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.

EU Adopted Position On Proposed AI Act

MEPs adopted Parliament's negotiating position on the AI Act. Talks will now begin with EU countries in the Council on the final form of the law. Amendments were adopted on 14 June and now the draft text of the legislation serves as the negotiating position between member states and the European Commission, which can be a lengthy process.

Trustworthy Digital ID

BixeLab has released a public primer on trustworthy digital identities. The primer recognises the importance of trust in online transactions in today's interconnected world. It suggests connecting digital to real-world identities and recommends consulting experts and following international security standards for biometrics implementation. It also highlights the need for independent validation and thorough testing to manage risks. The primer can be downloaded here.

Source from Facial recognition technology helped catch an 86-year-old Maine man who used his dead brother's identity to collect extra Social Security benefits. (David McNew / AFP/Getty Images)

Face recognition detects dual identities

Modality: **Face**, Attack Instrument: **Forged Documents**

Location: **United States** Date of report: **August 2023**

A California man has been convicted for assuming his deceased brother's identity for 58 years. The man used stolen identification and forged documents to live under his sibling's identity discreetly since 1965. He exploited this false identity to apply for a driver licence, social security benefits and other programs in his brother's name, causing significant problems within the Californian Department of Justice's systems. The fraud was discovered by the use of facial matching, which identified one physical individual interacting as two different people.

- **Potential targets**: any system or organisation that deals with personal identification and verification - such as licensing departments, financial institutions, and social systems.
- **Mitigation Strategy**: rigorous identity verification checks with biometrics where possible, regular audits of digital identity verification solutions and processes, and training and awareness programs to detect forgery.
- **Criticality: High** - this incident highlights the need for more robust and independently assessed identity verification systems to prevent similar cases of identity theft in the future.

Seamless Travel Using Digital Travel Credentials (DTC)

Finland has launched the first EU digital ID travel route with the UK and Croatia. This allows for seamless travel between the countries using digital identification. In related news, a tentative political agreement has been reached on a revised EU digital ID framework proposal, which aims to enhance the security and interoperability of digital identities across the EU. The proposed policy amends the 2014 eIDAS regulation, which governs public service access and transactions across borders within the EU.

Australia Announces Safe and Responsible AI Policy, Gallagher Urges for Digital ID Initiative

Australia's Minister for Industry and Innovation, Mr. Ed Husic MP, has recently announced a new government policy focused on the safe and responsible use of Artificial Intelligence (AI). Under associated new guidelines, AI applications should minimise bias, provide transparency, uphold privacy, and be held accountable for outcomes. The Minister emphasised that this policy will foster a strong AI ecosystem, safeguarding the public while also promoting innovation and growth. In a related development, Shadow Minister for Finance, Katy Gallagher has called for the government to act on the digital ID front. Given the EU's recent launch of its first digital identity wallet, Gallagher emphasises that it's time for Australia to establish its own framework for a secure, interoperable digital ID system.

Identity cards & Deepfakes

Modality: **Identity Fraud**, Attack Instrument: **Deepfake**
Location: **HK, CN**, Date of report: **August 2023**

Six individuals have been arrested in Hong Kong for defrauding victims of HK$200,000 using deepfake technology. The perpetrators impersonated victims using advanced face-swap software to access personal bank accounts protected by facial recognition systems. This is a significant threat to any system reliant on facial recognition technology as a primary form of authentication.

- **Potential targets:** any system using facial recognition as a form of authentication, particularly those used by government agencies, social platforms, and financial institutions.
- **Mitigation Strategy:** implementation of multi-factor authentication, liveness or presentation attack detection mechanisms , periodic assessments of security protocols, and robust governance processes.
- **Criticality:** Med-High - the threat posed by deepfake technology is increasingly concerning as it becomes more sophisticated and widely accessible, particularly for industries relying heavily on facial recognition technology.

Criminal organisation selling mule accounts

Modality: **Identity**, Attack Instrument: **Generative AI & Deepfake tools**
Location: **United States**, Date of report: **August 2023**

A recent discovery by a criminologist at Georgia State University has shed light on the activities of a transnational criminal organisation that has been stealing from the U.S. government since the onset of the COVID pandemic. This criminal group is engaged in the illicit trade of 'mule' bank accounts (accounts set up with stolen identity data) and generative artificial intelligence and deepfake tools, which facilitate sextortion and other scams. These services are offered to other criminals. The article highlights the existence of a "fraud-as-a-service industry" operated by international cybercriminal gangs worldwide. This industry is providing low-level criminals globally with the tools to defraud government agencies, carry out extortion, and commit similar offences using AI-powered and deep fake technology.

- **Potential targets:** government bodies and financial institutions in the U.S. and globally.
- **Mitigation Strategy:** enhanced security measures, including the deployment of algorithms capable of detecting deepfake attacks should be used, along with ongoing assessment of existing and emerging threat vectors. Rigorous testing of identity threats, covering end-to-end assessments of system vulnerabilities, should be conducted to counter various fraud methods, including social engineering attacks. Systems for robust identity verification governance are crucial.
- **Criticality:** **High** - the threat posed by the sale of counterfeit bank accounts, the "fraud-as-a-service" industry, and the distribution of generative AI and deepfake tools to extend the capability of less experienced actors is a significant and growing concern. The wider availability of these services will reduce the barriers to entry for small-scale criminals, allowing them to conduct more sophisticated attacks on biometric and identity systems.