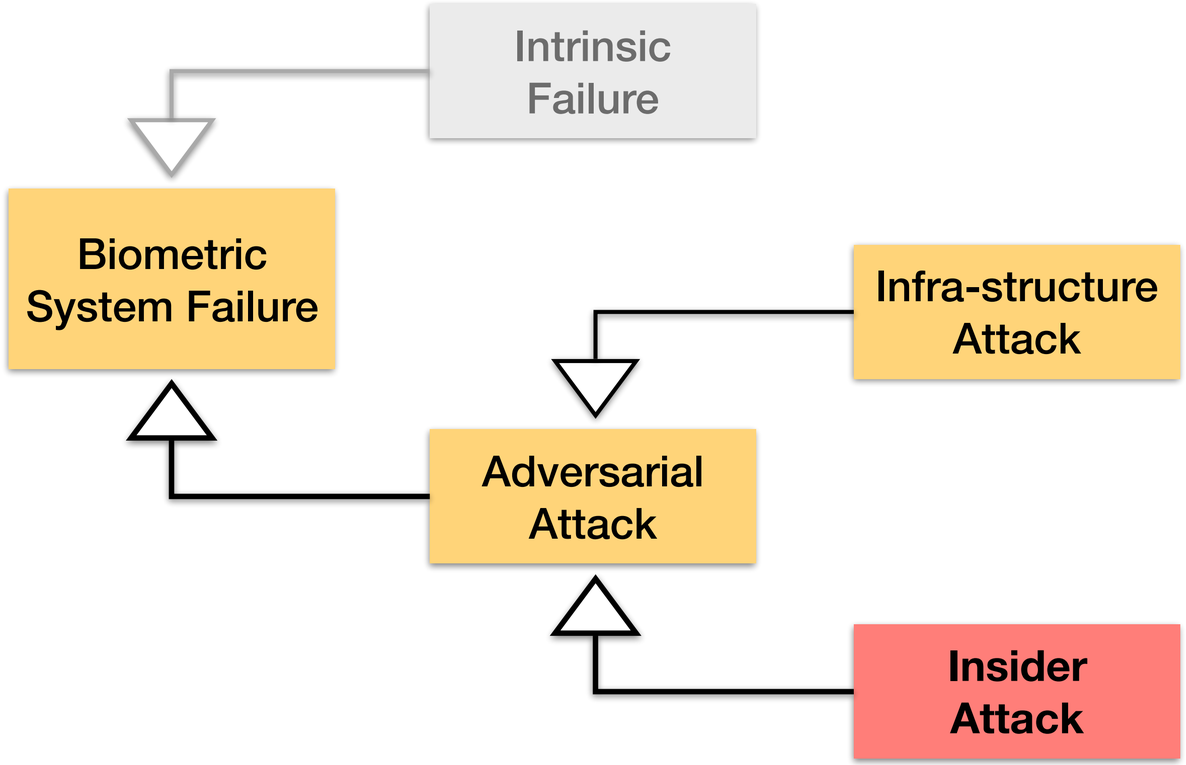
Attacks

Threat Model



Attacks

Threat Model

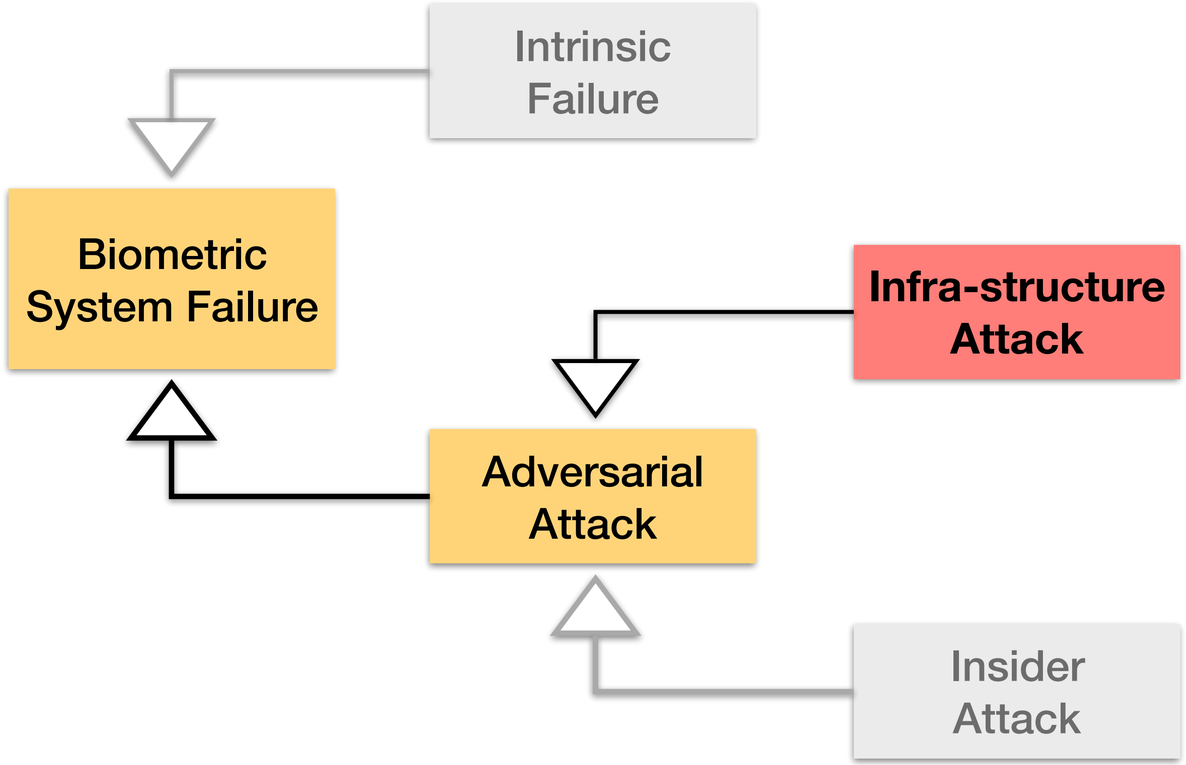


Friendly Fire
Attacks from *insiders* (system users or operators). Keep your system logs in good shape.

UNIVERSITY OF NOTRE DAME

