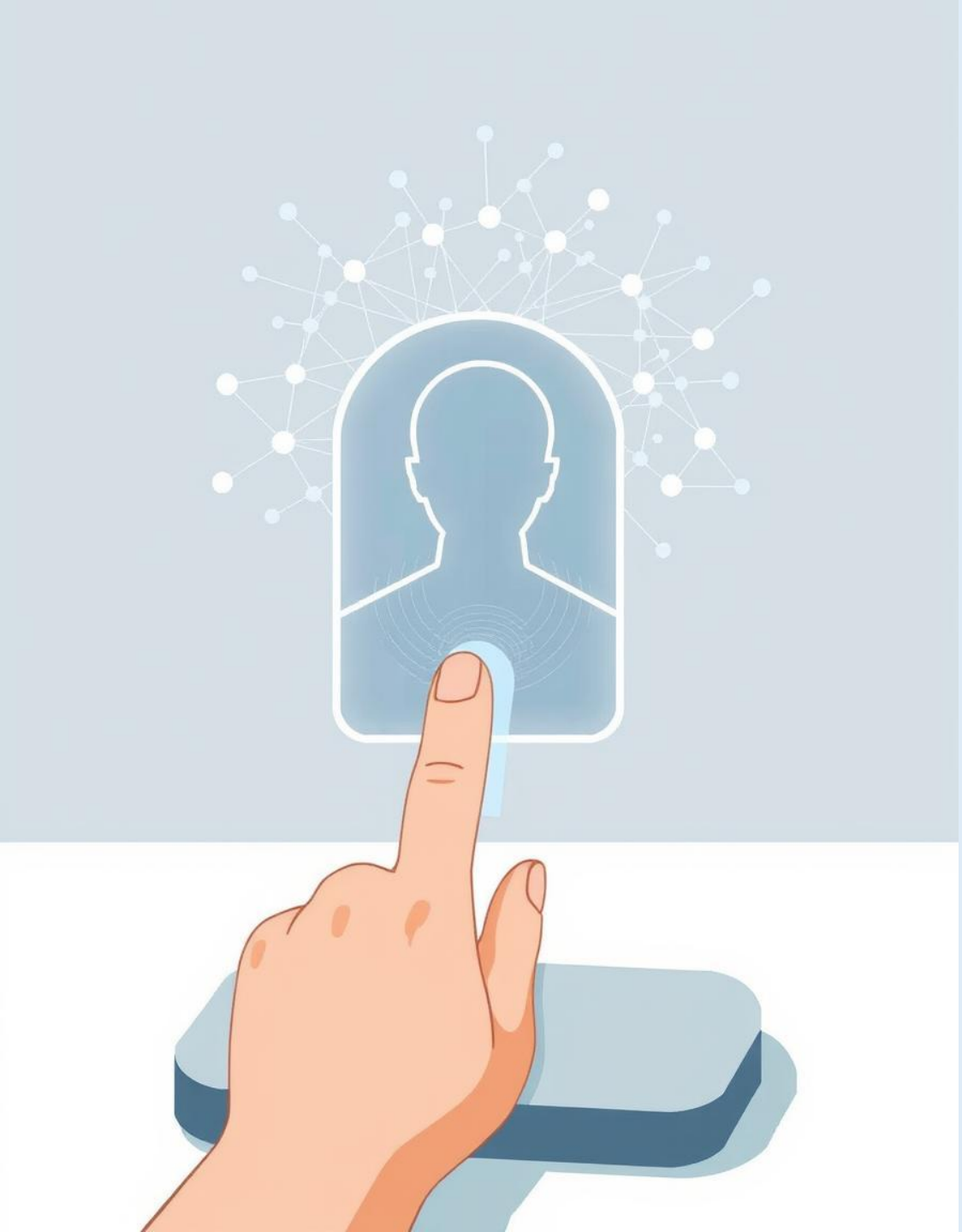


Biometric Spoofing: The Invisible Cyber Threat.

Understanding and mitigating the deceptive attacks targeting modern authentication systems.

