# I AM NOT WHO I AM

BYPASSING BIOMETRIC AUTHENTICATION SYSTEMS

- Oluwasefunmi Alabi

SHEF LABS TECHNOLOGY

# I Am Not Who I Am

Oluwasefunmi Alabi
[MOJ - UNIT27 - Havoc]

I love technology & freedom

Labs & Assessments

Snr. Security Engineer
Amazon
[Ex TikTok, Central Bank of Ireland, CCSI]

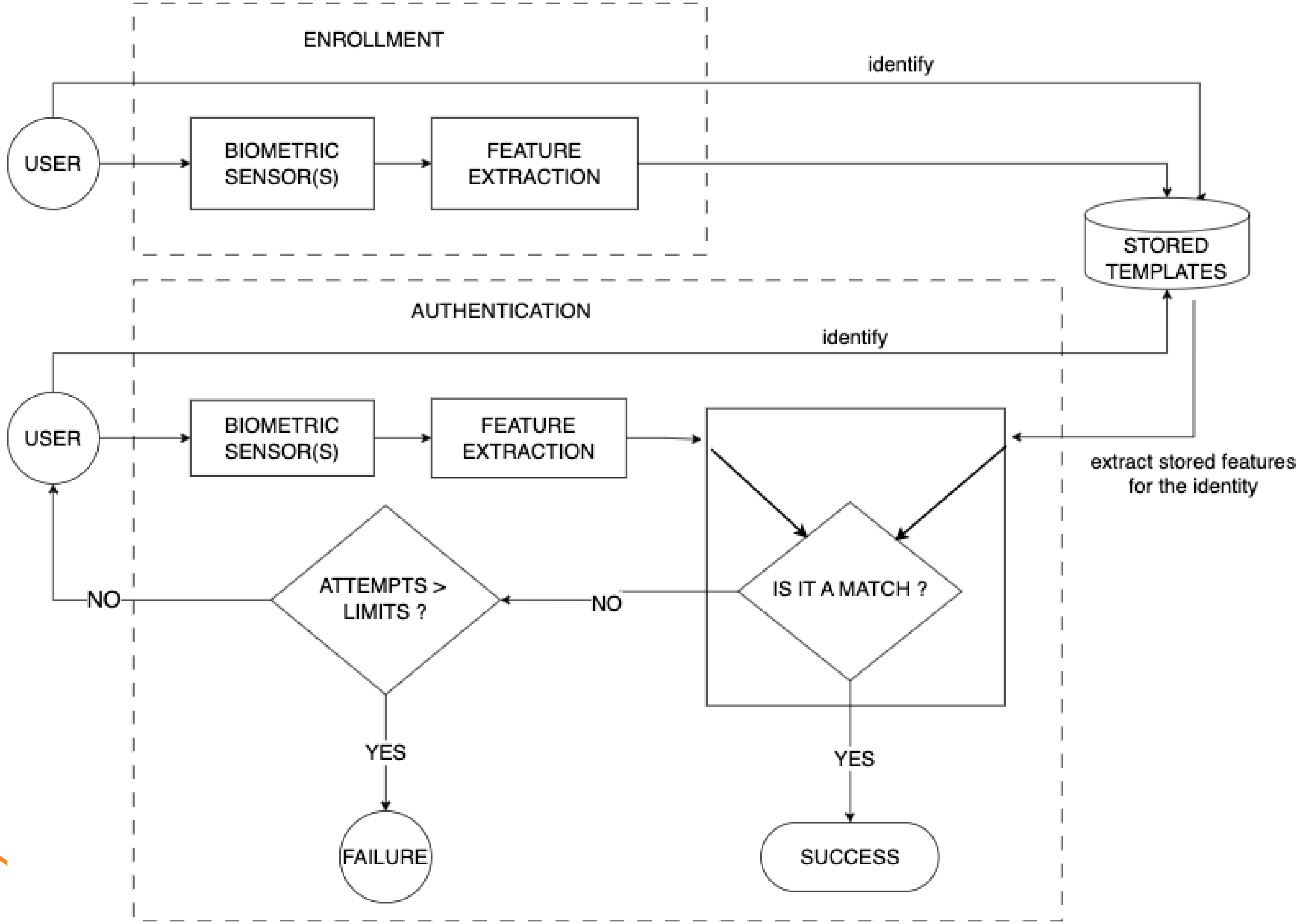
# Why Biometrics?