Attacks

Threat Model



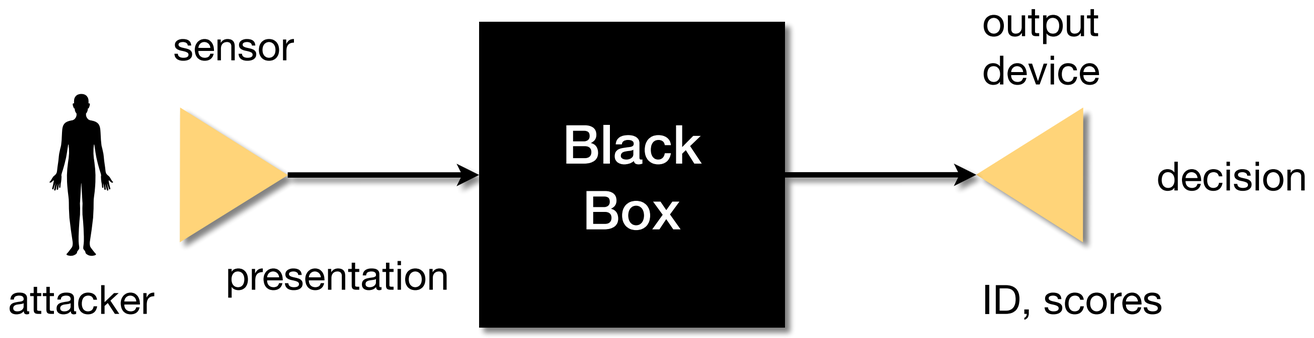
Types

Black box

White box

Attacks

Black Box Attack



Examples
Impersonation
Obfuscation
Spoofing

Attacks

Impersonation

When the attacker pretends to have somebody else's trait.

