

# **Basics II**

CSE 40537/60537 Biometrics

**Daniel Moreira**  
Spring 2020



# 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.



# 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.



impersonation

Adversarial attack:  
impersonation, spoofing, etc.



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.



obfuscation

Adversarial attack: obfuscation.

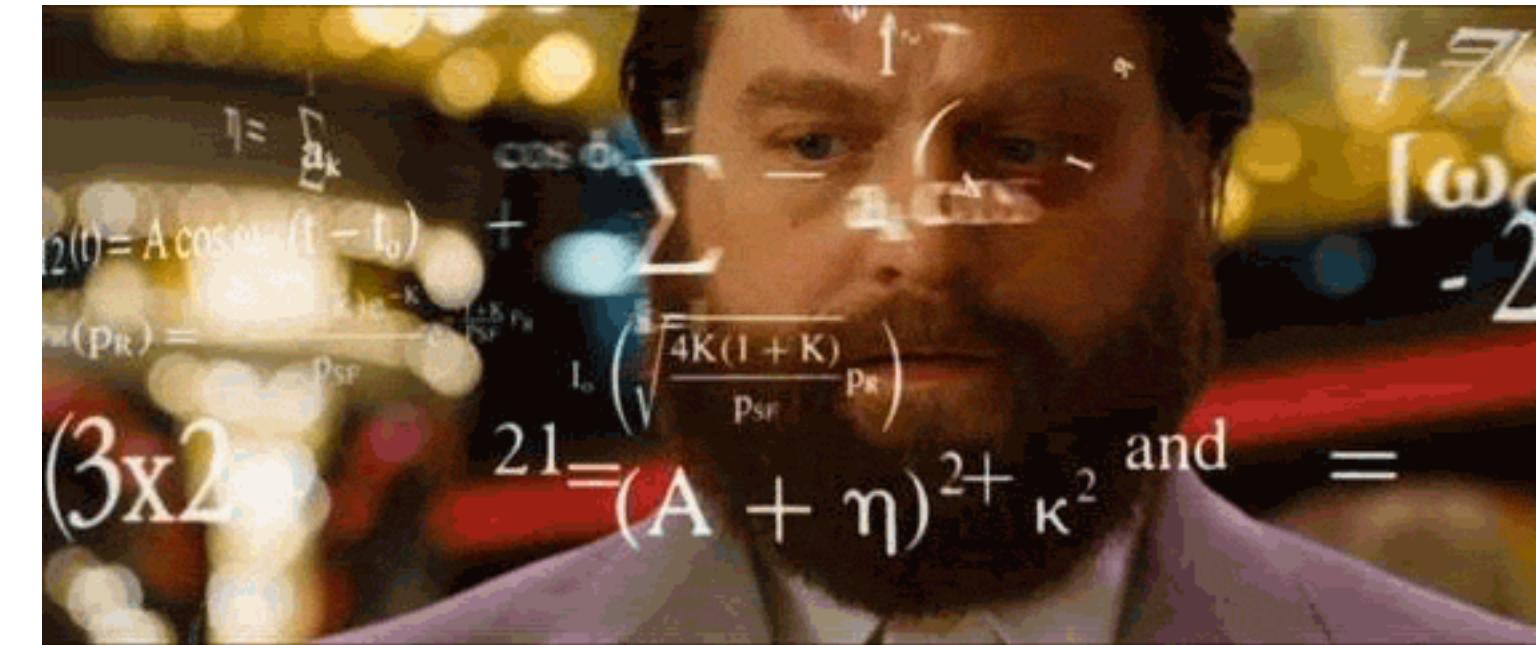
# Biometric System Errors

## 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 repudiation.



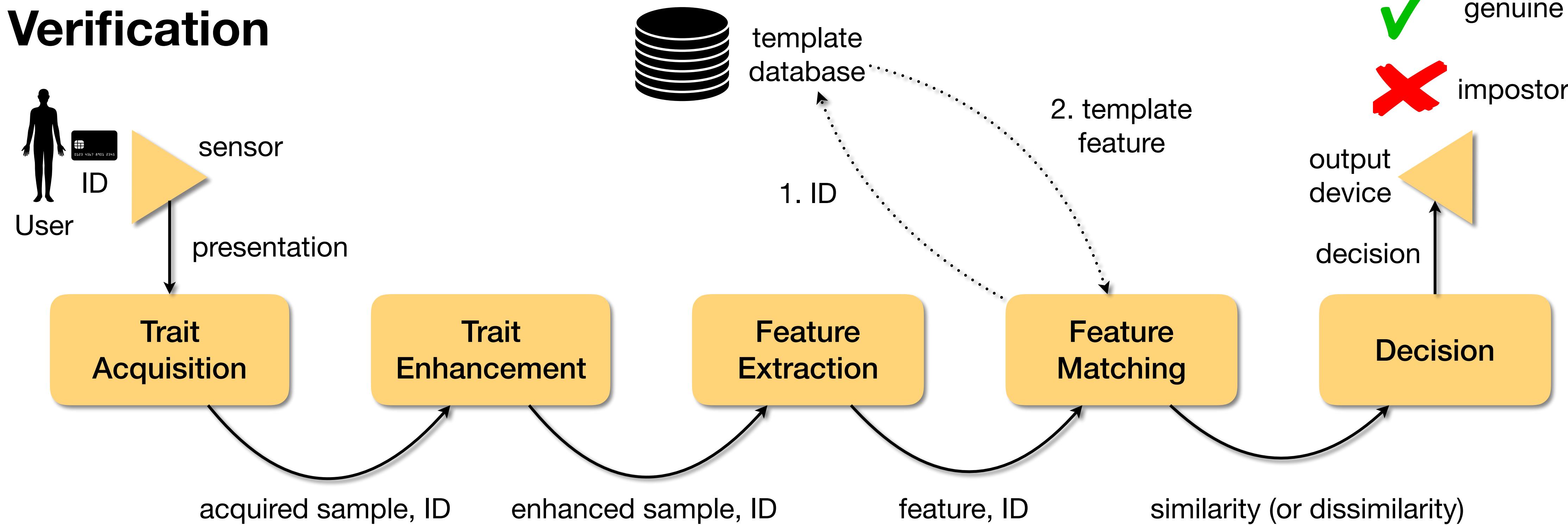
Let's see how to compute them!

### 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 causes an intrusion.

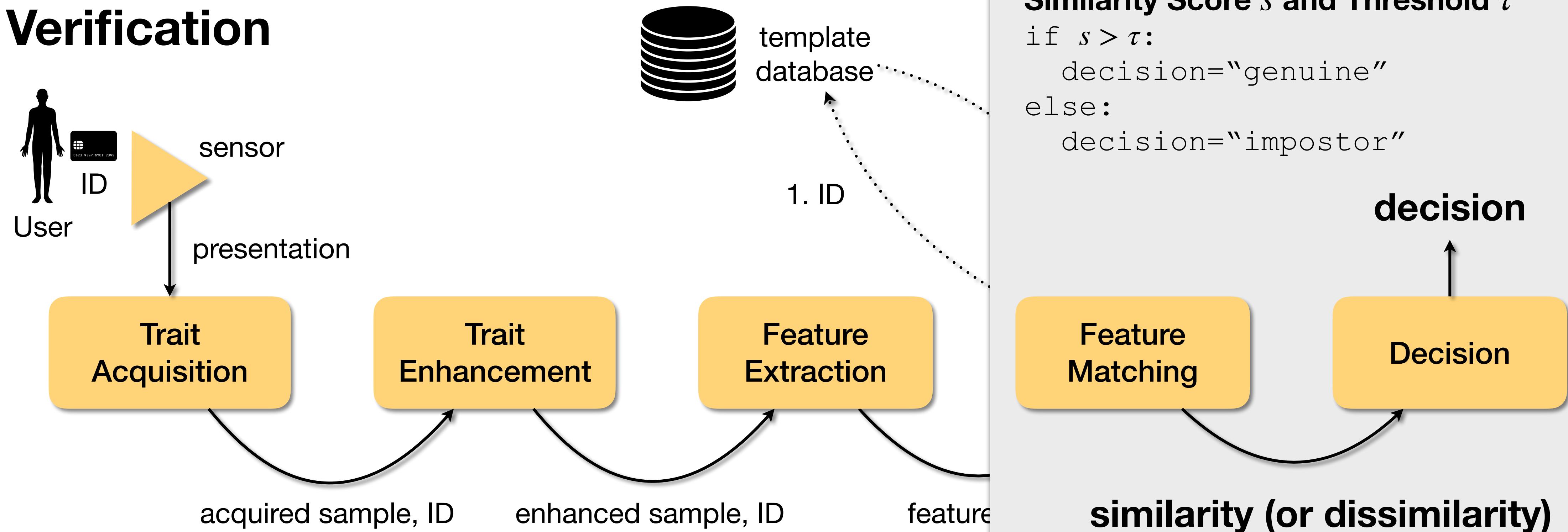
# Metrics

## Verification



# Metrics

## Verification

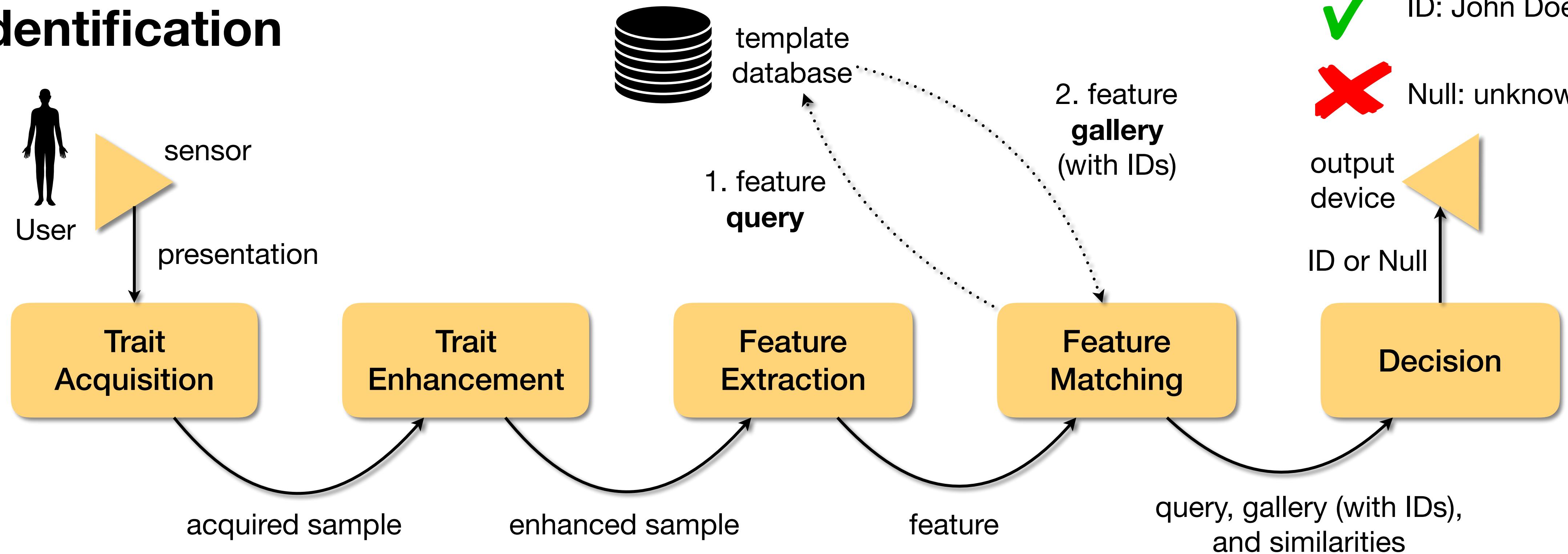


**Similarity Score  $s$  and Threshold  $\tau$**

```
if  $s > \tau$ :  
    decision = "genuine"  
else:  
    decision = "impostor"
```

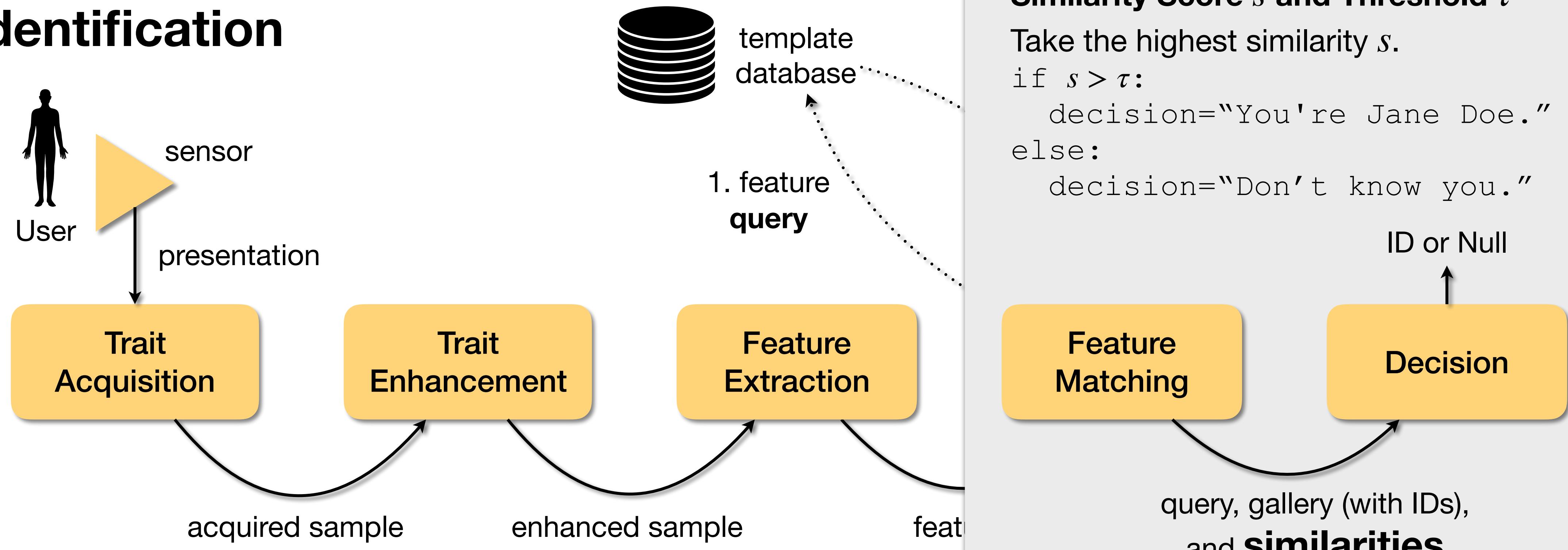
# Metrics

## Identification



# Metrics

## Identification



### Similarity Score $s$ and Threshold $\tau$

Take the highest similarity  $s$ .

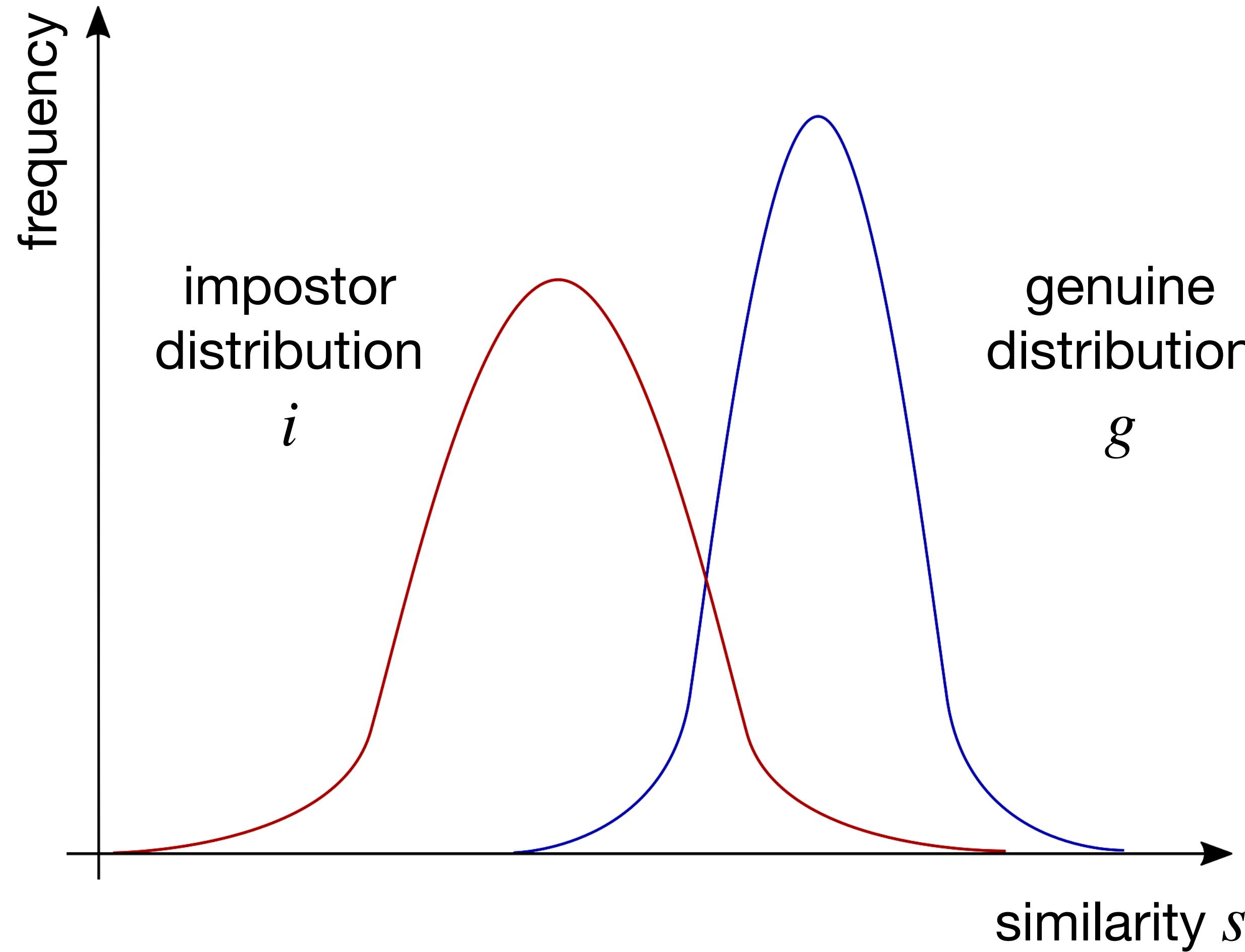
if  $s > \tau$ :

    decision="You're Jane Doe."