- Biometrics offer both convenience and security
- Increasingly replacing passwords and PINs
- Biometric market projected to reach $70B+ by 2030

# Types of Biometric Systems

- Fingerprint recognition
- Facial recognition
- Iris & retinal scanning
- Voice recognition
- Behavioral biometrics (gait, keystroke dynamics)

# How Biometrics work

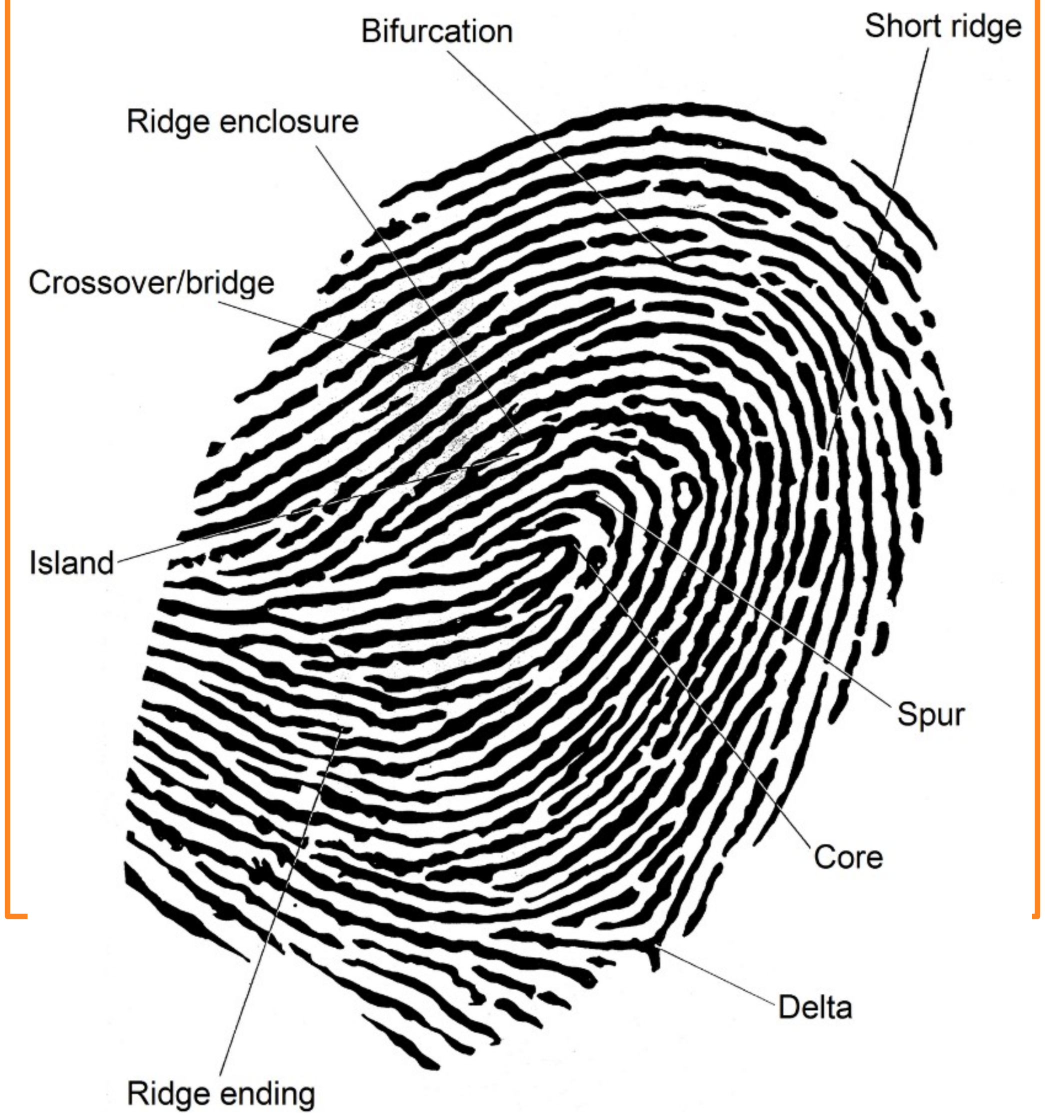


