

customer care solutions

from Nuance



white paper ::

A Nuance Education Paper

Getting Started: An Introduction to Voice Biometrics
2008

Biometrics 101: An Introduction to Voice Biometrics

introduction

This paper addresses the topics and areas of uncertainty that are most common for organizations beginning to consider voice biometrics as a security option for their business. The goal is to inform, to provide insight as to the possibilities of voice biometrics, and to help decision-makers answer initial questions. This paper does not provide an in-depth view of the Nuance Verifier technology, as that is available via other collateral on the Nuance web site at www.nuance.com. Topics discussed in this paper are:

- Use cases
- Common questions
- Important terms and concepts
- Key considerations

use cases

Current security practices of PINs, passwords and secret personal questions are not very secure, easily lost or forgotten, and regularly require being reset. Voice biometrics provides a relatively easy and cost effective solution to these problems.

Voice biometrics is most commonly applied via contact centers for telephone applications during which callers attempt to access sensitive data or services. Typically, voice biometrics are employed to verify a person's identity prior to granting access to a protected asset such as a bank account or authorizing an action such as a password reset.

Voice biometrics is also used outside of contact centers to provide secure access to physical locations or facilities. A simple handset is made available at a secure building or location entrance; an authorized person simply speaks into the phone to get verified via an automated application. Other uses include law enforcement's tracking of parolees who must call in to validate their location, military personnel call-home privileges, digital signature provision and employee scheduling systems. The applications are many, the security is high.

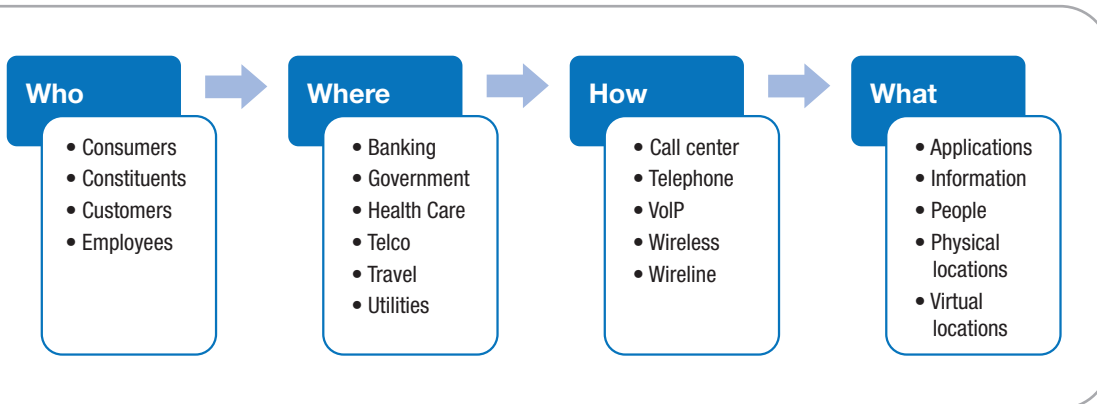


Figure 1: Use Cases for Voice Biometrics

common questions

What is a biometric?

A biometric system uses specific behavioral or physiological characteristics to determine or verify a person's identity. There are a many different types of biometric measures including iris scans, fingerprints, facial recognition, retina scans, spoken voice, signatures, keystrokes or even gait.

What is biometric authentication?

“Biometric authentication” is a generic term for the process of verification. It involves presenting a biometric for query, comparing the presented biometric to a stored template or model, and determining whether the individual has made a legitimate claim.

What is multi-factor authentication?

At its most basic, multi-factor authentication, sometimes referred to as “strong authentication”, refers to using more than one method to authenticate. Two-factor authentication, for example, uses two different factors for purposes of authentication. Human authentication factors are typically classified into three categories:

- Something the user has (e.g., ID card, security token, software token, phone, or cell phone)
- Something the user knows (e.g., a password, pass phrase, or personal identification number (PIN))
- Something the user is or does (e.g., fingerprint or retinal pattern, signature or voice recognition, or another biometric identifier)

Using more than one category of factor, such as requiring a password plus a biometric verification, offers stronger authentication assurance than just a single factor. The need for multi-factor authentication depends on the level of security required for a particular application.

