# Basics II (cont.)

CSE 40537/60537 Biometrics

**Daniel Moreira**

Spring 2022

UNIVERSITY OF NOTRE DAME

# Metrics


**In Practice**

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

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

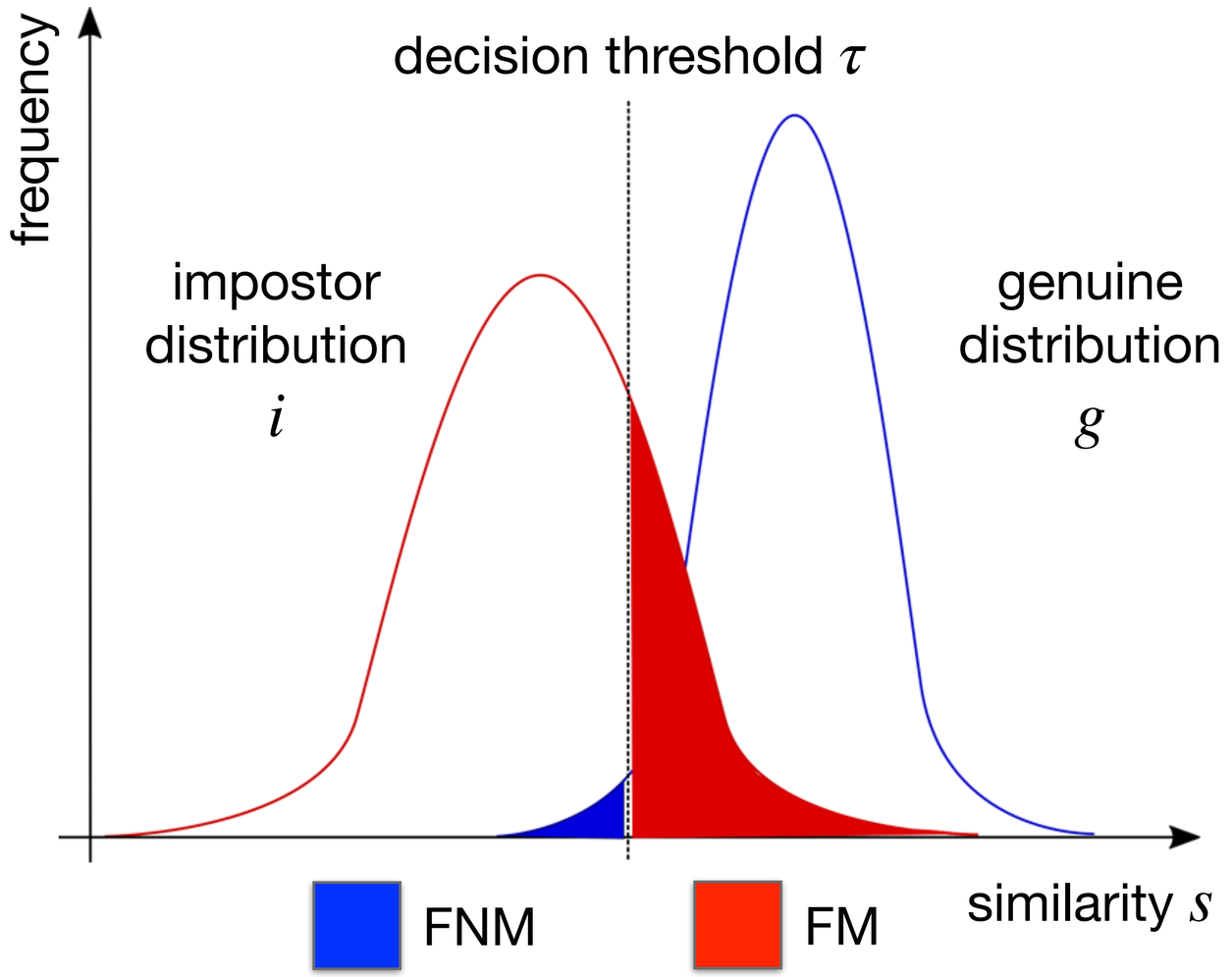
How many of the genuine comparisons are wrongly computed by the system?

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

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

UNIVERSITY OF NOTRE DAME

# Metrics




**What is the impact of changing the decision threshold?**

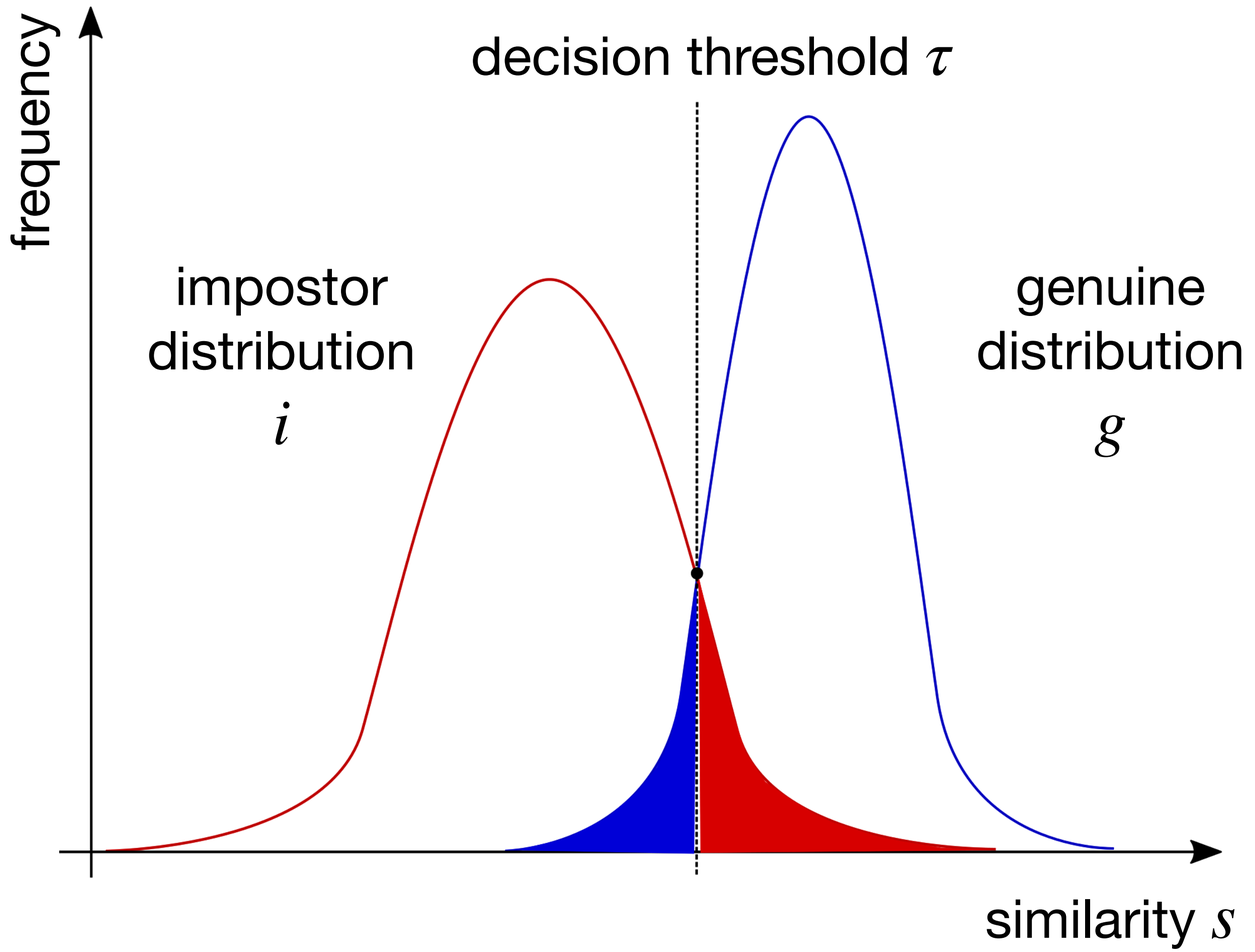
**The larger the value of $\tau$:**
The larger the value of FNM;
The smaller the value of FM.