# Fingerprint Recognition

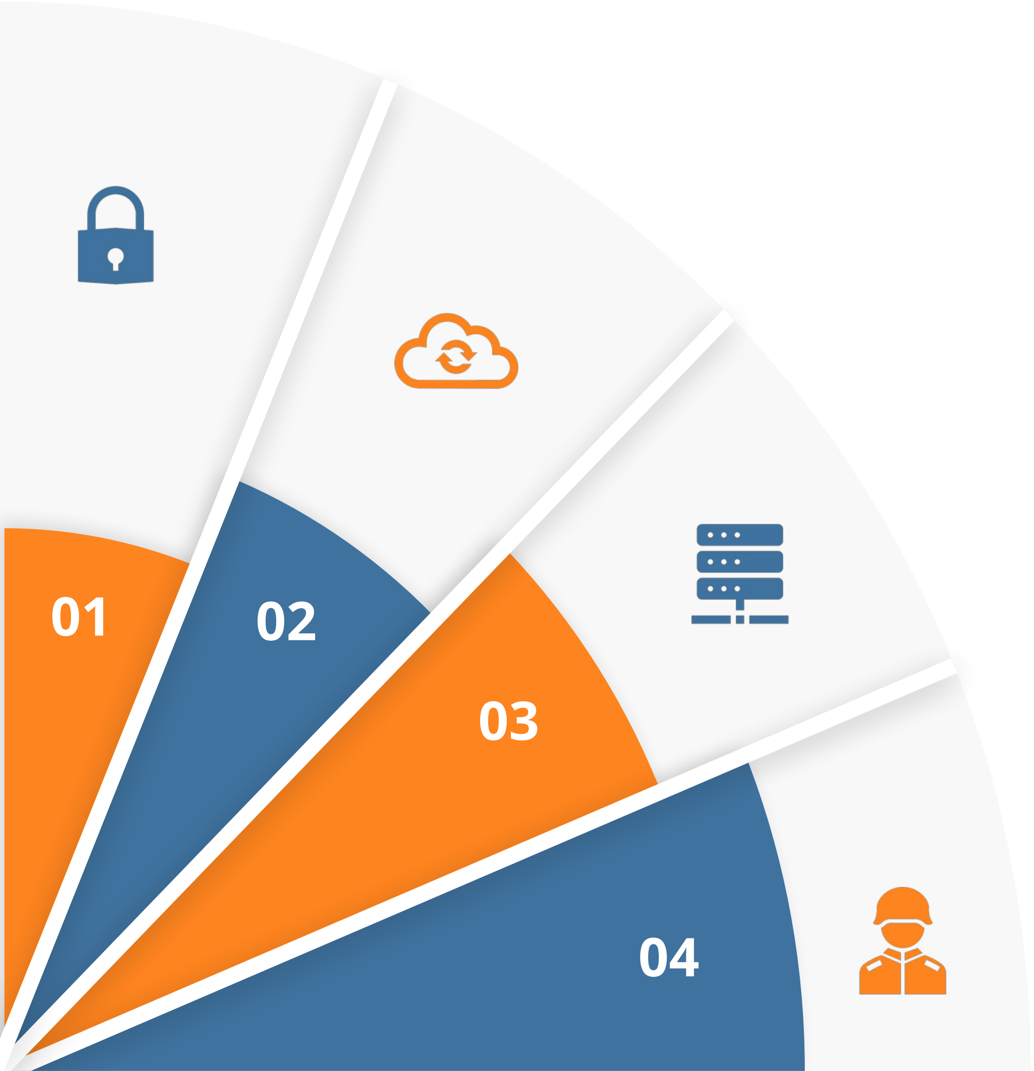
A fingerprint is an impression left by the friction ridges of a human finger.

Human fingerprints are detailed, nearly unique, difficult to alter, and durable over the life of an individual

Distinctive features of the fingerprint, generally known as minutiae



# Threat Surface Overview



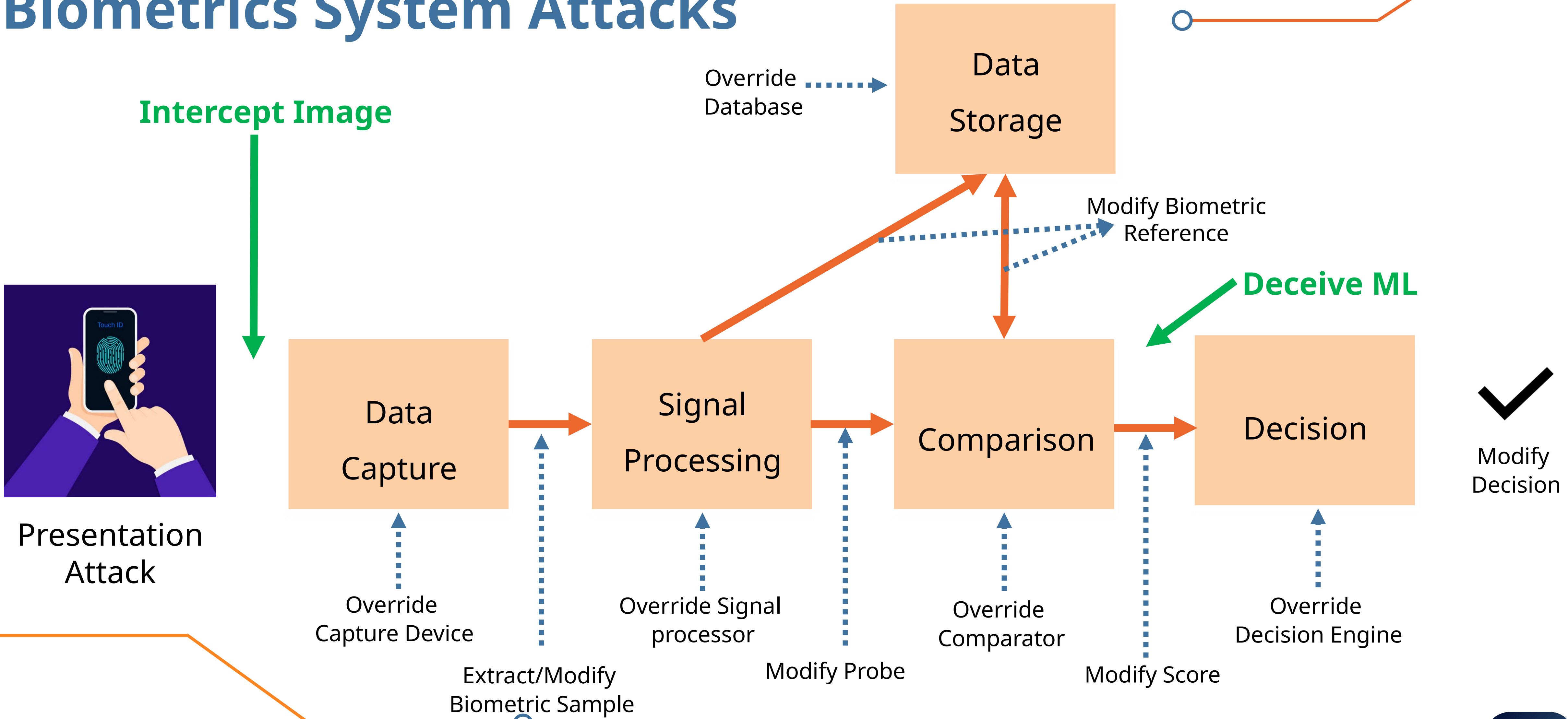
1 **Spoofing:** Fake fingerprints, faces, voices