Presented by:

- Jana Waleed Refaat
- Mohammed Hossam Sherif
- Youssef Khaled Shaarawy
- Mohammed Hossam Elsayed

Biometrics:

- unique measurable physical or behavioural characteristic
- used to verify someone's identity
- Used in phones, offices, airports, banks

Why Biometrics?

- **Enhanced Security:**
  - Stronger protection against unauthorized access.
- **Convenience:**
  - provide password-less authentication.
- **Efficiency:**
  - faster, more intuitive, reducing wait times and improving workflow.
- **Non-repudiation:**
  - offer genuine security advantages over traditional credentials.

The Question: Are they truly the safest way to log in or gain access to critical systems, or does this convenience hide a significant risk?

What is Biometric Spoofing?

1	**Definition:** ➢ **Deliberate imitation or manipulation** of biometric traits such as presenting a fake fingerprint, photo, or recorded voice. ➢ trick an authentication sensor and deceive authentication systems.
2	**Attacker's Goal:** ➢ Impersonation or gaining unauthorised access to secured systems, devices, or accounts. ➢ A common, everyday example is using a printed photo or a video replay to unlock a smartphone via facial recognition.
3	**The Irreversible Risk:** ➢ Unlike passwords, you cannot change a compromised biometric trait. ➢ Once compromised, the damage is **permanent and irreversible.**

Threat Model: Who is Attacking and How?

Passive Attacker

- Utilises publicly available data, to craft an attack.
- Data includes:
  - ➢ high-resolution photos from social media
  - ➢ voice recordings from videos

Active Attacker

- Wants to bypass liveness and detection protocols.
- This is done by:
  - ➢ Creating physical artifacts (molds)
  - ➢ Creating sophisticated digital constructs like **deepfakes**

Insider Threat & Supply Chain

Threats originating from within the organisation through compromised hardware and software components used in the biometric acquisition or processing pipeline.

Common Biometric Spoofing Techniques

Fingerprint Spoofing

- **Methods:** lifted prints, molds (silicone/gel), high resolution prints
- Attackers exploit visible artifacts like ridge shapes and pores.
- **Ease:** low cost, widely demonstrated in research by groups like the Chaos Computer Club.

Face Spoofing

- **Methods:** printed photos, video replays, screen replays, deepfake videos
- Posting selfies increases risk, as faces are public data
- Modern sensors use IR/depth analysis to combat flatness and lack of depth.

Voice Spoofing

- **Methods:** recorded audio playback, voice cloning, text-to-speech deepfakes
- **Used in:** in financial fraud, such as fake-CEO bank transfer calls.
- Voice data is easily captured from calls and online videos and can be and synthesized with AI..

