Dynamic Biometrics: The Case for a Real-Time Solution to the Problem of Access Control, Privacy and Security

Steven J. Simske

HP Laboratories
HPL-2009-317

Keyword(s):
security, biometrics, access control, identity

Abstract:

From a certain perspective, security is broken. The security authorization triangle (possession, knowledge, identity) has in some cases been reduced to a single point (knowledge) because of the limitations to possession attributable to virtualization, and because of the limitations to identity attributable to the use of static biometrics. This paper makes the case for a stronger security rights triangle - privacy, security and access control - underpinned by the resurrection of possession and identity through the use of dynamic biometrics. New technologies in mobile and cloud computing, pattern recognition and user interaction provide a potential path forward for an identity-matching ecosystem in which both privacy and security needs can be accommodated.

External Posting Date: September 21, 2009 [Fulltext] Approved for External Publication
Internal Posting Date: September 21, 2009 [Fulltext]

Presented at IEEE BIdS Conference, Tampa, Florida, Sept 22-23, 2009.

Dynamic Biometrics: The Case for a Real-Time Solution to the Problem of Access Control, Privacy and Security

Steven J. Simske, *Senior Member, IEEE*

***Abstract*—From a certain perspective, security is broken. The security authorization triangle (possession, knowledge, identity) has in some cases been reduced to a single point (knowledge) because of the limitations to possession attributable to virtualization, and because of the limitations to identity attributable to the use of static biometrics. This paper makes the case for a stronger security rights triangle—privacy, security and access control—underpinned by the resurrection of possession and identity through the use of dynamic biometrics. New technologies in mobile and cloud computing, pattern recognition and user interaction provide a potential path forward for an identity-matching ecosystem in which both privacy and security needs can be accommodated.**

I. Introduction to Biometrics for Security

BIOMETRICS, meaning the assignment of identity through the measurement of physical attributes or behavior, is increasingly used for security purposes. From authorization to authentication, security professionals are adopting more sophisticated measurements in an effort to staunch rampant theft of personal information, access privileges and even identity itself.

A non-exhaustive, but representative, set of human biometrics includes physical, behavioral and innate—or chemical—biometrics [1]. A brief description of these classes of biometrics, as defined for the purposes of this paper, is provided next.

Physical biometrics (Table I) include (1) face recognition—which is captured with increasing sophistication, even with non-frontal views and glasses or other obstructions; (2) fingerprint representation—which usually represents a few dozens points and/or curves of interest on one or more fingers; (3) hand geometry—physical outline, shape and/or size of the hand; (4) iris recognition—the peri-pupillary portion of the front of the eye; (5) retinal recognition—the photoreceptor layers inside the back of the eye; and (6) vein recognition—usually the earlobes, or more commonly on a hand. These physical biometrics are the most static of all biometrics. Relatively constant, if they are stolen, the stolen data stays relevant thereafter. If you are dependent on these for your identity, your identity is only as strong as the weakest link in the whole system around the biometrics. This could be access to measurement itself (e.g. collecting your fingerprint from a surface), to the sensor registers, the transmission, or the backend data/caches, etc.

Manuscript received June 15, 2009.

S.J. Simske is with Hewlett Packard Laboratories, Fort Collins CO 80528 USA (phone: 970-898-9561; e-mail: steven.simske@ hp.com).

Behavioral biometrics (Table II) include two biometrics often listed as "physical" biometrics; namely (1) heartbeat—the electrocardiogram or ECG/EKG, vectorcardiogram or VCG, blood pressure, cardiophonics, etc.; and (2) voice recognition—based on the individual's characteristic formants, or vocal resonant frequencies [2], accent [3, 4] or other identifying auditory identifiers. Since these biometrics are based on multiple signals—or a continuous signal—they are labeled here as "behavioral" since they cannot be computed from a single "scan".

TABLE I
PHYSICAL BIOMETRICS

Biometric	Measured Parameter
Face	Feature location, shape, size, etc.
Fingerprint	Whorls, points of interest, etc.
Hand	Shape, size, perimeter, etc.
Iris	Distribution of high-interest features
Retina	Vein, etc. distribution
Vein	Location map (size weighted)

TABLE II
BEHAVIORAL OR "CONTINUOUS" BIOMETRICS

Biometric	Measured Parameter
Arm sweep	Location and velocity
Fingerwriting	Location and velocity
Gesture	Location, velocity, shape and size of hand, etc.
Handwriting	Location and velocity
Heartbeat	ECG, VCG, pressure, sound
Keystroke	Latencies, pressures, etc.
Voice	Cepstrals, formants, accent, etc.
Walking	Gait

Other behavioral biometrics include (3) arm sweep action—analysis of how an arm moves through space; (4) fingerwriting—analysis of how a person uses a touchpad; (5) gesture analysis—analysis of how a person uses her hands in a task; (6) handwriting/signature—analysis of how a person writes; (7) keystroke dynamics—analysis of how a person types (latencies, pressures, etc.); and (8) walking (gait) analysis. These motion-based biometrics are also relatively "static" in the manner in which they are presently used, since storing information on multiple tasks in these areas is onerous or poorly supported. However, unlike physical biometrics, they offer a pathway to dynamic biometrics, described below.

Innate or chemical biometrics (Table III) are those not usually associate with physical or behavioral/continuous biometrics. These include, but are not limited to, (1) DNA or related (RNA, mitochondrial DNA, HLA typing, etc.) genetic

material; (2) tissue assay (chromatography, ligand binding, immunoassay [ELISA, etc.]); and (3) mass spectroscopy. These are typically more difficult to obtain than the physical biometrics, more expensive to analyze/assay, and no more suitable (being "static" information) than physical biometrics for the task of dynamic biometrics. For these reasons, innate biometrics will be discussed no further in this paper.

TABLE III
INNATE OR CHEMICAL BIOMETRICS

Biometric	Measured Parameter
Genetic	DNA, RNA, mDNA, HLA, etc.
Tissue Assay	Protein composition, etc.
Mass Spectroscopy	Chemical composition, etc.