What are the components of a biometric system?

A typical biometric system is comprised of five integrated components.

1. A sensor is used to collect the data and convert the information to a digital format.
2. Signal processing algorithms perform quality control activities and develop the biometric template.
3. A data storage component keeps information that new biometric templates will be compared to.
4. A matching algorithm compares the new biometric template to one or more templates kept in data storage.
5. Finally, a decision process (either automated or human-assisted) uses the results from the matching component to make a system-level decision.

What are the processes of a biometric system?

Biometrics systems follow four basic processes: collection, extraction, comparison and decision.

1. Collection involves using a sensor to capture the biometric traits and convert them to a digital format.
2. Extraction takes the digital data and converts the distinctive features into a compact template.
3. In the comparison step, the biometric system measures the likeness of the template to those in the database.
4. Based on the likeness, the system decides whether or not the submitted biometric matches one of the templates in the database.

How do I select a biometric technology?

The effectiveness of a biometric technology is dependent on the how and where it is used. Each biometric modality has its own strengths and weaknesses that should be evaluated in relation to the application before implementation. Key decision factors for selecting a biometric technology include evaluating the environment, throughput needs, population size and demographics, ergonomics, interoperability with existing systems, user considerations, etc. The careful evaluation of the key decision factors plays a crucial role in the success of the selected technology.

What is enrollment?

In a biometric system, an initial sample must be collected from known users to generate a reference model that will be used to evaluate all future samples collected. Since this model represents the secret code that will be used to lock out fraudulent access to the biometric system, it is important that the enrollment sample is collected from the correct person.

Therefore, an enrollment process typically involves authenticating a caller by some alternate means (perhaps by asking for a password or a series of knowledge questions) and then collecting a biometric sample from that person. Voice biometrics typically collects a series of sample phrases from the enrollee and uses them to generate the initial voice print.

What is speaker verification?

Peoples' voices are unique, just like their finger prints. Speaker verification, an application of voice biometrics, analyzes voice samples to extract key characteristics of a person's voice. This set of characteristics taken together is called a "voice print" (sometimes referred to as "voice template" or "voice model"). When a person enrolls into a system, a sample is collected. A voice print is extracted out of that sample and stored for future use. Simplistically, for verification, a voice sample is collected during a phone call and compared to the previously stored voice print. If they match, the speaker is verified. Speaker verification is sometimes referred to as voice authentication.

What is the difference between speaker verification and speaker identification?

Speaker verification is the process of verifying that an individual is who he or she claims to be via submission of an identity claim such as a name or account number. Verification checks that you really are Susan, seeking to pay a bill from your bank account.

Speaker identification is the process of associating an unknown speaker with a member in a population. Speaker identification, more commonly used in law enforcement, may capture a voice and cross-check it against a database of criminal's voices, looking for a match and therefore the identity.

Speaker verification is usually used in applications which require secure access. The systems operate with the user's knowledge and typically require their cooperation. Speaker identification systems are more likely to operate covertly without the user's knowledge.

What is the difference between speaker verification and speech recognition?

Speech recognition systems aim to understand the words that are being spoken. Speaker verification systems strive to confirm who is saying those words.

How secure is speaker verification?

Speaker verification technology from Nuance satisfies the most stringent security requirements. Nuance solutions capture specific physical characteristics of the human voice, using those characteristics to identify callers, something that other security measures just cannot do. This technology can also be a fundamental component of a multi-factor authentication approach. Speaker verification solutions support a highly secure, cost effective approach to customer multi-factor authentication over the voice channel.

Is speaker verification more secure than PINS and passwords?