FNM and FM are inversely proportional.



UNIVERSITY OF NOTRE DAME

# Metrics




**What to choose?**

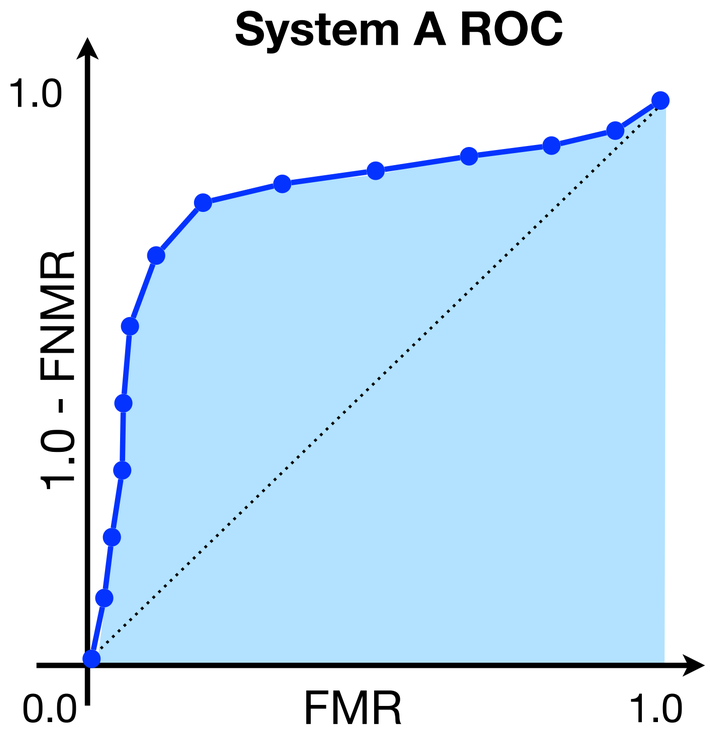
**Equal Error Rate (EER)**
Common practice.
Pick the threshold where FNMR = FMR.