II. SECURITY IS BROKEN BUT CAN BE FIXED

Security is broken. The security authorization triangle (possession, knowledge, identity) has in some instantiations boiled down to a single point (knowledge) because of the limitations to possession attributable to virtualization, and because of the limitations to identity attributable to the use of static biometrics. This paper makes the case for a stronger security rights triangle—privacy, security and access control—underpinned by the resurrection of possession and identity through the use of dynamic biometrics.

The security authorization triangle consists of possession (assurance that you have an object required for authorization in your possession), knowledge (you have information that is required for authorization) and identity (you are who you claim to be). One device that illustrates this triangle is the ATM (automated teller machine): to use it, you have the card (possession), know the personal identity number, or PIN (knowledge), and are being filmed by the surveillance camera (identity, at least in theory—though not generally validated at this time). A sometimes overlooked fourth element in security—location—is also known for an ATM.

However, not every authorization works this securely (ignoring the caveats with ATMs for the moment, such as lack of identity proof and the ease of fraudulent alteration of the interface [24]). As mentioned above, the security rights triangle in some cases degenerates to a single point (knowledge) because of the limitations to possession attributable to virtualization (which also may eliminate location), and because of the limitations to identity attributable to the use of static biometrics (or the omission of any of these). Consider logging into a computer. You can log in remotely, and you can claim to be any user whose password you have discovered (through stealth, intelligent guessing, keyboard entry trapping, coercion, bribery, etc.). It all boils down to knowledge. And once you're in, you stay in, with all the access rights and privileges of the user whose identity you have feigned. In addition, the recent explosion of social networking sites has rendered "personal" questions such as "What is you dog's name?" less secure [25]. Despite this, these types of "personal" questions continue to be used in a security role.

In addition, the most commonly used biometrics—face, fingerprint, iris, retina and vein matching—are static in nature. That is, they are facts—once known, they do not (appreciably) change. This means a randomly-selected person is not likely to have a static biometric that matches yours. But it also means that once information on one of your static biometrics is known, you cannot use the biometric anymore. And, simply using a different finger each time a previously-used finger is compromised is unsustainable.

It is easy to point out what is wrong with a solution. Providing an alternative—and hopefully a solution—is more challenging. I herein claim that to fix this broken security a transformation is needed. To describe this transformation, which involves a new security layer altogether, I next describe the security rights triangle.

If the triangle of possession, knowledge and identity are to collapse into a single point, it is best that it be identity. Not identity-as-knowledge, e.g. a fingerprint, but identity as in passing-the-Turing-test identity. Dynamic, session-based, interactive identity. The way we know if we're talking to our friend or her doppelganger identity. For this purpose, a security rights layer is proposed.

Any multi-user system has the right to impose a security policy on its users. Regulatory compliance and auditing concerns are only the starting point—all users of systems have expectations for security, and are familiar with different levels of security for different types of systems. Cash, less secure. Credit cards, more secure. Surfing the blogosphere, less secure. Loan approval, more secure. No system should compromise security to make lazy users happy. There is another way. In general, however, a higher level of security requires a reduced level of individual privacy.

Users, however, have the right to impose a privacy policy on the system. Some people don't want their web searches logged, others don't care. Some users want the shops they solicit to track their purchases (for coupons, in-store running shopping list, etc.), others want full anonymity. Regardless, privacy as dictated by the user is fundamental to customizing a multi-user system, except in extreme cases—for example, top security clearance applications, in which case individual privacy is hardly a concern.

Currently, security policies tend to impose a high upfront "cost", or annoyance, on the user—log in, provide password, use approved card or device, submit to surveillance, etc. Privacy policies, in addition, extend the burden for security. For a user to demand complete privacy, still higher security may be required. For example, "to earn the right for the system to securely destroy personal information during this session, you must give us more confidence that you are who you claim to be. Otherwise, we will be logging anything and everything in case we need to determine later who really was posing as you."

Playing off of these two policies—security and privacy—are the access control privileges granted. The new security layer proposed herein defines the access control as

variable—that is, dynamic throughout the session. This means that a dynamic means of granting access rights must exist. The means is dynamic biometrics, described next.

III. Dynamic and Challenge-Based Biometrics

Dynamic biometrics lead to dynamic **session-based security**. This means that the level of security can change during the session, and the level of authorization (e.g. access privilege) granted is adjusted to the current session confidence.

Dynamic biometrics are based on two or more behavioral biometrics. This can either mean: (1) The presence of two or more sensors for behavioral biometrics, or (2) the capture of two or more independent streamable behavioral biometrics. An example of (1) is a keystroke dynamics recorder which capture both latencies and pressures during keyboard entry. Another example is a touch pad that simultaneously records fingerwriting dynamics and pressure (e.g. a six-axis accelerometer-affixed touch pad). An example of (2) is an inertial device (e.g. 6-axis accelerometer) affixed to a person's hand, which records both macro-motion (arm motion/gesture) and finger motion/gesture.

For the security purposes introduced here, dynamic biometrics are more than simple combinations of individual biometrics. A dynamic biometrics system (DBS) also describes how the available biometrics are combined. If, for example, there are three biometric recorders available (speech recording, touch pad recording and inertia recording), then the DBS will indicate which attributes of these three biometrics, in combination, are best for validating the identity of the user.

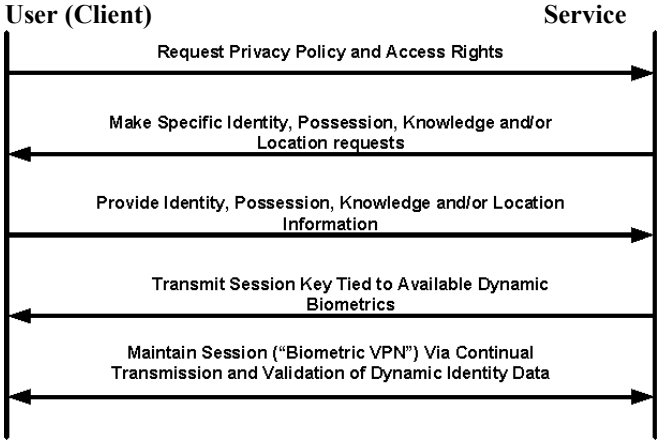

Fig. 1. Messaging between User (Client) and Service. Messages occur in time sequence from top to bottom.