Possible solution: use more than one trait (Multibiometrics).

https://www.click2houston.com/news/2019/09/18/divorce-deception-man-forges-wifes-name-on-divorce-papers-police-say/

UNIVERSITY OF NOTRE DAME

Attacks

Obfuscation

When the attacker tries to hide or modify their trait.

Possible solution: use more than one trait (Multibiometrics).

The Daily Dot

Debug | IRL

Is this wearable face projector being used by Hong Kong protesters?

A 2017 'Black Mirror'-esque art project gains a second life on social media.

Mikael Thalen— 2019-10-06 01:33 pm

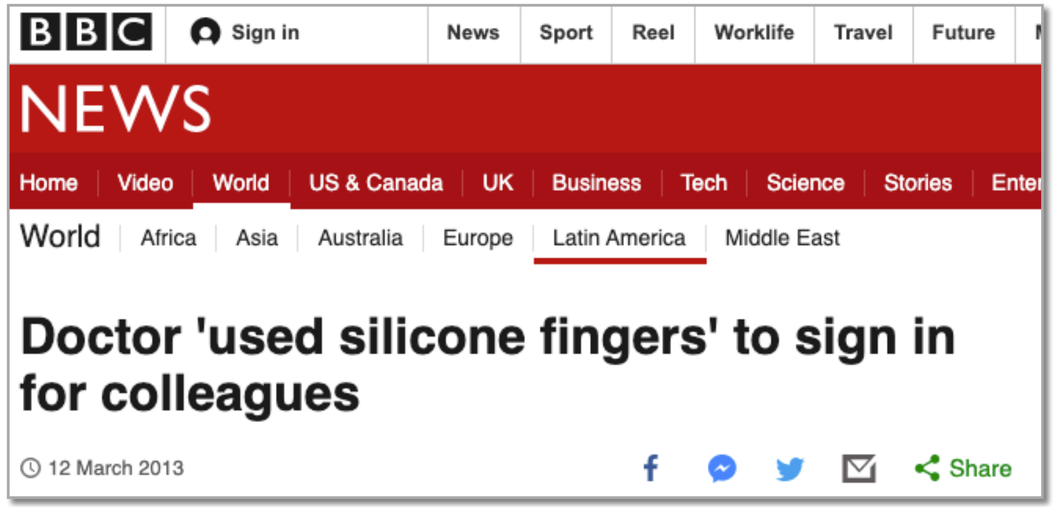
https://www.dailydot.com/debug/wearable-face-projector-hong-kong-protesters/

https://www.youtube.com/watch?v=_PoudPCevN0

UNIVERSITY OF NOTRE DAME

Attacks

Spoofing
When the attacker presents to the system a forged non-live trait.
Possible solution: detect trait liveness.