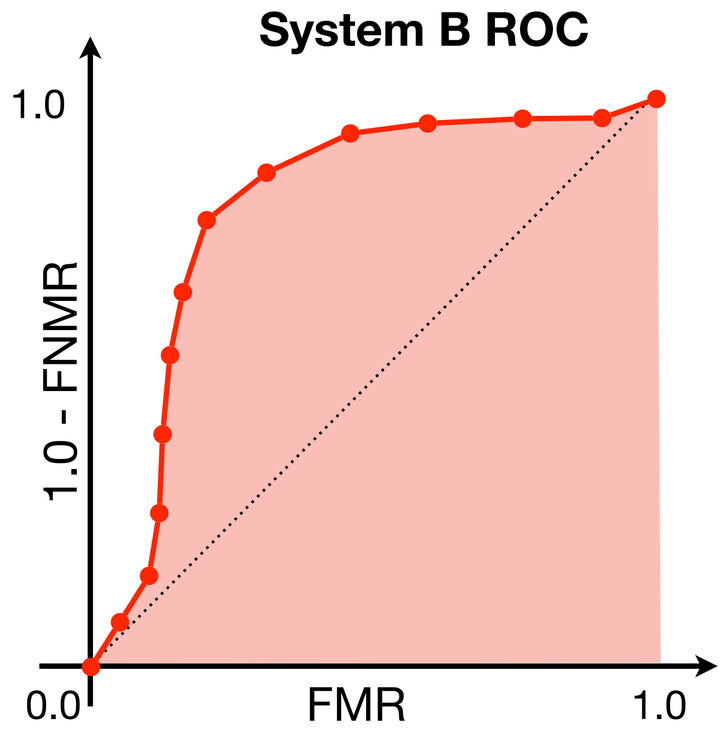


UNIVERSITY OF NOTRE DAME

# Metrics


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




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



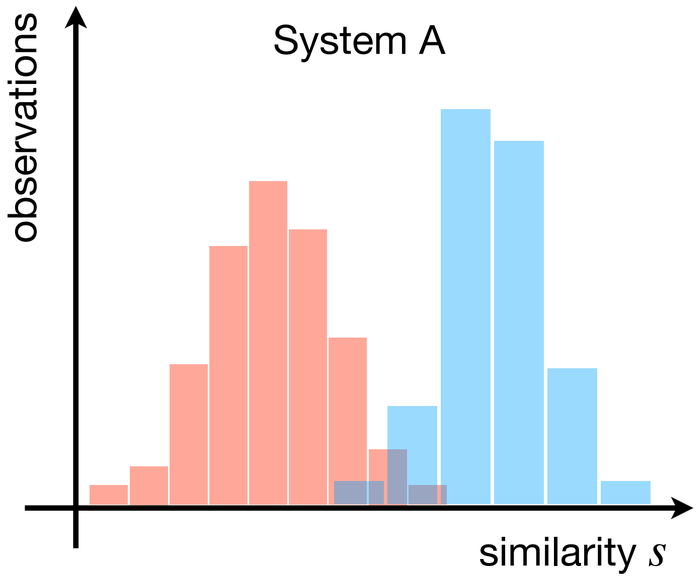
UNIVERSITY OF NOTRE DAME

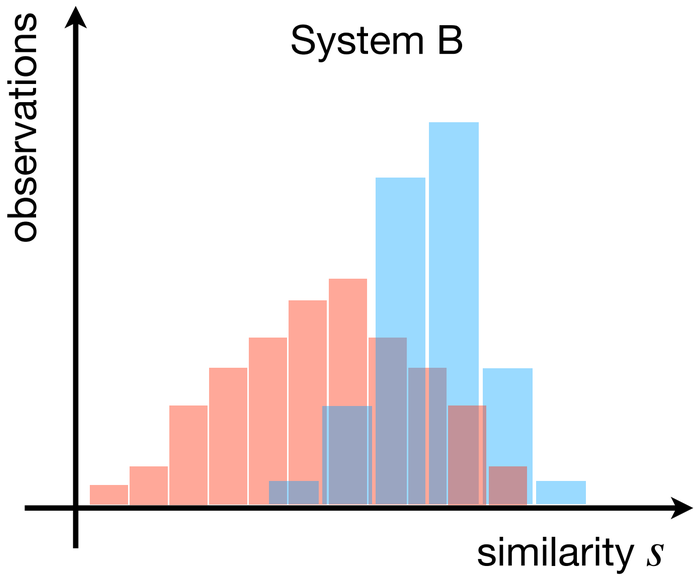
# Metrics

RECAP

**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 $\mu$ and standard deviation $\sigma$).

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

UNIVERSITY OF NOTRE DAME

# Metrics

RECAP

**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

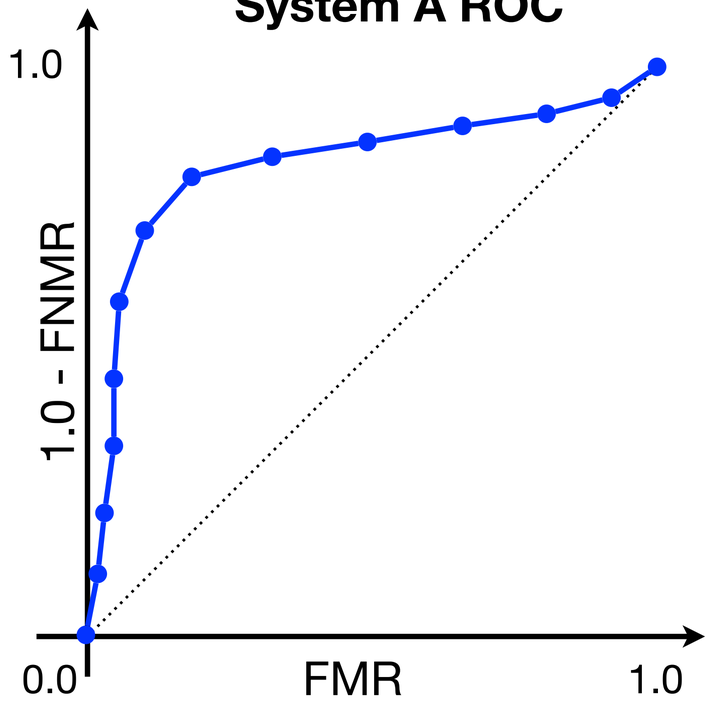
You want to maximize these instead of minimizing.

# Metrics

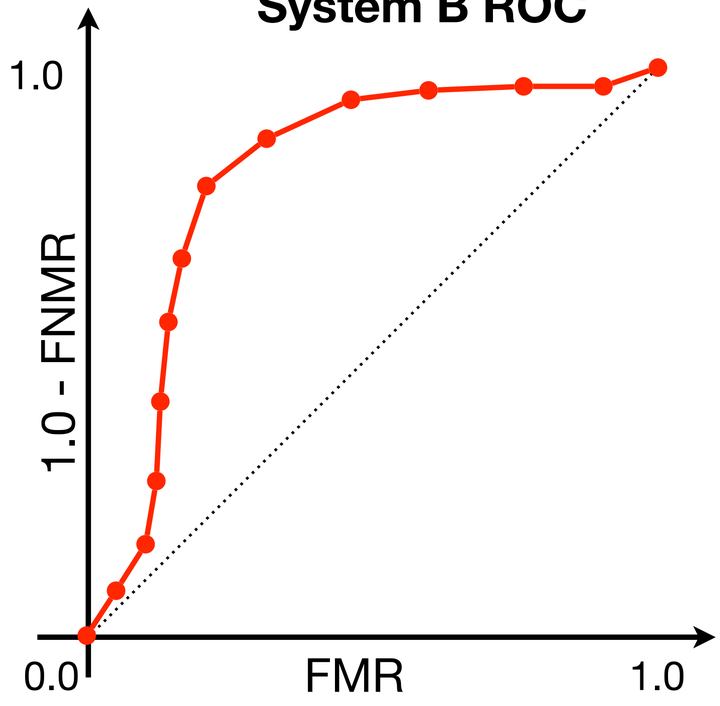

**How to compare two different systems?**
Biometric systems *A* and *B.*

Compute FMR and FNMR for a variety of thresholds.

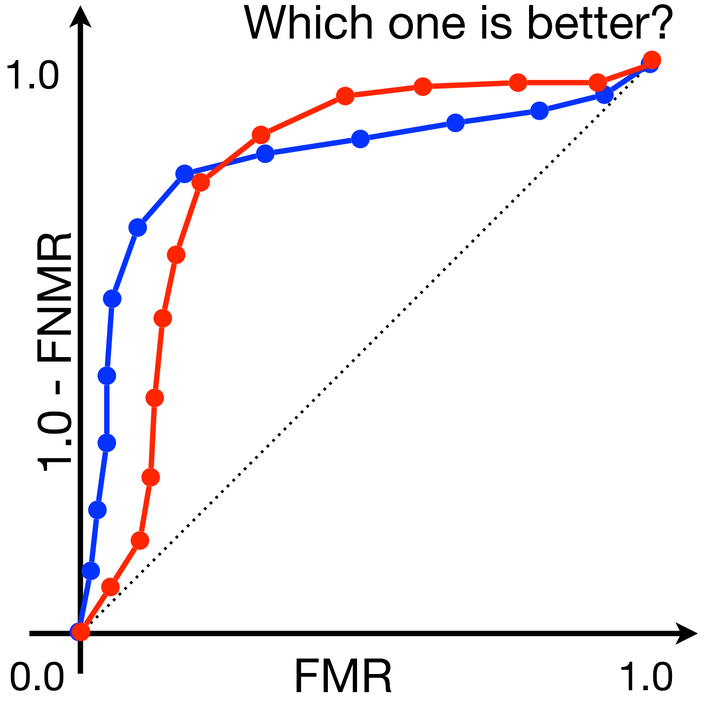
**System A ROC**




**System B ROC**




**Together**
Which one is better?




UNIVERSITY OF NOTRE DAME

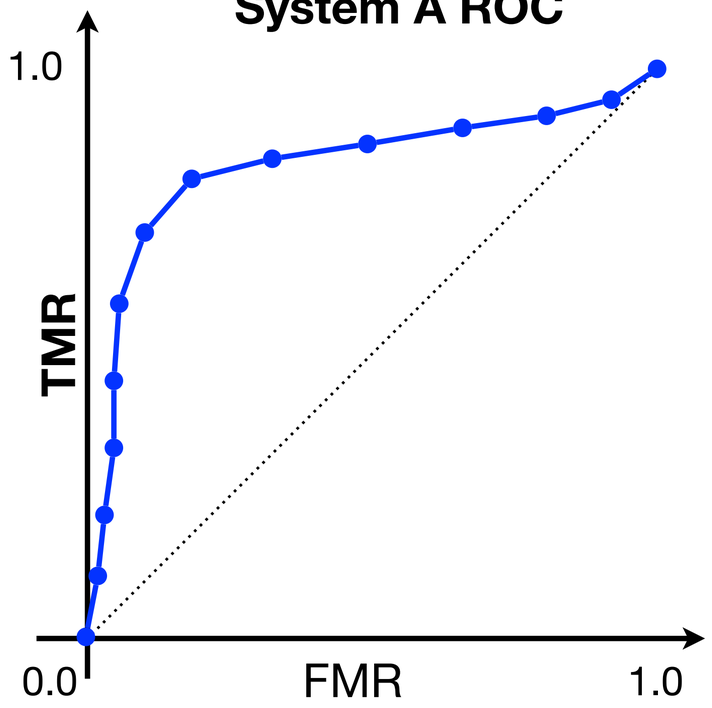
# Metrics

RECAP

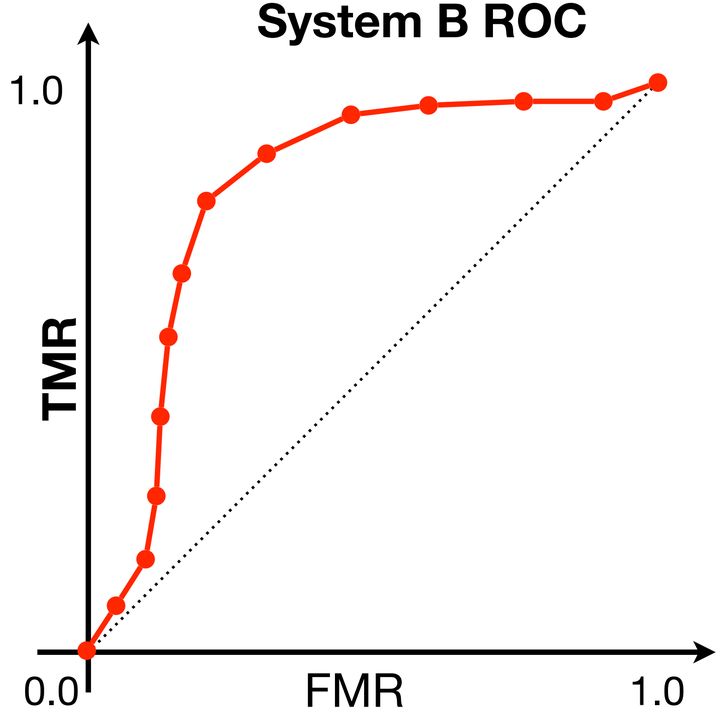
**How to compare two different systems?**
Biometric systems *A* and *B.*

Compute FMR and FNMR for a variety of thresholds.