Using a DBS, the "key" for how the individual biometric data streams are combined is the session key for possession, and the dynamic biometrics linked to/specified by the key validate the identity of the user. The messaging scenario for how this occurs is outlined in Figure 1.

In Figure 1, the user requests access to a service or set of privileges. The user's privacy policy is also provided or else the default privacy policy for the session is used. The service then requests specific information necessary to authorize the access with the desired level of privacy—per the discussion above, this is some combination of identity (preferably biometrics), possession, knowledge (e.g. password, answer to a challenge, etc.), and/or location. The service, meanwhile, assesses what combination of these resources {biometrics, possession, knowledge, location} are available. From this, a session "key" tuned to the available dynamic biometrics is conveyed to the user. User access to the service is thereafter maintained throughout the session by high confidence match between the user biometrics and the identity biometrics available to the service. In this way, a "biometric VPN" (virtual private network) is maintained, and the DBS can be considered a secure link between the individual and the privileged information provided by the service.

IV. Biometric Cepstrum

The dynamism of the DBS is provided by what is termed the biometric cepstrum. The general biometric cepstrum is based on the principal of the mel-frequency cepstral coefficients (MFCCs, described in [4] and elsewhere), which comprise a representation of an audio spectrum in which the coefficients are uniformly distributed over a log scale of the frequency. In other words, the cepstrum is a sampling of the audio spectrum that provides a "fingerprint" or "signature" of the spectrum (useful for classifying or distinguishing different speakers, etc.). The "biometric cepstrum" is herein viewed as any logical sampling of a biometric signal to cover the cepstral range sufficient for (differential) identification of individuals. In many cases (e.g. voice pitch), the sampling will be over a log scale; in others, it will be clustered in areas providing high differentiation (e.g. voice formants).

The general biometric cepstrum, then, is the set of coefficients for all of the biometric signals, designated $\hat{\mathbf{C}}$. If there are N signals, then B_1 is the cepstral set for signal 1, …, B_N is the cepstral set for signal N, and so the general biometric cepstrum is:

$$\begin{bmatrix} f_{11} \\ f_{12} \\ \cdots \\ f_{1\alpha} \end{bmatrix} \begin{bmatrix} f_{21} \\ f_{22} \\ \cdots \\ f_{2\beta} \end{bmatrix} \cdots \begin{bmatrix} f_{N1} \\ f_{N2} \\ \cdots \\ f_{N\omega} \end{bmatrix} \qquad \textbf{Equation 1}$$

where there are α, β, …, ω coefficients in signals 1, 2, …, N, where an individual signal's coefficient set is $\{f_n\}$. There is no restriction on the number of "signals" that can be obtained for a single type of sensor. For example, an inertial sensor can simultaneously sample vibration, speech and acceleration modalities, and using filtering and/or multiplexing separate them into different signals (with perhaps different numbers of coefficients) for Equation 1.

I define the signature set of signals, $\hat{\mathbf{S}}$, from the general biometric cepstral set, $\hat{\mathbf{C}}$, which comprises the set of all possible elements of the signature set, $\{\hat{\mathbf{s}}\}$. The current active biometric fingerprint, or signature, $\hat{\mathbf{S}}$, serves as the session

key, and is the current set $\hat{\mathbf{s}}$ of signature signals.

The signature can be determined in at least two ways. In the first, it can be provided by the service itself (*historical* signature). In the second, it can be determined through the interaction of the client with the service (*interactive* signature). The interactive signature $\hat{\mathbf{S}}$ is determined using, for example, a classifier such as a support vector machine (SVM) [5] or linear discriminant analysis [6].

The interactive signature is determined as shown in Equation 2. Here, the elements in $\hat{\mathbf{S}}$ are selected as those with minimal change under the conditions. However, since in general the latencies (e.g. relevant sampling intervals) of each biometric signal are different, this difference in time scale for the signals comprising $\hat{\mathbf{S}}$ is accounted for by the $k_i*\Delta t$ terms in Equation 3, where i indicates the i^{th} biometric and k_i is the time coefficient for the i^{th} biometric, which may be, for example, simply the default sampling rate for the i^{th} biometric signal.

$$\hat{S} = \min_{\hat{s}\in\hat{C}} \nabla \begin{bmatrix} f_{11} \\ f_{12} \\ \cdots \\ f_{1\alpha} \end{bmatrix} \begin{bmatrix} f_{21} \\ f_{22} \\ \cdots \\ f_{2\beta} \end{bmatrix} \cdots \begin{bmatrix} f_{N1} \\ f_{N2} \\ \cdots \\ f_{N\omega} \end{bmatrix} = \min_{\hat{s}\in\hat{C}} \frac{\partial \vec{F}}{\partial M}$$

$$= \min_{\hat{s}\in\hat{C}} \left\{ \begin{bmatrix} f_{11}(t+\Delta t) \\ f_{12}(t+\Delta t) \\ \cdots \\ f_{1\alpha}(t+\Delta t) \end{bmatrix} \cdots \begin{bmatrix} f_{N1}(t+\Delta t) \\ f_{N2}(t+\Delta t) \\ \cdots \\ f_{N\omega}(t+\Delta t) \end{bmatrix} - \begin{bmatrix} f_{11}(t) \\ f_{12}(t) \\ \cdots \\ f_{1\alpha}(t) \end{bmatrix} \cdots \begin{bmatrix} f_{N1}(t) \\ f_{N2}(t) \\ \cdots \\ f_{N\omega}(t) \end{bmatrix} \right\}$$