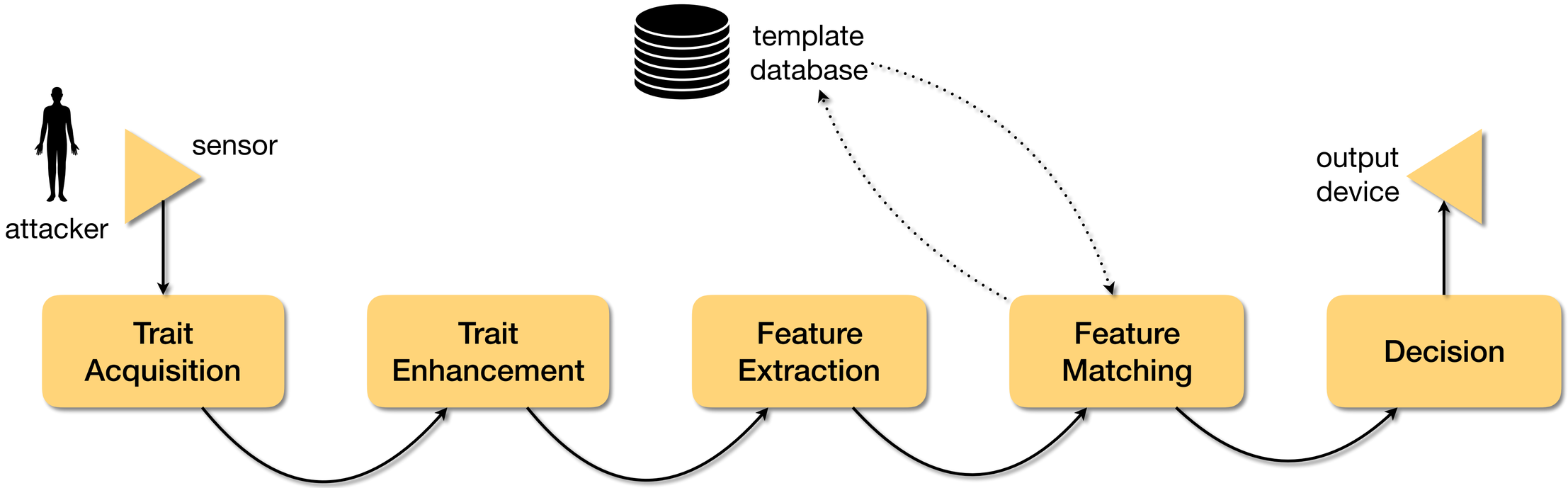
https://www.bbc.com/news/world-latin-america-21756709

A Brazilian doctor faces charges of fraud after being caught on camera using silicone fingers to sign in for work for absent colleagues, police say.

