ARMORVOX™

NEXT GENERATION VOICE BIOMETRICS

Delight your customers with seamless and secure voice authentication in any language on any platform

According to IBM[1], the average cost of a data breach is $3.92 million. Every organisation is vulnerable to data breaches and other forms of cyber-attack. Not even the top 500 companies are safe and are more likely to be targeted. Therefore, it is imperative to employ the best possible cybersecurity methods.

In a digitally focused world, traditional security methods have become time and cost-inefficient, requiring numerous external steps such as SMS tokens and email verifications. Traditional methods are failing to deliver satisfactory customer experience and strong security measures. Remembering PINs and passwords can be frustrating and can be easily stolen, hacked or misused. Customers waste precious time proving their identity through numerous security questions. In contact centres, the prolonged agent-handling times and jarred customer journeys can deter customers from using an organisation's services.

KEY BENEFITS

THE NEXT GENERATION OF VOICE BIOMETRICS

Designed to delight and deliver secure yet seamless customer journeys, ArmorVox™ is Auraya's proprietary voice biometric engine that provides voice authentication and fraud prevention capabilities. It is designed to make user authentication simple, fast and intuitive for all use cases and is powered for consistency in all channels and all languages.

IMPROVED CUSTOMER EXPERIENCE

Far too often customers avoid contacting customer support centres due to lengthy wait times and cumbersome processes. Customers are trapped in an IVR where they manually press numbers to direct themselves to the proper services. Once connected to an agent, they then need to authenticate their identity over a series of security questions which include disclosing PINs or sensitive information. The frustration of having to repeat this process for every call can add up. With ArmorVox, organisations can provide a solution that utilises voice identification and verification capabilities to seamlessly and quickly authenticate their customers' identity. Customers can be authenticated while engaging in the IVR, allowing personalised self-service, and if an agent conversation is desired, the agent can provide the needed information without needing to ask manual verification questions. With ArmorVox, organisations can actively or passively authenticate customers to allow for improved and frictionless user experience. There is no longer any need to remember PINs and passwords or repeat security questions, ensuring better customer privacy.

IMPROVED CYBERSECURITY

Every individual has their own unique voice. Many distinct voice characteristics are used to identify and verify a person. Physical characteristics such as the shape and size of a person's vocal tract and behavioural characteristics such as accent, speed of speech, cadence, pronunciation and emphasis are all accounted for when capturing voiceprints. ArmorVox takes advantage of these characteristics to generate highly secure and unique voiceprints. These voiceprints are also encrypted and cannot be reversed engineered so they cannot be used to hear what the person has said. Whether it is on-premise or cloud-based, all captured voice recordings and encrypted voiceprints does not leave the organisation's secure infrastructure. No one, not even Auraya, will be able to access the customer data without being granted access to the secure service.

ArmorVox leverages its patented features to ensure accuracy and security performance. These features ensure that the best possible quality of voiceprint is captured and allow customisation of security thresholds to ensure the desired level of security is set for each individual and each transaction, all while protecting the users and from fraudulent attempts such as using computer-generated voices, recorded voices or even twin voice attacks.

IMPROVED RESOURCE AND COST EFFICIENCY

Customers who are biometrically verified by a self-service bot can often get the service they want without talking to an agent, reducing agent handled calls. Calls with an agent can be made quicker by eliminating manual verification processes. With ArmorVox's active and passive authentication, agents can simply talk with the customers on inbound or outbound calls and verify their identity automatically. This benefit both customers and agents as customers can receive their service quicker and agents can provide greater engagement in a shorter time frame, allowing them to assist more customers overall due to the reduced agent-handling time.

ArmorVox can also help significantly reduce operational costs. There is no longer any need for additional security services such as SMS charges or RSA tokens. The whole experience is seamless and frictionless, all the while maintaining regulatory compliance such as Know Your Customers (KYC) and Anti-Money Laundering (AML) HIPAA, GDPR and the various privacy regulations in different jurisdictions.

KEY CAPABILITIES

VOICE ENROLMENT

ArmorVox can enrol multiple voiceprints for each user through text-dependent same-phrase, text-dependent unique-phrase, text-independent, text-prompted or digit-independent tokens. These voiceprints allow verifications with as little as 2 seconds of net speech. Some text-dependent verifications can be as short as 1 second of net speech. Additionally, ArmorVox is language-independent so users can enrol their voiceprints in their language. Importantly, no one has to enrol using a contrived and annoying phrase such as *"My voice is my secure password"*.

Voiceprints are created by extracting the acoustic parameters from a .wav file containing the spoken information. This .wav file can be sent from a digital device such as a computer or a tablet or collected from a conversation with an agent or a bot. After successful extraction, the original voice recording can either be deleted or stored in a secure archive. The voiceprint is encrypted and stored in a database under the control of the organisation. From here, the voiceprint will be used when verifying or identifying speakers in the future.

VOICE VERIFICATION

ArmorVox requests users to provide some identification such as calling line identification (CLI or ANI), or a spoken customer number, or phone number, or account identifier, or the IP address of the digital device that they are using. A voice sample is captured when they say the identification information and then matched with the enrolled voiceprint in the database. If the voiceprint match passes the security threshold then the person can proceed as 'verified'.

VOICE IDENTIFICATION

A voice sample can be captured and matched with a group of existing voiceprints in the database to produce a score. Using the score, the speaker's identity can be determined. Obtaining extra information such as device ID or account number can be used to further confirm their identity.

