Guide to Speaker Verification
&
Voice Biometrics

ICR Speech Solutions & Services
The Engine House
Ashley Lane, Saltaire
West Yorkshire
BD17 7DB

Tel: 01274 821111
e-mail: info@icr3s.co.uk
www.icr3s.co.uk

Contents

Who are ICR?

ICR is a leading provider of business-critical automated voice applications incorporating IVR, Speech Recognition, Voice Biometrics and many other periphery technologies. We work with companies in finance, mobile and fixed-line telephony, retail and utilities and this experience, coupled with our pragmatic and flexible approach ensures both project, and our customer's, success.

The company's continued achievements are realised through its ability to adapt to constantly evolving business and technology landscapes and to stay at the forefront of innovation for the benefit of its customers.

We aim to continue to meet and exceed our clients' expectations and generate overwhelmingly positive feedback from the likes of Lloyds Bank, Vodafone, Equinity, JD Williams and Lloyds Asset Finance. ICR offers solid expertise, a flexible approach and a willingness to go the extra mile.

Introduction to Speaker Verification

What is it?

Speaker verification using Voice Biometric technology is an automatic process that analyses human voice characteristics to determine whether a speaker (or caller) is the person he or she claims to be.

The technology and processes offer an accurate and efficient method of authenticating a person's identity and improving security for over the phone transactions. Security is increased as speaker verification measures voice characteristics that are difficult to duplicate by recording or impersonation.

Voice is essentially a biometric measurement very much like others which are more familiar such as fingerprint pattern, iris structure, retina structure etc. However, in real-life scenarios, voice has a number of advantages because of relative ease of implementation (it requires a normal telephone and not a specialist device), cost performance and convenience for the caller.

Why use it?

When facilitating commercial transactions over the telephone using IVR / Speech or contact centre agents, it's important to provide security and ensure privacy and fraud protection, whilst at the same time, providing callers with non-intrusive, efficient interactions; Voice Biometrics is a solution to these requirements.

Benefits of using speaker verification

Reducing Fraud

A fraudster can enter or speak a stolen account number and PIN during an Identification & Verification (ID&V) process. The addition of a speaker verification process provides a significant extra level of security to information based processes by employing something which the valid caller has and no-one else - their voice. The cost reductions associated with lower fraud levels alone have been sufficient for financial organisations to make a business case for implementing Voice Biometrics.

User convenience

Appropriately designed speaker verification processes can make the mandatory ID&V of a caller a much slicker process and so help to improve customer satisfaction scores

Resource usage

Speaker verification streamlines the ID&V process resulting in a shortened transaction time and a reduced overhead on infrastructure and therefore associated costs.

Positve customer perception

Identity theft and high-profile hacking attacks targeting enormous amounts of personal data are major concerns. Organisations which implement leading edge security measures are likely to be viewed more favourably than the competition, especially when the ID&V process actually improves. The logical effect is a consumer shift towards organisations who have implemented these systems.

How does it work?

To perform speaker verification, the biometric system validates a speaker's identity by comparing speech samples to an existing voiceprint for that speaker. The voice biometric technology performs three functions:

Enrolment of voice prints for new users.

During enrolment following a secure ID&V, a user provides enough speech samples to allow the system to "learn" the voice. The system creates a voice print, stores it in a database, and uses it to verify that user's identity when they subsequently call the service. The voice print is not a recording of the speaker's voice; it's a small file (approx 15-20k bytes) containing measurements of selected voice characteristics represented in a numerical format. The creation of these features is a complex mathematical process.

Verification of the user's voice.

Once enroled and when subsequently calling the service, the user asserts their identity by providing an identity reference such as an account number. The biometric system retrieves the voiceprint associated with that identity and the caller is then asked to speak some additional information for verification such as date of birth, a passphrase or prompted information, e.g. a random digit string. The voice biometric system validates or rejects the caller by comparing the voice characteristics within these utterances to the stored voiceprint.

Adaptation

Adaptation is the process of enhancing an existing voiceprint using new data. Adavanced voice biometric systems adapt the stored voiceprint on an ongoing basis when the caller uses the service.