Iris / Retina & Behavioral Spoofing

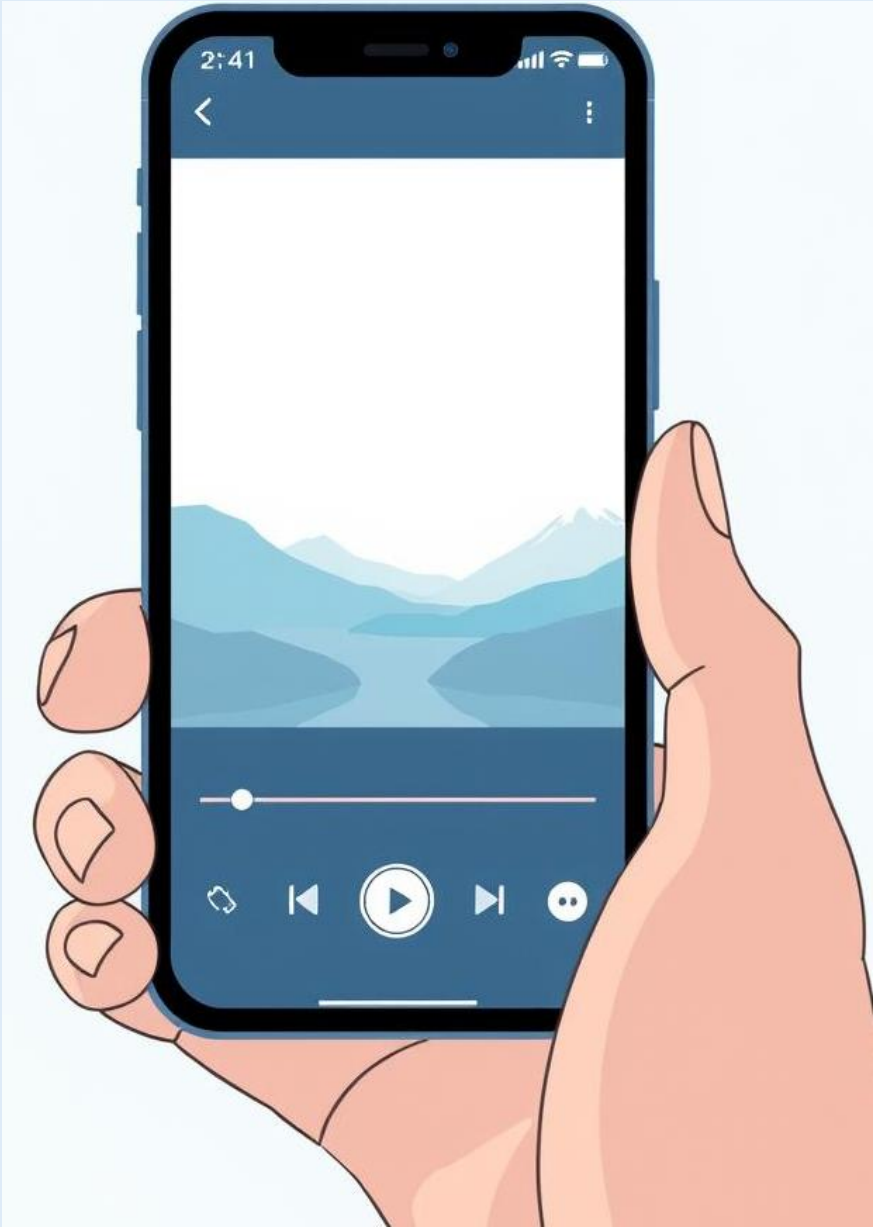
- **Methods:** attacks use printed images or contact lenses tricks
- Behavioural biometrics (e.g., typing patterns, gait) can be imitated by bots with enough data
- Higher-cost attacks but high-value environments (secure labs, borders)
- Behavioral biometrics are less “presented” but still spoof-able with enough data.

Real-World Impact: Exploitation by Organised Crime

Fraud rings are actively weaponizing biometric spoofing to breach high security systems and financial institutions.
The threat is no longer theoretical it's **happening now**.

- **80,000+ Face recognition spoof attempts** detected by ID.me in between June 2020 and January 2021 alone.
- **Synthetic Video Attacks:**
  - ➢ Fraud rings using deepfakes to bypass financial and insurance identity verification
- **Cross-Sector Targeting:**
  - ➢Banking, insurance, government, and healthcare systems increasingly targeted by organised crime.

The need for robust defence mechanisms is critical as sensitive data and assets are at stake.



Presentation Attack Detection (PAD): The New Defence Layer

PAD technology distinguishes genuine biometric samples from fabricated ones by analysing texture, movement, physiological markers, and environmental inconsistencies in real time.

Level 1: Basic Detection

➢Blocks simple , static spoofs like printed photos, replayed videos, static images providing a baseline security measure.

Level 2: Advanced Detection

➢Counters sophisticated attacks including 3D masks, deepfakes, synthetic audio by performing liveness analysis.