UNIVERSITY OF NOTRE DAME

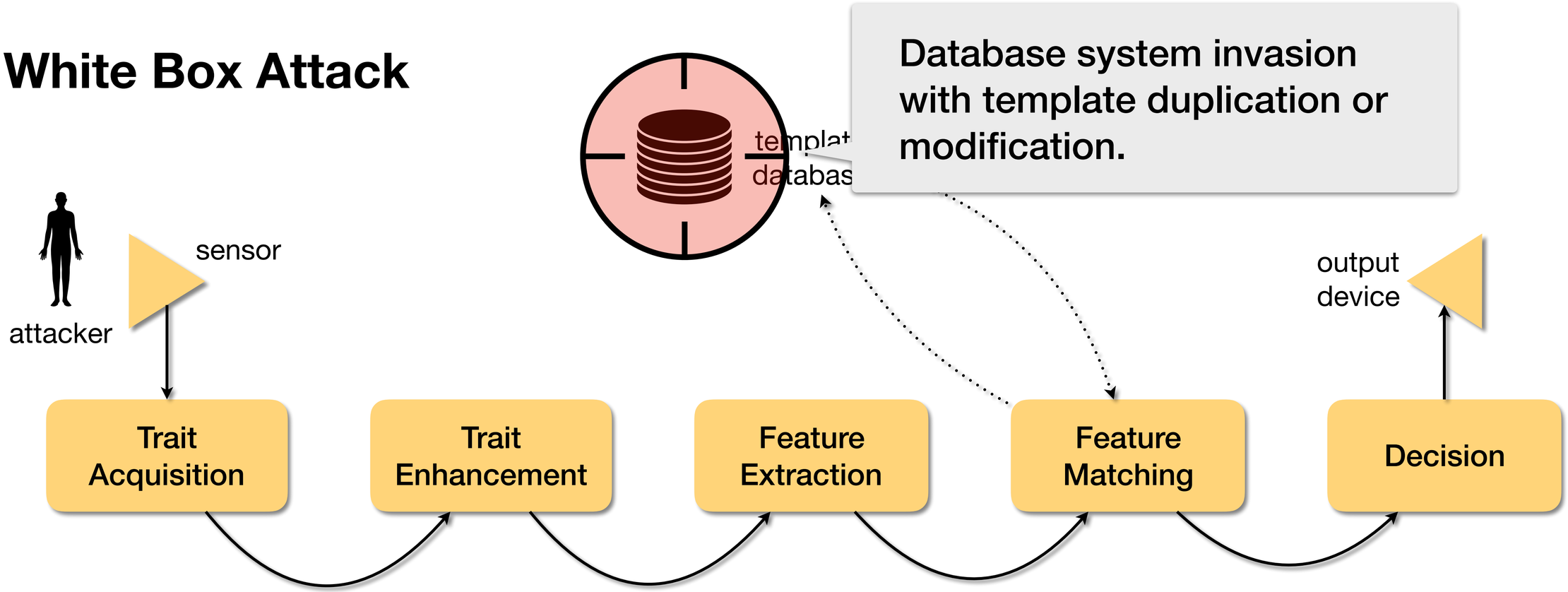
Attacks

White Box Attack



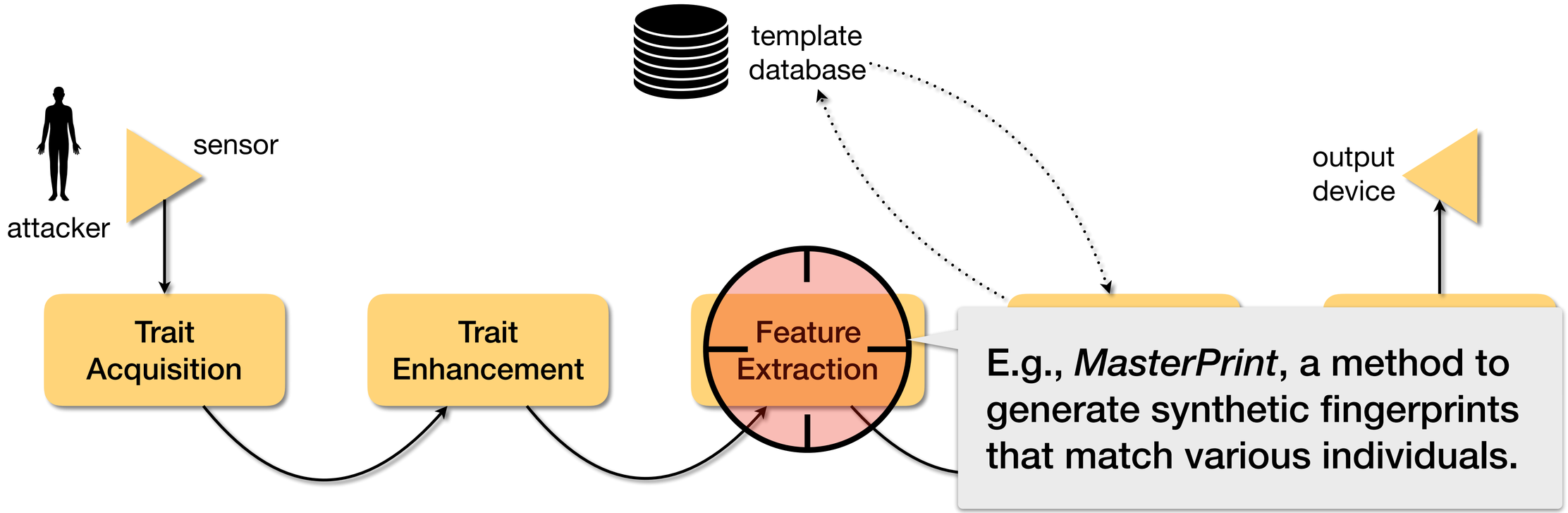
Attacks

White Box Attack



Attacks

White Box Attack



Attacks

MasterPrint

IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 12, NO. 9, SEPTEMBER 2017 2013

MasterPrint: Exploring the Vulnerability of Partial Fingerprint-Based Authentication Systems