2 Replay attacks using captured data

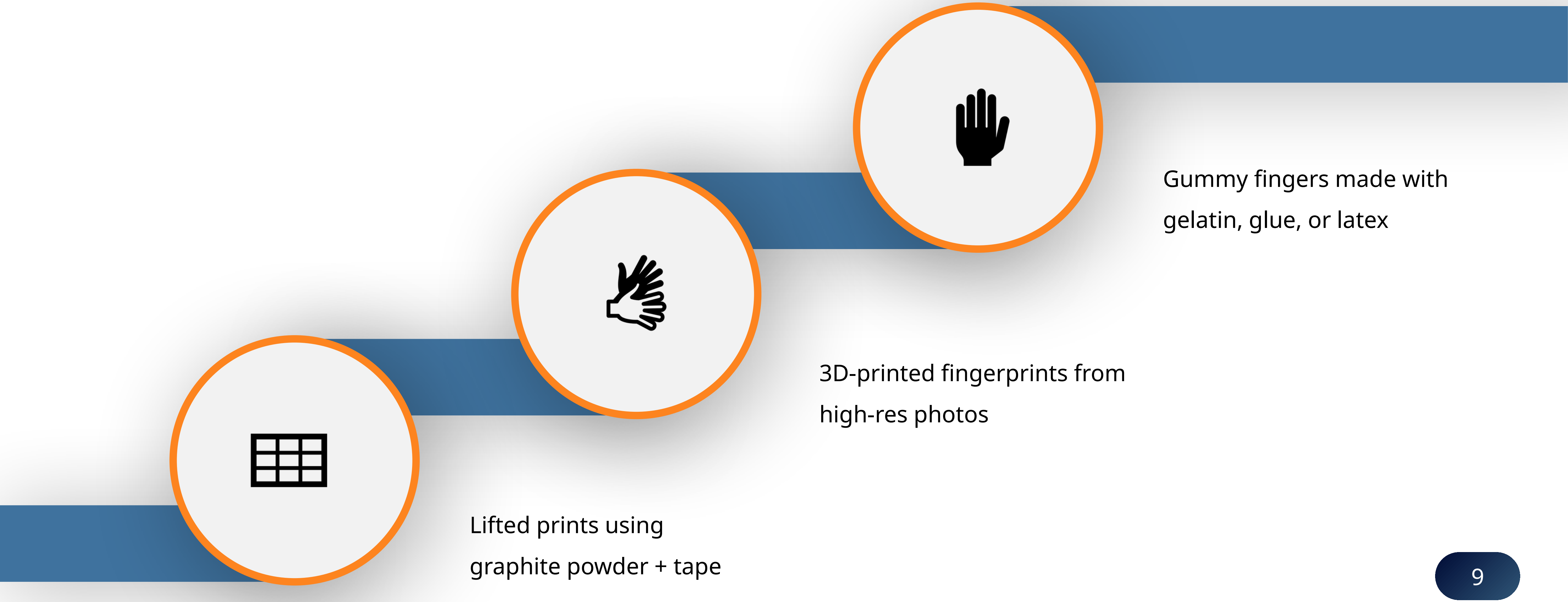
3 Sensor vulnerabilities and AI model manipulation

