Introduction to SVAPI

Judith Markowitz, Ph.D.
President, J. Markowitz, Consultants &
Member, SVAPI Working Group

What Is SVAPI?

Speaker verification application programming interface (SVAPI) is a open interface for developers of voice-biometrics (speaker verification, speaker identification, and speaker classification) applications. SVAPI Version 1.0 was deployed in the fall of 1997. It was the first API standard in the biometric industry.

SVAPI was constructed by the SVAPI Working Group, a committee of speaker-verification vendors, application developers, researchers, independent software vendors, end user organizations, and others interested in establishing API standards for biometrics. The SVAPI effort was sponsored by Novell Corporation.

Why Have API Standards for Speaker Verification?

One core objective of the SVAPI effort has been to make it easier for product and application developers to use voice-biometrics tools and technology. The SVAPI Working Group believes that this will encourage developers to proceed with plans they might have to incorporate voice biometrics into their products and applications.

Application and product development activity with voice biometrics is increasing. Both public and private sector organizations are using speaker verification, in particular, in a diverse range of security and monitoring applications. The deployment by Home Shopping Network for ordering, Intrust Bank for electronic transfer, and BMC Software for password reset are examples of growing use by the private sector. Numerous deployments of speaker verification for monitoring of home- and community-incarcerated prisoners and the implementation by the United States Immigration and Naturalization Service of speaker-verification security at a remote port of entry with Canada are illustrations of interest in the public sector.

There are numerous benefits associated with establishment of a standard API. The most notable of them are to

1. Make It Easier to Switch Products

It is treacherous enough for organizations to take a chance on a new technology without also having to bind themselves to a specific vendor and product. Yet, this is the situation that faces developers today. The reason is that each tool developer has its own API. Any change of products generally requires starting from scratch. There is no guarantee that

- the selected product (or vendor) will meet the requirements of the application,
- the product (or vendor) will survive, or
- the product will contain the best speaker verification technology for the application in the future.

These represent strong deterrents to using voice biometrics and other biometrics as well.

2. Address Issues of Large And Small Systems in a Systematic Manner
Until Home Shopping Network began deploying its speaker verification system, virtually all voice-biometrics applications had been fairly small. Increased concerns about the security of Internet transactions, the growth of voice portals, and enterprise-level data security issues highlight the need to address large scale applications and distributed systems. At the same time, there has been increased interest in deploying speaker verification in wireless telephone handsets and other hand-held devices. The SVAPI effort is addressing those issues by bringing together representatives from organizations involved in large and small application development.

3. Facilitate the Integration of Voice Biometrics with Other Tools
Integration covers a broad area that includes

- *Combining voice-biometrics tools from different vendors*
  When applications using different speaker verification products have different APIs the responsibility for making them work together rests entirely on the shoulders of the application developer. Some of those applications are using both speaker verification and small set speaker identification from different vendors. Some use text-dependent verification from one vendor and text-prompted verification from another. A standard API encourages application and product developers to engage in these activities by reducing the development challenges and risks.
- *Combining voice-biometrics with other biometric tools*
  Future security and monitoring applications will include multiple forms of biometric-based technologies. Creating a standard API for voice biometrics is one step towards making it easier to incorporate create multi-biometric applications. Creation of API standards for other biometrics would further enhance the growth of multi-biometric applications.

- *Integration with non-biometric security*

Many organizations recognize the limits of their existing security systems, but they prefer to enhance them rather than replace them with a new technology. Consequently, one of the most common application scenarios today is the integration of voice biometrics (primarily speaker verification) with non-biometric security systems already in place, such as card-access, PIN, and password systems. A standard API makes it more desirable to move forward with plans to use speaker verification.

- *Speech recognition*
  One of the strongest trends in the use of voice biometrics is to integrate speaker verification and/or speaker identification with speech recognition. Generally, this is done as an expansion of an existing speech-recognition application to include operations that require security. A standard for voice biometrics simplifies the system integration issues related to these applications.

SVAPI Mission

SVAPI is designed to be

- *An Open Interface*
  The SVAPI standard is not controlled by any single entity. This includes individual vendors and it includes Novell, the sponsor of the SVAPI effort. SVAPI does not focus on Novell environments nor is it limited to the environments in which Novell software operates. Rather, the workgroup designed an open standard industry-wide standard governing interaction between speaker verification tools and products and other software and operating systems.

- *A Cross-Platform Solution*
  The SVAPI Working Group believes that a basic requirement for widespread acceptance of a standard API is support of large-scale, distributed, and heterogeneous applications.

- *A Comprehensive Security Solution*
  SVAPI was designed to handle the principal requirements of data security, physical site security, land line telephone, cellular telephone, computer product security, monitoring, and other applications.

- *Extensibility*
  The SVAPI Working Group believes that a standard must be able to grow and evolve with the marketplace.

- *A Collaborative Effort*

SVAPI was designed by an industry-wide working group that includes leading speaker verification vendors, researchers, system integrators, computer software developers, and other interested organizations. Working group members include British Telecom, CitiCorp, Dialogic, IBM, ITT, Motorola, Novell, Oracle, T-NETIX, Texas Instrument, and the US Immigration and Naturalization Service

The SVAPI Working Group also recognizes that a specification meeting the aforementioned objectives must also be constructed so that it has no negative impact on accuracy for security, monitoring, or any other task performed by SVAPI-compliant engines.

The SVAPI Specification

SVAPI contains both high and low-level function and protocols. At the highest level are generic functions for enrollment, verification, identification, and classification. At the lowest level it is possible to indicate features of the sound stream. It also supports various types of scoring; and characterization of input from microphones and telephones.

The SVAPI specification supports the range of voice-biometrics engines in the marketplace: text dependent, text prompted, and text independent verification. It is constructed to be extensible in ways that support emerging features of future voice-biometrics engines.