Equation 2

$$\hat{S} = \min_{population} \left\{ \begin{bmatrix} f_{11}(t+k_1\Delta t) \\ f_{12}(t+k_1\Delta t) \\ \cdots \\ f_{1\alpha}(t+k_1\Delta t) \end{bmatrix} \cdots \begin{bmatrix} f_{N1}(t+k_N\Delta t) \\ f_{N2}(t+k_N\Delta t) \\ \cdots \\ f_{N\omega}(t+k_N\Delta t) \end{bmatrix} - \begin{bmatrix} f_{11}(t) \\ f_{12}(t) \\ \cdots \\ f_{1\alpha}(t) \end{bmatrix} \cdots \begin{bmatrix} f_{N1}(t) \\ f_{N2}(t) \\ \cdots \\ f_{N\omega}(t) \end{bmatrix} \right\}$$

Equation 3

Equation 3, in simplified form, becomes:

$$\hat{S} = \min_{\substack{population \\ i,j\in\hat{C}}} \left\{ \frac{f_{ij}(t+k_i\Delta t) - f_{ij}(t)}{k_i \Delta t} \right\}$$

Equation 4

where each signal in $\hat{\mathbf{S}}$ is comprised of the cepstral set of signal frequencies $\{\mathbf{f}\}$. The cepstral frequencies with the minimum instantaneous rate of change are, in Equation 4, assumed to be the least noisy, thus providing the most reliability for the task over the user's history. An individual is then identified by comparing $\hat{\mathbf{S}}$ to the individual's historical coefficients (at the "Service" end of Figure 1). This is further discussed in Section VI below, under "SYSTEM CONSIDERATIONS"; however, the advantages of using the cepstral elements with the least variance are obvious: they provide the minimum tolerance for the would-be imitator.

The signature $\hat{\mathbf{S}}$ is dynamic. A set of signals is relevant to a given portion of a session, and as such can be time-averaged to give the salient set of elements in N-ω space of the general biometric cepstral set, $\hat{\mathbf{C}}$ (the two-dimensional space whose dimensions are the number of biometric signals and the number of coefficients in each biometric signal) that together comprise the session key (or possession key). Within this set of fingerprinted coefficients, as mentioned above, a subset can be selected (automatically) for the purposes of identity key as described next. Other means of "scrambling" the biometrics for a multi-biometric input scheme such as this are possible, as described below.

For a given task, the generation of a biometric signature, $\hat{\mathbf{S}}$, is a classification problem requiring training the DBS, determining the optimal $\hat{\mathbf{S}}$ for the task, and using this $\hat{\mathbf{S}}$ thereafter for determination of identity. The methodology above (Equations 1-4) provides a simple but effective (linear in time domain for determining the best set, no iterations required) means of generating $\hat{\mathbf{S}}$, real-time. More accurate classification for specific tasks can be garnered using traditional classification techniques [5, 6]. As will be shown below, these traditional types of classification will be useful for challenge-based and/or cognition-based biometrics. Biometric fusion—combining two or more biometric signals into a single identity classification—may require advanced classification approaches. Increasingly, combined or hybridized classification based on the combination of nonparametric and parametric classifiers [7], the combination of multiple configurations of the same classifier [8], and the combination of disparate classifiers using meta-algorithmic patterns [9], are being investigated to improve the accuracy of various image, text and other classification tasks. These classification techniques will, in general, provide higher accuracy for specific biometric identity tasks, and may additionally be more robust to a system which requires a plurality of signals, in which the plurality also changes over time. The best choice of classifier will depend on the specifics of the dynamic biometric system, as described in the next section.

V. Dynamic Biometric System (DBS)

A. Speech as an Exemplar

To illustrate the movement from a biometric identity system to a dynamic biometric system (DBS), voice recognition and automatic speech recognition (ASR) are considered. Combined I refer to these as "auditory biometrics", and they provide several advantages as a starting point for a DBS. First off, auditory skills—language and music production and cognition—are arguably the skills most distributed throughout the human cortex [10]. As a second point, humans without disabilities are very capable at recognizing voices and even short samples of familiar music, making ground truthing, or training, of the system, relatively easy. Third, auditory data is one-dimensional, offering data

throughput and processing advantages. A fourth advantage is the vast amount of voice recognition and ASR research that has been performed to date, as overviewed in references [11, 12] and elsewhere.

Speech processing in the general sense is concerned with the relative magnitude of frequency coefficients. This includes the MFCCs, as described above [4]. Additional frequency representations include perceptually-motivated MFCCs [13, 14], which open the pathway to task-specific cepstral coefficients (TSCCs). TSCCs can be crafted to more adequately cover the expected range of response when completing a specific auditory task. As an example, if an emotive response is measured (or triggered), a TSCC which better represents maximum and mean of the first derivative of the pitch contour [15] will provide better emotion recognition. TSCCs can also be crafted using transformations of the MFCC, such as through cepstral mean subtraction, to provide more accurate speaker identification [16].

Additional work on emotion recognition in auditory data streams has shown that auditory data can be used for simultaneous establishment of identity and emotion determination [17]. Emotion detection is important so that emotional state can be compensated for during identity determination, and so that emotion can be used as another factor in identification of the speaker. This supports the use of hybridized classifiers as discussed above [7, 8, 9]. There is increasing recognition that the combination of cognition-based, machine intelligence and natural language processing (NLP) approaches will be necessary to move voice and speech recognition forward [18]. It is likely that, as the biometric and identity research communities consider the challenges identified herein for the successful creation and deployment of a DBS, they will also further the research on each of the distinct signals/biometrics of interest.

B. DBS Session Needs

The DBS is concerned with two different session needs. These are (1) proving that you are the person you purport to be, which is required for access privileges; and (2) proving that you are not you, which once established signals an end to the session. Errors against (1), termed "false positives" for identity, are more serious when the data or resources accessed are higher security. Errors against (2), termed "false negatives" for identity, on the other hand, are more serious when disconnection is disruptive. From a security perspective, then, the DBS is usually designed to prevent false positives. However, this is in general a more difficult classification task.

These needs align with the distinction between identity (what name best matches this biometric data?) and determination (does my biometric data match the database data?) [1]. As an example, for identity, suppose for a given dynamic biometric signal in a DBS, the odds of any two users "matching" is 1 in 10^3. If the requirement is that false positive errors only have a 1 in 10^9 chance of occurring, then three independent signals with odds of false identity of 1 in 10^3 must be used to establish identity.