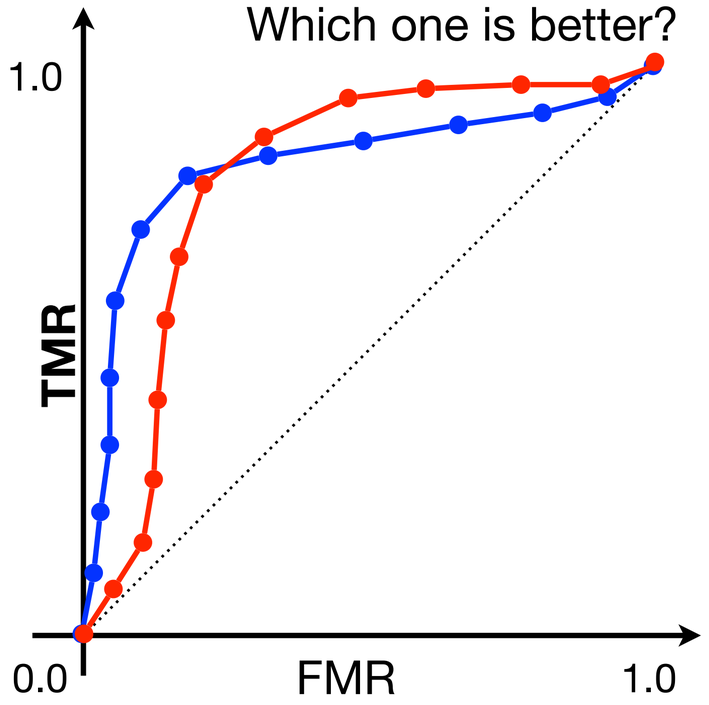
**System A ROC**




**System B ROC**



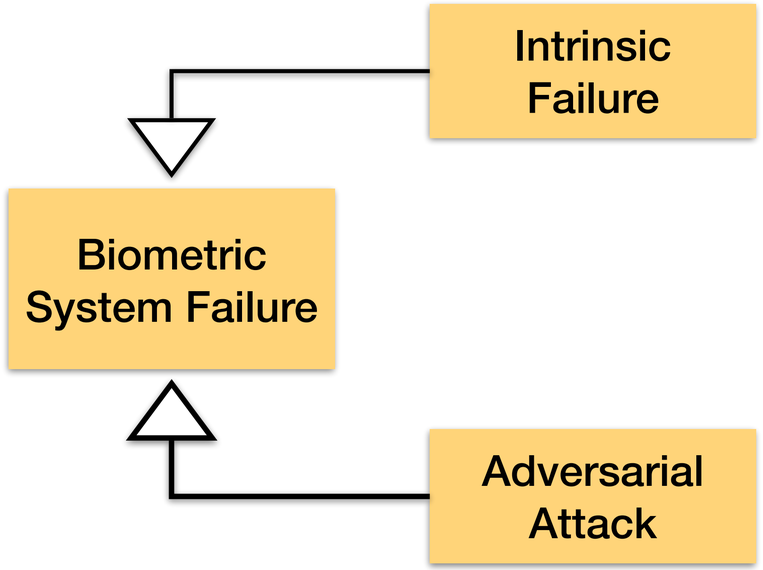

**Together**
Which one is better?




UNIVERSITY OF NOTRE DAME

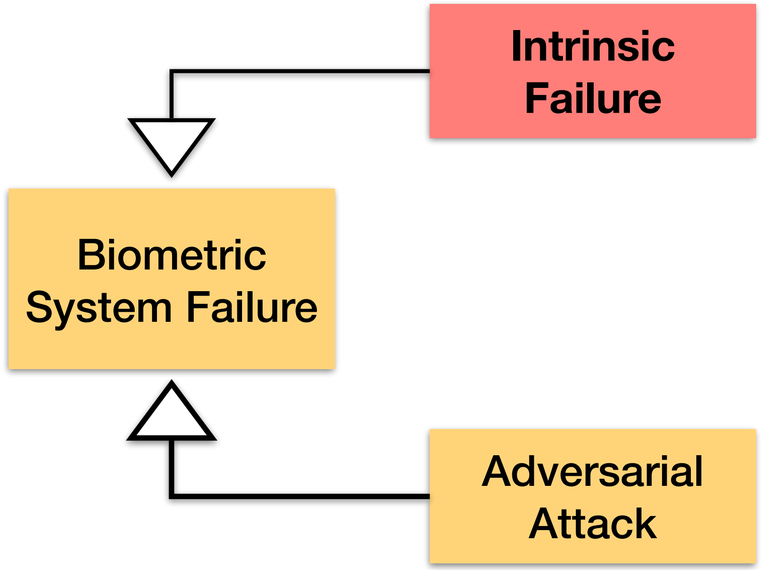
# Attacks

## Threat Model



# Attacks

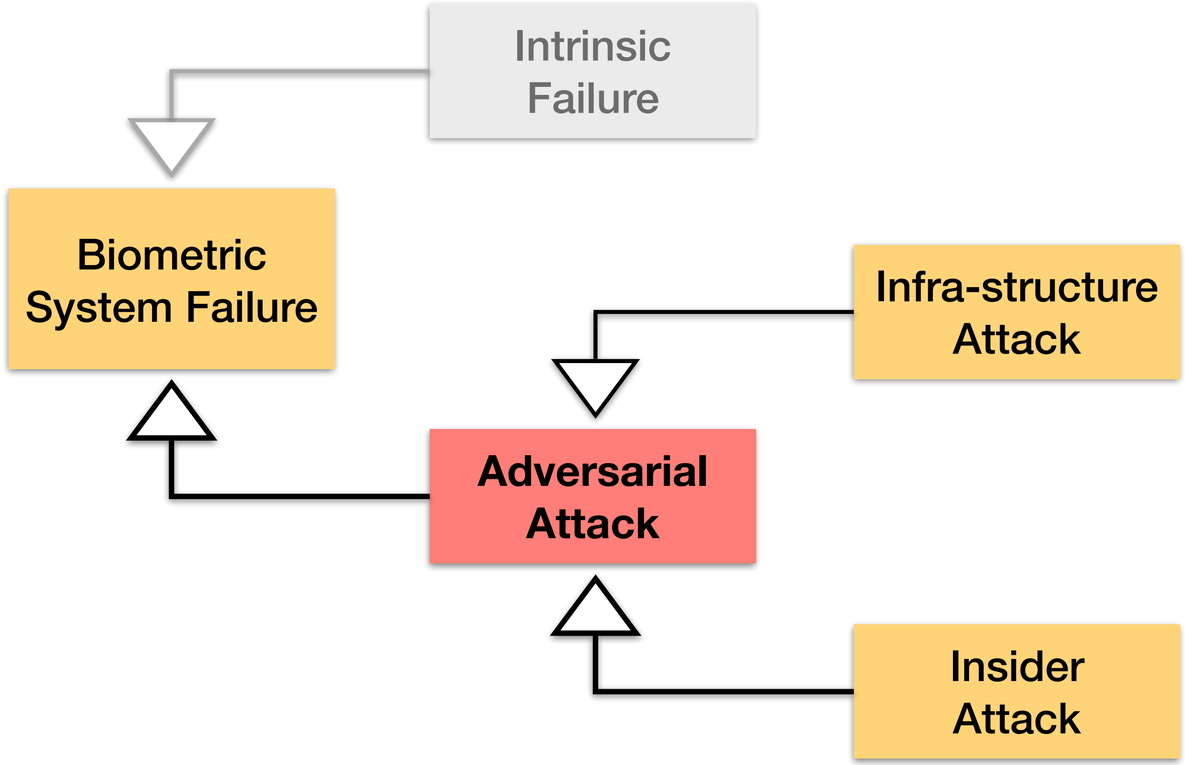