FRAUD PREVENTION

ArmorVox helps prevent fraud in real time. ArmorVox can crossmatch over 125 million voiceprints per hour on a single server to check for potential duplicate voiceprint enrolments. The duplicate enrolments can be screened to check for fraudulent activity. This process can be used to identify fraudsters and add their voiceprint to a 'suspected fraudster' list. This fraudster list can be updated with voiceprints created from the historical recordings of calls that were later found to be fraudsters. ArmorVox's fused active and passive modes allow a combination of digit-independent and text-dependent and text-independent voiceprints to be created from recordings of fraudsters calls. These voiceprints can be added to the 'suspected fraudster list' and used to detect fraudsters attacking the organisation in the future. This fused speech recognition and digit-independent mode allow for Playback Protection and Synthetic Voice Protection. Playback Protection combats recorded voices by requesting random digit or text-dependent challenges. Synthetic Voice Protection combats generated or modified voices through machine learning algorithms and synthetic voice artefact detection.

KEY FEATURES

TUNED UBM

With ArmorVox's built-in machine learning algorithms, the core models of the engine are automatically tuned to generate optimal results. This feature is capable of reducing the False Reject Rate by over 50%, where the prior initial success rate is already at a highly effective level.

ACTIVE LEARNING

Speakers always sound a little different each time they use the system to do a verification. Their voice may change because of behaviour or using different devices or channels. Sometimes, people change the way they say certain phrases. With Active Learning, ArmorVox uses machine learning algorithms to continually adapt and learn from a speaker's past and present interactions. This greatly improves the quality of their voiceprint, ensuring higher success rates and increased accuracy. After three active learning cycles, this feature is capable of reducing the False Reject Rate by over 90%, where the prior initial success rate is already at a highly effective level.

SPEAKER-SPECIFIC THRESHOLDS AND SPEAKER-SPECIFIC BACKGROUND MODELS

When creating voiceprints, ArmorVox uses a patented process to create a Speaker-Specific Background Model which improves the security performance for each individual. Machine learning algorithms also create a Speaker-Specific Threshold. With both Speaker-Specific Thresholds and Speaker-Specific Background Models, ArmorVox can set levels of security for each voiceprint to meet the desired security outcomes required by the organisation. This allows organisations to specify the desired False Accept Rate for each type of use case.

This patented feature ensures that every user in the system achieves the specified security outcome, rather than having a global system-wide general threshold which may lead to discrepancies in security levels between speakers. This feature improves customer experience and security performance by reducing the False Reject Rate by a further 60% whilst maintaining the specified False Accept Rate consistent for every individual voiceprint.

CROSS-CHANNEL COMPATIBILITY

Auraya's patented process enables users to enrol their voiceprint and verify their identity on any digital channel such as enrolling from a secure mobile app or web session and using the voiceprint for verification purposes on any other channel such as in the IVR, agent conversation or digital chatbot. ArmorVox can be deployed in on-premise or cloud-based solutions, whether it is a legacy telephony solution or on cloud-based platforms such as Amazon Connect. Additionally, with Auraya's patented HTML5-compliant browser-based voice enrolment and verification processes, users can interact with voice biometrics anywhere via a browser in their smartphones or computers.

RAPID CROSS-MATCHING

Real-time fraud detection and prevention is a crucial necessity in today's cybersecurity world. With millions of hackers attempting to break firewall security and exploit other breaches and loopholes, an organisation must always be ready to detect and prevent these potential attacks. In addition to enhanced security and delightful user experience, ArmorVox can provide real-time fraud detection background tasks such as impostor mapping and duplicate spotting. This means that ArmorVox can post immediate feedback if the user who is being enrolled in that specific instance is a known fraudster or someone who is already enrolled but under a different identity. ArmorVox achieves this through its fast cross-matching speed of over 125 million voiceprints crossmatched per hour on a single server. Moreover, the speed is dependent on the CPU of the server being used. If an organisation requires faster cross-matching speed to accommodate a larger activity, it can simply increase the number of servers.

FUSED ACTIVE AND PASSIVE MODES

Organisations may want to use different identifiers to enrol and verify their users. Alternatively, users may want to enrol their voice in different ways. Providing options not only increases security and versatility, but it also improves user experience. With ArmorVox, organisations can use either text-dependent same-phrase, text-dependent unique-phrase, text-independent, text-prompted or digit-independent voiceprint tokens for enrolling and verifying their users. Additionally, organisations can also use a combination of tokens to deliver faster verification. With this feature, organisations can use phone numbers, customer account numbers, employee numbers and other identifiers to enrol and verify their users as well as implement random phrases or digits to protect against fraudulent attacks.

PLAYBACK PROTECTION

Fraudsters may attempt to break into an organisation's system through recorded voice playback. They do this by capturing samples of the targeted user's voice and playing it back during the verification process. Fortunately, ArmorVox combats this playback attack by requiring the user to say a new random set of digits during the verification process. Unless the fraudster is presented with the same set of digits that directly matches to the one that the fraudster has recorded previously, then playback attack will fail all the time. If organisations are concerned about fraudsters recording each digit and playing it separately from a keyboard, then the organisation can implement random phrase detection instead.

SYNTHETIC VOICE PROTECTION

Fraudsters may try to break into an organisation's system by using synthetically generated voices. Basic synthetic voices lack the subtle nuances and voice characteristics that make it 'human' and are relatively easy to detect. Sophisticated synthetic voice generators can be detected using ArmorVox's model detect functionality. ArmorVox can be used to enrol a sample set of voices from these sophisticated synthetic voice generators. This model can then detect the specific artefacts that the synthetic voice generator has in any variation of the voices that are created from that generator. These models can then be added to the organisation's fraudster list, where ArmorVox can crossmatch any future attempts to detect synthetic voices.

EASY DEPLOYMENT

Integrating ArmorVox to your existing on-premise or cloud-based solutions is easy. You can do-it-yourself or use one of your trusted technology partners.

[1] IBM. (2019). *2019 Cost of a Data Breach Report*. Retrieved from https://www.ibm.com/security/data-breach