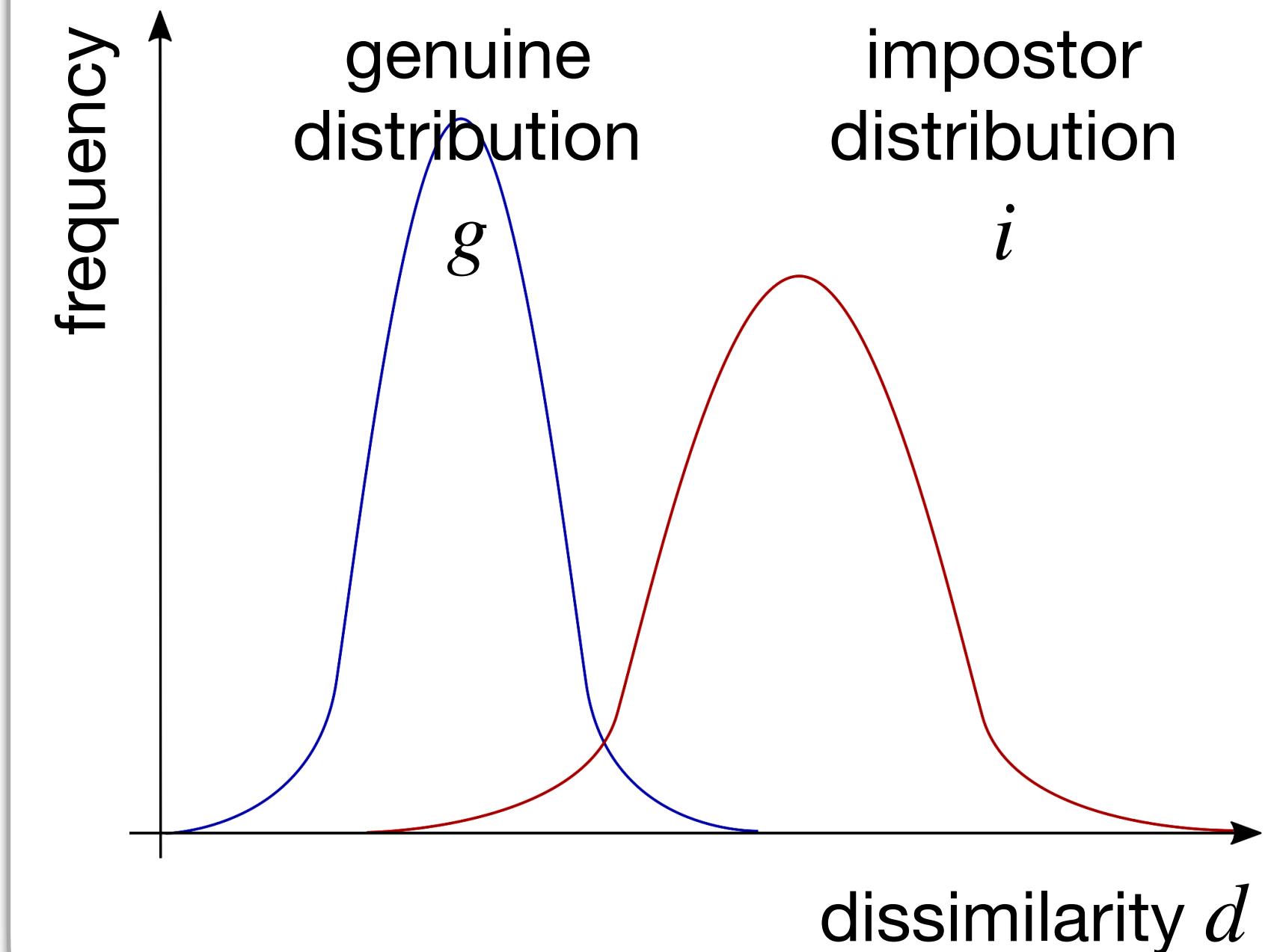
else:

    decision="Don't know you."

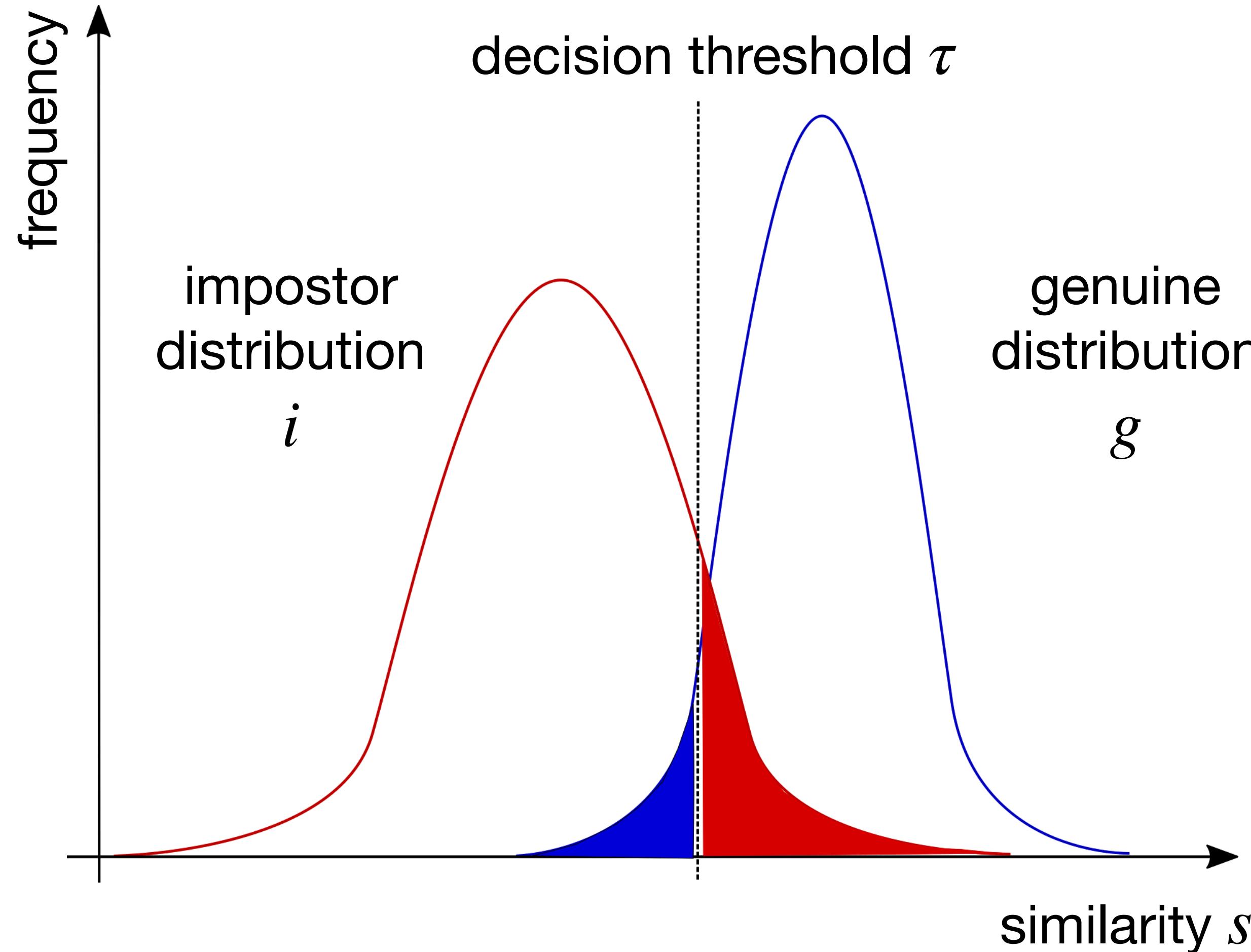
# Metrics



In case of dissimilarities...



# Metrics



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

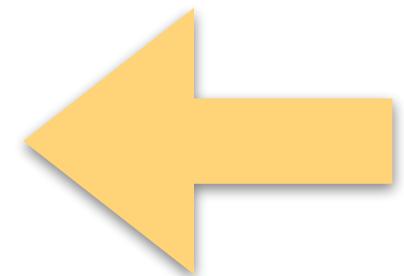
$$\boxed{\quad} \quad FM(\tau) = \int_{\tau}^{\infty} i(s) \, ds$$

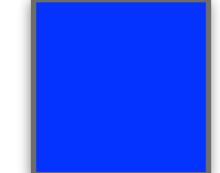
# Metrics

## In Practice

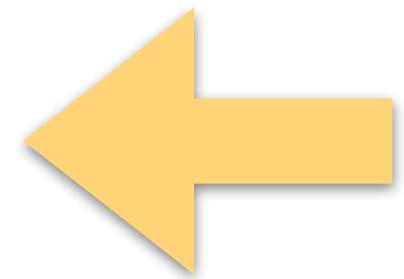
False Non-Match Rate (FNMR) and False Match Rate (FMR)

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




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

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




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

# 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 correctly computed by the system?

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

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

# Metrics

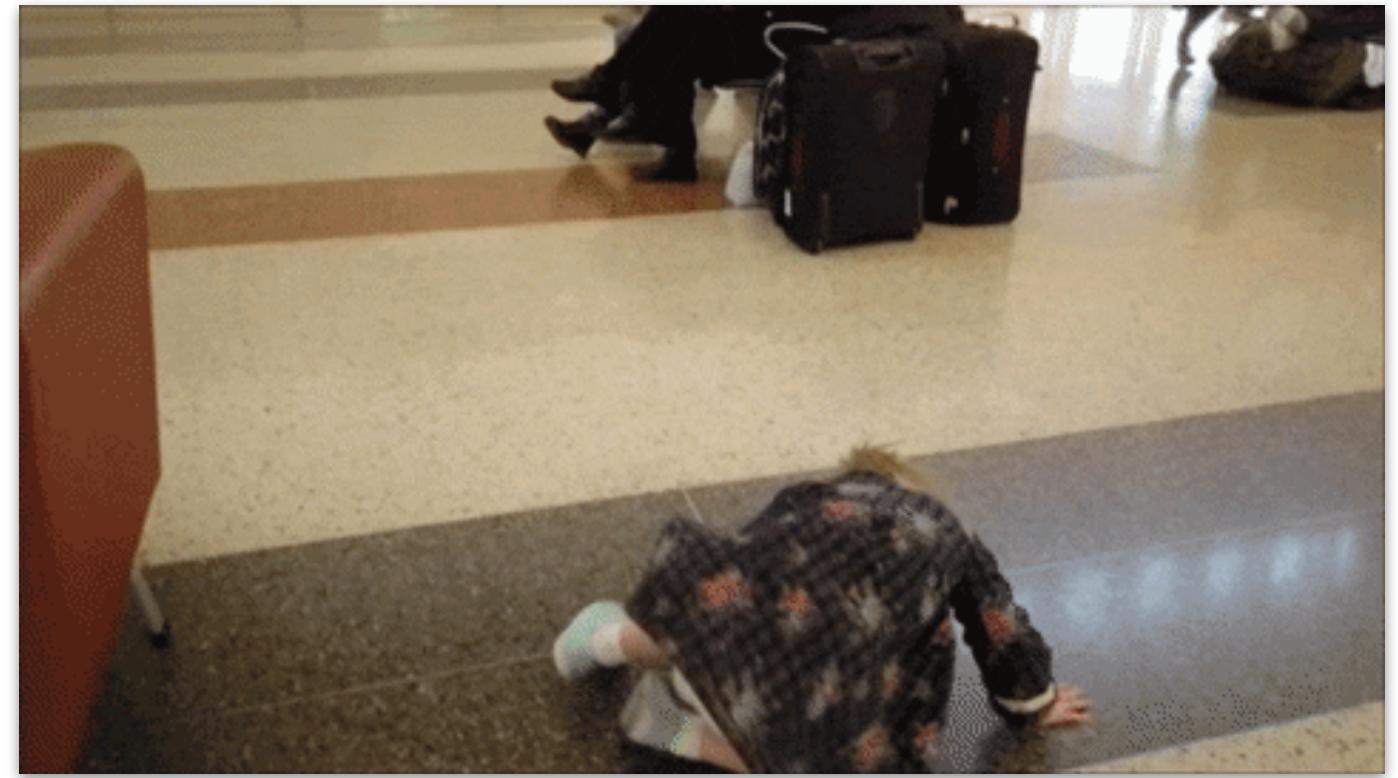
## In Practice

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**

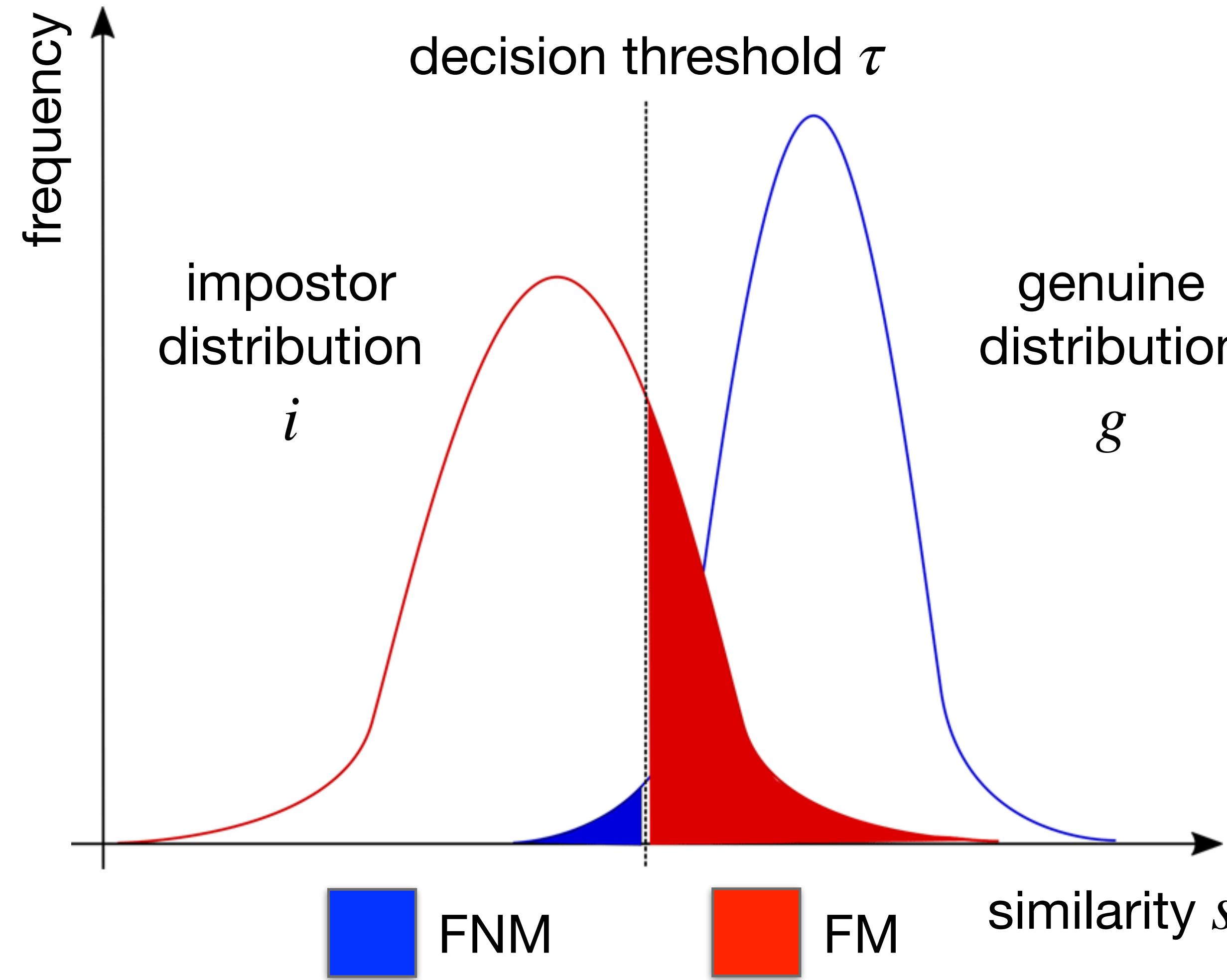
5K people per hour, 14h per day (70K people per day)

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  $\tau$ :**  
The larger the value of FNM;  
The smaller the value of FM.

FNM and FM are inversely proportional.