4 **Adversarial AI:** Tricking machine learning with crafted inputs

# Biometrics System Attacks



# Case Study: Fingerprint Hacking



Lifted prints using graphite powder + tape

3D-printed fingerprints from high-res photos

Gummy fingers made with gelatin, glue, or latex

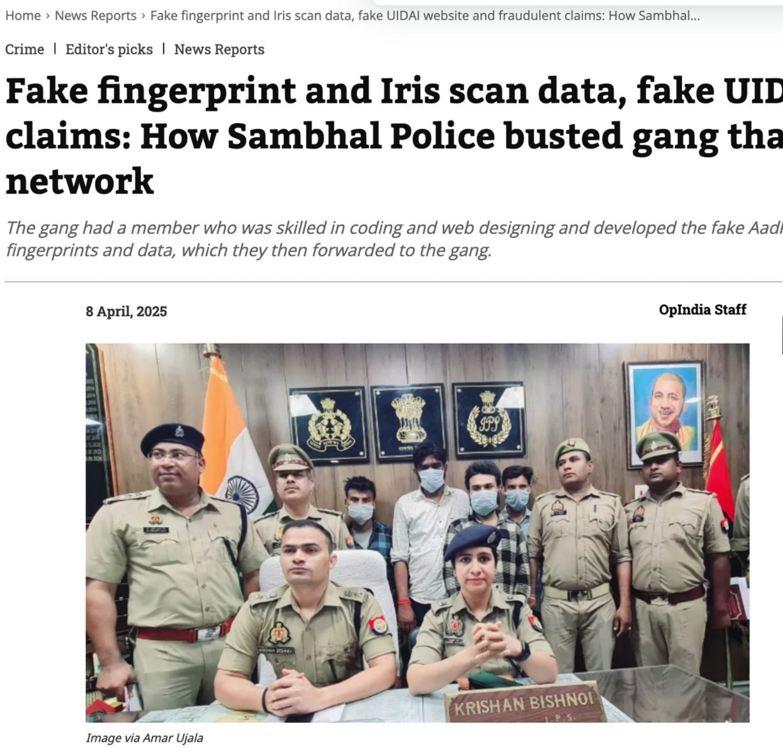
# Real-World Biometric Failures

📱 Chaos Computer Club bypassed iPhone TouchID with latex prints

🎭 Android facial unlock spoofed with selfies

👥 Chinese facial payment systems tricked with high-res images

# Biometrics Presentation Attacks



Home › News Reports › Fake fingerprint and Iris scan data, fake UIDAI website and fraudulent claims: How Sambhal... Updated: 8 April, 2025

Crime | Editor's picks | News Reports

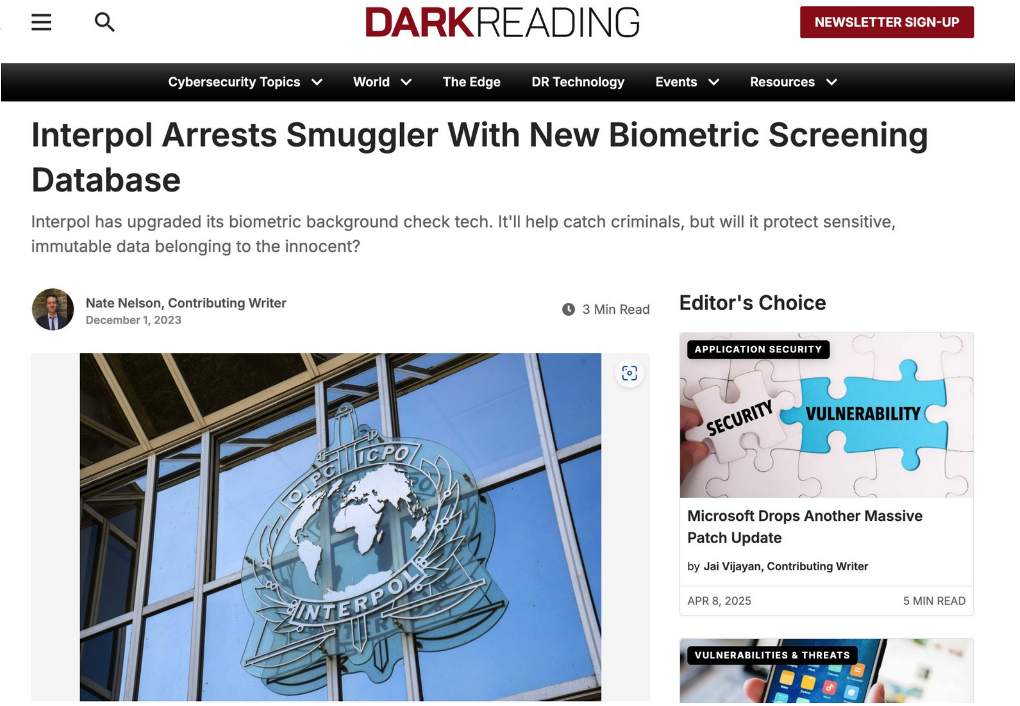
## Fake fingerprint and Iris scan data, fake UIDAI website and fraudulent claims: How Sambhal Police busted gang that ran a AADHAR forgery network

*The gang had a member who was skilled in coding and web designing and developed the fake Aadhaar portal. Retailers employed this portal to collect people's fingerprints and data, which they then forwarded to the gang.*

8 April, 2025 OpIndia Staff

*Image via Amar Ujala*

(2025) *Sambhal police bust Pan India gang who used to make changes to aadhar through fake documents to claim money through schemes, 4 arrested*, *OpIndia*. Available at: https://www.opindia.com/2025/04/fake-fingerprint-iris-scan-data-fake-uidai-website-and-fraudulent-claims-how-sambhal-police-busted-gang-that-ran-a-aadhar-forgery-network/



## Interpol Arrests Smuggler With New Biometric Screening Database

Interpol has upgraded its biometric background check tech. It'll help catch criminals, but will it protect sensitive, immutable data belonging to the innocent?