After establishing identity, the purpose of the DBS is to restrict access privileges if/when the system's confidence in the user's identity drops. This type of analysis is based on the detection of rare, key events, a key current area of research in ASR [18]. Creativity is the rule for such "true negative" determination. For example, an ASR engine can look for evidence of outside-accent formants [4]. A heartbeat monitor can look for a non-characteristic electrocardiogram (ECG) or vectorcardiogram (VCG). A challenge-based system, as described below, can request the user to provide feedback for which the user has the lowest historical variance (the optimal biometric cepstral as defined in Equations 2-4) for any of the signals measured.

C. Proving and Disproving Identity

The signature set, $\hat{\mathbf{S}}$, determined from Equation 4 or other approach, can be used in combination with a unique "Session Key", or workflow key, $\hat{\mathbf{W}}$, stored with the Service and not transmitted or shared with the User (client) as shown in Figure 1. This key, $\hat{\mathbf{W}}$, can be determined in multiple ways, depending on the needs of the Service, including but not limited to:

(1) Historical basis: past user interactions in any/all of the biometric modalities are used to determine the set of salient coefficients. This "historically-based" $\hat{\mathbf{W}}$ is likely to be similar to that determined by Equations 2-4.

(2) Confidence basis: coefficients with highest classification confidence are chosen. These provide a $\hat{\mathbf{W}}$ that is likely to be similar to that determined by Equations 2-4.

(3) "Randomized" selection of the coefficients to prevent reverse engineering.

(4) Coefficients that are linked to the set $\hat{\mathbf{S}}$—e.g. they are a hashed set. Suppose the overall set of elements in N-ω space of the general biometric cepstral set, $\hat{\mathbf{C}}$, are placed in a single sequence. Each coefficient selected for $\hat{\mathbf{S}}$ is represented as "1", and each coefficient not selected as "0". Thus, the set $\hat{\mathbf{S}}$ is represented as a binary sequence, suitable for hashing, scrambling, or other operation to transform $\hat{\mathbf{S}}$ into $\hat{\mathbf{W}}$.

Proof of identity is required in at least three situations: (1) establishing the session; (2) increasing access rights; and (3) re-asserting identity when the confidence of the DBS is insufficient to allow current access privileges. From a security standpoint, it is important to prove with accepted tolerance that the identity of the person using the DBS is correct. Ideally, the confidence in identity matches or exceeds the confidence level required to access the rights (data, services, etc.) currently authorized by the DBS. If not, more frequent determination of identity—e.g. through addition of more biometric signaling—is required.

General Bayesian probability is used to determine the confidence in identity, as shown here:

$$p(A \mid B) = \frac{p(B \mid A) * p(A)}{p(B)} = \frac{p(B \mid A) * p(A)}{p(B \mid A) * p(A) + p(B \mid !A) * p(!A)}$$

Equation 5

Here p(A) is the probability it is you, p(A|B) is the probability of it being you if event B occurs, p(B) is the probability of event B occurring, p(B|A) is the probability of event B occurring given it is actually you, p(B|!A) is the probability of B occurring given it is not you and p(!A) is the probability of it being not you, or 1-p(A). The overall probability p(A|**β**) may comprise a vector **β** of many events $B_1, B_2, \ldots, B_N$, as shown in Equation 6.

$$p(A \mid \beta) = \frac{\sum_{i=1..N} p(B_i \mid A) * p(A)}{\sum_{i=1...N} [p(B_i \mid A) * p(A) + p(B_i \mid !A) * p(!A)]}$$

Equation 6

Equation 6 provides the means for combining multiple biometric signals to determine statistical confidence for identity. A different set of probabilities is stored for each biometric signal under a variety of conditions—e.g. under different emotional states for voice, different bodily postures for heartbeat, etc.

Equation 6 also can be used to compute the probability that it is not you, or p(!A|**β**) (simply switch "!A" and "A" in the equation). While setting $p(A) \geq (1\text{-}10^{-9})$ is a reasonable rule (one in a billion chance of it not being you), it is not as obvious what setting should be used for p(!A) to discontinue access privileges. This setting depends on several factors, including (1) the signal-to-noise ratio (SNR) in the signal; (2) the relative stability of the signal for identifying the individual (Equation 4); and (3) the odds of the metric identifying someone else with higher odds (herein termed the person-to-population ratio, or PPR).

This list of factors identifies interesting research opportunities in biometrics and, more generally, in analytics. One research thread for dynamic biometrics will be how to dynamically (and reliably) assign a probability value for p(A) and, with most likely more difficulty, p(!A). In addition, meta-algorithmic patterns [9], capable of intelligently combining the output of multiple biometric systems, will be crucial for these determinations. How are multiple biometrics combined to give the best overall confidence that a person is who she claims to be; or that someone else is now posing as her? The use of a current biometric signature, $\hat{\mathbf{S}}$, allows for different biometrics to contribute differentially to the assessment of identity over time, making the identity of the user much more difficult to steal/spoof.

D. System Architecture

In order to provide a dynamic biometric signature, a dynamic biometric system (DBS) such as that shown in Figure 2 is required.

