BixeLab

17 February 2023

Revised edition 13 September 2023

I.D. RISK ALERTS

Open Source Edition

Identity and Biometric Vulnerabilities | Threats and Risks | Mitigations

Welcome

The I.D. Risk Alerts newsletter (open source edition) is a quarterly newsletter with analysis on recent ID fraud, biometric threats and identity vulnerabilities that are already known in the public domain. A comprehensive bi-annual report is will also be available to BixeLab subscribers soon.

Updated FIDO Testing Standards

The FIDO Alliance has released a new set of criteria for biometric testing. This includes BioLevels 1,1+,2 and 2+. The levels 1 & 2 will require **25** test subjects, whereas levels 1+ & 2+ require **245** (as per the previous FIDO standard).

Vendors seeking FIDO certification for biometric solutions should be mindful of the new criteria.

New privacy laws (AU)

Australia is releasing new privacy laws, including extensive reference to biometrics. Detailed analysis will be published by BixeLab within the next month.

Source from Essex Police UK

The brothers wore latex masks during the robbery

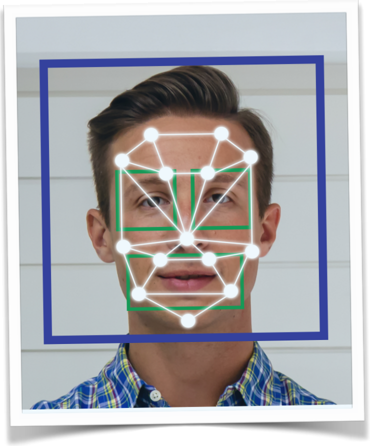
Latex Face Mask

Modality: **DNA**, Attack Instrument: **Latex Mask**

Location: **UK**, Date of report: **27 Sept 2021**

Latex masks were used in a robbery undertaken in the UK. Two brothers have been jailed following a jewellery shop robbery in Epping (UK). The pair wore extremely lifelike latex masks—simulating aged faces and balding heads—to avoid identification. During the robbery, the offenders threatened staff with bladed weapons and restrained one with cable ties. A valuable watch was stolen. Although the masks effectively disguised the offenders, they were later identified by DNA matching after evidence (including the masks) was found in the boot of their car.

- **Potential targets**: any systems secured by human face recognition, potentially including immigration controls, passports, financial services, law-enforcement.
- **Mitigation Strategy**: training for frontline officers on detection and risks associated with latex masks. A second authentication factor should be used to mitigate risk, and PAD testing for automated systems.
- **Criticality: High** - this type of attack is possible in both human and auto face identification systems, and of particular concern for enrolment attacks.



What is Presentation Attack Detection (PAD)?

The use of an artificial device, like a latex mask, to impersonate a person's biometric(s) in order to manipulate a biometric system is known as a presentation attack. The process of detecting and alerting to such attacks (known as presentation attack detection, or PAD) in biometric systems is critical for the utility and reliability of biometrics. Ongoing PAD assessment is crucial, even where a biometric system has an extremely low error rate, as it might be susceptible to novel presentation attacks. For additional training, BixeAcademy provides a range of biometric training courses.

What is Biometric Identity Binding?

Biometric identity binding (also referred to as 'anchoring') refers to the process of linking a validated individual identity to an associated biometric record. This binding allows confidence that a specific individual has been identified when there is a later biometric match.

Revised edition 13 September 2023

Fake Fingerprints

Modality: **Finger**, Attack Instrument: **Rubber Thumb**
Location: **India**, Date of report: **Feb 2023**

Police in India have arrested two suspects from a gang responsible for defrauding 440 victims using cloned fingerprints. The suspects were using Aadhaar-Enabled Payments System (AEPS) to steal money from victims' accounts. They were using a biometric machine, a rubber thumb impression printer, polymer liquid and temperature modulator to clone fingerprints. The suspects had collected the Aadhaar numbers and fingerprints of more than 100,000 people in India. Police found the gang was involved in 128 fraud cases.

•**Potential targets**: population registries using fingerprints, digital banking apps.

•**Mitigation Strategy**: use of two or more authentication factors, and PAD testing on detection of synthetic fingerprint. Training for frontline users in this risk type.

•**Criticality: Med-High** - a particular concern for unsupervised fingerprint systems that do not have tested PAD.

Deep Fake Faces

Modality: **Face**, Attack Instrument: **Deep Fakes** Location: **China**, Date of report: **Apr 2021**

A high-profile tax fraud scheme has been detected in China, where two offenders used facial images bought from the black market to create synthetic identities and set up a fake company issuing invoices worth up to 500 million yuan. The methods used to cheat the system included simulated eye movement and lip-syncing videos, bypassing facial recognition security measures of the relevant electronic identity verification system (eIDV).

- **Potential targets**: systems relying on using face recognition for remote identity verification.
- **Mitigation Strategy**: PAD for systems to detect the use of deep fake images. Additional audit steps in eIDV systems to permit manual review.
- **Criticality: High** - any eIDV system not assessed recently or at PAD 2 level may be at risk.