Aditi Roy, *Student Member, IEEE*, Nasir Memon, *Fellow, IEEE*, and Arun Ross, *Senior Member, IEEE*

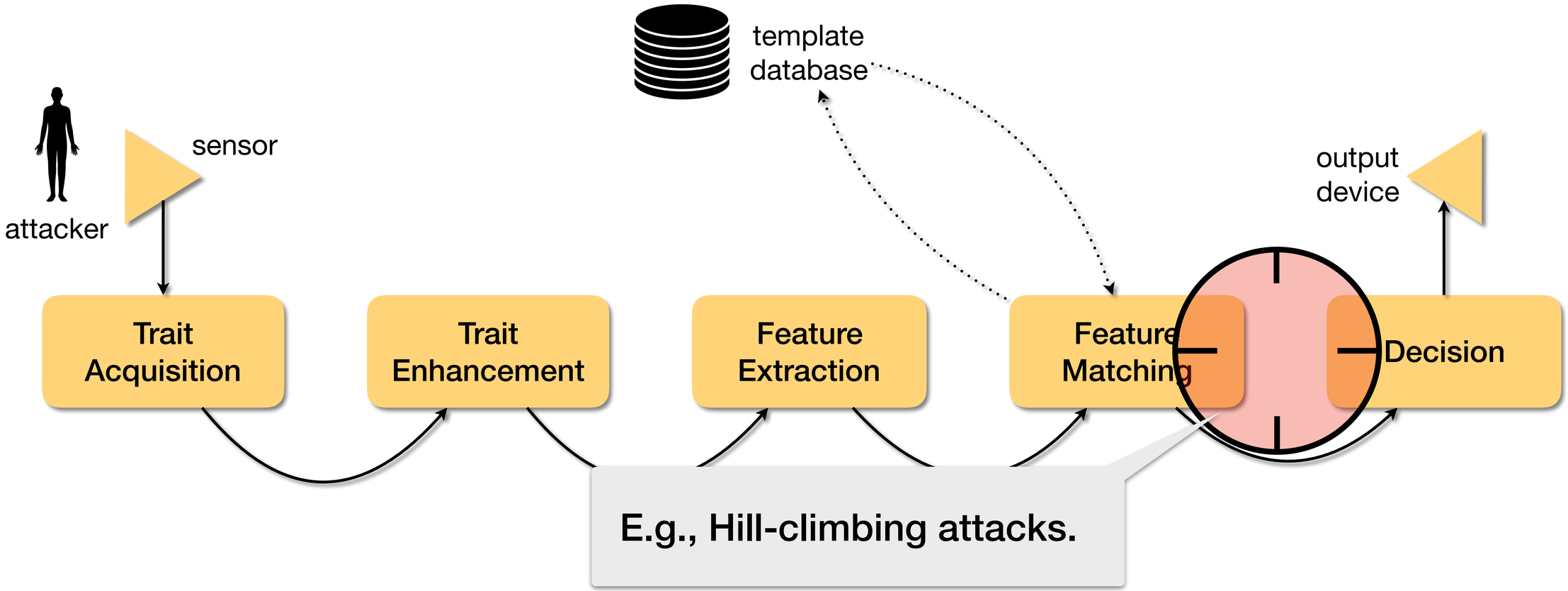
templates. This paper investigates the possibility of generating a "MasterPrint," a synthetic or real partial fingerprint that serendipitously matches one or more of the stored templates for a significant number of users. Our preliminary results on an