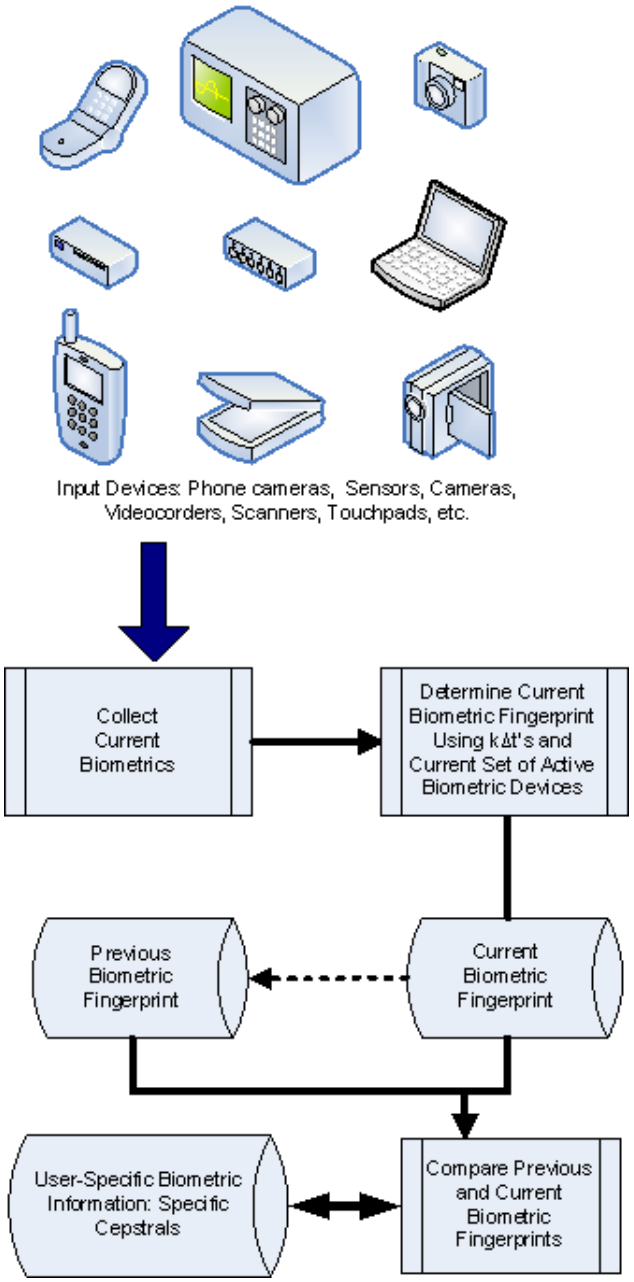

Fig. 2. Dynamic biometric system (DBS) on-ramp.

Input devices to the DBS include any of the commonly used image sensing devices such phone cameras, digital cameras, scanners, inspection systems, video-recorders, etc., which are the analogues to the human "visual" sense. Three other prominent human senses—auditory, somatosensory, and inertial (the "vestibular" system in humans)—are also covered well by readily-available devices such as microphones, touch pads and accelerometers. Current trends in nanofabrication and sensor-based environmental monitoring combine to ensure the ubiquity of low-cost sensors hereafter. Sensors can also be provided for chemical (analogous to the human "gustatory" and "olfactory" senses). Sensitivity beyond human range (e.g. ultraviolet, infrared, radar, and ELF sensors) and sensors for other factors (temperature, pressure, humidity, etc.) can also readily serve

as inputs.

These input devices, combined, provide the general biometric cepstral set, $\hat{\mathbf{C}}$, which is the set of current biometrics collected. The current active biometric "fingerprint" or signature, $\hat{\mathbf{S}}$, is then determined using Equation 4 or other means. The current and previous biometric signatures are then compared to deduce if the identity of the person is statistically likely to be unchanged. This approach provides a significant advantage over raw computation of p(!A), since the active session will generally compensate for differences in signal quality, sensor calibration, speaker health/condition, etc. Additionally, having the "previous biometric fingerprint" provides a constraint, which greatly narrows the class of users that can successfully maintain "connection" through their biometric responses.

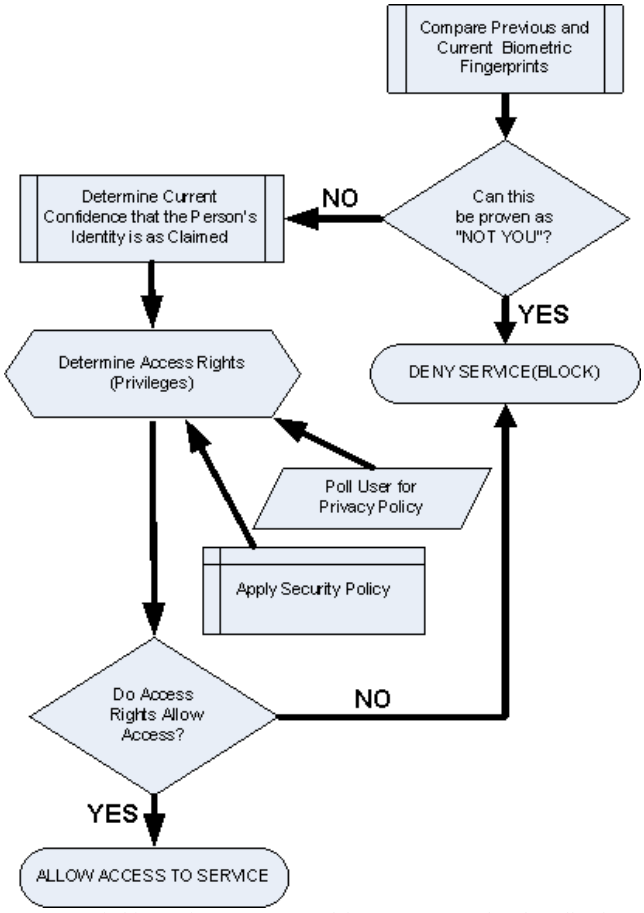

Fig. 3. Dynamic biometric system as used for access control and application of security and privacy policies.

In Figure 2, the user-specific biometric information is managed by existing identity management systems (IMS). Reference [19] describes three primary types of IMS: (1) for account management; (2) for organizational profiling of user data; and (3) for user-controlled context-dependent role and pseudonym management. Solutions to IMS for the federation [20] and enterprise [21] exist, and can be used to provide the IMS for the DBS of Figure 2. As most of the currently available identity management systems manage user identities at the service/application level, they are in general supportive of the DBS outlined in Figures 2-4.

In Figure 3, the decisions made by an appropriately deployed DBS are shown. Once the previous and current "fingerprints" $\hat{\mathbf{S}}$ are compared, the value p(!A) is computed. If it is statistically certain (with the system's desired level of confidence) that the person is not the person claimed, then services (augmented access control, etc.) are denied. If p(!A) is not sufficient to disprove purported identity, then p(A) is computed and logged. This is important for several reasons:

(1) **Auditing**. IPv6 and other standards may provide the means to tie environmental information (e.g. through sensors) to session security [26]. When these or their alternatives are deployed, the registry (database) associated with the DBS can be used for auditing, compliance, analytics, and other purposes.