## Threat Model




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

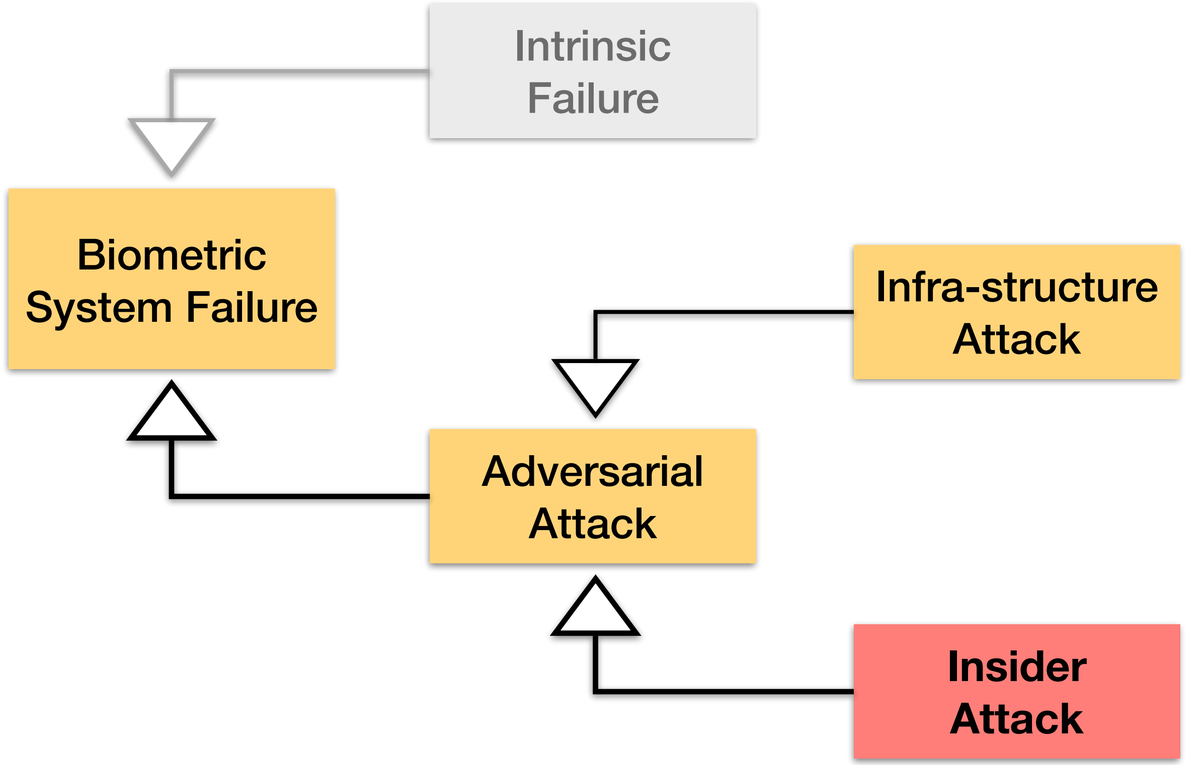
# Attacks

## Threat Model



# Attacks

## Threat Model





**Friendly Fire**

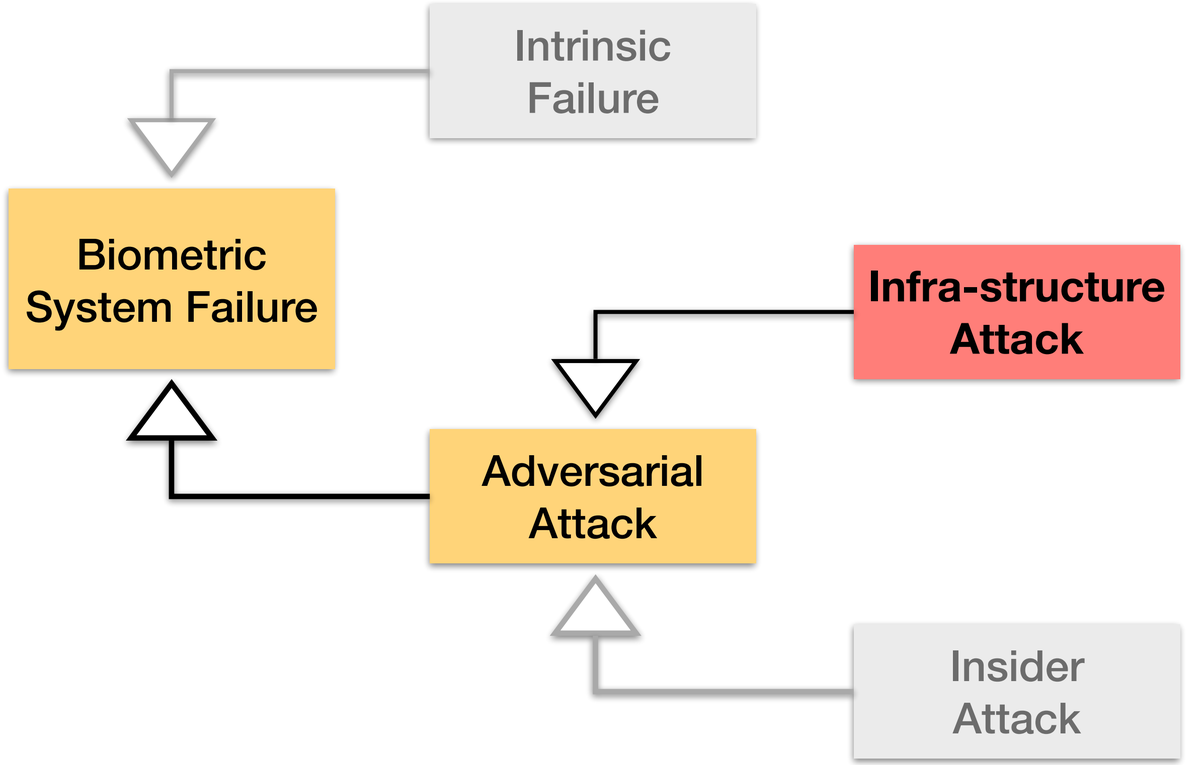
Attacks from *insiders* (system users or operators). Keep your system logs in good shape.



