

The Development of Destination-Specific Biometric Authentication

Andrew R. Mark
President, Smart Tone, Inc.

Smart Tone, Inc., (“STI”) a developer of biometric authentication systems, has developed a unique method to authenticate a user of its system without the drawbacks normally associated with biometric characteristics, such as the creation of a stable electronic identifier that can be used to track and monitor a user and thus greatly reduce his or her privacy.

Biometrics is the science of identifying a person through the electronic examination of his or her physical characteristics (e.g. fingerprints, voice, or retina patterns). These methods are extraordinarily useful as protections against fraud as well as an impediment to unauthorized electronic access to data networks. Biometric systems allow only those persons possessing a unique biological characteristic to present themselves as the authentic person in a non-face to face transaction over the telephone or a computer network.

It has been generally accepted knowledge in industry that increased security is only possible if a person’s privacy is diminished or somehow compromised. For example, most people are required to submit a Social Security number with virtually every application for any conceivable product. The Social Security number theoretically increases security because it is possessed only by the correct individual and therefore could only be known to that person. However, the more the number is dispersed through society, the easier it becomes for a person to be tracked by its activity. A Social Security number becomes a common identifier.

A biometric characteristic is also capable of becoming a common identifier. Normally, the biometric authentication process involves a comparison of a “live” personal characteristic with one that has been stored on a database. The existence of these databases provokes great concern, since a biometric characteristic, like a Social Security number, can be used to track a person’s movements and transactions.

However, the existence of digitized biometric data must cause *greater* concern because it identifies a person with extremely high levels of accuracy. While a driver’s license, Social Security number or credit card number may be stolen secretly and used to impersonate someone, a biometric can be linked only to a specific individual (with only small levels of false identifications) so that fraud may be discounted. In other words, if a biometric can be traced to one person,

it must be from that person.

As security methods such like biometrics become more reliable and pervasive, public criticism has grown in response to their increasing use. The global economy now moves towards the routine electronic storage and dissemination of all types of information. The legitimate fear expressed by many is that once an individual's biometric characteristics are incorporated within worldwide electronic communications, they will allow anyone to track them and attain personal information about the owner's likes, dislikes, political viewpoints, sexual habits, and health history. It can and should be argued that since biometric systems can potentially effect Constitutionally protected areas of a person's life, it should become necessary for biometric a system to accommodate privacy interests.

Smart Tone, Inc. has developed a biometric system that can perform high-level security functions to identify an individual without the use of a universal identifier. The STI platform accomplishes this by performing cursory analysis of a person's voice pattern for authentication. It compensates for any loss of security due to the cursory analysis by incorporating a user device into its functioning which transmits dynamically changing personal identification data to a platform. However, Smart Tone's method is not limited to voice alone, but may be implemented with any type of biometric (retina, fingerprint, etc.).

The elements of the STI authentication system are:

A. A user device, called a SmartKey™, which includes a tone dialer about the size of a car key that can fit easily onto any key chain, as well as access numbers for up to 50 user-selectable countries.

B. A State Machine

a. that acts as a user-specific utterance evaluator, which determines upon registration:

(i) If a proposed utterance can produce consistent and reliable values repeatedly derived from the phonetic composition of the utterance (i.e., it contains robust elements which can survive impairments caused by voice channel transmission and their subsequent normalization so that the same values may be derived from them reliably over time);

(ii) Whether the impaired iterations contain the same phonetically identifiable elements as the unimpaired elements; and,

(iii) If all the modified and unmodified utterances of the user's proposed passphrase derive the same values;

AND

b. which during every authentication:

(i) Normalizes the communication channels to eliminate transmission (including microphone and line) variances;

(ii) Evaluates the utterances into phonetic elements (identifies phonemes, bracketed frequencies and duration levels); and

- (iii) Converts identified elements into numerical coefficients;
 - A. A destination specific encryption of the derived user ID; and,
 - B. A numeric description of the user which is destination specific.

The following paragraphs will describe how the system operates and will assume the use of voice as the chosen biometric.

STEP ONE: Issuance of the Devices: It is very important that the SmartKeys™ be issued in such a manner to prevent STI from gaining personal information about the future user of the device. One method is to place an intermediary between the issuer of the device (e.g. phone card company, credit card company) and STI. In STI's plan, the Issuer shall provide a list of names and addresses from its customer database to a regional distributor for the SmartKeys™. The distributor will send invitations to customers which contain an issuer-specific toll-free number for them to dial to request the STI service. Each letter also contains an invitation number the customer must enter over the telephone. Once the user has made the phone call, the distributor will send the SmartKey™ to user at the address provided by the issuer or to a shipping address if it has been approved by the distributor's customer service. The user will receive the SmartKey™ by mail along with instructions on how to use the key and to complete registration.