(2) **Denial of service**. When there is a large change in p(!A)—independent of change in $\hat{\mathbf{S}}$ for example—then the access privileges currently authorized can be denied. Regaining of these access rights requires re-authorization, e.g. through behavioral biometrics, multiple biometrics or challenge-based biometrics as described in the next section.

(3) **Biometric (identity) descriptor**. The data collected, if associated with the correct identity throughout the interaction, can then augment the individual's biometric descriptor—the historical biometric data associated with the user. This information can be rolled back if needed. However, augmenting this provides for adaptation of the user's behavior through time.

(4) **Evidence**. The information collected by the system can be encrypted, stamped and retained for later evidentiary purposes, if allowed in the jurisdiction.

Next, the privacy and security policies are applied, with direct implications on the required p(A) and p(!A) values. With the given set of {security policy, privacy policy, p(A), p(!A)}, the individual can be allowed different levels of authorization. For example, if $p(!A) < 0.001$ after having collecting the original biometric signature, then generic (read-only) access may continue to be granted while $p(!A) < 0.1$, advanced (read-append) access while $p(!A) < 0.01$, and full access (read-write-append) while $p(!A) < 0.001$. More generally, the following policies may be applied:

(1) While $p(!A) < T_{ro}$, read-only access is granted

(2) While $p(!A) < T_{ra}$, read-append access is granted

(3) While $p(!A) < T_{rwa}$, read-write-append access is granted

where T_{ar}=threshold probability for the specific access rights (ar) and $T_{rwa} < T_{ra} < T_{ro}$. Various access right privileging strategies can be adopted, although the graceful change in access rights incumbent with this approach make it relatively easy to maintain baseline access rights (that is, continue a task at hand) without continual need for ongoing biometric input. Then, additional access rights can be attained through successful input of identifying biometric input.

E. Biometrics Used in a DBS

Useful biometrics in a DBS include physical and behavioral biometrics. Physical biometrics are garnered from

a discrete (single) interrogation—usually termed a "scan"—while behavioral biometrics are acquired from a continuous (multiple) interrogation—usually termed signal acquisition. Physical biometrics include face, finger, hand, iris, retinal and vein scanning, as discussed above. Behavioral biometrics include dynamic bodily movements, speech and touchscreen interaction [1]. Behavioral biometrics offer the relative advantage of being resistant to false matching. To support behavioral biometrics, it is important to provide a broad enough set of comparative behavioral data such that a true match can be made. This is a principal benefit provided by the biometric descriptor, or historical biometric data.

VI. System Considerations

A. Choice of Biometric Signals

An important system consideration is the choice of biometric signals. Due to the high bandwidth requirements and difficulties with illumination, among other factors, visual biometrics are not always suitable. Also, mobile devices help to make auditory and touch biometrics increasingly important in this area. Inertial (acceleratory) and chemical biometrics are also increasingly important, and benefit from the increasing maturity of nanotechnology-based sensors.

Speech has been useful as a biometric at least since the invention of the telephone. Humans are very adept at voice recognition, and language interpretation includes the ability to differentiate between, for example, declaration and interrogation solely from the inflection (rising or falling pitch). Cepstrals are a primary tool for automatic speech recognition (ASR), and the concept of the biometric cepstral is straightforward. The min gradient approach outlined here is effective since the elements of $\hat{\mathbf{S}}$ effectively form an "identity key", comprising the hardest set of cepstral elements to fake—having the lowest tolerance to imitation.

Behavioral speech biometrics include changes in inflection, pitch, loudness, timbre, rhythm, etc., with emotion, state of health and other factors. Obviously, identity "passwords" can be created that more accurately identify the purported speaker's voice characteristics—choosing from the historical biometric data the word or words which provide the minimum p(!A)—if a higher level of access privilege is needed or if identity confidence for the current level of access privilege is not being attained.

B. Acquisition of Biometric Signals

Biometric signals can be collected continually, as is the case for face recognition from video, speech recognition from voice data, and fingerprint or gesture recognition through a touch-screen.

Additionally, when current identity confidence is statistically insufficient, more interruptive methods of obtaining biometric data are required. Two such methods are (1) challenge-based biometrics and (2) cognition-based biometrics. A challenge-based biometric is a prompt for user input that is used to re-establish identity. Existing challenge-based prompts include requesting the re-entry of a password, or the re-swiping of a fingerprint (which is actually a biometric challenge). Cognition-based biometrics are concerned with the person's ability to perform a given task. The cognitive aspect can be based on user history; i.e., the user may have rehearsed the response or provided it in the past—such as a signature or a vocal response to a query. Although disruptive to the user's task, the user already understands that occasional re-assertion of identity is needed to ensure security. Importantly, challenge- and cognition-based biometric tasks may be requested sequentially until either identity is established with sufficient statistical confidence or until the access control rights are revoked.

For behavioral, challenge-based and cognition-based biometrics, latency (timing considerations) in the user's response is important. Identity counterfeiting is made more difficult when differences in the adeptness of an individual to respond are measurable and unaffected by connection. This is consistent with where a DBS is best deployed—when there is a fast and reliable internet connection.

C. Applications

The DBS can be used for virtually any system requiring security, privacy and access control. Centering next-generation security systems around biometrics provides additional advantages. The sensors used to provide access control can also be used to provide environmental or personal monitoring. In medical applications, biometrics can provide both security through identification and clinical information suitable for analysis and interpretation by medical professionals. One example is the electrocardiogram (ECG). Information from the ECG and its related vectorcardiogram (VCG), blood pressure profile and heart sounds, can provide a "signature" for the individual under resting, sitting, standing and other conditions, with values for p(A) and p(!A) that, while modest, are suitable for patient identification in a clinical setting. The clinical value of these sensor-input biometrics are obvious.