UNIVERSITY OF NOTRE DAME

# Attacks

## Threat Model

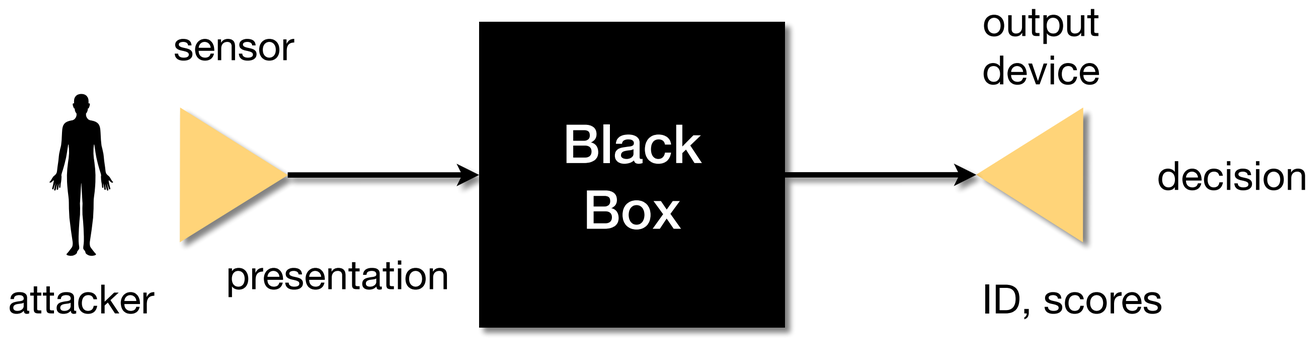




**Types**
Black box
White box

# 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).

Click2Houston.com 54°F SIGN IN

NEWS SPORTS THINGS TO DO FIND YOUR CITY DISCOVER HOUSTON LIFE WEATHER TRAFFIC NEWSLETTER

LIVE KPRC 2 News at 6 SHOW MORE

NEWS

Taisha Walker, Reporter

Published: September 18, 2019, 6:57 pm

Tags: News, Local, Crime

Sign up for our Newsletters

Enter your email here!

**Divorce deception: Man forges wife's name on divorce papers, police say**

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.

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

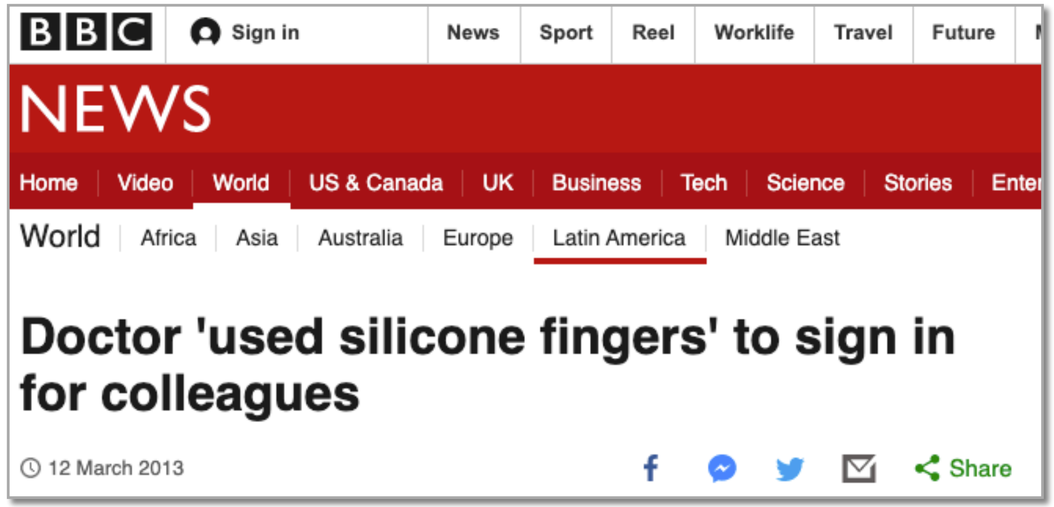
https://www.youtube.com/watch?v=_PoudPCevN0



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

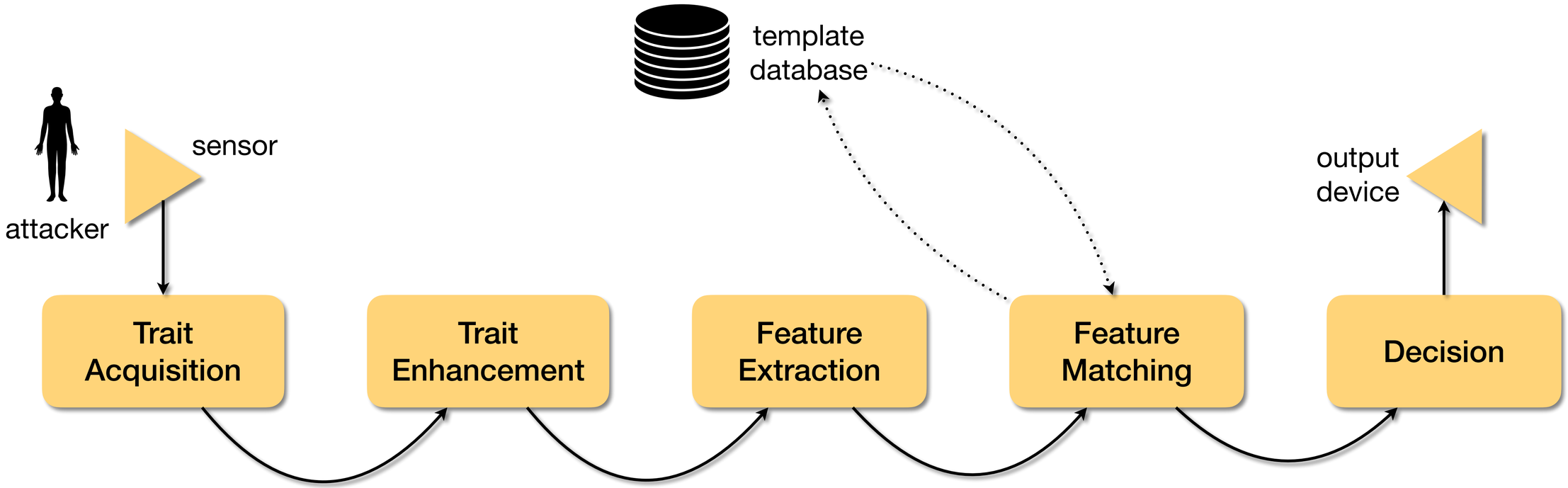
A Brazilian doctor faces charges of fraud after being caught on camera using silicone fingers to sign in for work for absent colleagues, police say.



