BixeLab

1 March 2024

I.D. RISK ALERTS

Open Source Edition

Identity and Biometric Vulnerabilities | Threats and Risks | Mitigations

Welcome

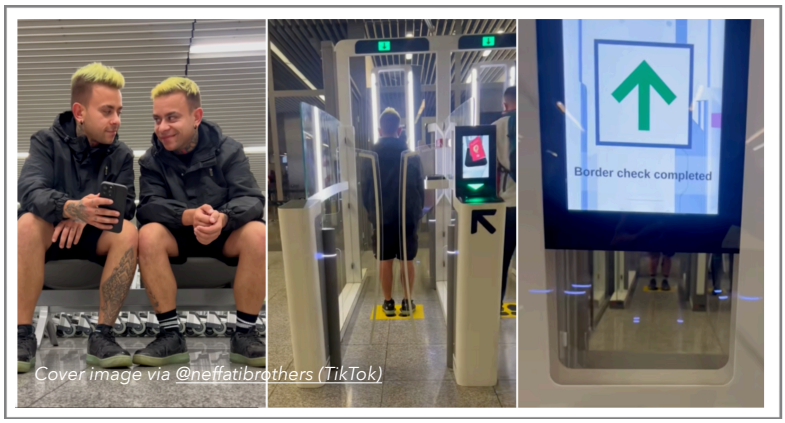
The I.D. Risk Alerts newsletter (open source edition) is a quarterly newsletter with analysis on recent ID fraud, biometric threats and identity vulnerabilities that are already known in the public domain. A comprehensive bi-annual report will also be available to select BixeLab subscribers.

Greece Starts Issuing New ID Cards

The Greek government began issuing advanced identity cards on Monday, 25th September. These cards are embedded with a microchip and feature enhanced security measures compliant with European Union directives, aimed at preventing counterfeiting and identity theft. This development is part of a wider trend towards digital identity systems within the EU and reflects similar calls for modernisation in countries like Australia.

Government response to the Privacy Act Review Report

The Australian government has released its official response to a review report on the Privacy Act 1988, acknowledging the need for stronger privacy protections for Australians. Among the government's agreed recommendations is the introduction of a new 'privacy right to erasure', which will allow individuals to request the deletion of personally identifiable data held by businesses.



Cover image via @neffatibrothers (TikTok)

Identical Twins Allegedly Deceive Airport Security

Modality: **Face** Attack Instrument: **Misuse of Real Identity Documents**
Location: **Airport** Date of report: **Sep 2023**

Two identical twin brothers allegedly bypassed airport security by interchangeably using their own passports, casting doubts on the effectiveness of the implemented biometric systems. The twins, leveraging their identical physical features, were able to deceive the facial recognition and fingerprint systems at the airport. Another experiment by two identical twins attempting to interchange their passports last year also passed the airport security gate. These incidents exposed the potential vulnerabilities of biometric systems when confronted with identical twins, and underline the need for better management of such scenarios.

- **Potential targets**: airports, border control point, immigration departments, or any systems utilising facial recognition or fingerprint technology for verification.
- **Mitigation Strategy**: continuous system auditing, staff training, adequate system configuration, and retuning supported by testing.
- **Criticality: High** - the incident underlines the potential loopholes within the multi-modality recognition system, forcing a re-examination of the current verification methods and technology, particularly when considering identical twins.

Government's Facial Recognition System to Undergo More Testing due to Low Success Rate

The New Zealand government's facial recognition system, which aims to support the country's move towards digital services, is due to undergo further testing following reports of a low success rate. Trials of the system found a 55% match rate in cross-matching facial images to passport photos. The government remains committed to developing its digital identity verification capacities and plans to improve based on testing results.

Jordan Aims for One Million Active National Digital IDs by End of 2023

The Jordanian government has set a 2023 target to issue 1 million digital identities, pioneering comprehensive government services. As of the end of August 2023, 500,000 citizens were using their digital IDs to access government services, and the nation hopes to have 3.5 million citizens using digital IDs to access public services by 2025. "So far, a total of 960 government services have been automated, accounting for 40 per cent of the Economic Modernisation's executive plan relating to the digitisation of government services and operations," said Minister of Digital Economy and Entrepreneurship, Ahmad Hanandeh.

High Machine Malfunction in Sydney Airport's Biometric System

Modality: **Face** Attack Instrument: **Technical Malfunctions**
Location: **Australia**, Date of report: **November 2023**

The 22 SmartGates and 40 self-service kiosks at Sydney International Airport are intended to streamline the processing of international arrivals. However, with an average of 88 malfunctions a month, these devices have instead become a source of frustration and inconvenience, for both newcomers and returning Australians alike. Despite these concerning numbers, the rollout of replacement SmartGates to address these issues isn't scheduled for completion until July 2024. According to the Australian Border Force, the rate of fault and malfunction relates to the original SmartGates' age, as they were first introduced in 2009. However, the new third-generation SmartGates, that rely on biometric comparisons of the traveller's face with their passport, are already improving the situations at Brisbane and Perth International Airports.

- **Potential targets:** airports, customs departments, international passengers, and entities relying on biometric technology.
- **Mitigation Strategy:** accelerating technology upgrades, regular maintenance, and continuous monitoring.
- **Criticality: High** - the consistent malfunctions undermine the capacity of the current system and causing unnecessary stress for new arrivals.

