



SecuriVox delivers text and language independent speaker verification with cross channel capability and high resistance to background noise



SecuriVox Speaker Verification

SecuriVox Speaker Verification

Product overview

The need to verify the identity of individuals is a growing challenge for industries ranging from financial services to air travel. As the volume of transactions performed online and via telephone continues to increase there is also a need for reliable methods of authenticating remote customers and users.

A new level of security

Speaker verification (also known as voice authentication) is a biometric authentication technology that offers a solution to the problems of identity fraud and password abuse by using the unique characteristics of an individual's voice to confirm their identity in applications ranging from phone banking to automated check-in.

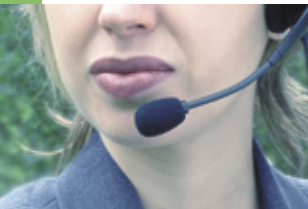
How it works

In order to use speaker verification individuals must first enrol by providing short samples of speech that are then used to automatically build a unique user template. Once enrolled, an individual's identity can be verified at any time simply by comparing a short utterance with their unique template. Both enrolment and verification can be performed via fixed and mobile telephones, the Internet or across a company network.

The benefits

The key benefits associated with speaker verification include:

- **Increased security:** speaker verification delivers a powerful extra level of security beyond that possible with passwords or PINs, both of which are vulnerable to a range of well documented abuses.
- **Enhanced user convenience:** speaker verification allows enhanced levels of security to be implemented with maximum convenience by making use of the most natural and intuitive of interfaces, human speech.
- **Additional cost savings:** as well as savings achieved through reducing fraud, speaker verification can be used in automated verification processes that allow identities to be confirmed without the need for human intervention.
- **Cost effective deployment:** the deployment of speaker verification can be very cost effective in comparison to other biometric technologies in that it makes use of existing telephony or network infrastructures with minimal requirement for additional hardware.



The SecuriVox difference

As well as providing the benefits previously outlined, SecuriVox Speaker Verification has been designed to deliver a number of key features that ensure effective deployment across the widest possible range of real world applications:

- **Cross-channel capability:** SecuriVox's advanced channel normalizing algorithms ensure that users can be verified on any channel (e.g. fixed-line phone, mobile or web) regardless of the channel used to enrol.
- **Text independent:** Truly text independent operation means that verification does not require the user to repeat any of the phrases that were used for enrolment. As well as the obvious security benefit, this capability also means that background verification can be performed during natural speech.

The SecuriVox Difference – Verification "on the fly"

As well as being suitable for use in automated enrolment and verification, the fact that SecuriVox Speaker Verification is text independent means that it can be used to perform enrolment and verification during natural conversation. This is particularly powerful in applications such as phone banking where customers interact directly with customer service agents. This capability removes the need for a time-consuming authentication procedure at the beginning of each call, which in turn means reduced costs and enhanced customer satisfaction.

- **Language independent:** SecuriVox Speaker Verification is entirely language independent, which means that the same high level of security is immediately available across all territories, with no need to wait for particular languages to be supported.
- **Persistent templates:** SecuriVox Speaker Verification has been designed to ensure that, unlike most similar systems, the unique templates that are created for each user during enrolment do not need to be continually retrained or refreshed. As well as simplifying deployment, this also ensures that the system is able to confidently verify infrequent users.

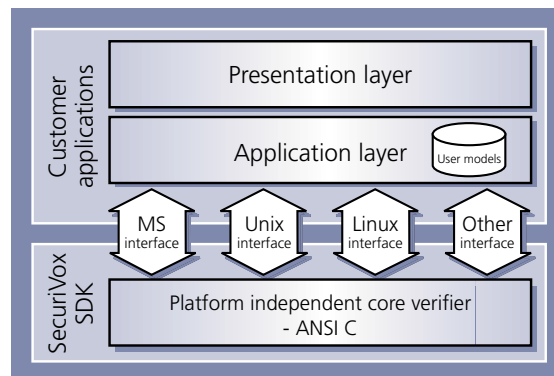
The SecuriVox Difference – Unique Audit Capability

The persistent nature of the unique user templates created by SecuriVox means that they can be used to provide a valuable audit trail. Simply by storing a sample of speech at the time of a transaction it is possible to verify at a later date who initiated the transaction.