UNIVERSITY OF NOTRE DAME

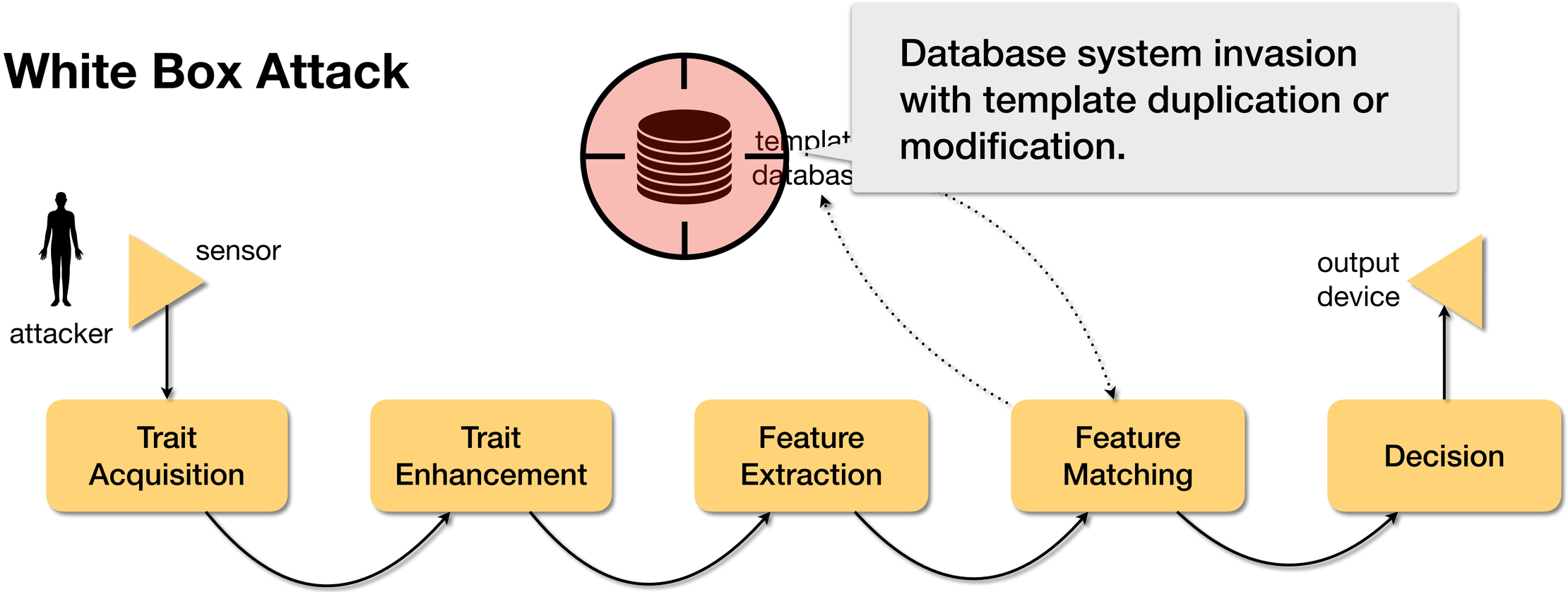
# Attacks

## White Box Attack



# Attacks

## White Box Attack

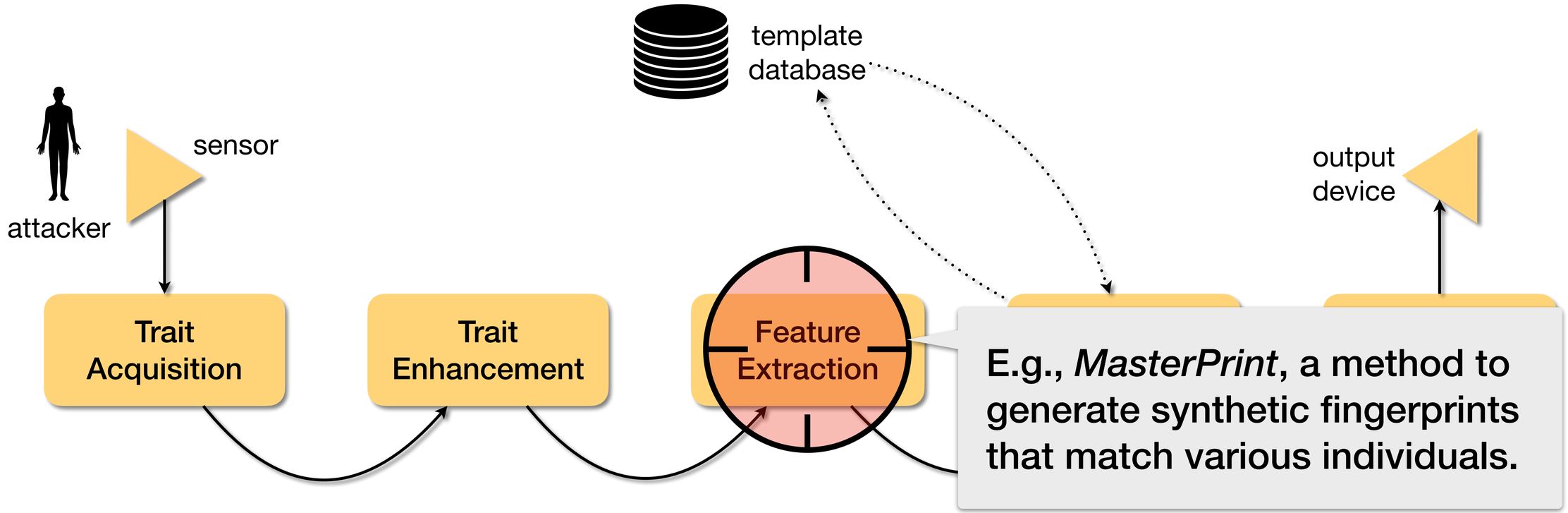





UNIVERSITY OF NOTRE DAME

# 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

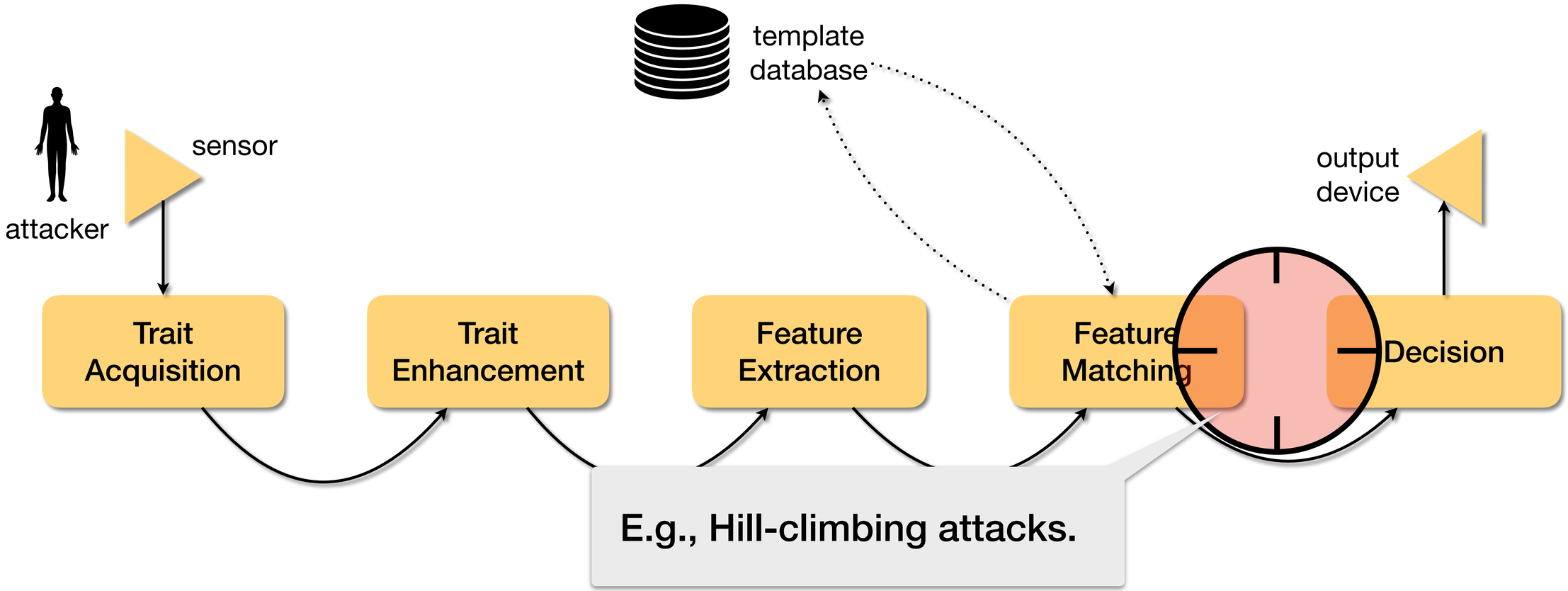
https://www.cse.msu.edu/~rossarun/pubs/RoyMemonRossMasterPrint_TIFS2017.pdf