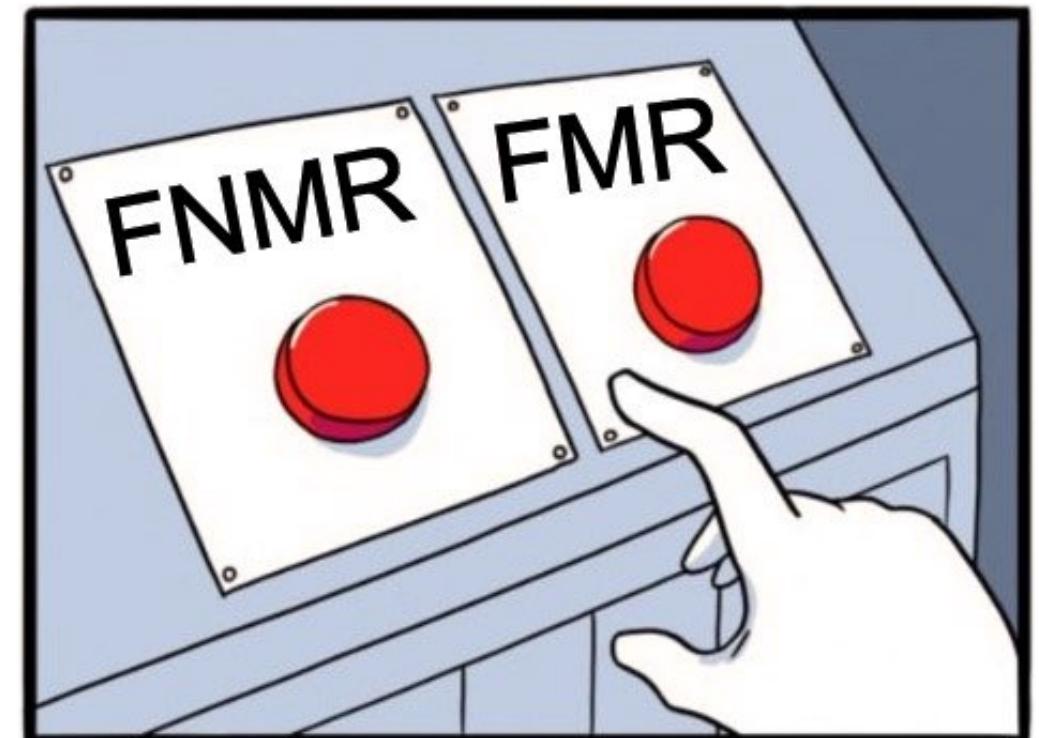
# Metrics

## What to choose?

### **Small FNMR**

Suitable to avoid denial of service and repudiation.

Increases intrusion probability, though.

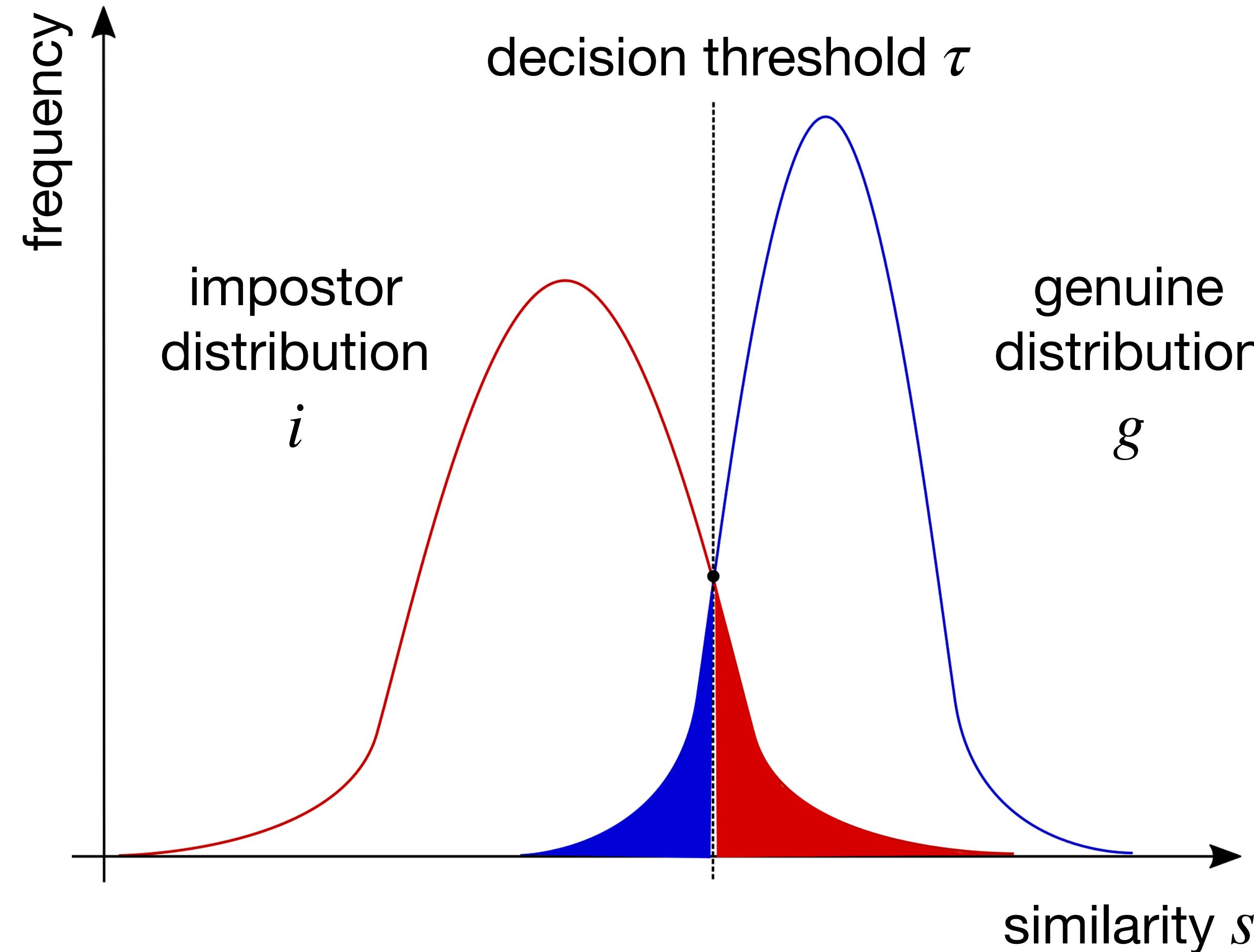


### **Small FMR**

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  
FNR = FMR.

# Metrics

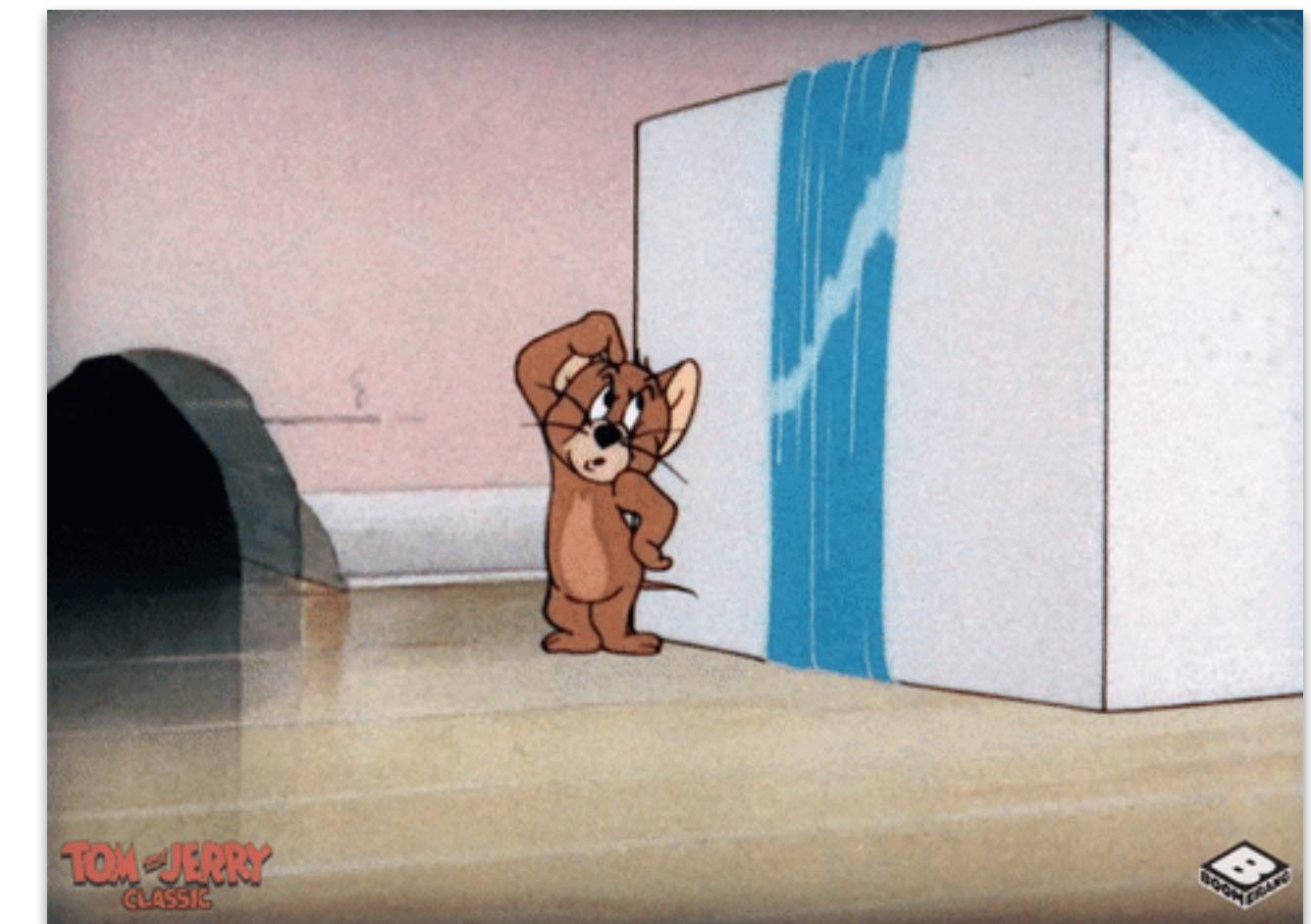
**How to compare two different systems?**

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)?



# Metrics

**How to compare two different systems?**

Biometric systems  $A$  and  $B$ .

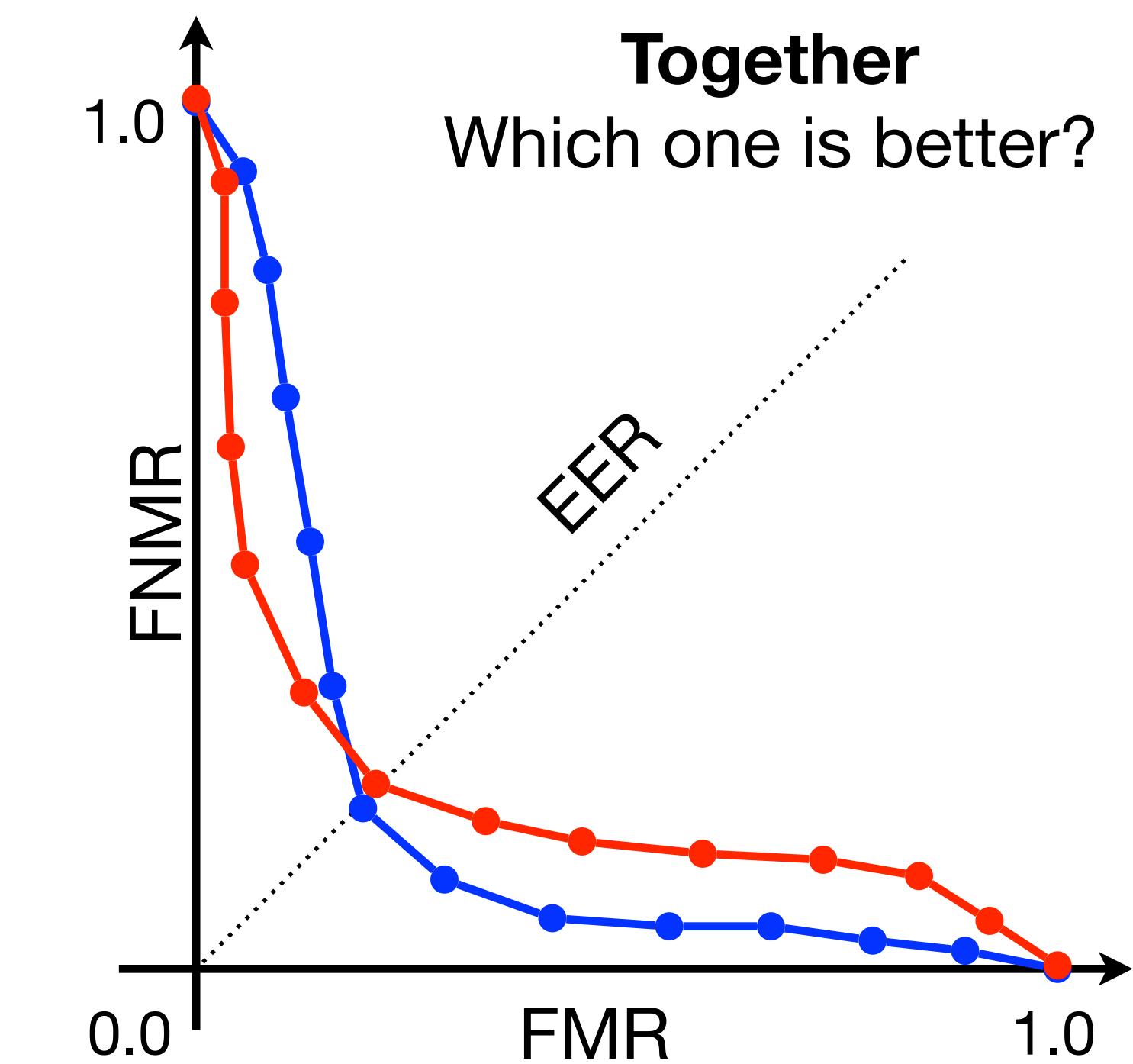
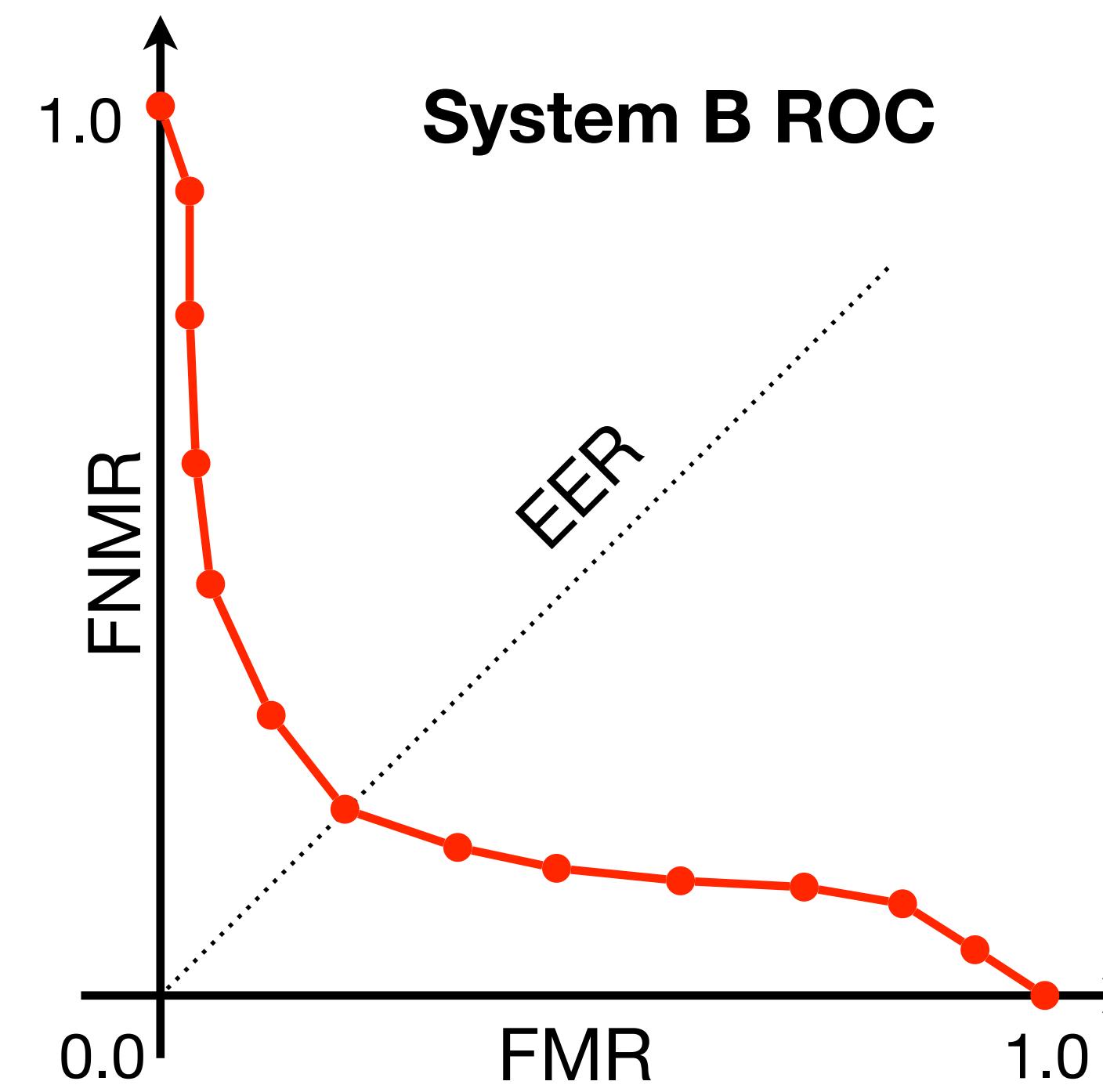
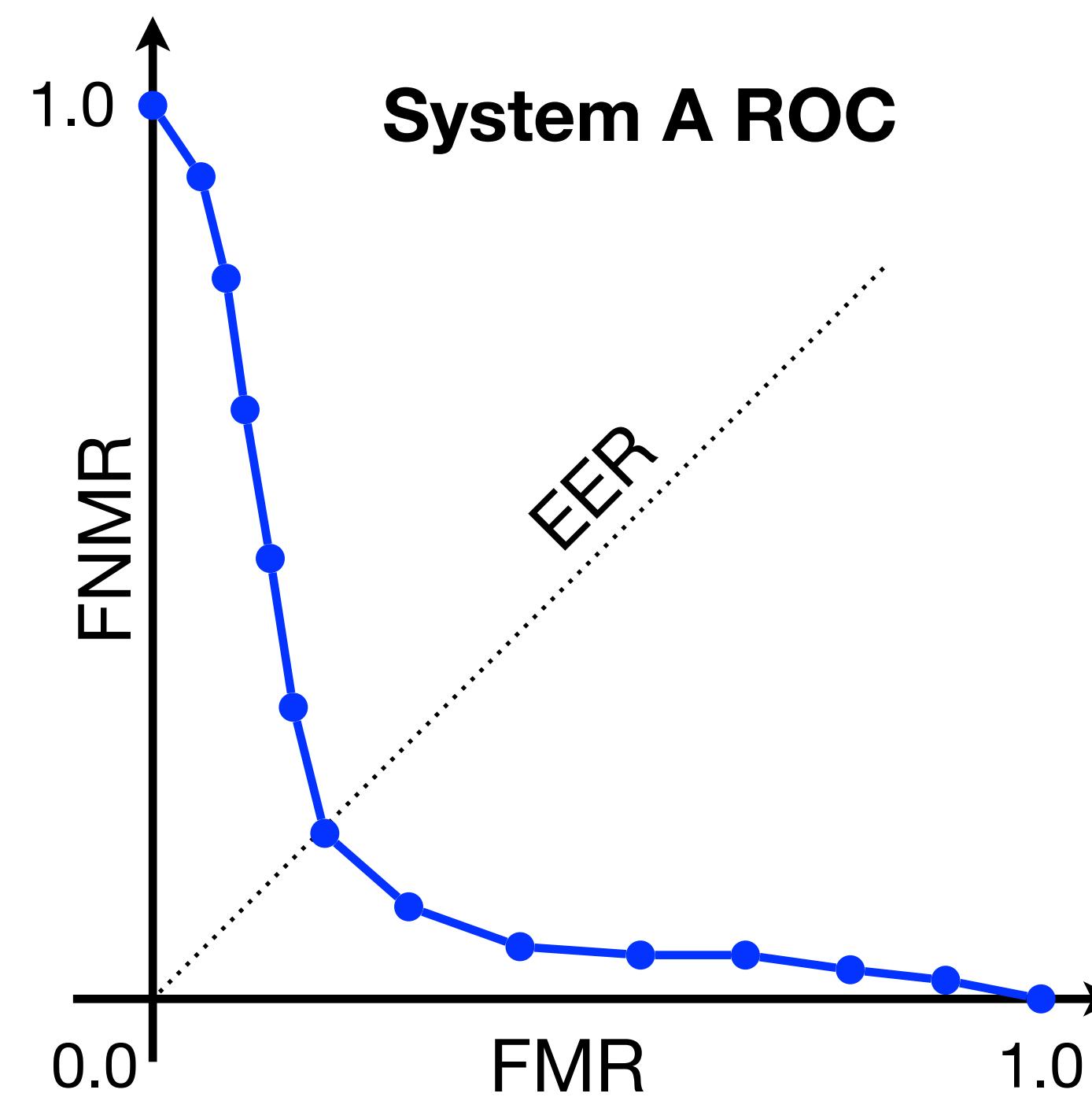
**Use a Receiver Operating Characteristic  
(ROC) curve (2/3)**



