VoiceVault ViGo - Security

How ViGo delivers a secure voice biometrics solution

Title: VoiceVault ViGo - Security

Part number: VV/VIGO/DOC/201/A

VoiceVault Inc.

400 Continental Blvd

6th Floor

El Segundo

CA 90245

USA

(310) 426 2792

info@voicevault.com

Table of Contents

Introduction

The ViGo system provides voice biometric identity verification for mobile devices. It delivers this using an Amazon Web Services hosted VoiceVault biometric engine, and standardized configurations optimized for use in mobile apps.

The ViGo system comprises the full ecosystem for implementing voice biometric identity verification in mobile apps. This eliminates many of the hurdles traditionally associated with the deployment of voice biometrics and it provides ready-made components right out of the box that facilitate app development and deployment.

Amazon Web Services Security

The ViGo server-side components are hosted using AWS and are compliant with a wide range of security and data protection protocols and standards provided by the platform. The ViGo platform leverages these providing ViGo customers with a robust and secure voice biometric service.

AWS has achieved ISO 27001 certification and has been validated as a Level 1 service provider under the Payment Card Industry (PCI) Data Security Standard (DSS). Annual SOC 1 audits are successfully evaluated at the Moderate level for Federal government systems as well as DIACAP Level 2 for DoD systems. For more information, and for a full list of the compliance and data protection standards provided by AWS, follow this link http://aws.amazon.com/compliance/.

VoiceVault Fusion System

The VoiceVault Fusion Enterprise voice biometric engine at the heart of the ViGo infrastructure sits inside the VoiceVault AWS Virtual Private Cloud (VPC) with no external access. The only externally accessible channel is to the Web Services API that sits on separate boxes to the database servers, and is limited to HTTPS access only via SSL 3 / TLS 1.1 and above, all controlled through the AWS firewall.

As well as the physical and access security provided by an industry-leading organization, it is also essential that software applications are developed utilizing secure development practices. VoiceVault has fully integrated security best practices into our software development lifecycle, and verify the security of internally developed applications to mitigate risk from internal and external sources.

Through a third-party Vendor Application Security Testing (VAST) programme from Veracode, the VoiceVault Fusion Enterprise system has been verified as passing CWE/SANS TOP 25 and OWASP TOP 10 scans, providing the high-level of assurance required for use within the most demanding companies such as Financial Organizations.

ViGo Biometric Security

Any ViGo system is based on a set of standard configurations that deliver high-levels of security without compromising user convenience. This standardization removes the need for any configuration, optimization or setup when integrating and deploying a ViGo-based mobile app.

The settings underpinning the standardized configurations have been derived from mobile app deployments in the financial services industry where very high levels of security are paramount – but where usability remains a crucial factor in app usability.

Anonymized voice prints

The voice print created during voice registration is at the heart of the ViGo voice biometrics system. These voice prints are digital representations of a registrant's voice in a proprietary format, and cannot be listened to or reverse engineered to extract user audio. Even if it were somehow possible to extract the voice print for a registered user, there would be no feasible way to use it to compromise that user's security in ViGo.

In addition, there is no personally identifiable information held that links the voice print to the specific individual whose voice print it is. Each voice print is tied to a unique identifier, but these are only associated with personal data such as name, address etc. in the client-side of any ViGo solution. There is no way for anyone to use the ViGo library or API to extract personal information for any user.

Biometric data storage

The ViGo database stores information required by the ViGo voice biometric system. This includes:

- Biometric data, including a user's voice print
- Configuration data, including thresholds and processing-related settings
- Transactional data, including live enrollment/verification dialogues
- Audit data, including audio audit trail for enrollments and verifications

All of the static, dynamic and transient data used by the ViGo system associated with voice registration and verification is stored in the database.

Standardized settings

ViGo is designed to deliver a false accept rate of 0.01% at a false reject rate of ~3% when it is incorporated into an app using the ViGo-recommended UI and development best practices, as outlined below.

In practical terms, this means that ViGo is pre-configured to deliver 99.99% success at rejecting impostors, and 97% success for accepting genuine users first time.

Each of the phrase and digits modes provided out-of-the-box is configured for this same high level of voice biometric accuracy, and the overall optimization of ViGo includes in-app data capture functionality and processing capabilities to maintain these levels of accuracy over time. For phrases, the minimum length is 7 words and the phrases supplied out-of-the-box with ViGo are all 7+ words long.

Achieving ViGo levels of biometric security

The delivery of the ViGo accuracy levels is achieved through the incorporation of the ViGo voice biometrics into a multifactor authentication solution. In such a solution a third factor is used to supplement the first and second: ownership of the device (something you *have*), and the ViGo voice biometrics (something you *are*). This additional factor would typically come into play if voice biometric identity verification has not been successful, such as when the environment is particularly noisy for example.

This third factor can be any security measure or mechanism that is possible to implement in a mobile app such as a PIN or swipe pattern, both of which are implemented as examples in the ViGo demo app. The incorporation of a third factor is *mandatory* in a ViGo deployment, and is used by your app to trigger voice print adaptation mechanisms within the ViGo voice biometric system.

Voice print adaptation in ViGo

As stated above, the ViGo levels of security and accuracy are achieved when ViGo is part of a multifactor authentication system. Within such a system adaptation process are used to update the registration voice print using audio captured during the verification process.

Within ViGo, adaptation is used maintain the required levels of security by talking into account changes in user behavior and environment. In this, it minimizes the chance of a genuine user being falsely rejected by the voice biometric system.

There are two types of adaption that are always both used. One happens automatically and one requires the mandatory third-factor to be incorporated into an app or solution.

Automatic adaptation is configured into the ViGo system and is triggered if a verification attempt is successful and if the system decides that the ‘score’ lies within a certain range.

The ‘third-factor adaptation’ process is triggered if the users’ score lies within a certain range that is above a strong reject threshold level. At this trigger point, a user has in effect been rejected by the system but the user can, through the re-establishment of ground truth, confirm that they are who they claim to be.

Ground truth can be re-established in any number of ways and the mechanism used will be defined by the security requirements of your application. It could be anything from entering a user-defined PIN or swipe (as is the case in the ViGo demo app) or having the user speak to a call center agent and respond to some knowledge based questions.

If ground truth is re-established, the speech sample in question is used to adapt the voice print so that next time the user finds themselves in that environment they will score much higher as their voice print now contains speech representative of the new environment.

Replay detection

The replaying of recordings is a common attack vector in voice biometrics systems and ViGo incorporates replay attack detection mechanisms as standard.