UNIVERSITY OF NOTRE DAME

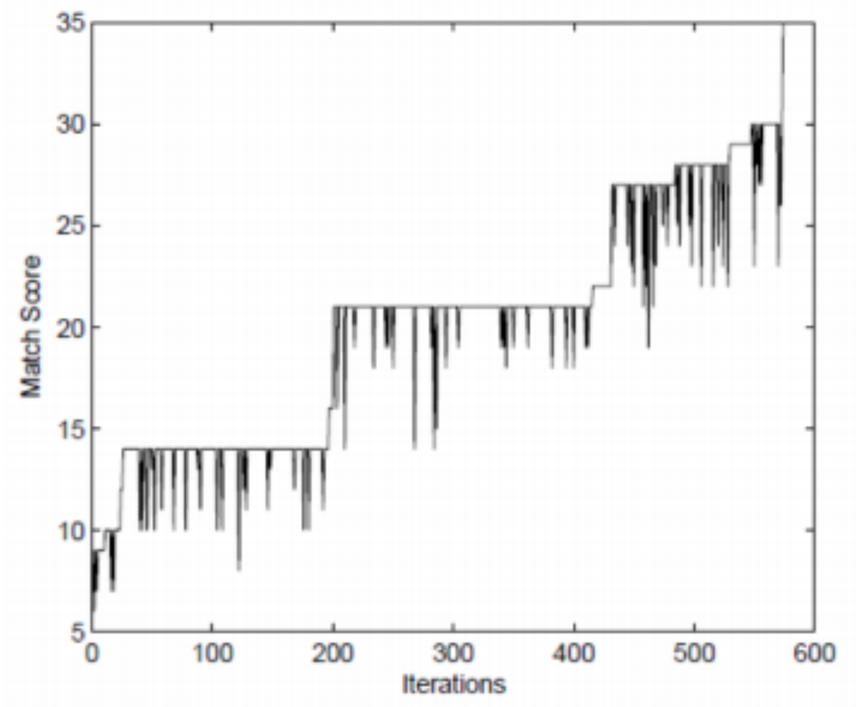
# Attacks

## White Box Attack



# Attacks

**Hill-climbing Attack**
E.g. Fingerprints

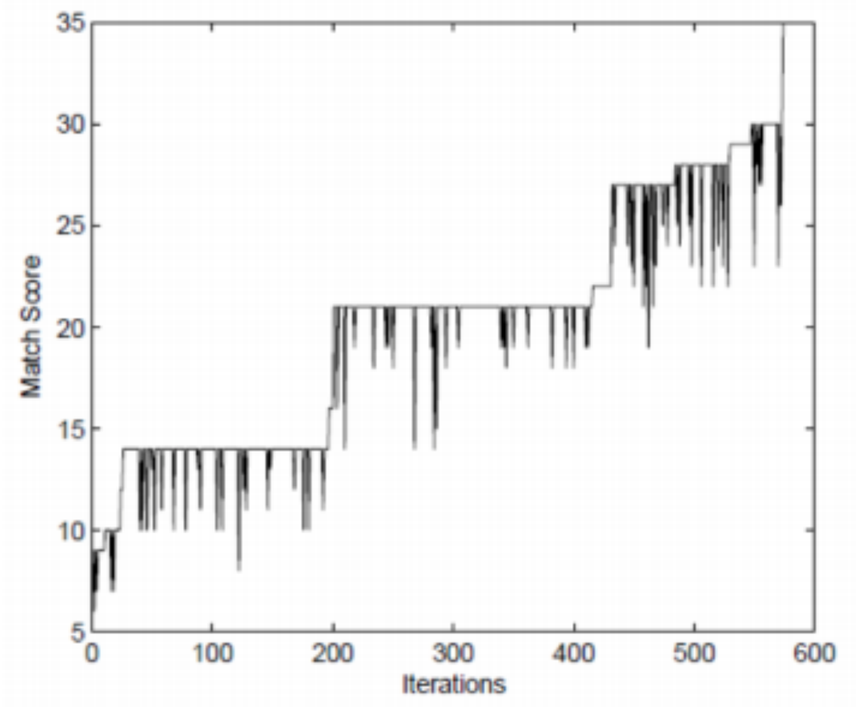



The attacker iteratively provides synthetic trait samples to the system. At each iteration, the attacker observes how the similarity scores are progressing.

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

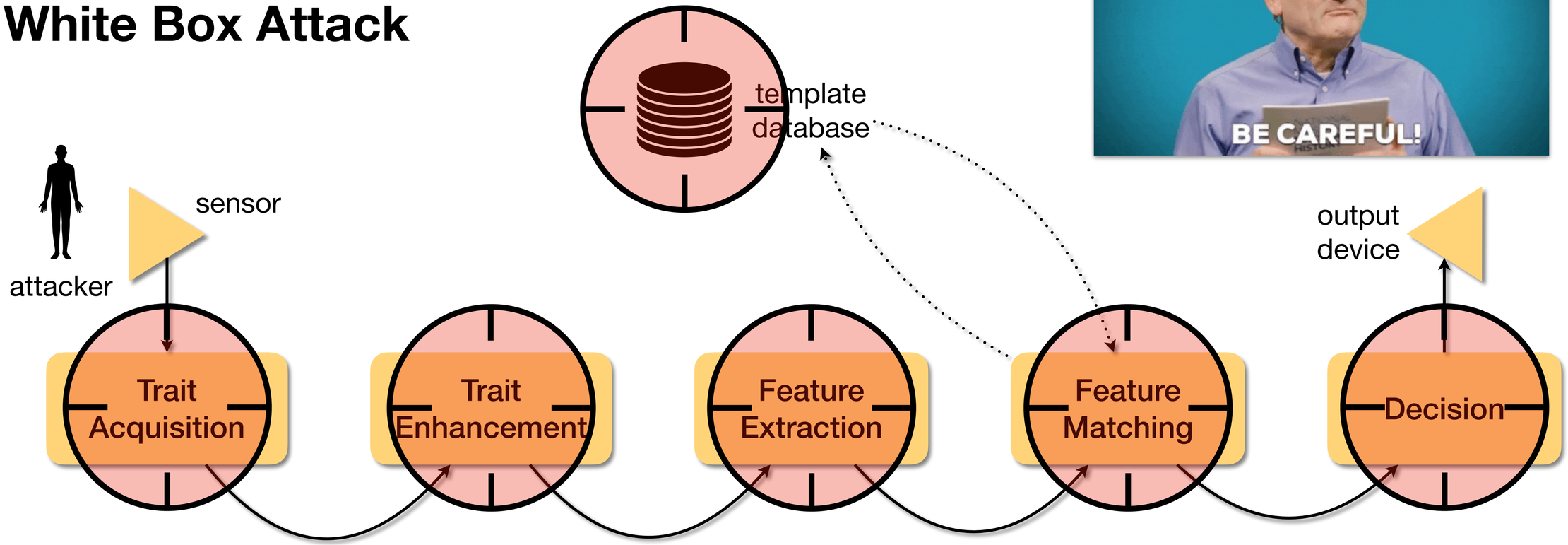



With such progress feedback,
the attacker can guide the generation of better and better synthetic fingerprint samples, up the point of trespassing the decision threshold.

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).