- **Resistant to background noise:**
Successful verification is possible even in the presence of significant background noise.

Simple and flexible deployment

SecuriVox Speaker Verification is available in the form of a software development kit (SDK). The SecuriVox SDK comprises of a platform independent core verifier with a number of platform specific interfaces or encapsulations. This allows developers to use the same core technology to quickly and easily incorporate the benefits of speaker verification into the widest possible range of telephony and Internet based applications.



This approach also simplifies integration with other technologies such as speech recognition for example, and helps minimise the impact on existing processes. More information on deployment and integration is available by contacting the company.

In summary

SecuriVox provides truly text and language independent speaker verification technology with cross-channel capability, persistent templates and high resistance to background noise. From phone banking to automated check-in, SecuriVox Speaker Verification can provide increased security for applications and information while enhancing convenience for customers and users.

SecuriVox Speaker Verification

Technical overview - SDK

The distinctive performance and features of SecuriVox Speaker Verification are the result of a unique design philosophy. This has also ensured that deployment is simple and flexible while offering developers the ability to optimise the level of security without being subject to the key compromise normally associated with biometric technologies.

Security without compromise

SecuriVox's unique design effectively decouples the False Acceptance Rate (FAR) and False Rejection Rate (FRR) which means that, unlike almost all other speaker verification and biometric systems, they are independent of each other. In conventional systems the developer must choose an accuracy threshold that is essentially a trade off between FAR and FRR. A very low FAR (i.e. a high level of security) would normally be accompanied by an increased FRR. (i.e. reduced user convenience.) and vice versa. This means that applications based on conventional system designs normally require a balance to be struck between usability and security. (see fig.2) As a result developers may in fact accept a slightly lower level of security in order to ensure usability of the system.

The fact that SecuriVox has independent FAR and FRR delivers the following key benefits:

- There is no need to set accuracy thresholds.
- The FRR is very close to zero and is in fact dependent only on utterance length and general signal quality. This effectively eliminates the inconvenient false rejections that are normally associated with high levels of biometric security.
- The FAR becomes a design parameter that can be determined on a case-by-case basis with negligible impact on FRR. This means the FAR and therefore the level of security is proportional to the computational power and time available.

Therefore with SecuriVox Speaker Verification (as can be seen in fig. 3), there is no need to compromise between security and user convenience as both the FAR and FRR can be optimised independently.

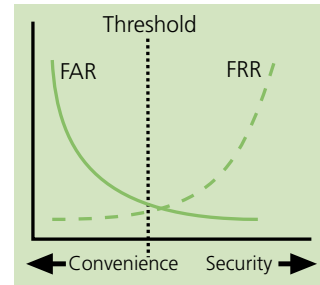


Fig 2 - Conventional design with threshold

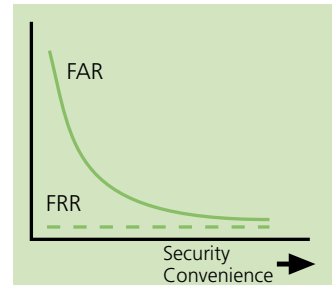


Fig 3 - SecuriVox design removes threshold

Summary specification

The table below provides an overview of the level of performance that can be expected in a typical real world deployment. The specification details are indicative and may be subject to change (up or down) as system parameters are optimised to suit specific applications.

Enrolment sample size	5-10 short phrases (10-20 sec's)
User template size	20-50kbytes
Verification sample size	Approx. 3 seconds.
Time to verify	< 1 second
Speech data formats	16 bit PCM
Sampling rate	8Khz
Accuracy	FR: ~ 0% FA: < 0.5%
Channels supported	Telephone, PC, Internet.
Operating Systems	Windows NT, 98, 2000, XP Unix, Linux (available soon) Others on request



ABOUT SecuriVox Limited

SecuriVox's unique speaker verification technology adds a new level of biometric security to applications ranging from phone banking to automated check-in. Simply by capturing a short utterance you can ensure that an individual is who they say they are, regardless of how they choose to contact you. SecuriVox speaker verification technology protects you and your customers from identity fraud and password abuse while reducing costs by enabling both automated and background verification.

SecuriVox is based in Dundee, Scotland with offices in Edinburgh and London.

For more information visit www.securivox.com or call +44(0)1382 66 88 11.