BixeLab

19 June 2023

Revised edition 13 September 2023

I.D. RISK ALERTS

Open Source Edition

Identity and Biometric Vulnerabilities | Threats and Risks | Mitigations

Welcome

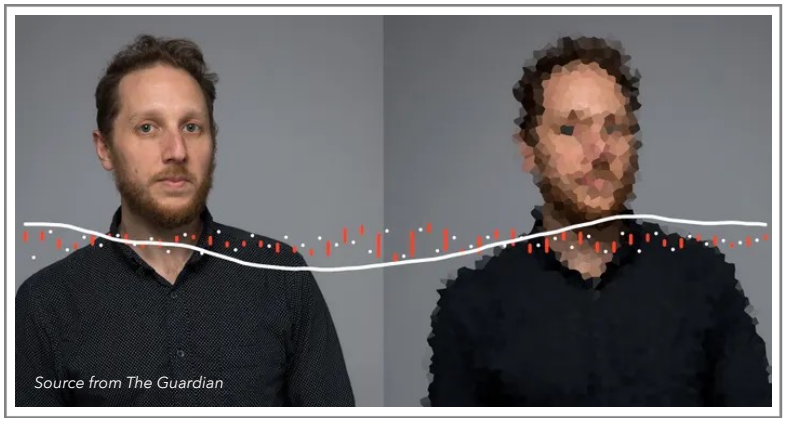
The I.D. Risk Alerts newsletter (open source edition) is a quarterly newsletter with analysis on recent ID fraud, biometric threats and identity vulnerabilities that are already known in the public domain. A comprehensive bi-annual report will also be available to BixeLab subscribers.

Comprehensive AI Regulations - EU

The European Parliament is developing an AI Act. Once approved, this will be world's first set of laws regulating Artificial Intelligence. The draft rules follow a risk-based approach and establish obligations for providers and users, depending on the level of risk the AI can generate.

NIST Identity and Access Management

The National Institute of Standards and Technology (NIST) has published a draft roadmap for identity and access management and is now seeking inputs before finalisation. It provides methodology and processes for identity risk management processes and assurance level selections.



AI Generated Voices

Modality: **Voice**, Attack Instrument: **AI Generated Voice**

Location: **AU,UK**, Date of report: **March 2023**

A Guardian journalist used an AI-generated voice to replicate their own voice, successfully allowing them to simulate unauthorised access to their personal Centrelink self-service account. In order to use voice authentication, individuals must possess the account holder's customer reference number (which is typically not publicly accessible but often included in correspondence), and samples of the account holder's voice. This incident is similar to an earlier instance where a cybersecurity researcher in the UK successfully accessed their bank account using a synthetic clone voice created with easily accessible AI technology.

- **Potential targets**: any system using voice recognition as a standalone form of authentication, particularly those used by government agencies and organisations that hold sensitive information such as financial institutions.
- **Mitigation Strategy**: implement multi-factor authentication and ensure currency of Presentation Attack Detection (PAD) testing, including for new and emerging threats.
- **Criticality: High** - significant vulnerability for organisations using standalone voice authentication for access to sensitive information, and for services which may later be presented with stolen information.

What is deep fake fraud?

United States legislation defines "deep fakes" as:

2018 Malicious Deep Fake Prohibition Act: "the term 'deep fake' means an audiovisual record created or altered in a manner that the record would falsely appear to a reasonable observer to be an authentic record of the actual speech or conduct of an individual."

2019 DEEP FAKES Accountability Act: "The term 'deep fake' means any video recording, motion-picture film, sound recording, electronic image, or photograph, or any technological representation of speech or conduct substantially derivative thereof— (A) which appears to authentically depict any speech or conduct of a person who did not in fact engage in such speech or conduct; and

(B) the production of which was substantially dependent upon technical means, rather than the ability of another person to physically or verbally impersonate such person."

Digital Driver's Licence

Modality: **Identity Theft**, Attack Instrument: **Stolen data**
Location: **United States**, Date of report: **March 2023**

A US man has been sentenced to over five years in federal prison for defrauding financial institutions using a state-authorised digital driver's licence (DDL) mobile app. By stealing the personal information of an incarcerated individual, the perpetrator successfully opened accounts and obtained loans using the DDL. He also deposited fraudulent checks at various banks. The case highlights the vulnerability of digital identification systems and the need for robust security measures.

• **Potential targets**: government departments, financial institutions relying on digital identification systems for customer verification and account management, individuals whose personal information is stolen.

• **Mitigation Strategy**: identification and licensing authorities should employ multi-factor authentication and conduct regular PAD testing. Service providers at risk of presentation of stolen information should maintain risk awareness training, document verification processes, and use second-tier authentication (preferably biometric).

• **Criticality:** Med-High - financial institutions are attractive targets due to potential financial gain. Government agencies issuing digital IDs may be targeted to gain unauthorised access to sensitive personal information.

Passports and Medicare Cards Stolen

Modality: **Identity Theft**, Attack Instrument: **Stolen data**
Location: **Australia**, Date of report: **Apr 2023**

Australian lending company, Latitude Financial, has suffered a data breach resulting in the theft of sensitive customer data, including passport details and Medicare numbers. The breach was discovered by the company during an investigation of a third-party data storage provider, which had been accessed by an unauthorised party. The exposure of this information and potential for its future use in identity theft creates significant risks for any system authenticating users through personal details alone.

- **Potential targets**: Service providers which authenticate users via personal data, and any organisation that holds sensitive personal information.
- **Mitigation Strategy**: implement multi-factor authentication with liveness testing, secure first-party and third-party data storage, and provide training on risks associated with stolen personal data.
- **Criticality:** High - affects many service providers and organisations, with the potential for identity theft, reputational damage and loss of trust, as well as financial impacts.