Deployment Modes

Speaker verification can be deployed in a number of different modes:

Text-Dependent Mode

Verification is performed on a password or passphrase. This mode is sometimes considered to be less convenient for the user than alternatives as they have to remember their password or passphrase. However, the caller can be given the option to create their own passphrase which, unlike internet based passwords, may be more easily recalled. A passphrase for a speaker verification system is not restricted by the same kinds of rules associated with internet based passwords such as minimum / maximum number of characters, capital letters, must contain numbers etc.

Text-Prompted Mode

A verification process that asks the user to repeat random numbers and/or words. This is easier for the user in that no passwords or PINs need to be remembered.

Passive / Text Independent Mode

In the contact centre environment this mode is applied during a customer's conversation with an agent. Verification is performed in the background and carried out independently of the spoken content. A traffic light representation may be visible on the agent's screen and only when the agent sees the 'green light' during the conversation may they proceed to process transactions or divulge sensitive data.

A separate application for text independent mode is in the area of forensics and law enforcement. The voice biometric technology can be activated to analyse, in real-time or after the event, a telephone conversation involving a suspected criminal to help prove beyond any reasonalbe doubt that that person on the call.

Blacklisting

This deployment references a pre-populated database of known fraudsters / criminals - the 'Blacklist'. In a contact centre environment the voice biometric engine is programmed to run in the backgrouind against high volumes of calls simultaneously. The purpose is to analyse the voice prints of callers, compare them to the known Blacklist in real-time and flag when a Blacklisted caller is on the line. The operation will have a procedure in place to deal with the blacklisted callers appropriately.

Where is speaker verification and voice biometrics being used?

Although originally used in covert intelligence gathering speaker verification is now a mainstream technology with several real-world deployments by commercial organisations and government and within customer facing and internal environments.

Customer facing commercial operations

A number of large financial organisations, such as Banks and share-dealers, have deployed the technology and many more are considering it. Telco's and content providers are also interested in voice biometrics for restricted access to services and the gaming industry for the same reason.

Government

Voice biometrics is increasingley being used by governments and Australasian governments have been particularly innovative; Centrelink, the Australian Social Security Service, was one of the first government agencies to deploy a high-volume service based on voice biometrics in a landmark deployment. Also, the New Zealand Inland Revenue has enroled 40% of the countries adult population into its solution for providing efficient and secure access to its services.

Developing countries such as the Philipines have also been keen to exploit the benefits of the technology with a solution which facilitates secure customer access to a wide range of government services. This is particularly interesting in a country such as the Philippines where the possibility of accessing services from within remote geographical regions is of great benefit

Internal Operations

One of the most popluar applications for internal deployments is password resets in help-desk environments. A number of applications are also being considered in the recruitment industry for convenient provision of time-sheet information by temporary staff and ID&V for the same when arriving on-site.

Advantages of Voice biometrics over other biometric measures

Voice has a number of advantages over other biometric measures.

Voice is non-intrusive

The authentication of the individual can take place as part of a normal telephone call. There is no or little inconvenience to the user while they are being authenticated and the user does not need to touch anything or learn a new operating device.

Voice is easy to use

The vast majority of people can use a telephone (any of the many types) to communicate. For the user this is all that is required for speaker verification. There is no positioning of fingers, heads, or eyes to gain access.

Flexible

Voice is a very flexible means of authenticating a caller's identity. Callers can be authenticated with or without needing to remember passwords or PINs. However, adding knowledge-based questions to the process can provide improvements in security.

No new infrastructure required for the user

Most people either own or have access to a telephone

Cost

Primarily because of the lack of need for hardware the rollout of speaker verification is relatively cheap compared to other methods (especially for high-volume implementations).

Deployment factors to Consider

Accuracy levels alone do not measure successful implementations of speaker verification systems. There is a wide range of factors that need to be considered before deployment:

Natural voice variations

How well will the system cope with colds, daily voice variations and long-term voice variations caused by factors such as ageing (see Adaptive technology)?

Mix of communication channels

How well will the system handle different phone types - landlines, mobiles, etc?

Background noise

How well will the system handle background noise - talking, street noise, road noise in cars, airports etc?

