Voice recognition – benefits and challenges of this biometric application for access control

Published on 9 Jun 2010

Consumers prefer voice recognition technology for biometric identification

Voice recognition is the most preferred form of biometric identification among consumers. Derek Scheips for ASSA ABLOY Future Labs outlines the concept behind this technology and some of its uses and drawbacks.

With all types of biometric applications on the rise, voice-based authentication is one approach that seems to engender less resistance among users than other biometric forms of security. Voice recognition is non-contact, non-intrusive and easy to use.

According to a Unisys survey, the biometric measures ranked by consumer preference are: voice recognition (32%), fingerprints (27%), facial scan (20%), hand geometry (12%), and iris scan (10%). This ranking seems to confirm that people prefer convenience and familiarity when choosing a biometric technology.

Dr. Judith A. Markowitz is a speech and biometrics consultant based in Chicago, whose clients...
include Motorola, VoiceVerified and West Corporation. According to Dr. Markowitz, the first step to understanding this kind of biometrics is to make the key distinction between voice / speech recognition - a system's ability to process "what a person is saying" - and speaker verification, "technology based on an individual vocal physiology and behaviour to validate a claim of identity."

**How speaker verification with voice recognition works**

Voice recognition technology is possible after making a digital model of an individual's voice that can serve as a stored profile or template of that voice print. Words and phrases are broken down into various kinds of frequency patterns that, taken together, describe someone's unique way of speaking. The templates are stored in databases for matching like other kinds of biometric data.

These systems can be text dependent or text independent (and sometimes a combination) and used, for example, to control access. For the first option, numbers or phrases can become spoken passwords that can be compared to a sample of those same words that was acquired during
enrolment. Text independent technology does not require a pass phrase but analyzes the speaker’s free speech for unique vocal characteristics.

Big pluses of speaker verification are its widespread acceptability and ease of use for callers, as well as the relative inexpensiveness of basic systems compared to some other biometric options (especially if voice authentication is integrated into a telephony system for, say, a financial services firm that already has voice recognition as part of its customer service).

Not surprisingly, most applications for speaker verification involve a phone, for such commonplace actions as conducting telephone banking or consumer transactions, password reset and checking customer accounts of many sorts, and securing access to the very telephones themselves.

**Practical applications of speaker verification**

When it comes to protecting physical access, speaker verification can be used, for instance, to log warehouse employees with wearable/portable voice-data collection systems as they move about an environment during work, or to facilitate remote alcohol testing of DUI-convicted felons on community release. Speech verification combined with GPS is also being used to keep track of security guards to make sure they are making their rounds, and not relying on friends to do it for them.
Unlike most forms of biometric identification devices, voice activation recognition works in subzero temperatures.

Dr. Markowitz highlights two examples in the United States of speaker verification's potential for protecting access: "The city of Baltimore, Maryland had a system on the doors of five of its city buildings to monitor employee access during off hours, where the system was also used for time-and-attendance log on. This includes logging on at one's desk computer. They were experiencing theft and this addressed the problem."

Speaker verification was also used as part of a multi-security system that controlled the border crossing at Scobey, Montana, until all such remote monitoring systems were dismantled after 9/11. Observes Markowitz: "Since Scobey sometimes dipped to 60 (51 Celsius) or more degrees below zero, it wasn't feasible to use most other form of biometrics. But today, voice verification is not generally thought of for site access because there are so many other ways to control a space and some of the other biometric methods, such as fingerprinting, are faster.

Other challenges with voice recognition

Additionally, as security expert Glen Greer notes, voice recognition for access systems is not terribly reliable. "It is my experience that voice-based systems have very high error rates, particularly in terms of false rejections."
Many challenges affect its accuracy. These include poor-quality voice samples; the variability in a speaker's voice due to illness, mood, changes over time; background noise as the caller interacts with the system; and changes in the call's technology (digital vs. analogue, upgrades to circuits and microphones, etc).

Another critical issue is the lack of established international standards. "We need a standard application programming interface (API) to reduce the issues with cost, interoperability, time-to-deployment, vendor lock-in, and other aspects of building applications," observes Markowitz. "So far, law enforcement, telecommunications services, and financial services in different countries, are using speaker verification but an API standard will make it easier and more attractive for integrators and others."

Derek Scheips
Freelance Writer
Assa Abloy Future Labs
Access control manufacturers address biometric myths & end user miscon...

A number of misconceptions exist about the capabilities and technology of biometrics, perpetuated in popular culture by films a...