Nate Nelson, Contributing Writer
December 1, 2023

3 Min Read

Editor's Choice

APPLICATION SECURITY

Microsoft Drops Another Massive Patch Update

by Jai Vijayan, Contributing Writer

APR 8, 2025 5 MIN READ

VULNERABILITIES & THREATS

*Interpol arrests smuggler with new biometric screening database*. Available at: https://www.darkreading.com/cyber-risk/interpol-arrests-smuggler-biometric-screening-database - 2023

THE 420
Friday, Apr 11, 2025
Trending | Cyber Crime | Economic Fraud | Corruption | Legal | Tech Talk | Policy & Initiative | Opinion & Research | Fa
Home | About us | The420 Search Engine
Newslette

Biometric Cloning: 2 Hackers Arrested For Copying Fingerprints And Withdrawing Money Using Aadhar Based Payment

CYBER CRIME

## Biometric Cloning: 2 Hackers Arrested For Copying Fingerprints And Withdrawing Money Using Aadhar Based Payment

The420.in (2022) *Biometric cloning: 2 hackers arrested for copying fingerprints and withdrawing money using Aadhar based payment*, *The420.in*. Available at: https://the420.in/biometric-cloning-2-hackers-arrested-for-copying-fingerprints-and-withdrawing-money-using-aadhar-based-payment/

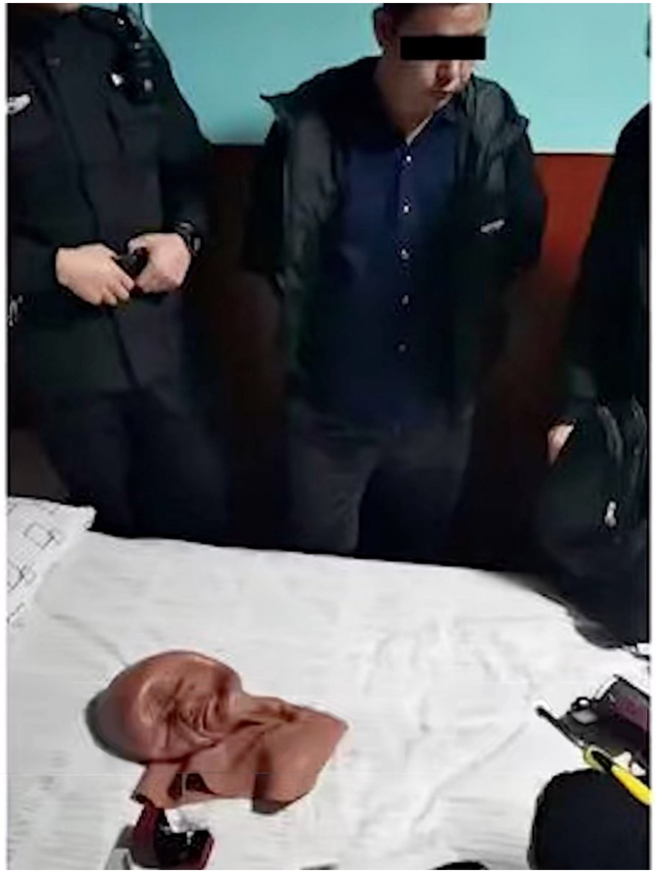
# Case Study: Facial Recognition Spoofing

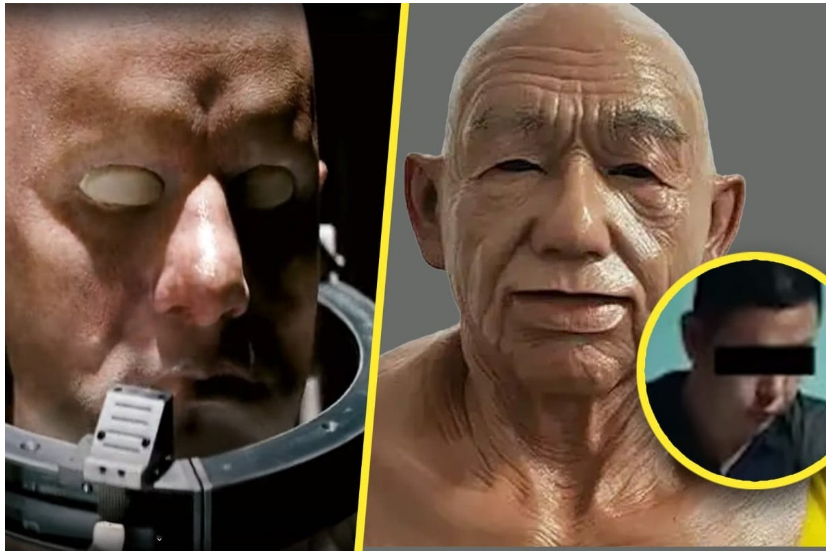
Spoofing with 2D printed photos, 3D masks, and videos

Adversarial patches can fool AI vision models (cause misidentification)