Level 3: Continuous Protection

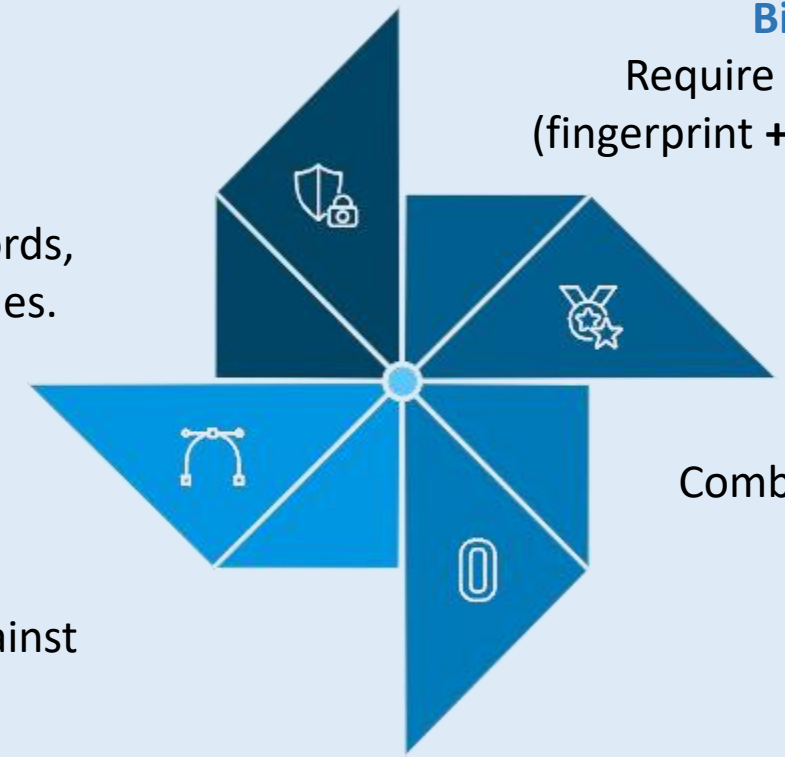
- Involves real-time learning systems that adapt to emerging attack vectors and zero-day threats, maintaining an agile defence posture.

Multi-Layered Security Strategies Against Spoofing

- Single-layer defences are insufficient.
- Leading organisations implement comprehensive security ecosystems combining multiple authentication factors.

Biometric Fusion
Require multiple distinct traits (fingerprint + face + iris) for verification.

MFA
Combine biometrics with passwords, security tokens, or one-time codes.



Zero-Trust
Combine Never trust, always verify every access request requires fresh authentication.

Continuous Testing
Perpetually update PAD systems against evolving attack methodologies.

Behavioural Analysis
Monitor usage patterns and flag anomalous access attempts automatically.

Challenges and Future Directions

Emerging Challenges

- AI deepfakes growing more realistic and difficult to detect.
- Privacy concerns around biometric data collection and storage
- Ethical implications of constant surveillance and identification
- Cross-border regulatory inconsistency.

Future Innovation

- International projects like TABULA RASA and BEAT advancing anti-spoofing.
- Machine learning models detecting deepfakes with higher accuracy
- Quantum-resistant biometric encryption standards
- Collaborative threat intelligence sharing across industries.

Case Study: Deploying Hardened Biometric Authentication

A case study made by the **leading identity security firm 1Kosmos** deployed advanced Presentation Attack Detection (PAD) to counter real-time synthetic video attacks targeting financial institutions demonstrating its tangible benefits in a live, production environment.

60%

Fraud Reduction

Decreased fraudulent access attempts across financial services clients by deploying sophisticated anti spoofing.

99.2%

Detection Accuracy

Successfully identified blocked and spoofed biometric samples in live transactions