PINs and passwords are easily compromised through intentional theft, user apathy and even shoulder surfing. According to Secure Enterprise Magazine, the average person has eight passwords to manage. 55% of people write down at least one password, and 9% write down all their passwords. Gartner Group research shows that in a typical enterprise, 30% of all help-desk calls are password-reset requests, and in some businesses, they account for as much as 60%.

Voices cannot be compromised, stolen or forgotten. A study by Touchpoint Consulting determined that consumers are comfortable using voice authentication as a means of secure access. Seventy-four percent of participants felt that speaker verification was more or equally secure than PINs.

Does voice biometrics technology impinge on privacy?

Like any technology, voice biometrics is defined by its usage. Biometrics is neither inherently privacy-protective nor privacy-invasive. The uses and controls of a biometrics system are what impacts privacy. With respect to applying privacy laws to biometrics, an important concept is the distinction between the two forms of biometric recognition: identification and verification.

Identification biometric systems are used to figure out who a person is and can occur without the person's knowledge or consent. Because identification systems require a databank that may contain personal information, and because they can be used without the subject's knowledge or consent, such as in surveillance, the privacy concerns are intensified.

Verification biometric systems work like PIN's or passwords. Unlike identification systems, verification systems are used on a purely voluntary basis, i.e. not secretly. Verification systems make sure you are who you claim to be. The need for the subject's consent greatly reduces the privacy concerns.

Despite the growing use of biometric technology, very few laws currently exist that even mention biometrics, let alone the use of biometrics with respect to privacy. Recognizing this, many governing and standards' bodies around the world, including the US Congress, the US Department of Justice, the National Science & Technology Council (NSTC), the Biometrics Institute, the National Biometric Security Council, are reviewing biometrics and the privacy implications.

How is voice biometrics used in the contact center?

In the contact center, voice biometrics is used primarily for secure access to information or assets. A speaker verification solution is based on a voice print provided by a user when enrolling. Nuance's speaker verification system then stores the voice print in the system database. Later, when the customer calls in to request access, the system compares the caller's voice to the print on file. If it is unclear, it may ask for additional information, or it may route the caller to a live customer service agent. Or, depending on the level of security the company has requested, it may refuse access.

Speaker verification is a natural fit for phone-based applications via the contact center because the system can be seamlessly integrated into the existing self-service experience of the caller

According to ContactBabel's report "US Contact Center Operational Review 2007", for a contact center with existing identity verification procedures of 20 seconds and ten million inbound calls per year, implementing a speaker verification system could save \$6.5 million each year.

Are Nuance solutions secure against recording and playback attacks?

Biometric authentication solutions must ensure that the biometric sample is actually collected from the person being authenticated. This can be particularly challenging over a phone network where there is no way to see whether the caller on the other end of the phone line is actually speaking or is playing a high quality recording of another person's voice.

Speaker verification solutions from Nuance prevent recording and playback attacks in several ways. First, Nuance technology can identify characteristics of a recorded vs. live voice. Secondly, some systems deploy multi-factor authentication as part of the security strategy. This requires more than just the spoken voice, often combining knowledge authentication, e.g., something that a caller knows, with speaker verification. Thirdly, Nuance solutions can implement a challenge-response method where the caller is instructed to repeat a short sequence of random phrases that could not have been pre-recorded.

What if a caller has a cold?

The complexity of the human voice allows for analysis of a large quantity of data points. While one part of the vocal tract may be affected by a cold, Nuance speaker verification can still accurately verify the caller's identity based on those parts of the vocal tract that are unaffected. Only extreme vocal change conditions, such as laryngitis, will prevent the caller from successfully accessing the system.

Don't voices sound different with time of day, age or sickness?

Voice does change over time, but Nuance speaker verification solutions are designed to handle those changes. To handle slow aging-related voice changes, Nuance systems regularly update users' enrolled templates. Voice changes during the day, such as "wake up voice", although noticeable to human ears, are ignored by the engines.