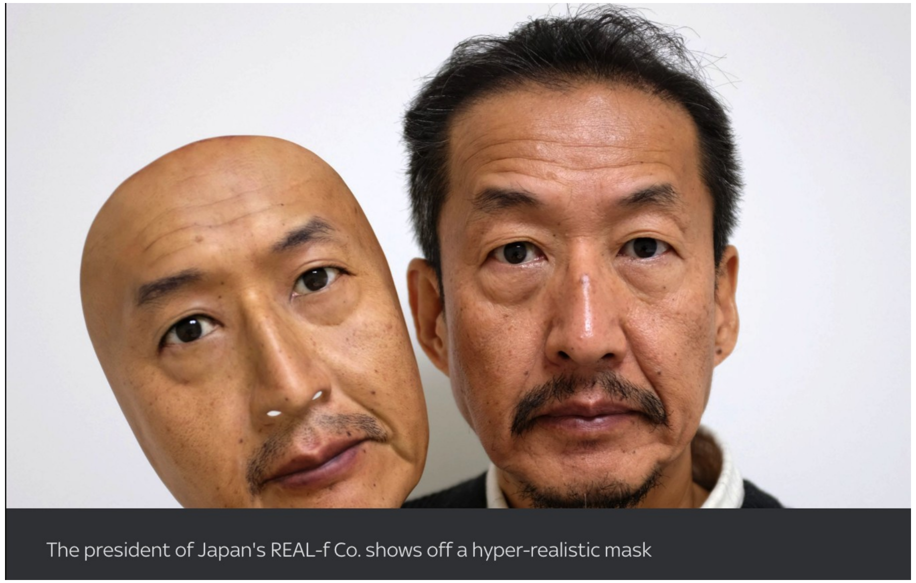
Deepfake tools increasingly capable and accessible

# Biometrics Presentation Attacks





Facial view of mask



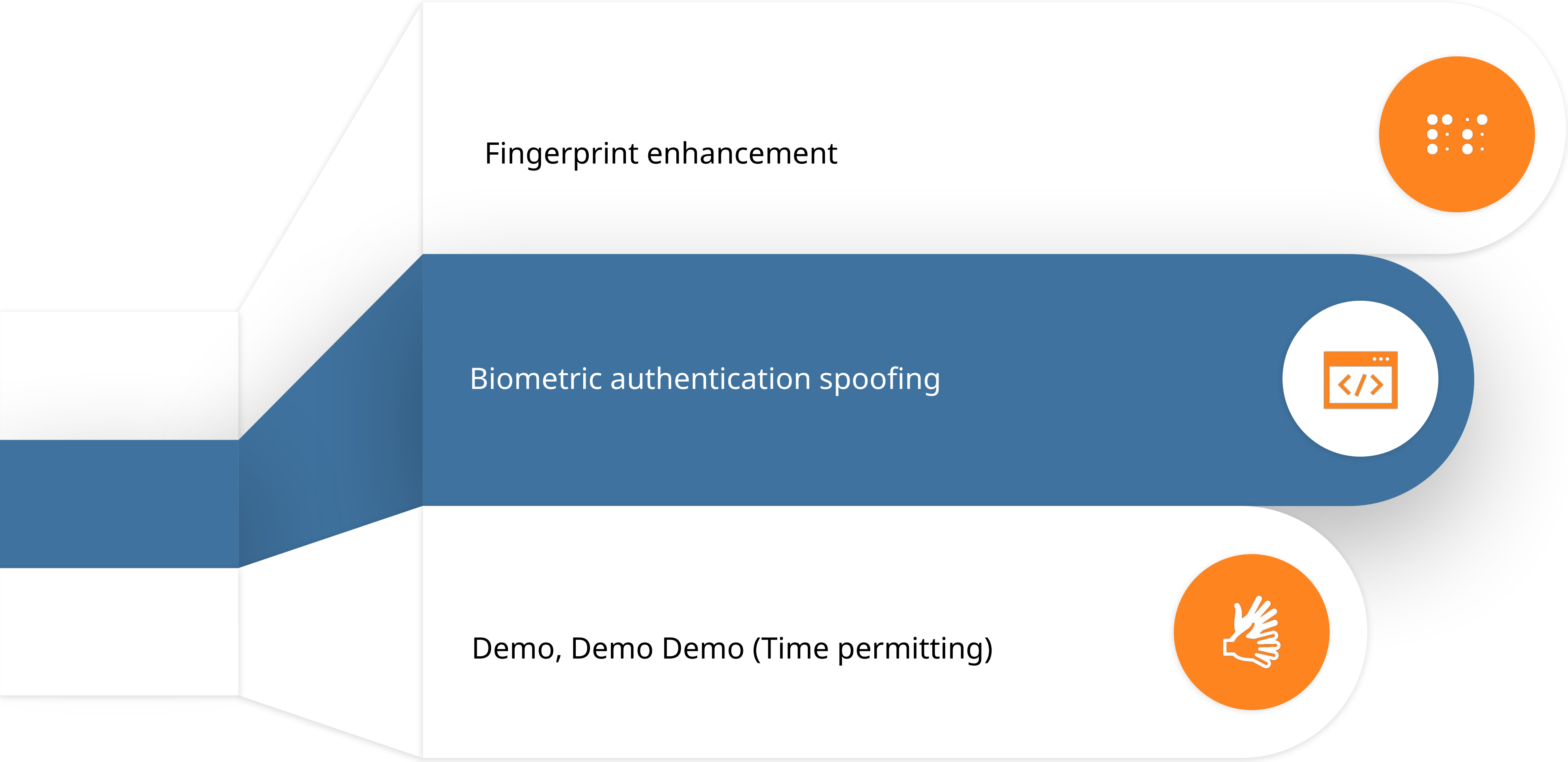
The president of Japan's REAL-f Co. shows off a hyper-realistic mask