https://www.cse.msu.edu/~rossarun/pubs/RoyMemonRossMasterPrint_TIFS2017.pdf

UNIVERSITY OF NOTRE DAME

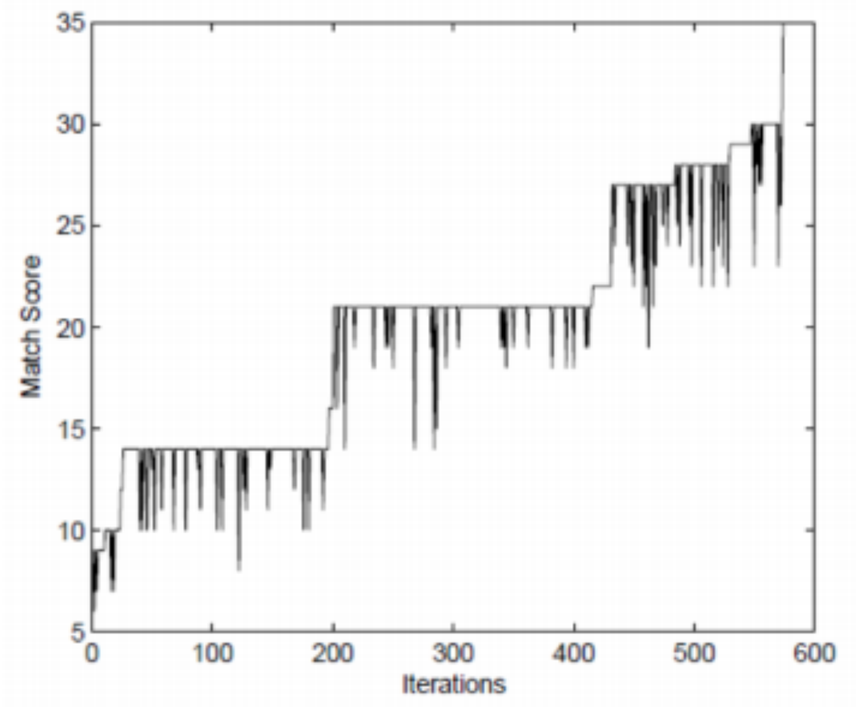
Attacks

White Box Attack



Attacks

Hill-climbing Attack
E.g. Fingerprints

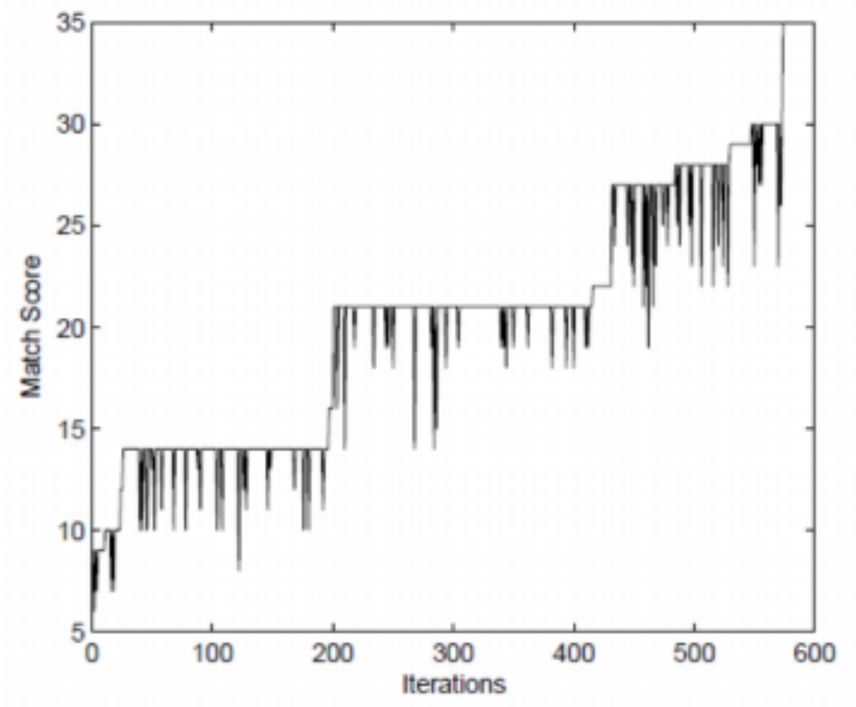


The attacker iteratively provides synthetic trait samples to the system. At each iteration, the attacker observes how the similarity scores are progressing.

