

Conversational Biometrics

Highlights

Detect and prevent fraud

Improve security and user experience

Award winning biometric recognition accuracy

Combine multiple verification sources, including voice biometrics and spoken knowledge using patented dynamic policy management

Support for various environments and telephony platforms using an open XML/TCP architecture

Harnessing Speech Technology to Combat Credit Card and Banking Fraud

What is Conversational Biometrics?

Conversational Biometrics (CB) combines powerful and accurate acoustic text-independent speaker recognition with additional verification sources such as spoken knowledge to create the most flexible and robust user verification and detection solution to the banking fraud problem.

Legacy user verification systems are designed to validate an identity claim of a user by eliciting input such as passwords, keys, and biometric data. However, in real life users do not just get accepted. They get accepted to a certain degree of security that allows them to carry out specific tasks. IBM Research has recently addressed that requirement by introducing the concept of *security policies*. A system that uses CB does not necessarily accept a user solely on the basis of single identity evidence, but may prompt the user to provide multiple and additional sources of identity evidence until the rules mandating the security policy are satisfied. This approach provides the flexibility of adapting the way users get verified to the level of risk. By prescribing a tighter policy, the user's

identity can be verified to a very higher degree of certainty. On the other hand, for low risk transactions, user verification can be performed in an efficient and cost effective manner.



The benefit of using speech for user verification

When user verification is performed by a conversational system such as an automated voice response unit, the rich information present in the user's voice should be used for user verification. A user's voice conveys both knowledge (content) and a biometric indication of the user's identity. Conversational Biometrics uses the *same* speech signal to verify both the user's knowledge and the user's voice. Every user utterance is shipped to a text independent speaker recognition engine for automatic voiceprint analysis, as well as a speech recognition engine that extracts the spoken text.

Policy Management

Based on the security policy, a CB Policy Manager (CBPM) decides at any point of interaction with the user

whether to elicit more speech from the user, accept the user, or reject. Every new utterance is analyzed both for content (spoken text) and for speaker characteristics (biometrics). The CBPM can be used to combine acoustic verification with knowledge verification. However, it actually provides a much broader framework that allows to dynamically combine any multiple verification sources, such as possession-based verification (e.g. key, caller-ID) and other types of biometrics (e.g. fingerprint, iris).

The CBPM is a framework that allows dynamic generation of verification challenges on the fly, such that the verification session will obey a predefined security policy. It has access to a pool of possible verification challenges, or Verification Objects (VO's). Examples of a VO include knowledge topics (mother's maiden name, favorite color, application-specific topic), possession-based VO's (caller-id or key), and different biometrics (fingerprint, keyboard stroke, retina). A security policy is a Finite State Machine (FSM) that at each state includes either a specific VO or a list from which a VO will be randomly chosen at run time. The FSM always ends in either *acceptance* or *rejection* of the user.

When a user enrolls in a CB system, a user *profile* is created, including the different VO's that may be used to verify that user. For example, if the user provided knowledge data such as mother's maiden name or favorite color, then both the questions and the answers will be in the profile. The CB system also requires the user to provide a voice sample from which an acoustic speaker model (or "voiceprint") is created.

When the system receives a request to verify a user in accordance with a policy, it loads the policy, and invokes the first VO in the policy state machine. Based on the result of the first invoked VO (level of acoustic score, match of knowledge value, etc.) the system determines which state of the policy FSM to branch to, and consequently what next VO to invoke. This process

iterates until either an acceptance or rejection state is reached. Since the decision is made in run-time, based on the actual result of each invoked VO, the VO's are said to be generated dynamically.

Ongoing Verification

Is it still you?

Legacy verification systems use a dedicated verification session to determine the user's identity. However, the IBM Conversational Biometrics System uses a text-independent speaker recognition engine that allows user verification to continue in the background *after* the user has already been verified. Verification can continue while the user interacts either with an automated banking system or a human agent.

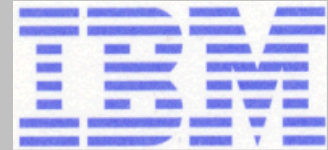
Fraud Prevention and Detection

Conversational Biometrics may be used for user verification and fraud prevention. It can also be used together with existing rule-based and neural network transaction analysis fraud detection systems. For example, the acoustic speaker recognition engine can be used to determine the user identity in non-repudiation cases. It can also efficiently analyze large amounts of recorded audio to detect "familiar" voices from previously detected fraud cases.

Award Winning Biometrics Engine

How well does it do?

IBM Research has recently won the first place, among 25 worldwide participants in an evaluation conducted by the U.S. National Institute of Standards and Technology (NIST). The evaluation is comprised of a speaker verification task on challenging cellular telephony conversational speech.



Contact:

Ganesh Ramaswamy, Ph.D.
Manager, Conversational Biometrics
IBM T. J. Watson Research Center
1101 Kitchawan Rd.
Yorktown Heights, NY 10598
(914) 945-1833
ganeshr@us.ibm.com

<http://www.research.ibm.com/CBG>