Interactive Voice Response (IVR) Voice Verification

Definition/Description

IVR voice verification is a biometric authentication technique used when a telephone call is involved—principally with call centers. It provides additional security in a channel that depends heavily on humans, and, as a result, is vulnerable to fraud resulting from social engineering attacks. Without IVR voice verification, fraud can be committed by answering security questions using compromised customer data. IVR voice verification is one of the few, if not the only, biometric method available to call centers.

Voice recognition is more customer friendly than knowledge-based authentication, and requires less time when interacting with customers, improving call center processes.

Applicability

Channel	Applicable?	Use Case	Applicable?	Stakeholder	Applicable?
In-app [merchant app]	NA	Customer onboarding	Yes	Merchants	Yes: internal
Mobile browser	NA	Authentication (onboarding)	Yes	Issuers	Yes: internal
Desktop/laptop computer	NA	Authentication (transaction)	Yes	Issuer processors	NA
Phone	Yes	Authorization	NA	Wallet/online payment providers	NA
		Post-authorization review	NA	Acquirer processors	NA

Technical Features/How the Technique Works

Voice biometrics require a "voiceprint" for each customer which is then used for authentication. Words are broken down into segments based on dominant frequencies and are stored digitally in a database. There are two common methods of voice recognition: active and passive. Active requires the customer to speak a set phrase to create the voiceprint. Passive uses normal conversation to create the voiceprint.

Voiceprints associated with known fraudsters can also be used to identify risks.

Risks Associated with Technique

The European Union General Data Protection Regulation (GDPR) lists biometrics as one of the methods that requires customers to opt-in. Organizations need to be very aware of privacy issues when implementing any system that uses biometrics.[1]

[1] "The importance of consent and privacy when deploying voice biometrics," PrivSec report, June 24, 2019, https://gdpr.report/news/2019/06/24/the-importance-of-consent-and-privacy-when-deploying-voice-biometrics/

Privacy poses an issue for this technology, as with all biometric technologies. Biometrics are unique to individuals and cannot be replaced if compromised. The manner in which the voiceprints are stored is critical.

Hacking using a pre-recorded voice sample is a risk. This can be prevented using a challenge-response system that requires the user to repeat a requested word or phrase.

Voiceprints can be affected by physical condition, heightened moods, or background noise, resulting in a failed verification.

Customer Impact/Level of Friction

Other than the initial step of providing the voice sample, this technique has minimal to no impact on customers.

Implementation Considerations

Vendors provide IVR software packages for IVR, and consultant companies may provide ratings of the various packages. Implementers should review vendor offerings to find the one best suited to their requirements.

Although not a requirement, companies may want to verify that the IVR voice recognition software has been assessed by a reputable company that determines the security risk of third-party software.

Maturity

Although the concept of using voice biometrics has been around since 1867 when Alexander Melville Bell invented Universal Alphabetics, it was in 1976 that Texas Instruments created a device that could accurately determine an individual's voiceprint. The first international patent for voice recognition was filed in 1983. In the late 1990s, voice recognition was used at U.S.-Canada border crossing. The private banking division of Barclays was the first to deploy this technology as the primary means of identifying call center customers in 2013.[2] The technology has advanced so significantly that some IVR companies guarantee a 99.99% success rate for identifying individuals.

Applicable Industry Standards

The ANSI/NIST-ITL 1-2011 standard documents the data format standards needed for the interchange of biometric data such as IVR. ISO/IEC JTC 1/SC 37 is another standard developed for biometrics.

Publicly Available Statistics on Implementations and Use

According to Voicevault, it is expected that the global market for speech and voice biometrics to be $5.1 billion by 2024.[3]

[2] https://en.wikipedia.org/wiki/Speaker_recognition

[3] "Let's Get the Facts Straight about Voice Biometrics," Voicevault, May 18, 2016, https://voicevault.com/lets-get-facts-straight-voice-biometrics/

Further Reading

https://www.nice.com/engage/real-time-authentication/

https://www.sestek.com/2018/11/fighting-against-call-center-fraud-with-voice-biometrics/

https://www.nice.com/engage/blog/passive-voice-biometrics-in-an-active-channel-2287/

https://www.biometricupdate.com/wp-content/uploads/2014/05/Voice-Biometrics.pdf

https://voicevault.com/the-difference-between-active-and-passive-voice-authentication-in-contact-centers/

Source Document: This technique is extracted from the *Card-Not-Present (CNP) Fraud Mitigation Techniques* white paper. That white paper was developed to provide a high-level document that directs readers to relevant fraud mitigation techniques while providing easy access to details about the solutions. The white paper is available at: https://www.uspaymentsforum.org/card-not-present-cnp-fraud-mitigation-techniques/