Martinez-Diaz et al.
Hill-Climbing and Brute-Force Attacks on Biometric Systems: A Case Study in Match-on-Card Fingerprint Verification
IEEE ICCST, 2006

Attacks

Hill-climbing Attack
E.g. Fingerprints

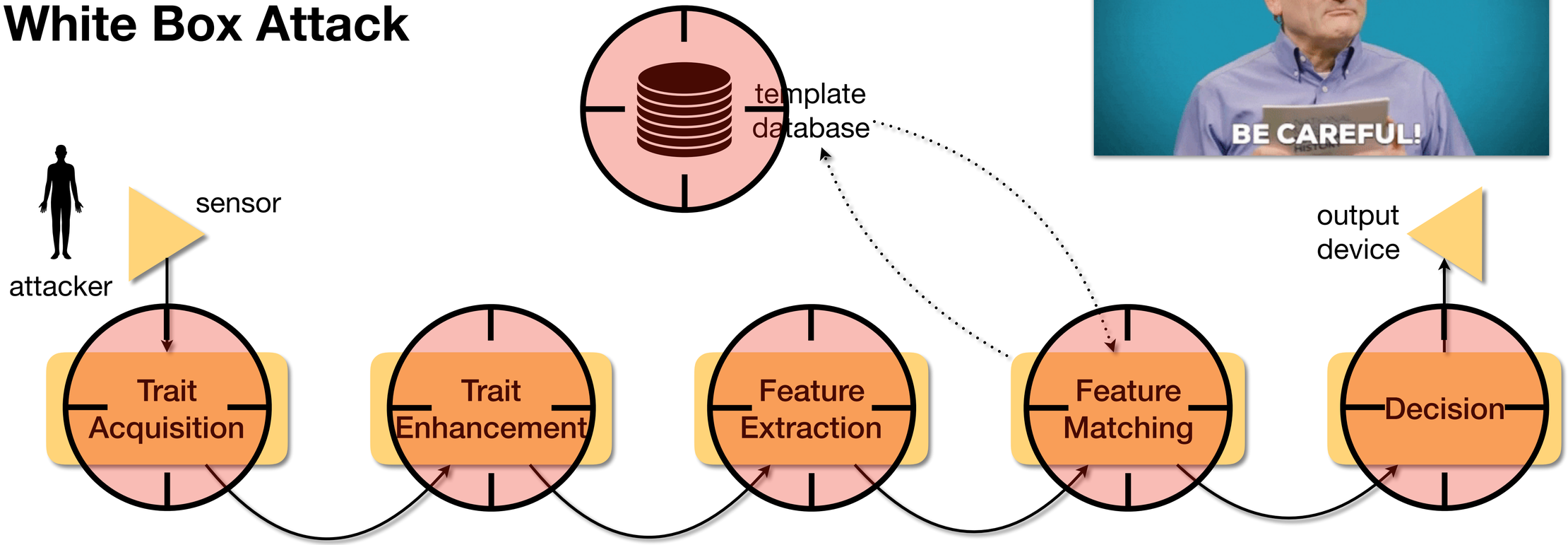


With such progress feedback,
the attacker can guide the generation of better and better synthetic fingerprint samples, up the point of trespassing the decision threshold.

Martinez-Diaz et al.
Hill-Climbing and Brute-Force Attacks on Biometric Systems: A Case Study in Match-on-Card Fingerprint Verification
IEEE ICCST, 2006

Attacks

White Box Attack



UNIVERSITY OF NOTRE DAME

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).

Acknowledgments

This material is heavily based on
Dr. Adam Czajka's and Dr. Walter Scheirer's courses.
Thank you, professors, for kindly allowing me to use your material.

https://engineering.nd.edu/profiles/aczajka
https://www.wjscheirer.com/

UNIVERSITY OF NOTRE DAME