0.8%

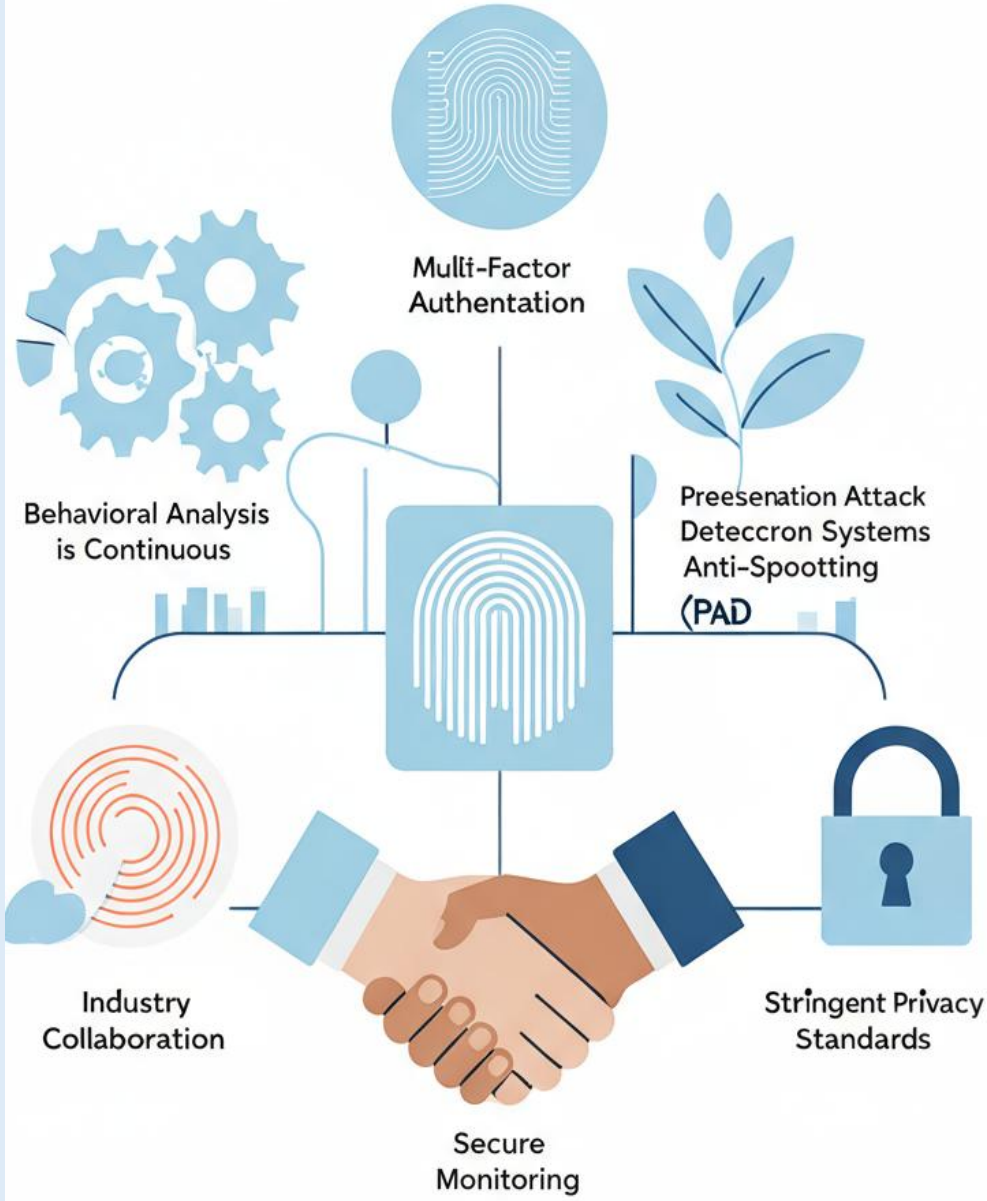
False Positive Rate

Minimal impact on legitimate user experience, ensuring that only true fraud attempts are blocked.

Key Takeaway: Staying Secure
Staying Secure in the Biometric Race

- Biometric spoofing is a growing cyber threat.
- Mitigation against it requires multi-layered defences, continuous innovation, dynamic, evolving, and anticipatory strategies.

- Embrace Layers: Implement comprehensive multi-factor authentication and biometric fusion.
- Innovate Always: Continuously update PAD systems to counter evolving deepfake methodologies.
- Share Intelligence: Collaborate across the industry to identify and respond to new threats swiftly.
- Protect Identity: Maintain stringent privacy and encryption standards for all biometric data.



From Theory to Reality: The Spoofing Challenge

We've explored how biometric spoofing works, now let's see how we can detect and defend against it through our live demo where we'll show:

- Real-time demonstration of a **simulated biometric spoofing attempt.**
- How detection systems recognize **liveness** and **authenticity.**

Now on to our LIVE Demo

Detecting and Defending against Biometric Spoofing