# Metrics

**How to compare two different systems?**

Biometric systems  $A$  and  $B$ .

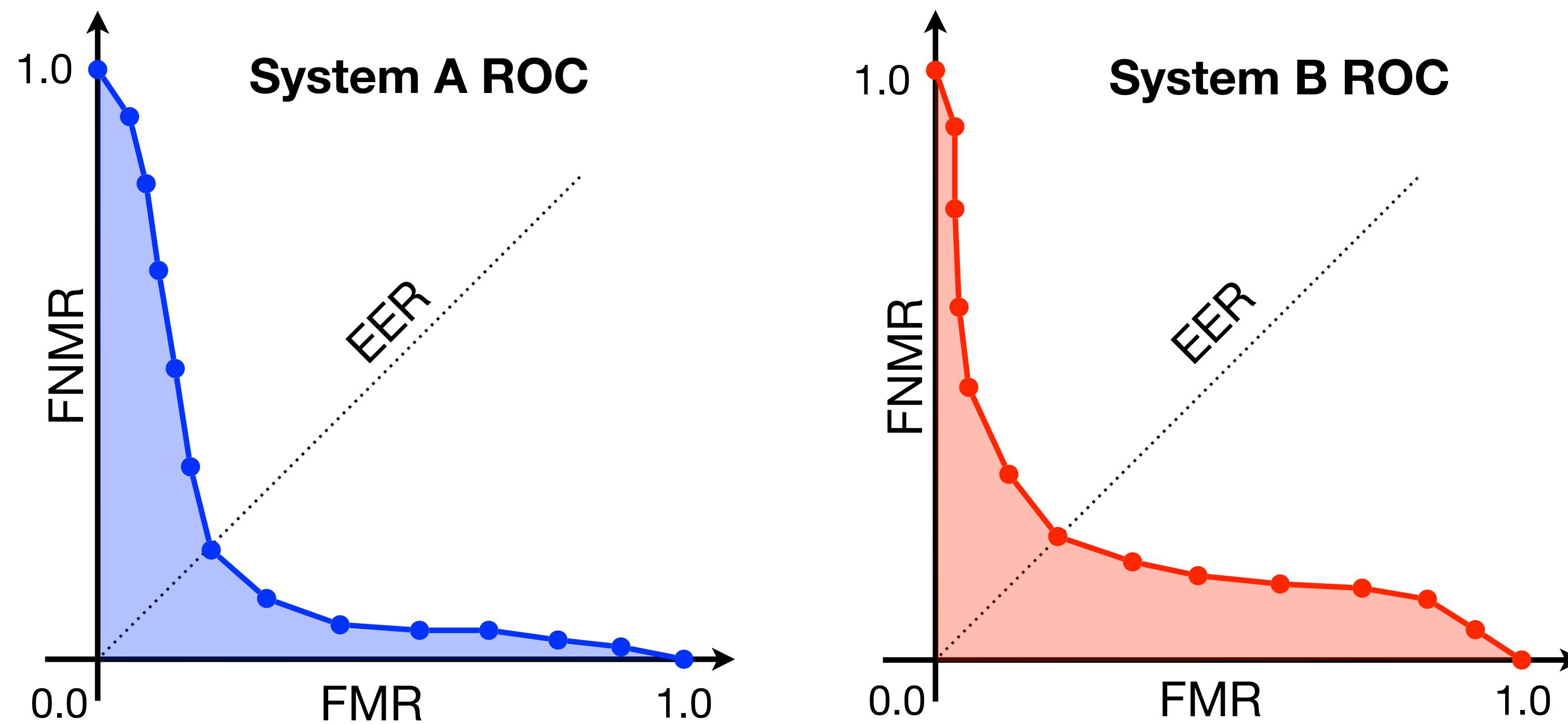


Compute FMR and FNMR for a variety of thresholds.

# Metrics

**How to compare two different systems?**

Biometric systems  $A$  and  $B$ .



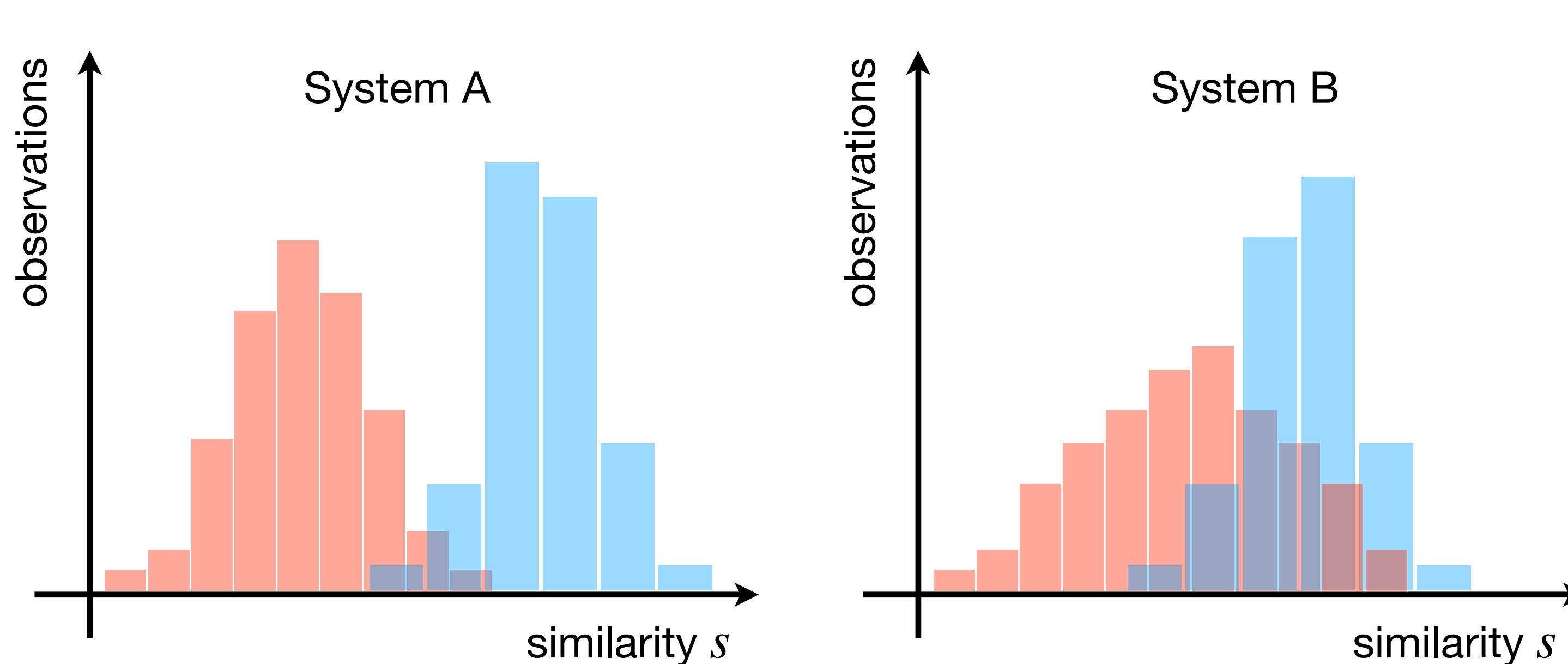
**Which one is better?**  
Compute the  
Area Under The Curve  
(AUC).  
The best solution  
presents smaller AUC.

# 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?

# 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**:

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

Hypothesis: the distributions are Gaussians (with mean  $\mu$  and standard deviation  $\sigma$ ).

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)

Number of falsely rejected biometric samples due to problems in acquisition.

### Failure to Enroll (FTE)

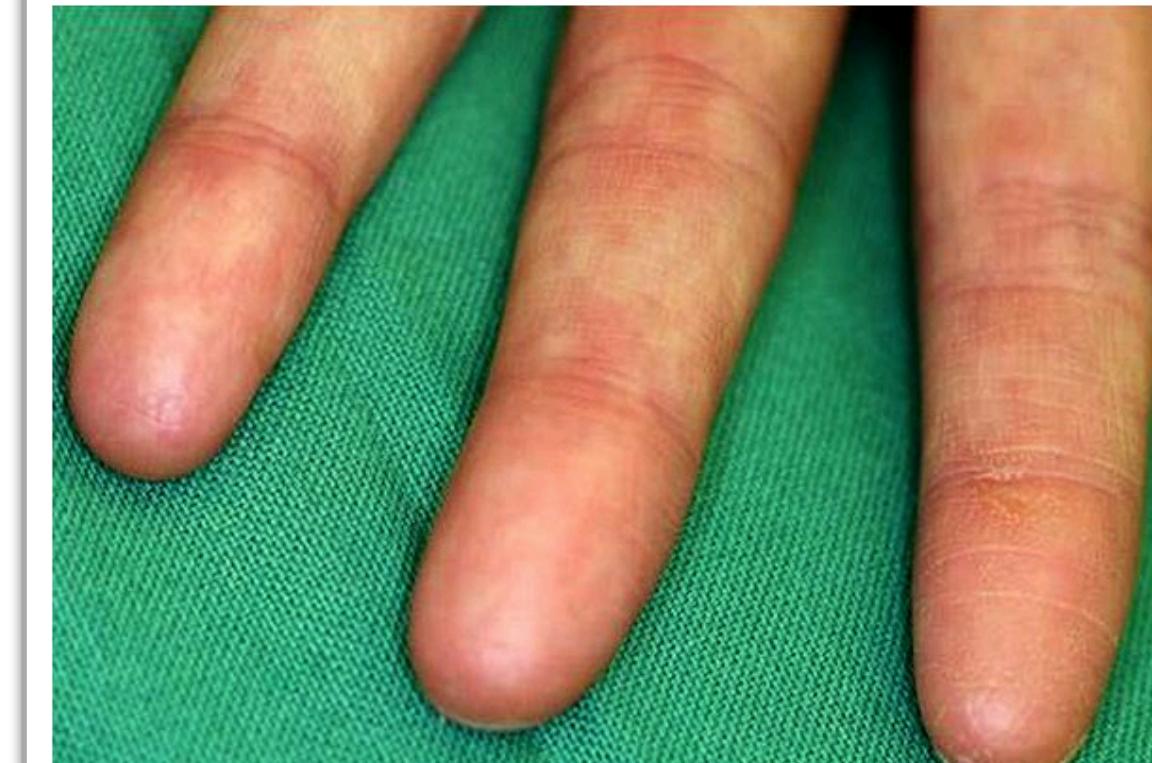
The same as FTA, but during enrollment.