Scalability and high availability

The system requires scalability and 100% availability.

Accuracy

A function of voice biometric technologies allows the organisation to adjust the confidence level required for a successful verification. The higher the confidence level required the greater is the number of ‘false rejects’ and vice versa. The optimum confidence level is often decided prior to a full customer facing deployment during the stages of internal and external proofs of concepts and Pilots. The level of confidence required will be specific to the operating organisation and the type of transactions being governed.

Rejections

A process is required for handling rejections – both true and false. For example when someone fails the voice biometric verification they may be routed to an agent or a separate automated application and asked to provide answers to additional security questions.

Voiceprint database

Who owns it and are voice prints stored centrally or are they distributed?

How long should voiceprints be kept for and are there any regulations governing their use and how they should be stored?

Integration

How will the voice biometric technology be integrated with existing systems – telephony, IVR, speech recognition, voice recording systems, agent desktop applications and host systems

Speaker Verification Process

One of the most important decisions is to decide which mode of speaker verification is most suitable for the organisation and its customers (see deployment modes).

Risks

There are a number of identifiable risks which need to be recognised, analysed and assessed when considering Speaker Verification and Voice Biometrics.

No recognised standard

There are a number of credible suppliers of speaker verification technology, each with their own proprietary solution and whilst there may be voice biometric standards they are not enforceable, as governments have not, as yet, issued any regulations or even guidelines.

RISK = Your chosen solution may not be the standard adopted by other financial institutions in the future (either by choice or legal enforcement) and therefore it may become redundant.

Privacy and access to voice prints

Up to the point of writing there have not been any significant public, or other, outcries about privacy or the threat of voice print theft. However, it's debatable whether the greater threat is from public organisations (e.g. the government) or private company misuse rather than the criminal underworld.

Whilst people are sometimes wary of providing biometric data, it's worth pointing out that, at the time of writing, a voice print cannot be reverse engineered to create a sample of a person's voice.

RISK = Any misuse or abuse relating to privacy or unauthorised access to voice prints could tarnish industry implementations.

Press Misinterpretation

There are relatively few deployments of speaker verification and the success of these is not known in the public domain. There is a danger that with few deployments any negative publicity from the press could have a major impact on the short-term future success of the technology.

There is also a general lack of understanding of the benefits of the technology and how it needs to be deployed to be successful. Voice biometrics cannot succed in isolation; it should be seen as an additional security layer and implemented accordingly.

RISK = Performance however satisfactory for the operating organisation could be misinterpreted by the press and thereby lead to customer concerns.

Customer/User Acceptance

We assume customers will appreciate speaker verification as it improves convenient access to services and reduces the risk of fraud. However, customers need to be told the benefits of speaker verification to increase awareness and promote an understanding of its capabilities.

RISK = Without being told the organisation's intentions or the potential benefits customers could be put-off Speaker Verification.

Summary

ICR believes that the introduction of Speaker Verification will have a measurable positive effect on customer care and cost reduction. The key reasons for this are:

Improving the security of the ID&V process.

Existing ID&V processes are open to fraud and provided the initial enrolment process is secure speaker Verification results in a much more secure ID&V process.

Making the ID&V process easier

Customers are currently required to know too many identification and verification tokens which differ from one organisation to the next and existing processes are lengthy and inconvenient. Using an automated speaker verification process with voice biometric technology is far more natural, faster and customer friendly.

Better utilisation of internal resources.

Existing processes are lengthy and use up valuable telephony resources such as ACD and IVR ports. Using a speaker verification process leads to completion of customer ID&V in less time which frees up valuable infrastructure capacity for other customer services.
Where speaker verification replaces a manual ID&V process conducted by an agent the agent is free to undertake more rewarding and productive tasks.

Why Choose ICR for Speaker Verification deployments

ICR has real-world experience of implementing speaker verification solutions, its vendor independence, experience of designing speaker verification implementation processes and project delivery set us apart from the competition.

Contact Details

ICR Speech Solutions & Services
The Engine House
Ashley Lane, Saltaire
West Yorkshire
BD17 7DB

Tel: 01274 821111
e-mail: info@icr3s.co.uk
www.icr3s.co.uk