Can background noise influence a system's ability to verify?

Nuance technology uses special filters that handle background noises, thus permitting analysis of the relevant voice signal.

Can a caller use any telephone?

Nuance supports all telephone standards currently in use. Users may call from various telephones, mobile or landline, regardless of which type of phone they may have enrolled with.

How long does it take to enroll?

Enrollment is an automated process which takes less than a minute. During the process, a caller is asked to repeat keywords 3-4 times. Nuance guides the user through the enrollment process and confirms successful completion.

important terms & concepts*

TERM	DEFINITION
Biometric	A measurable physical characteristic or personal behavioral trait used to recognize the identity of an <i>enrollee</i> or verify a claimed identity.
Biometric application	The use to which a <i>biometric system</i> is put.
Biometric data	Extracted information taken from a <i>biometric sample</i> and used either to build a reference <i>template</i> on <i>enrollment</i> , or to compare against a previously created reference <i>template</i> .
Biometric sample	A <i>biometric</i> measure presented by the <i>user</i> and <i>captured</i> by the data collection system.
Biometric system	An automated system capable of capturing a <i>biometric sample</i> from an end <i>user</i> , extracting <i>biometric data</i> from the sample, comparing the data with one or more reference <i>templates</i> , deciding on how well they <i>match</i> , and indicating whether or not an <i>identification</i> or <i>verification</i> of identity has been achieved.
Capture	The process of taking a <i>biometric sample</i> via a <i>sensor</i> from a <i>user</i> .
Enrollment	The process of collecting <i>biometric sample(s)</i> from a person, and the subsequent preparation and storage of reference <i>template(s)</i> and associated data representing that person's identity.
Failure to acquire rate (FTA)	The failure to acquire rate is the proportion of attempts for which a <i>biometric system</i> is unable to <i>capture</i> an image of sufficient quality. When a <i>biometric system</i> allows multiple attempts, <i>FTA</i> measures <i>failure to capture</i> over these multiple attempts.
Failure to enroll rate (FTE)	The failure to enroll rate is the proportion of the user population for whom the <i>biometric system</i> is unable to generate reference <i>templates</i> of sufficient quality. It is the equivalent of <i>FTA</i> for the <i>enrollment</i> process, and depends on the procedures used in <i>enrollment</i> (which may differ from the procedures for later identification). It includes those who, for physical or behavioral reasons, are unable to present the required <i>biometric feature</i> .
False Acceptance	An incorrect <i>identification</i> of an individual, or an incorrect <i>verification</i> of an <i>impostor</i> .
False Accept Rate (FAR)	The probability that a <i>biometric system</i> will incorrectly identify an individual, or will fail to reject an <i>impostor</i> . For a positive (verification) system, it can be estimated from: (the number of false acceptances) ÷ (the number of impostor verification attempts).
False Rejection	A failure to <i>identify</i> or <i>verify</i> a genuine <i>enrollee</i> .