STEP TWO: Evaluation of the Voice Characteristics. This step occurs during the registration process when a person utters a proposed pass-phrase that is "recorded" within the system for evaluation. (This is done before the phrase shall ever be used for authentication purposes). Evaluation requires the person to speak the passphrase three times. The system (1) examines the utterance for its phonetic content and derives values based on those components; (2) Normalizes the utterance based on patented "System Adjustment Tones" ("SATs") and derives values based on the components; and, (3) Imposes wire-line impairments on the normalized utterance and derives the same values.

The system then examines all the derived values and determines which values are consistent between each of the three versions and are therefore the most reliable information for authentication purposes. Inconsistent values will be ignored. Any remaining, consistent values are strung together to form an identification number. Once the system determines that the resulting number is robust enough for identification purposes, it notifies the user that the chosen pass-phrase is acceptable for use as an identifier in an authentication and records the values. However, it must be noted that the person's individual voice patterns has NOT been placed on file.

STEP THREE: A Normal Authentication. Once this evaluation session is complete, a user may perform a voice authentication with any destination. When the user makes the connection to the STI platform, a voice prompt will ask the user to use his or her SmartKey™ and speak the same pass-phrase with which the user registered.

After the person speaks the passphrase into a microphone or other input device, the platform, as during the evaluation process, breaks the sentences down into syllables and assigns values to the phonetic components (phonemes) as it did during registration. The components include: (1) an identification number for each syllable; (2) a value for the duration of each syllable; (3) values for the frequency ranges of the syllables; (4) values for average duration of the phonemes; and, (5) a ranking of the frequency levels.

However, the platform cannot locate the user's voice file using the phonetic alone. The SmartKey™ is designed to emit a dynamic identification string used to identify the key. The STI platform uses this number string to locate the numerical coefficients related to the person's voice within the platform. The device-data emitted creates a number string identical to name of the person's voice file. Those coefficients cannot be found without the data from the key itself so that BOTH key and the person must act together to complete an authentication.

Once the correct file is located and the data within is compared to the live sample given, the appearance of the same robust phoneme selections, cadences, frequency ranges and relative phoneme levels in combination with full word text recognition provides an excellent, high-security means of user-specific verification.

The result is a number string, called a Destination ID, which represents a person's voice pattern as alphanumeric values. STI then encrypts the number string with a special algorithm used only for that particular destination. This encrypted Destination ID produces the identification values, called a Destination-Specific User Identification number ("DSUID"), which the destination uses to authenticate a person.

Therefore, during a SmartKey™-initiated call, information regarding the identity of the user is always protected from improper disclosure. Additionally, the DSUID's destination specific encryption insures that the user's identity is known at only one destination, unless the user should request the identity be known at another destination.

The DSUID is generated in such fashion that reversal of the string is simply not, as a practical matter, possible. The DSUID is an identifier that is generated algorithmically using a two inputs- the unique, 128-bit user ID, which identifies the user's SmartKey™, and a 64-bit identifier representing the Destination. The Destination ID is encrypted using a symmetric encryption algorithm, while the User ID acts as the 'key'. The result of this manipulation is the User's Destination Specific User Identity. While the Destination will always receive the same DSUID for a specific customer, the DSUID, unlike a Social Security number, that is received at one location is not applicable (or used!) at any other visited destination and cannot be used for the purpose of pooling data or cross-database queries without the user's specific authorization.

Once the platform has transmitted the DSUID to the destination system, the destination shall search its records for it. If the destination has no record of the DSUID transmitted, the destination will conduct a manual authentication (i.e. with a live person such as a customer service representative) which requires the person to input personal information to identify the person as someone authorized make any transaction. When the destination recognizes the person, it will equate the identification number string with that person.

In the future, when the values delivered match what the destination has recorded as an authorized person's values, an authentication may take place. If they do not match, access to the destination's system would be denied to the user.

If the values presented are notably similar to the values on record, yet not identical, the system could request personal information from the user via voice prompt (Social Security number, date of birth, etc.) which would provide the extra security to allow the transaction to be completed.

The Smart Tone system, which combines a user device, one or more biometrics, and destination-specific encryption can and will provide high-level electronic security without the loss of personal privacy.