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/>

# Metrics

## Other Metrics (3/4, 4/4)

### ***Positive Metrics***

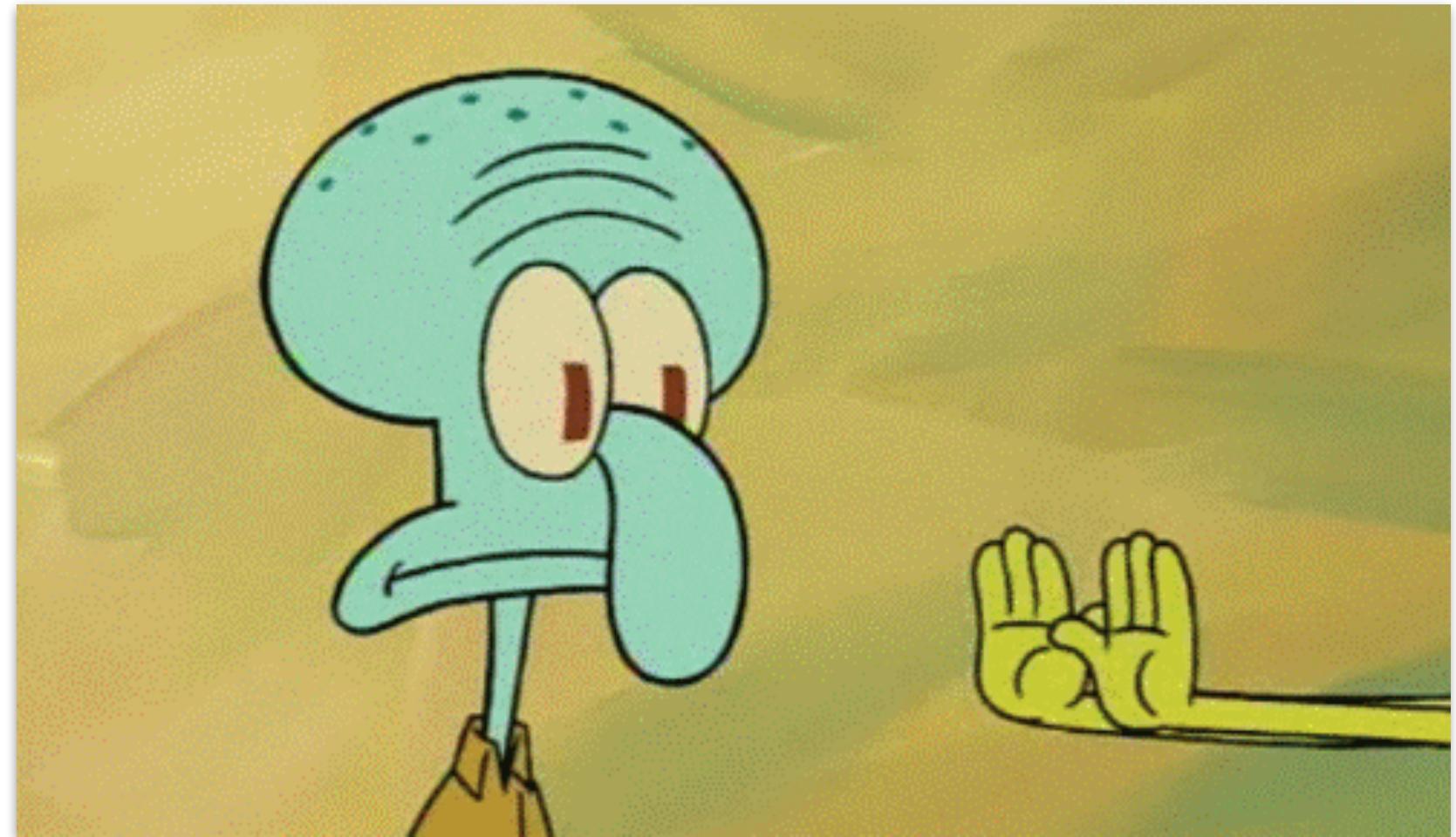
#### **True Non-Match Rate (TNMR)**

$$\text{TNMR} = 1.0 - \text{FNMR}$$

#### **True Match Rate (TMR)**

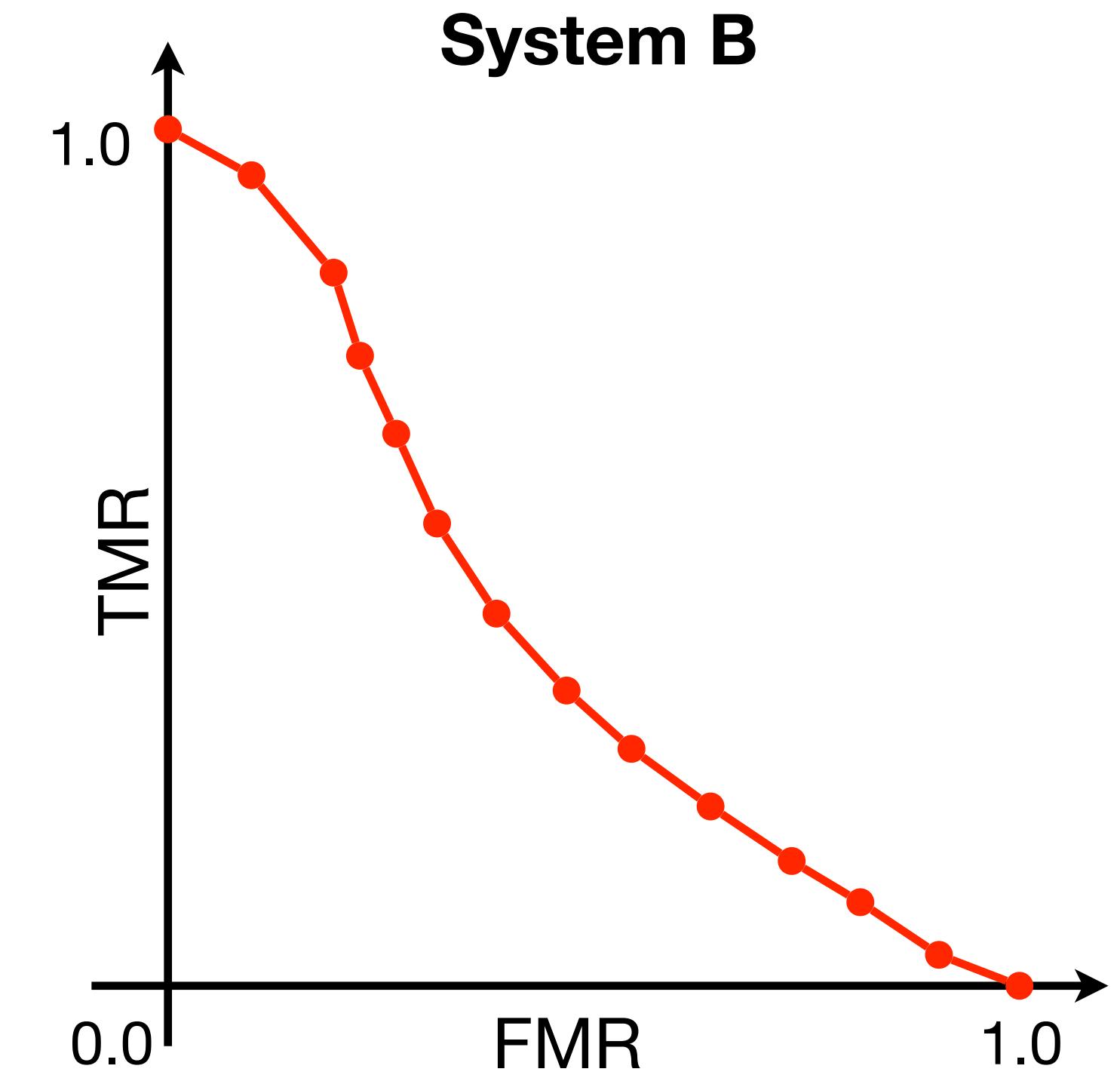
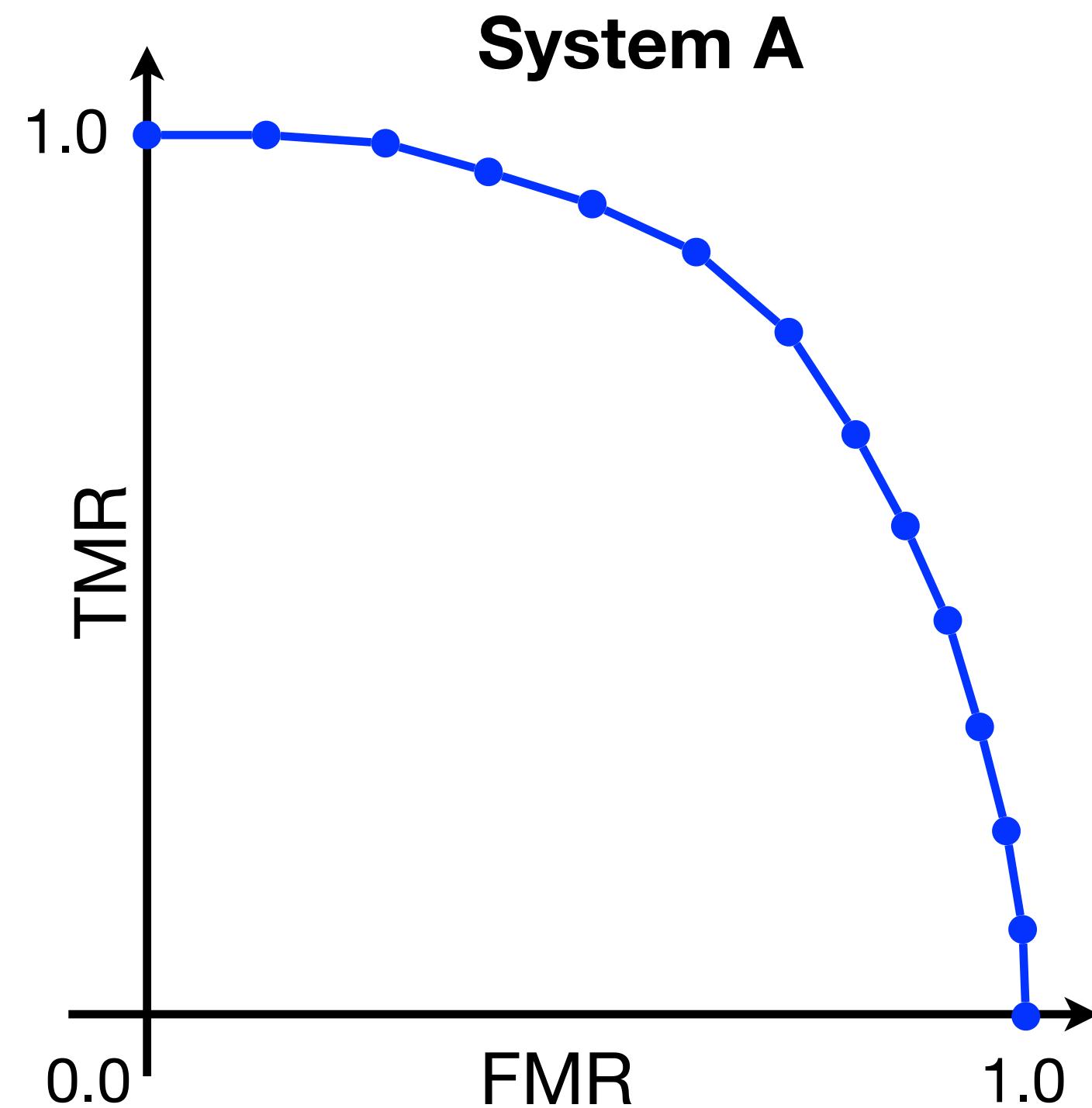
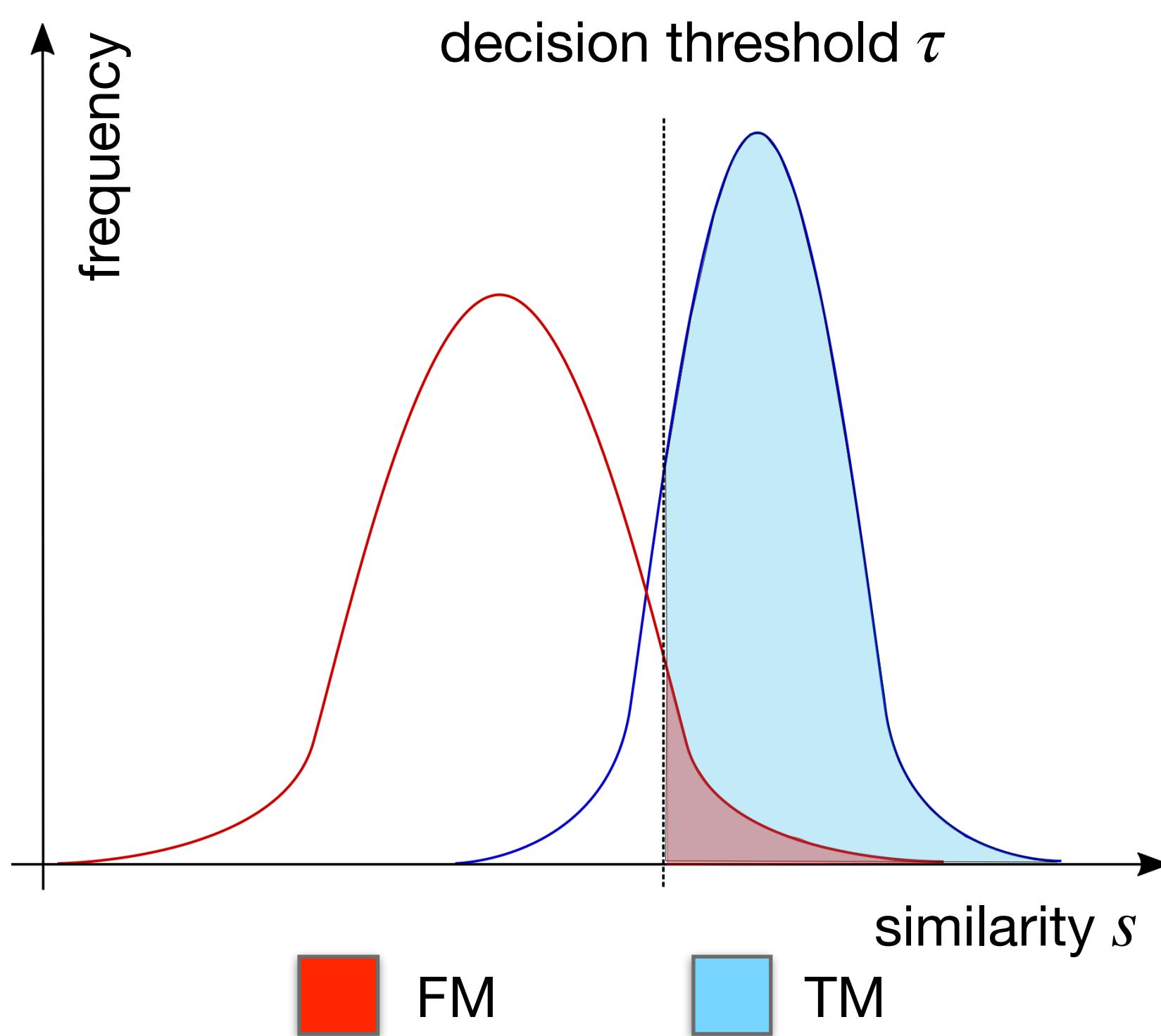
$$\text{TMR} = 1.0 - \text{FMR}$$

You want to maximize these instead of minimizing.



# Metrics

## TMR and FMR-based ROC

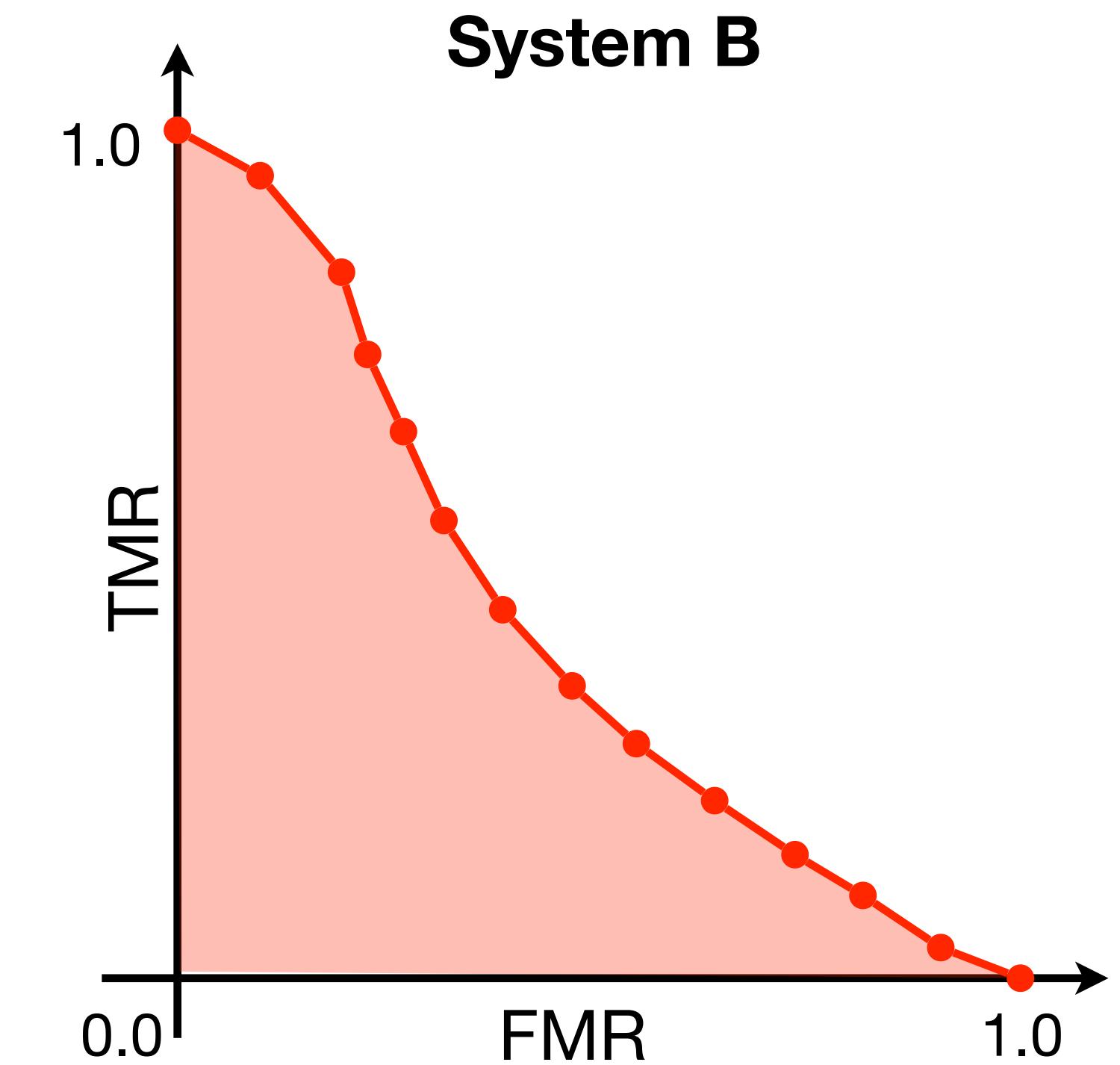
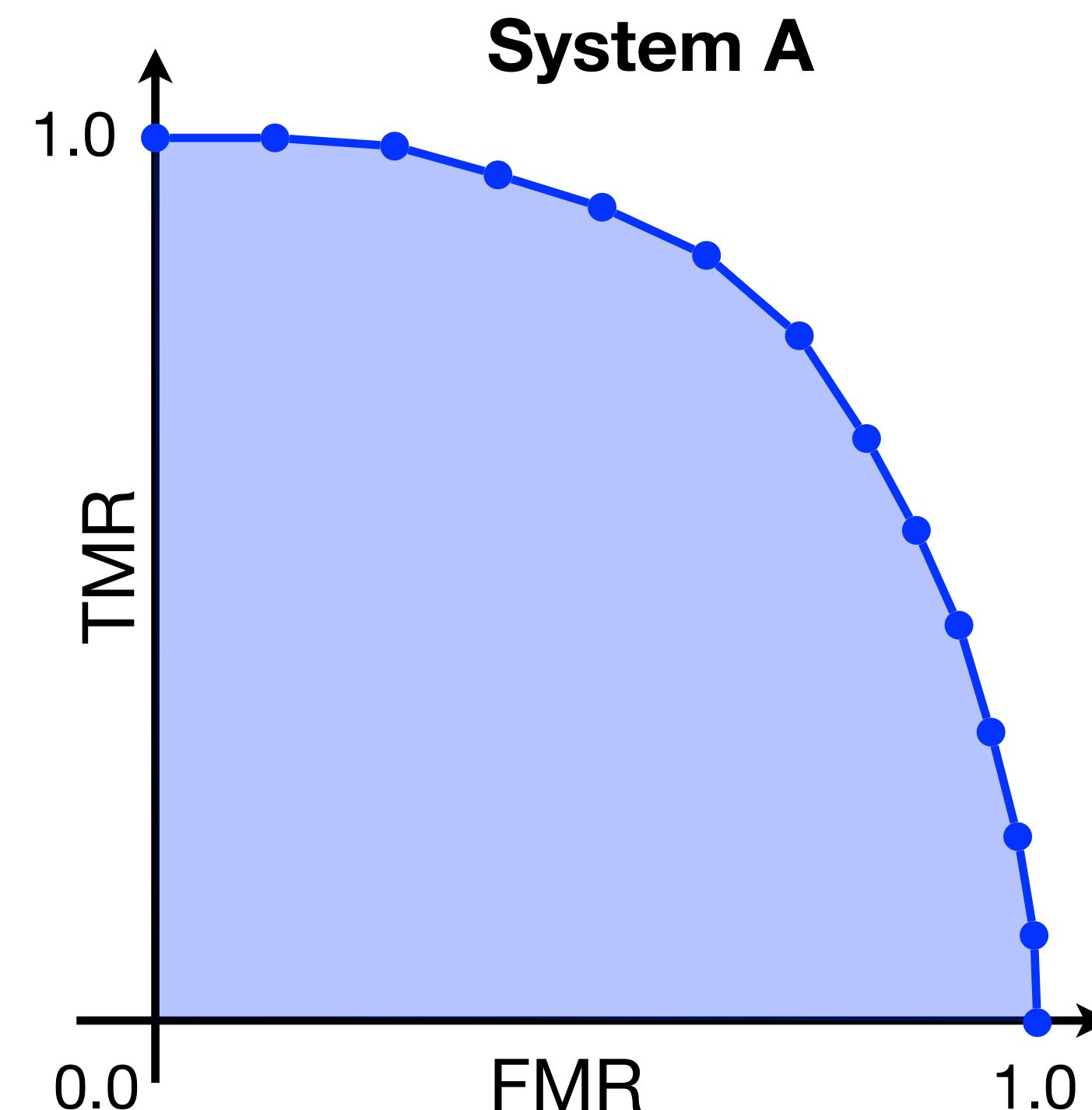