TERM	DEFINITION
False Reject Rate (FRR)	The probability that a <i>biometric system</i> will fail to identify a genuine <i>enrollee</i> . For a positive (verification) system, it can be estimated from: (the number of false rejects) ÷ (the number of enrollee verification attempts).
Identification	The process of using a submitted <i>biometric sample</i> for comparison against the set of enrolled <i>templates</i> to match a <i>user</i> to an <i>enrollee</i> . (Normally used only in <i>one-to-many</i> systems)
Identification system	Identification systems, where the user makes no explicit claim to identity, may be compared to verification systems. Without a claimed identity, the <i>biometric system</i> does a <i>one-to-many</i> process of <i>comparison</i> against all <i>enrollees</i> in its database.
Impostor	A person making a false claim about <i>identity</i> to the <i>biometric system</i> .
Matching score	A measure of similarity or dissimilarity between the <i>biometric data</i> and a stored <i>template</i> , used in the comparison process.
Negative claim	A claim by a <i>user</i> not to be enrolled in the <i>biometric system</i> . This may be needed to establish that double claims are not being made.
One-to-many matching	See <i>identification system</i> .
One-to-one matching	See <i>verification system</i> .
Positive claim	A claim by a user to be <i>enrolled</i> in the <i>biometric system</i> . An explicit claim is often accompanied by a user identification, and may also be associated with a password or PIN.
Sensor	The physical hardware device used for <i>biometric capture</i> .
Template	A user's stored reference measure based on <i>biometric feature(s)</i> extracted from <i>biometric sample(s)</i> .
Template ageing	The gradual change of a user's <i>biometric feature(s)</i> which requires periodic updating of the user's reference <i>template</i> .
Threshold	A parametric value used to convert a matching score to a decision. A threshold change will usually change both <i>FAR</i> and <i>FRR</i> – as <i>FAR</i> decreases, <i>FRR</i> increases.
Verification	The process of using a submitted <i>biometric sample</i> for comparison against a <i>template</i> to match a <i>user</i> to a known <i>enrollee</i> . (Normally used only in <i>one-to-one</i> systems, where the user may also have to specify a user name and/or password or PIN)
Verification system	Verification systems, where the user explicitly claims an identity, may be compared to <i>identification systems</i> .

* Provided by CESG (Communications-Electronics Security Group), the Information Assurance (IA) arm of GCHQ (Government Communications Headquarters) in the UK.

key considerations moving forward

Procedures & Usability

A working voice biometric system needs established procedures to define how it works and how it maintains security. Perhaps most importantly, attention must be turned to the usability of the system: how will users interact with it, and in what circumstances? Some key considerations include:

- What procedures will be used for user enrollment? How will the enrollment process check the identity of the enrolled person?
- How is a user treated if the system (wrongly) rejects him or her?
- Should multi-factor authentication procedures be implemented for heightened security?
- Is the system to be used for positive identification (making sure that the potential user is the person claimed) or for negative identification (preventing the enrollment of someone already known to the system)?
- Will it be used overtly (as for normal identification systems) or covertly (e.g. for surveillance)?
- Will users be regularly exposed to the system and therefore familiar with it, or is usage likely to be infrequent?

Costs

As for any decision on project management, a justifiable business case will be needed – in which the biometric system is compared with a number of other options. In addition to costs of purchase, installation, training, maintenance etc. which are part of any IT system, the following need to be considered for biometrics:

- Costs of enrolling users,
- Costs of alternative procedures (for failure to enroll, or failure to accept),
- Costs for environmental controls.

Other IT Aspects

In considering a biometric system, other aspects of IT systems need to be considered. For example:

- What computer resources (CPU power, template storage space, networks etc.) are required?
- Are there maintenance and backup costs?
- Will there be hardware and/or software upgrades later?

about Nuance Communications

Nuance is in the business of helping companies better support, communicate with and understand their customers while maintaining operational efficiency goals. Nuance currently supports over 8 billion care interactions around the world. No other company has as much experience as Nuance in understanding how customers interface with a care operation. Our vision is to make every customer interaction a winning experience. For more information about our customer interaction solutions, business consulting and professional services, please visit www.nuance.com/care or call 781-565-5000 and say “care.”

Copyright © 2008, Nuance Communications, Inc. All right reserved. Nuance, the Nuance logo, The experience speaks for itself, AccuBurst, Dynamic Language Detection, Grammar Builder, It's Me, Listen & Learn, Say Anything, Speak As One, SpeechObjects, V-Builder, Nuance Verifier, Nuance Vocalizer, Nuance Voice Platform, Nuance Voice Web Server, V-Optimizer, and Voyager are trademarks and/or registered trademarks of Nuance Communications, Inc. and/or its affiliates in the United States and/or other countries. All other trademarks are the properties of their respective companies. WP 071008 NUCC205