EU Standards Agency Reports on Deepfake Threats

Modality: **Face & Voice** Attack Instrument: **Deepfake**
Location: **Europe** Date of report: **Sep 2023**

European Telecommunications Standards Institute (ETSI) has released a comprehensive report on deepfakes, highlighting the threats presented to identity security and the integrity of personal information. The report emphasises the proliferation of deepfakes in today's digital landscape, which are sophisticated enough to create highly realistic images or audio recordings that can be difficult to distinguish from the authentic specimen. The rise of such technology has precipitated a surge in identity theft incidents and the spread of misinformation, posing serious challenges and potential financial losses for both individuals and businesses.

- **Potential targets:** organisations and systems that use biometric modalities for identification and verification – finance industries, defence agencies, political institutions, media organisations, and ordinary individuals.
- **Mitigation Strategy:** implement and regularly test robust deepfake detection systems. Enhance biometric security to prevent identity theft. Educate the public on deepfake risks through awareness programs. Develop legal regulations to control deepfake creation and distribution, ensuring accountability and reducing misinformation.
- **Criticality: High** - the rise of deepfakes presents a significant security threat through their potential ability to circumvent traditional biometric systems.

Australia's myGov Scams Result in Major Financial Loss

Modality: **Identity Theft** Attack Instrument: **Stolen Data**
Location: **Australia** Date of report: **November 2023**

Australia's digital identification program, myGov, has reported a loss of AU$3.1 billion (US$2 billion). The website, which was linked to thousands of fraudulent accounts connected to the dark web, has faced significant issues with ensuring user security. These issues have reportedly resulted in losses of AU$557 million (US$373 million). In an attempt to combat these scams and mitigate future threats, myGov plans to switch from password verification to face or fingerprint recognition.

- **Potential targets:** online government services, citizens using these services, and digital identity systems implemented by corporates and other institutions.
- **Mitigation Strategy:** introduce biometric verification methods, such as facial and fingerprint recognition, to strengthen user authentication processes. Implement multi-factor authentication and conduct user education on secure password practices. Conduct periodic security audits to ensure the system's defences are updated in line with the latest cyber threats.
- **Criticality: Extremely High** - this incident underlines the large-scale impact that digital scams can have on government programs, prompting a rethink of security protocols. The move towards biometric verification should be supported by continual testing.

Pakistan Cracks Down on Fake ID Cards

Modality: **Identity Verification** Attack Instrument: **Fake IDs**
Location: **Pakistan** Date of report: **November 2023**

Pakistan's National Database and Registration Authority (NADRA) is clamping down on fraudulent identity cards, in response to the prevalent rate of fake ID scams. NADRA, which is responsible for monitoring the identity documents of millions of Pakistanis, has set up a dedicated cybersecurity wing to manage the rising threats of fraudulent practices. In addition, NADRA has deployed biometric-enabled systems to prevent further security breaches.

- **Potential targets:** NADRA, the citizens of Pakistan, or other government agencies and private organisations requiring identity verification.
- **Mitigation Strategy:** stricter controls on identity fraud, the promotion of cybersecurity, the use of biometric technology for identity verification, and tougher penalties for offences.
- **Criticality: High** - the prevalence of fake IDs can lead to significant security breaches, highlighting the need for more robust and reliable identification systems.

AI Facial Recognition Falsely Incriminates Man

Modality: **Face** Attack Instrument: **Incorrect AI Face Matching**
Location: **United States** Date of report: **November 2023**

An American man named Robert Williams was wrongly detained after being falsely identified as a suspect in a theft case by AI facial recognition. The computer system used by law enforcement agencies incorrectly matched Williams with surveillance camera footage of the actual thief. This error highlights the need for hybrid approaches, and review processes to hybrid approaches and periodic monitoring of deployed automated systems.

- **Potential targets:** law enforcement agencies, security companies and any system using facial recognition.
- **Mitigation Strategy:** regular updates to AI mapping techniques, implementing a policy of human verification of AI detection, advance training and awareness of AI bias and error, added context analysis for identification, and better governance.
- **Criticality: High** - this incident highlights the need for better governance throughout the lifecycle of biometric systems as well as the potential consequences of using technology beyond its intended remit. The need for better training for front-line personnel in these processes is also evident.

Casino Security Breaches Illustrate Identity Management Challenges

Modality: **Data Breaches** Attack Instrument: **Cyber Hacking**
Location: **United States** Date of report: **November 2023**

Two noteworthy security breaches at leading casinos in the United States have led to the significant loss of sensitive customer data, displaying the increasing challenges in identity management. This issue has been seen not just in the US, but around the globe as cybersecurity attacks grow in both severity and frequency. Millions of individuals' personal data, including finances and other sensitive information, were exposed due to the breaches.

- **Potential targets:** casinos, hospitality sectors, and other industries handling a significant amount of personal identifiable information, such as healthcare, financial institutions, and online retailers.
- **Mitigation Strategy:** implement advanced security measures, including MFA and regular audits. Foster trust through open communication and transparent incident handling. Conduct comprehensive cybersecurity training and establish a governance framework aligning with regulations. Prioritise privacy with strict controls and clear policies.
- **Criticality: High** - the breaches underscore a critical gap in existing identity management procedures, highlighting the susceptibility of industries to sophisticated cyberattacks.