# Metrics

## TMR and FMR-based ROC

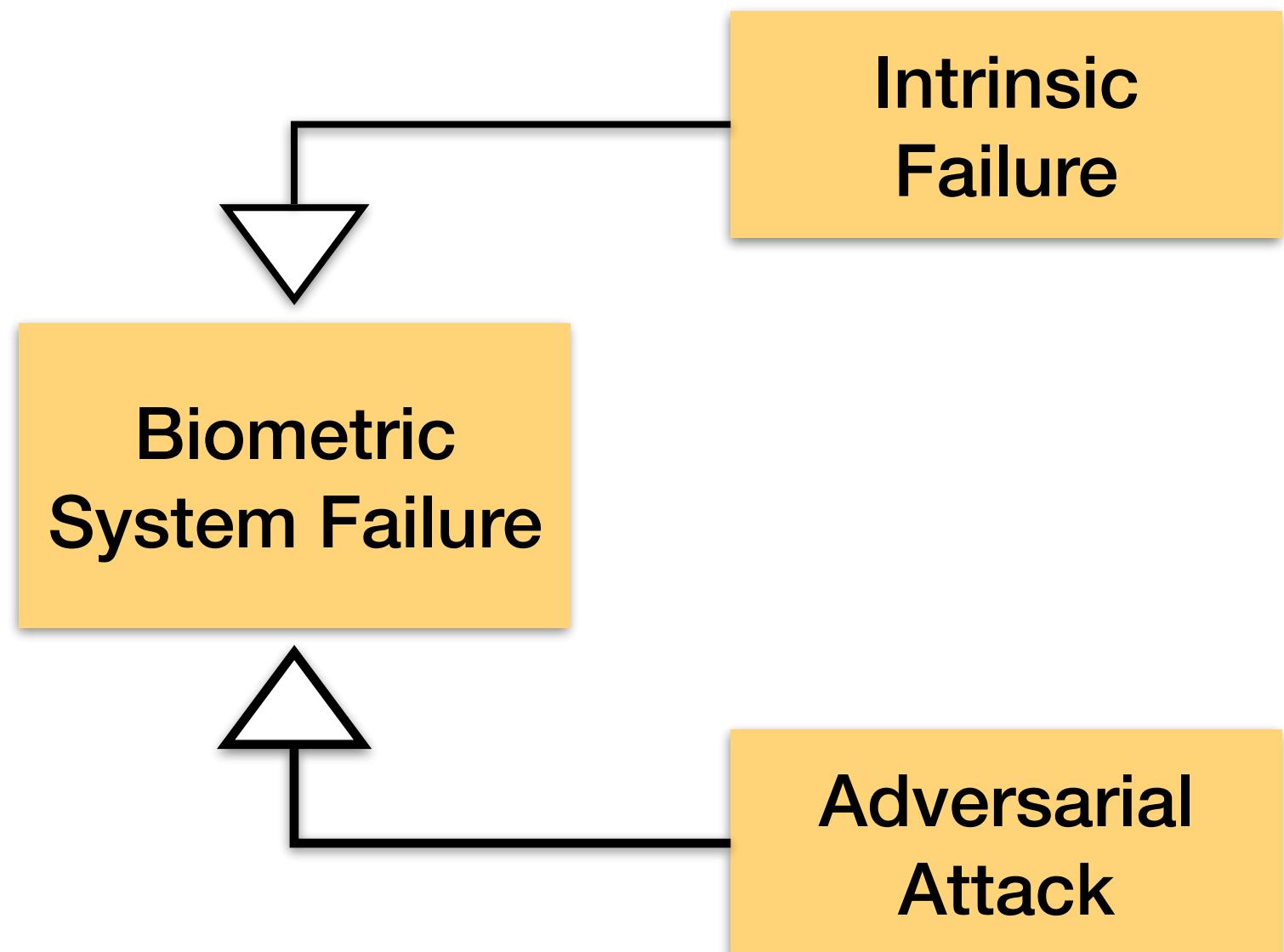
**Which one is better?**

The best solution  
presents **larger AUC**.



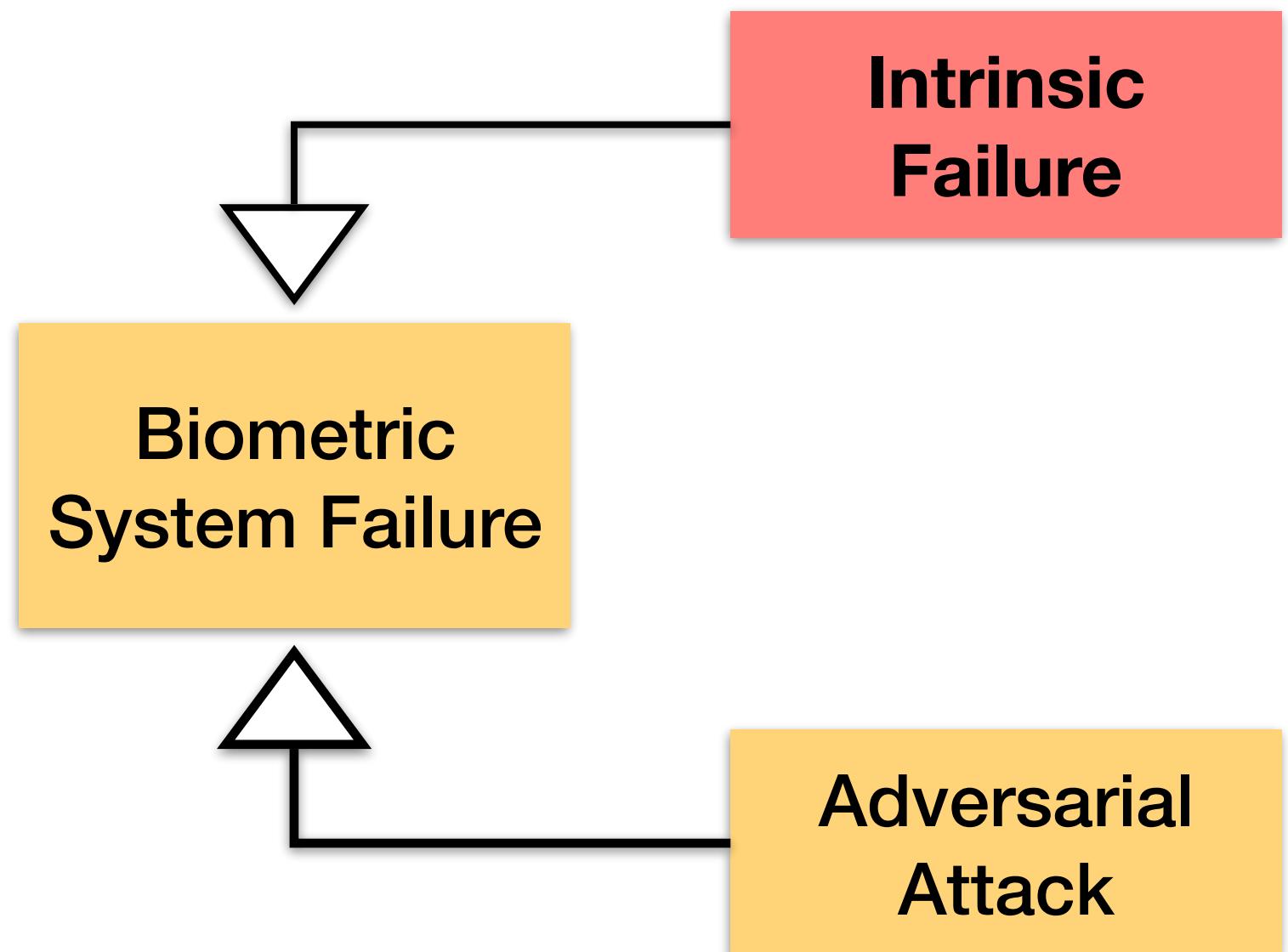
# Attacks

## Threat Model



# Attacks

## Threat Model



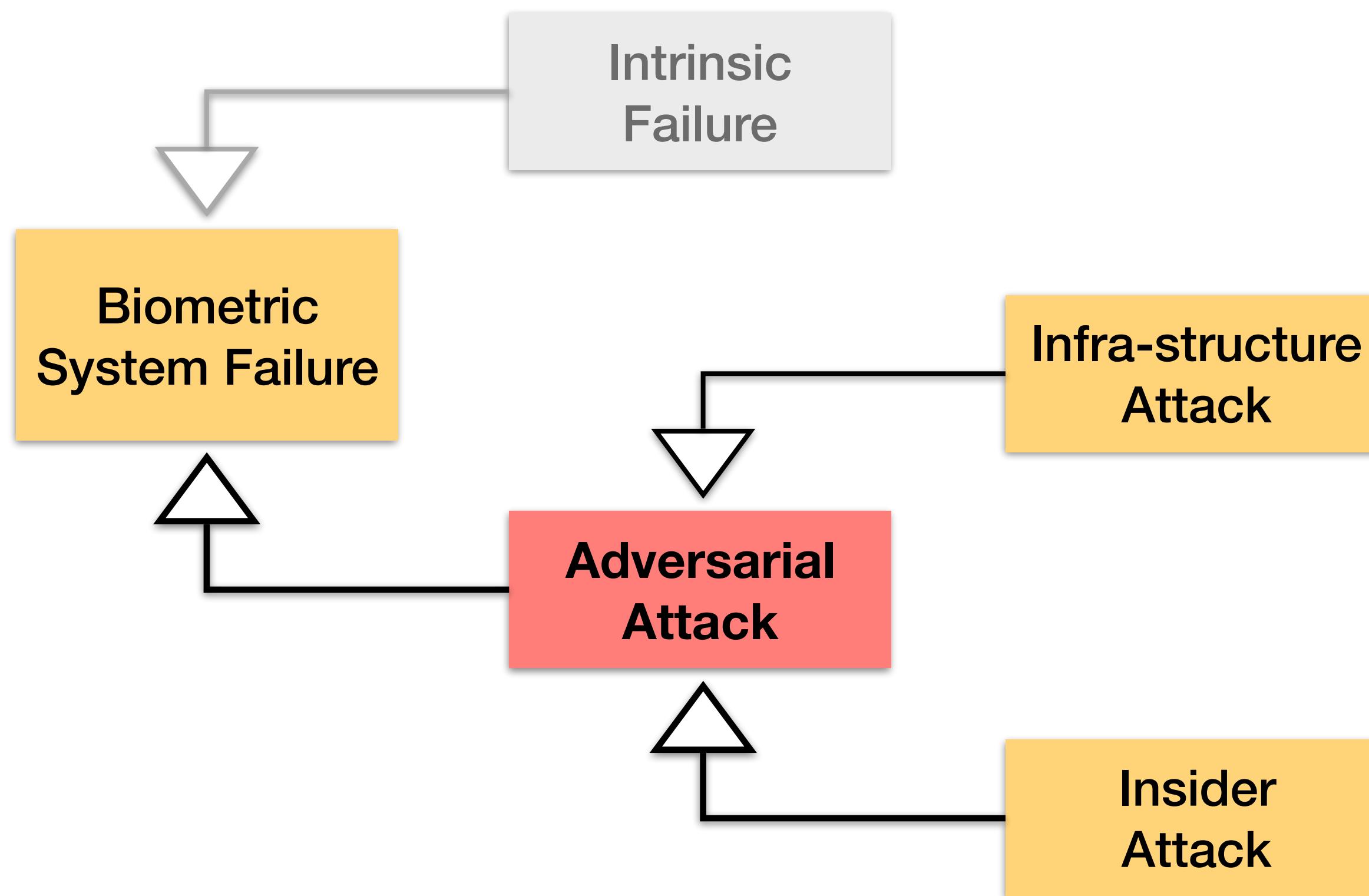
### Not attacks

Errors due to the limitation of the solutions and due to hardware stress.