President of Japan’s REAL-F Co with hyper-realistic mask

Shanghai China, 2nd April 2024 - Suspect apprehended with mask on table

*China burglar in hyper-real silicone old-man mask snared in 24 Hours* (2024) *South China Morning Post*. Available at: https://www.scmp.com/news/people-culture/trending-china/article/3256172/china-burglar-hyper-real-silicone-old-man-mask-steals-valuables-worth-us14000-caught-within-24-hours

# Live Demo or Tool Showcase



Fingerprint enhancement

Biometric authentication spoofing

Demo, Demo Demo (Time permitting)

# Defense Strategies

**Liveness detection**: Movement, warmth, blinking, pulse, pupil dilation

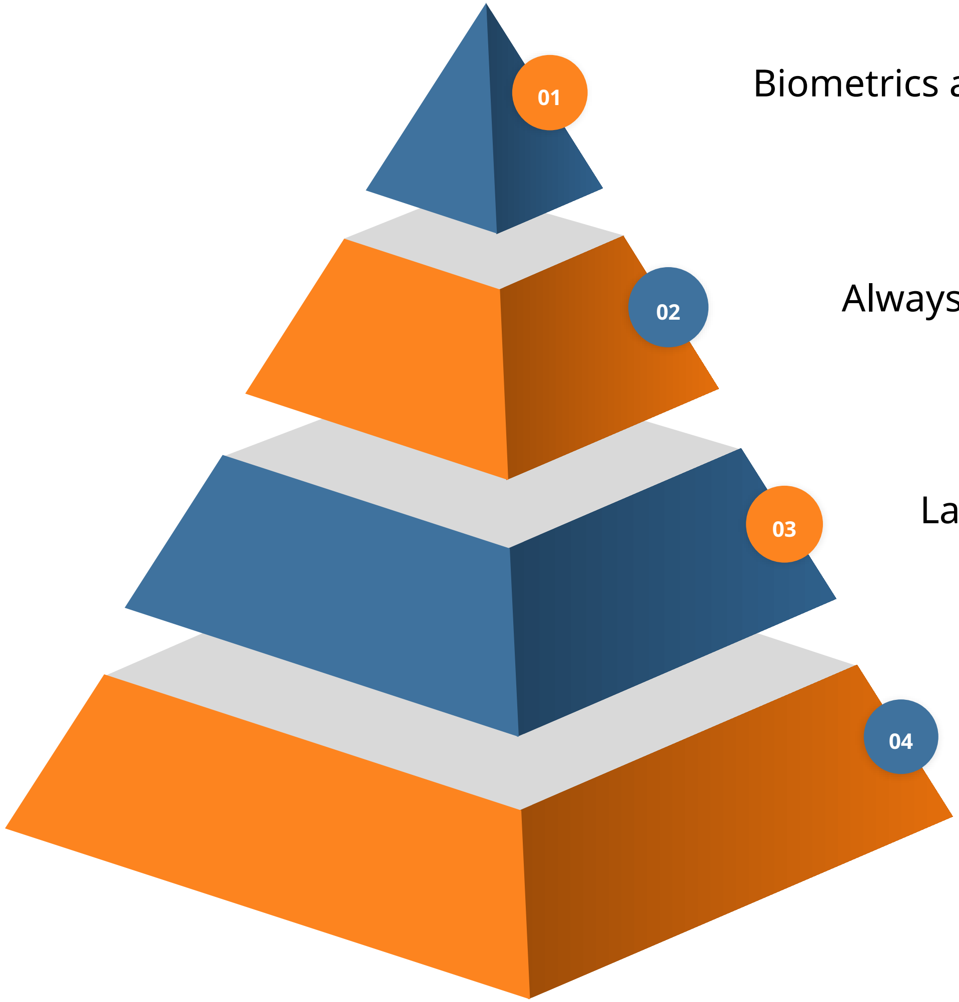
**Multi-modal systems**: Use two or more biometric types (face + voice + PIN)

**AI-driven spoof detection and secure sensor design:** Texture, reflection analysis

# Future of Identity

- Biometrics can’t be changed once leaked
- Facial recognition
- MFA and zero-trust systems still needed
- Biometric data permanence & ethical issues
- Exploration of decentralized storage (blockchain biometrics?)
- Privacy concerns: Tracking, mass surveillance, identity theft

# Key Takeaways



Biometrics are hackable and must not stand alone

Always assume spoofing is possible — and test for it

Layered defense is critical, not optional.: MFA, liveness checks, red teaming

Stay ahead with research, red teaming, and AI defense

# Q&A + CONTACT

THANKS FOR ATTENDING!

**LET'S CONNECT:**

- Twitter: @moj_alabi
- LinkedIn: Sefunmi A.
- Website & Blog: https://sheflabs.com

SHEF LABS CYBER ACADEMY MMXVII WE SECURE I.T BETTER

SHEF LABS TECHNOLOGY