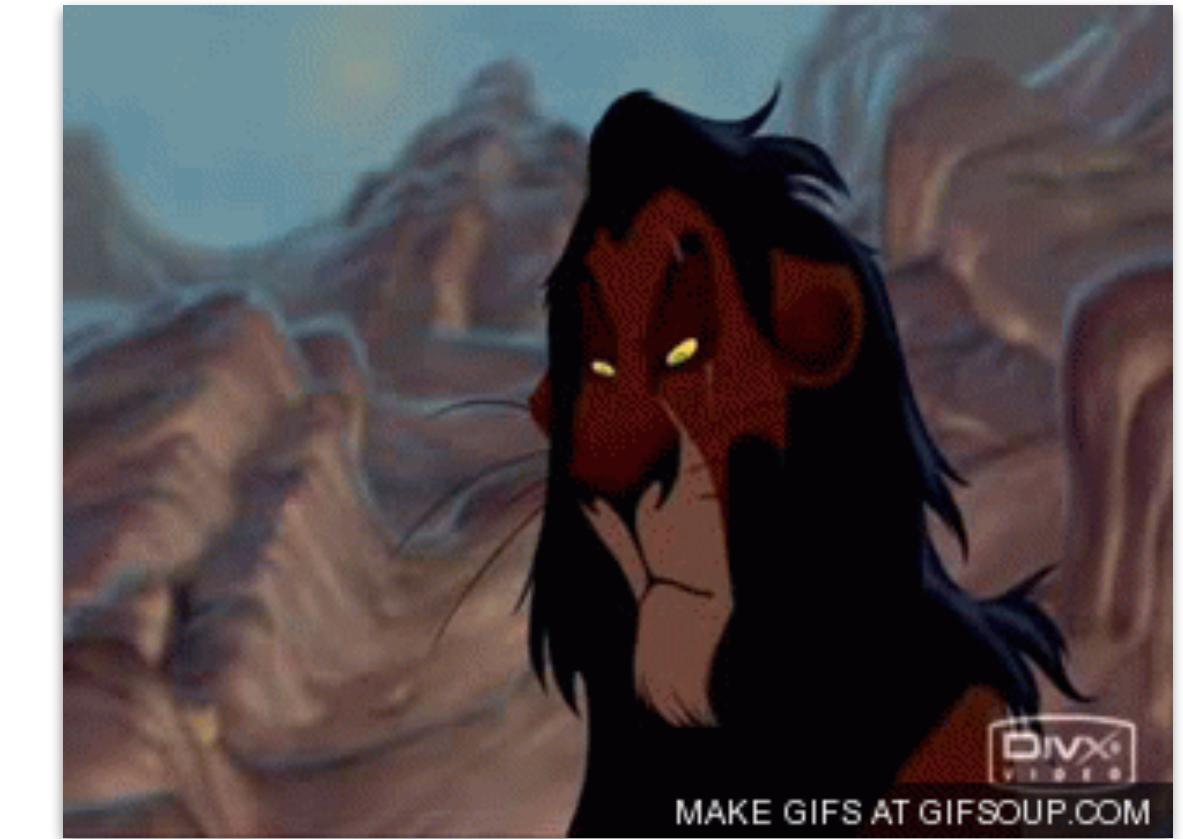
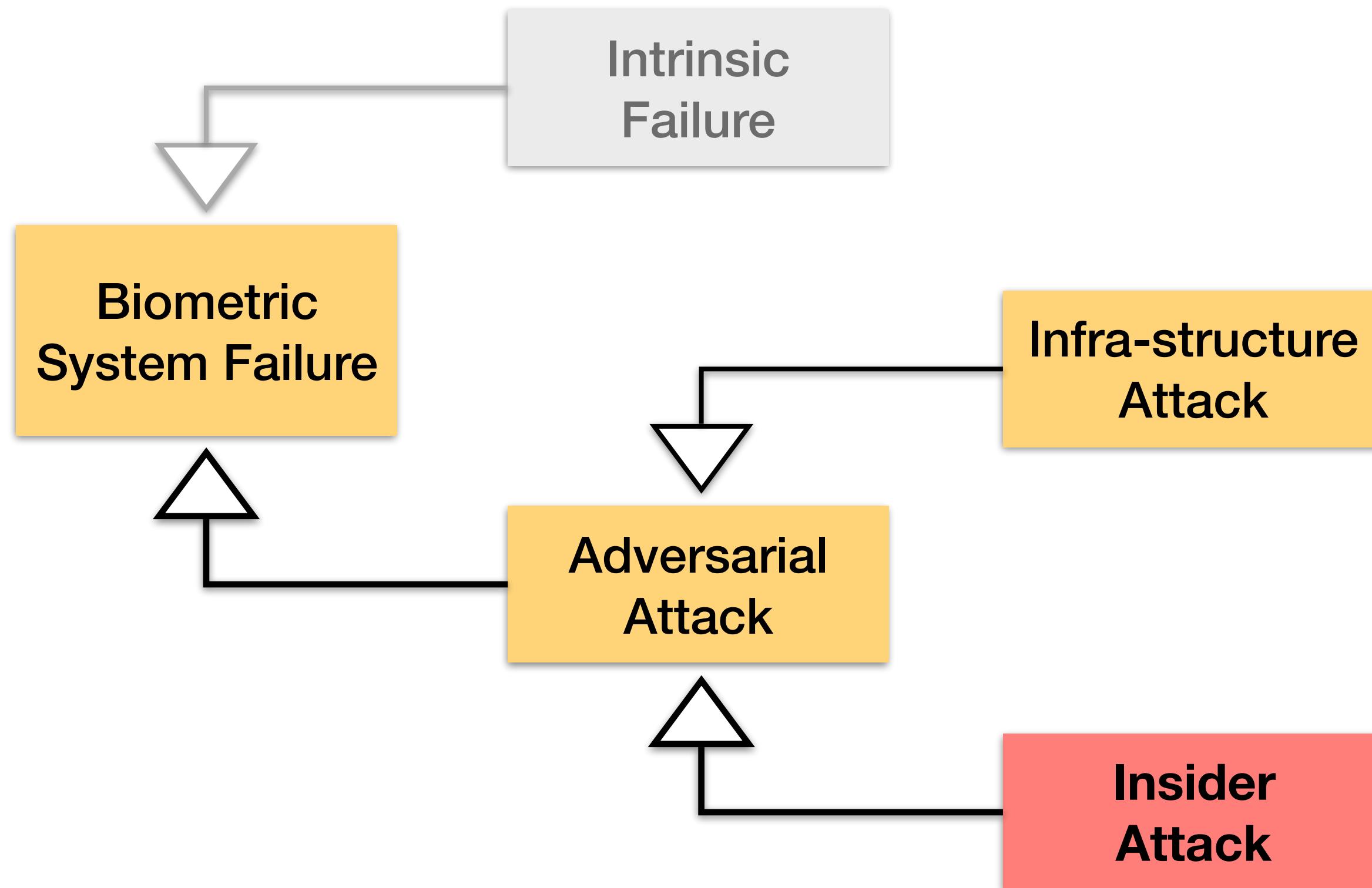
# Attacks

## Threat Model



# Attacks

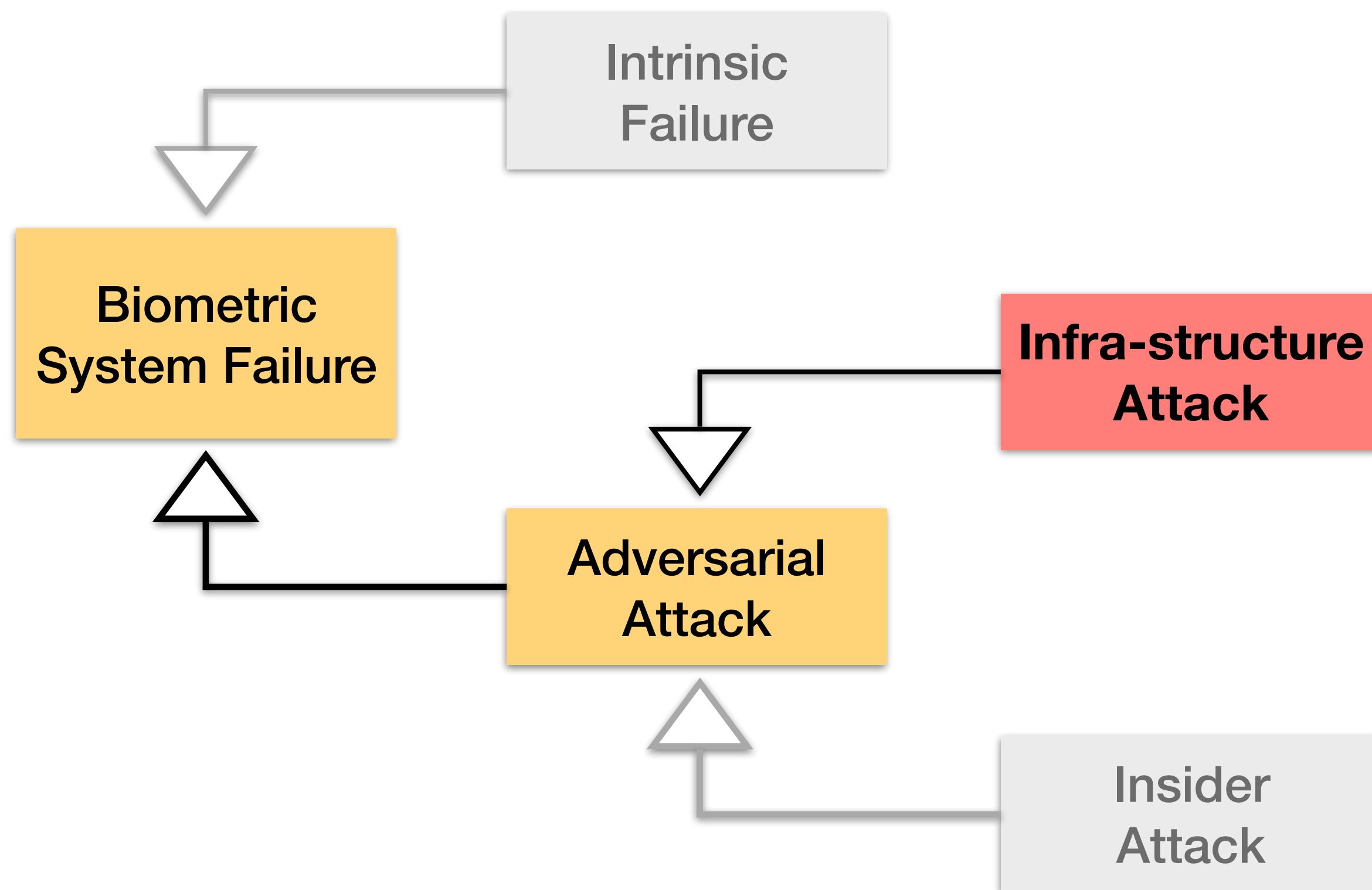
## Threat Model



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

# Attacks

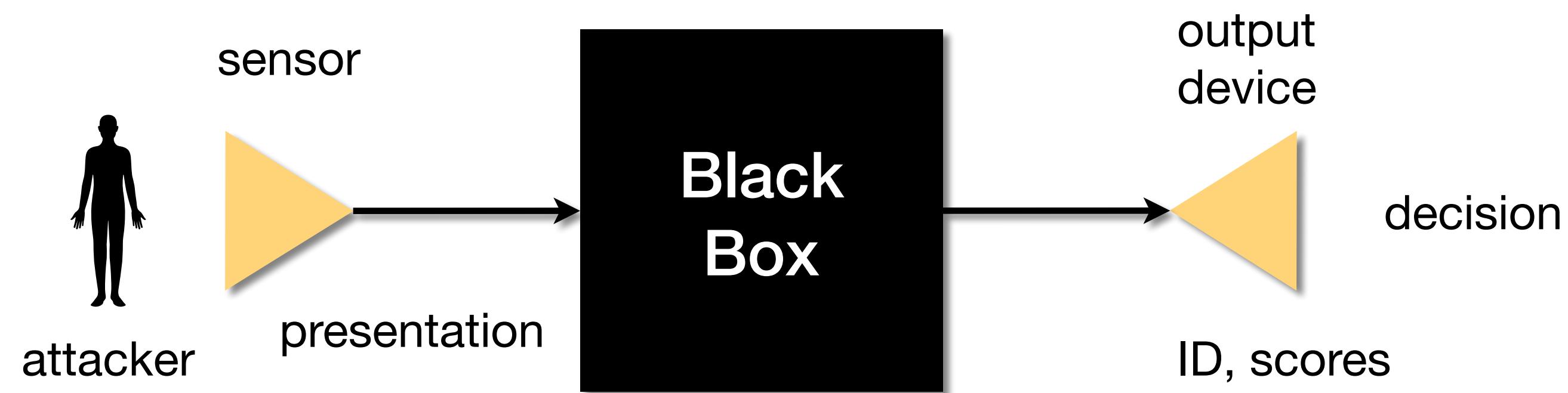
## Threat Model



**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).



The screenshot shows a news article from Click2Houston.com. The header includes navigation links for NEWS, SPORTS, THINGS TO DO, FIND YOUR CITY, DISCOVER, HOUSTON LIFE, WEATHER, TRAFFIC, and NEWSLETTER. It also shows the temperature (54°F) and a sign-in button. The main headline reads "Divorce deception: Man forges wife's name on divorce papers, police say". Below the headline is a summary: "A Houston man now has to answer to his wife and the courts. Harris County Precinct 4 deputies said Paul Nixon, 51, tried to deceive the Harris County District Clerk's office by forging his wife's signature on divorce papers." There is a "Sign up for our Newsletters" section with an input field and a submit button.

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

# 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.youtube.com/watch?v=\\_PoudPCevN0](https://www.youtube.com/watch?v=_PoudPCevN0)

<https://www.dailymotion.com/debug/wearable-face-projector-hong-kong-protesters/>

# Attacks

## Spoofing

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

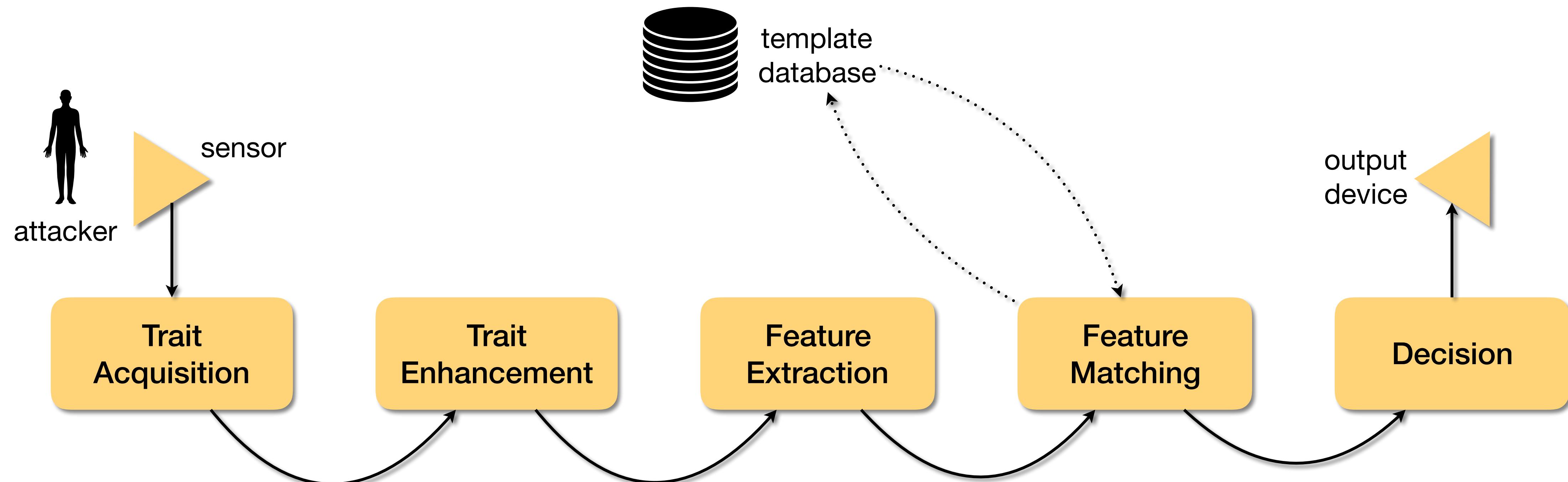
The screenshot shows the BBC News website. The top navigation bar includes the BBC logo, a sign-in link, and categories like News, Sport, Reel, Worklife, Travel, and Future. Below this is a large red banner with the word "NEWS". The main headline reads "Doctor 'used silicone fingers' to sign in for colleagues". Below the headline is a timestamp "© 12 March 2013" and sharing icons for Facebook, Twitter, Email, and a "Share" button. The URL at the bottom of the screenshot is <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.

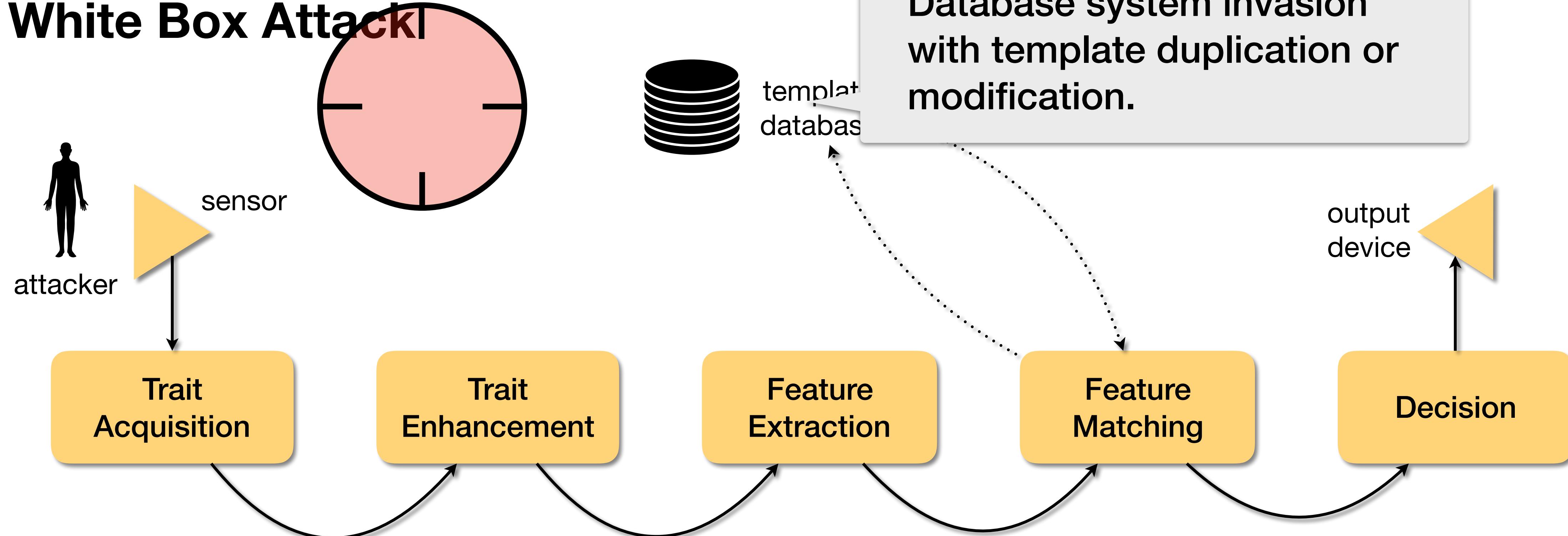
# Attacks

## White Box Attack



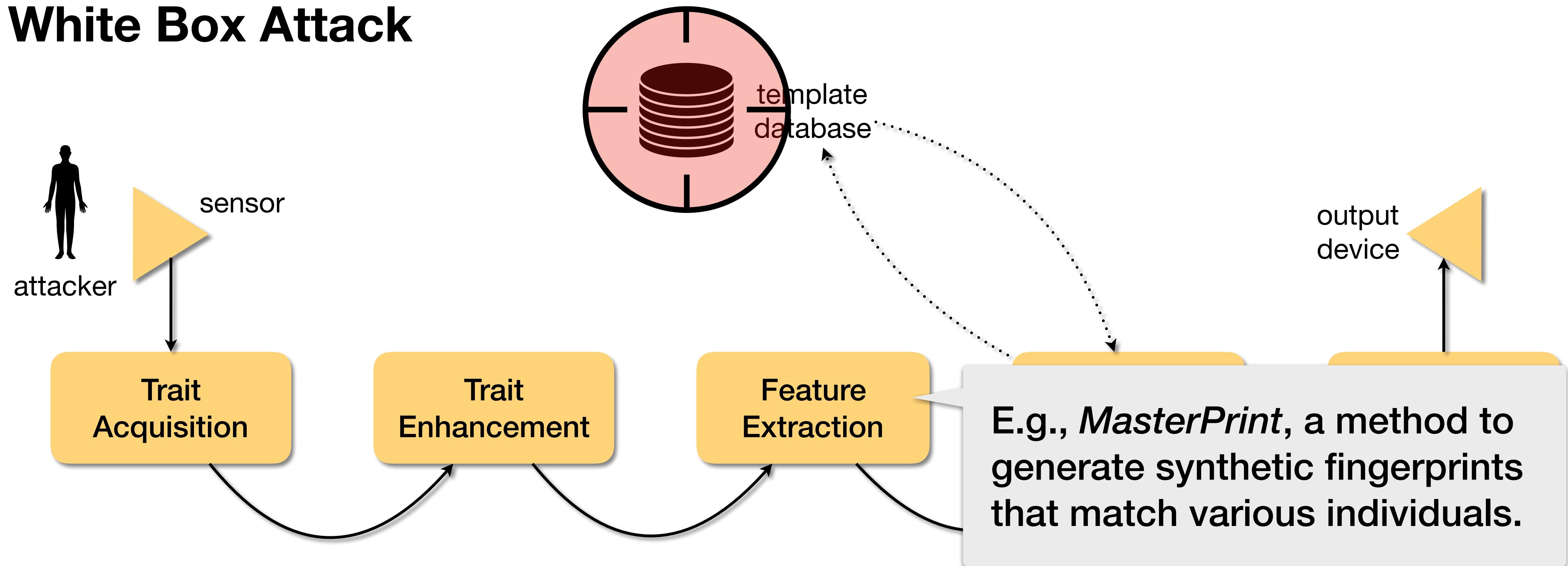
# Attacks

## 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*

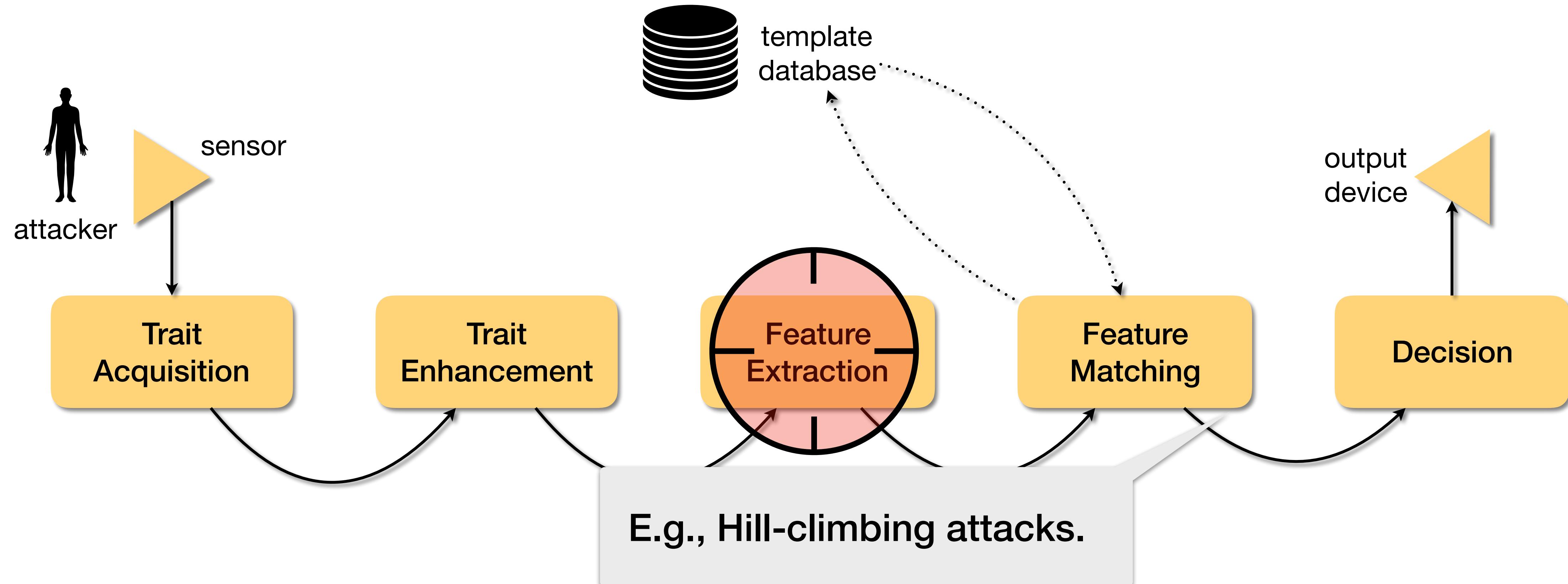


[https://www.cse.msu.edu/~rossarun/pubs/  
RoyMemonRossMasterPrint\\_TIFS2017.pdf](https://www.cse.msu.edu/~rossarun/pubs/RoyMemonRossMasterPrint_TIFS2017.pdf)

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

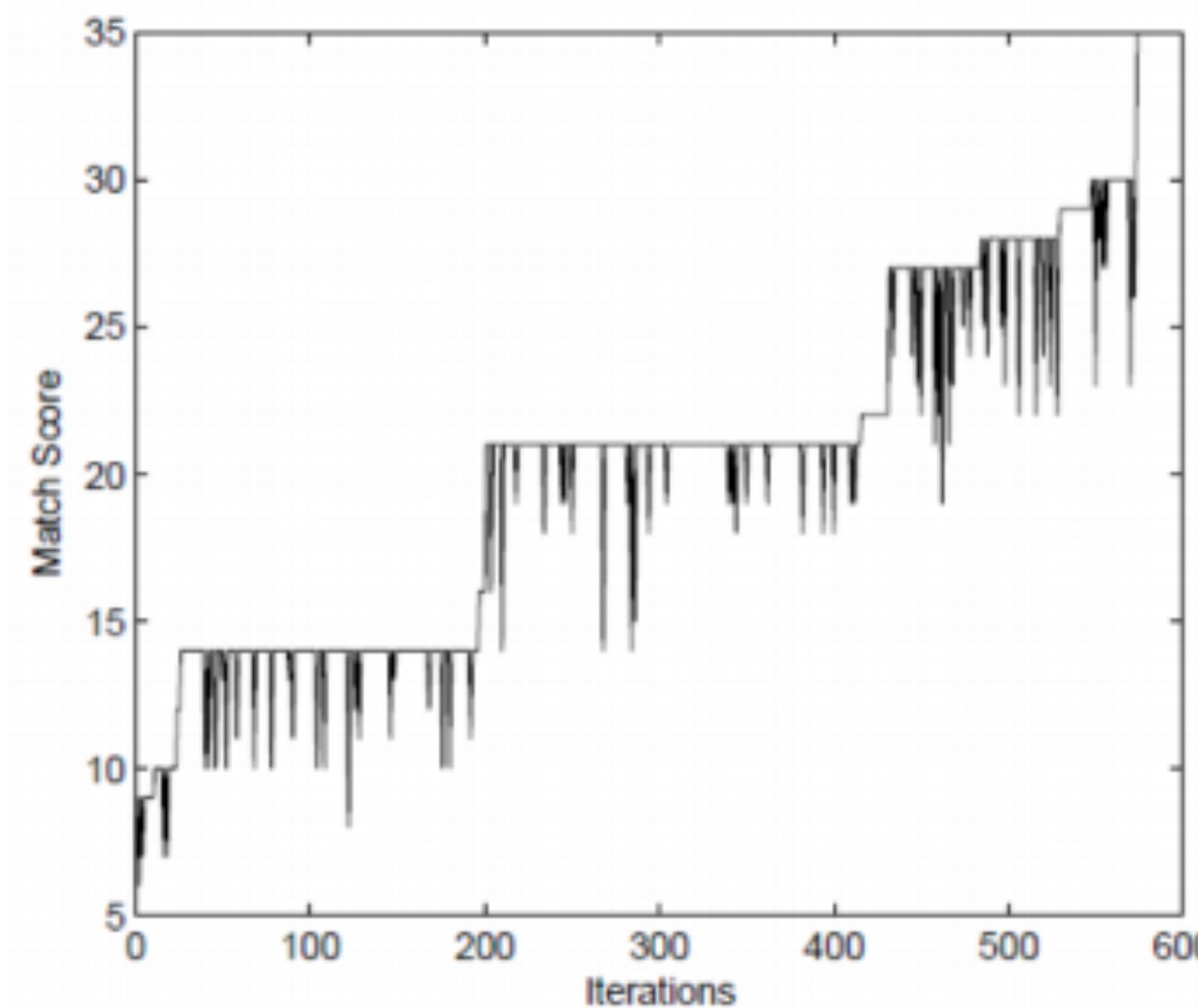
# Attacks

## White Box Attack



# Attacks

## Hill-climbing Attack E.g. Fingerprints

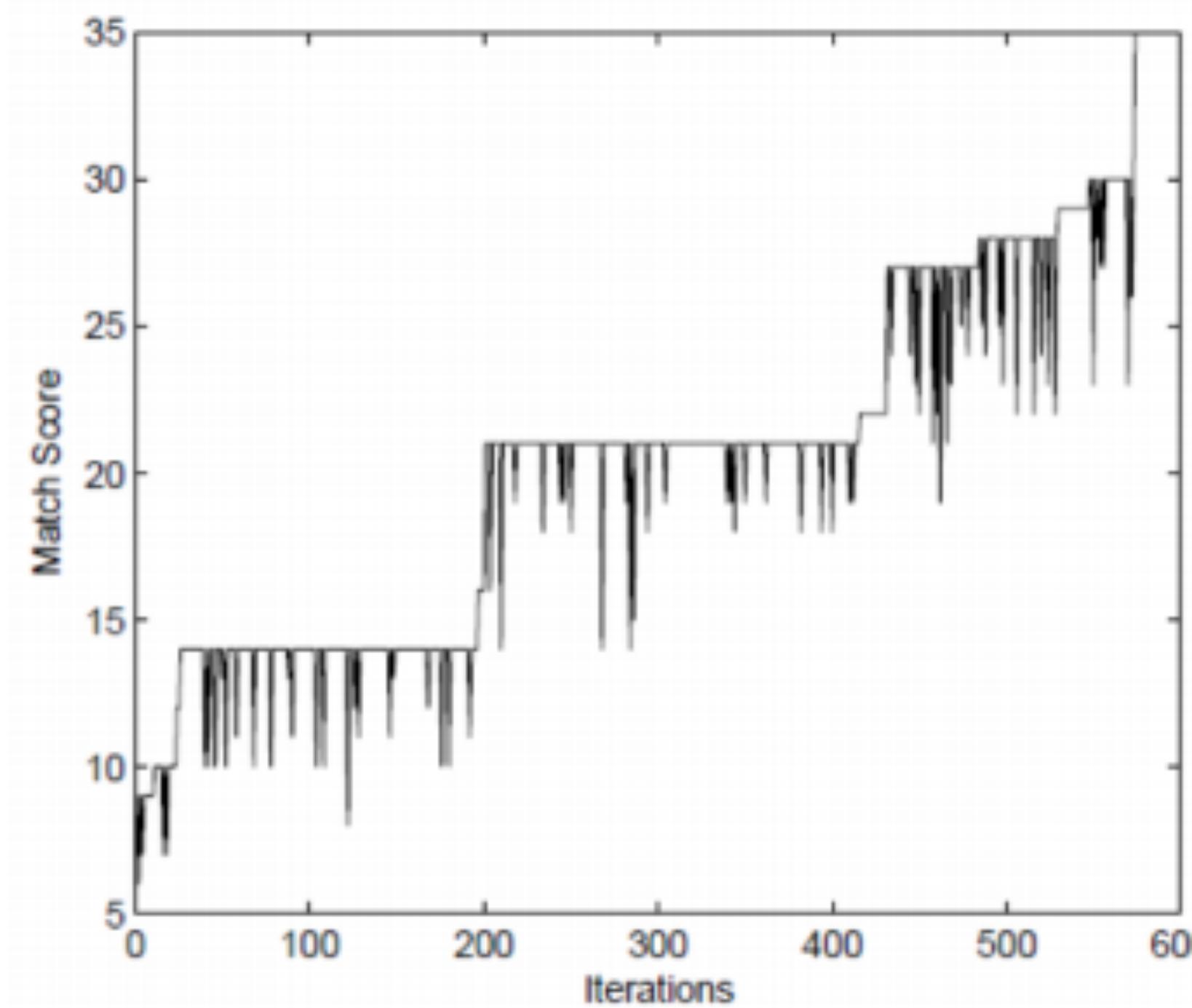


The attacker iteratively provides synthetic trait samples to the system. At each iteration, the attacker observes how the similarity scores are progressing.

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

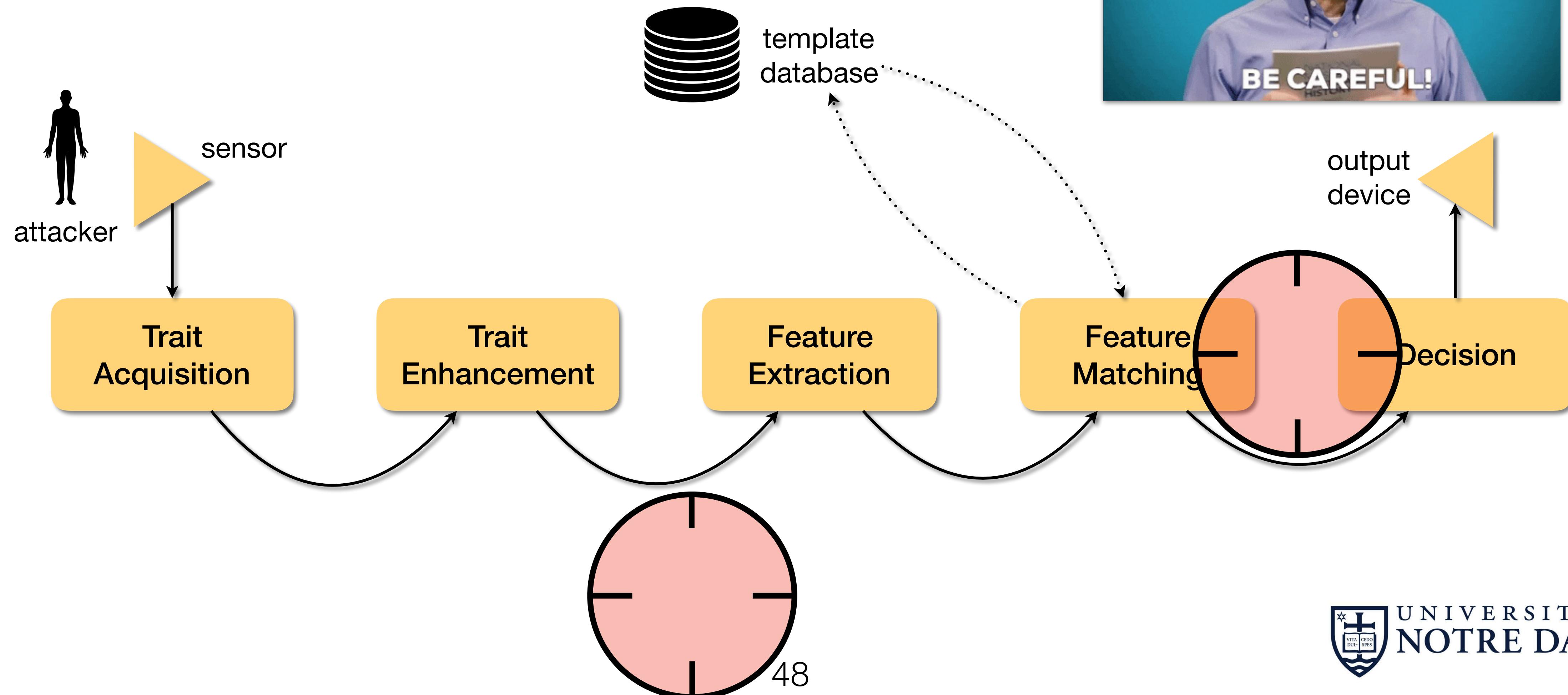
## Hill-climbing Attack E.g. Fingerprints



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

## White Box Attack



# Attacks

## Attack Assignments

Don't forget: we will try and see attack attempts in our assignments. You'll have the chance to be attackers.



# 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).