The DBS will prove useful in financial, political and corporate—collectively designated "enterprise"—security systems. Here, the auditing and evidence aspects of the DBS can be deployed consistent to the governance of the system. As such, compliance with the DBS can be, largely, determined by the service, with obvious incumbent advantages to user policy adherence.

From a research standpoint, the development and deployment of a DBS offers several further threads of interest. Massive amounts of ground-truthed (training) data are accumulated, since the biometric data can be directly associated with a given user. The DBS, therefore, can provide a central repository of biometric data, useful for analytics and data-mining purposes. This data may be helpful in determining better usability for applications, more facile means of gathering user biometric data to ensure security, privacy and access right policies, and more generally for the community concerned with the connection between biometrics and health, safety and environmental monitoring.

Ultimately, the goal of the DBS is to disappear into the

background—or at least become as non-disruptive as possible. There are compelling current trends that support this goal. The "traditional" WIMP (window, icon, menu, pointing device) paradigm faces competition from new human-machine interaction models such as touch and voice control. Gesture and facial expression control—if not direct brain control—models may also augment the experience. Clearly, the human-computer interface is no longer a generic mouse-and-keypad. The new modes for interaction are largely based on, not coincidentally, biometrics. This should make collecting dynamic biometric information suitable for maintenance of a "biometric VPN" easier and less invasive.

D. The DBS as a Distributed Architecture

The use of the DBS in enterprise systems is consistent with the trend to move applications, services, data and information (analyzed data) to a so-called "cloud" service, with mobile, desktop and data center access to the service possible "any time, any place". The structure of the cloud supports the needs for privacy, as well. Session keys based on $\hat{\mathbf{S}}$ are maintained by the service, as well as the full history of the user's interactions. In some ways, the mobile/ubiquitous on-ramp to the service can actually support both security and privacy. An eavesdropper would not be able to "sit" on a single machine or access port to capture the biometric history, even if the eavesdropper could deduce which coefficients of which signals were being trafficked during each session.

VII. Future Considerations: The Biometric World

The timing of the first IEEE International Conference on Biometrics, Identity and Security (BIdS) is not accidental. We stand on the precipice of a jump into the unknown—one could just as easily argue the jump has already occurred [22]. A jump into an unprecedented world based on biometrics, ubiquitous sensing, and the accumulation—not to mention analysis and storage—of vast amounts of data relating to identification and tracking. And, somewhere, behind all this data, scalable and effective policies for security, privacy and access control must be designed and deployed.

The "biometric world" is, in many ways, a logical extension of the linked world of today. A sensory and surveillance backbone overlaid on the next-generation (IPv6 and beyond) Internet is not only possible—it's already being built. Location information (due to the increasing ubiquity and decreasing cost of GPS-enabled devices and sensors) will rise to complement possession, knowledge and identity, furthering the need for an architecture in which a variety of policies can be deployed simultaneously and with ease of scaling.

How are security and privacy to be simultaneously provided in this biometric, sensor and data rich world? The time to design such a system is now. Instead of the perennial trade-off between security and privacy, perhaps the DBS offers the possibility of building both into the system from the beginning. A first pass of the architecture to achieve this is a system based on session security through sensing (Se3).

Figure 4 depicts a simplified view of the connections between the key elements of the Se3 system. Privacy policy, rather than being retrofitted, is explicitly designed into every node and link in the system.

Security policy is applied through the session keys, created from the signature set, $\hat{\mathbf{S}}$, and through the use of biometric identity verification. Privacy policy can be implemented in a number of ways. As one example, if the user wants the highest level of privacy, she may wish for no information to be stored locally. This means any biometric data stored from past sessions must be stored in the cloud, and in general the user will need to provide more substantial biometric information to prove identity when initiating the session.

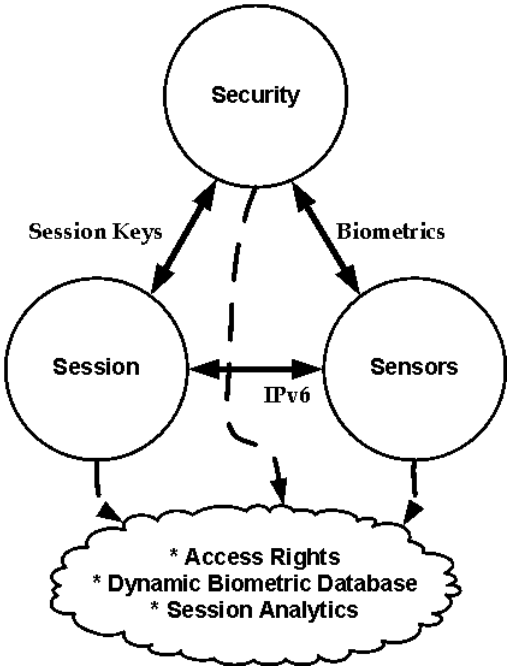

Fig. 4. Se3 (Security, Session, Sensors) system with cloud connection.

As the IPv6 protocol is adopted, sensors will be connected like other devices on the internet. Varying levels of privacy can be provided through the choice of IPv6 deployment. Generic 128-bit IPv6 uses a globally unique MAC address, which can track the user and his equipment. However, privacy extensions for IPv6 have been standardized to provide anonymity, if necessary [23].

The service supporting the Se3 system implements and validates both the security and privacy policies, performs the statistical analysis necessary for establishment or revoking of identity, provides the correct access rights, and stores user biometrics in the correct format. Session analytics are captured and used, as appropriate, to update the user's biometric history.

VIII. Conclusions

The dynamic biometric system (DBS) outlined in this paper takes into account current trends in sensing, identity research, mobile devices, cloud services and advanced biometrics. The DBS is meant to provide a fix for the collapse

of identity and possession into knowledge. The DBS provides a call for action on new research in security, privacy, biometrics and biometric fusion.

Many aspects of this system posit interesting research challenges. Specifically, correcting for differences in location, connection quality, device quality and model, health/condition of the user, and the effective selection of the dynamic biometric signals to collect. Location and connection quality will impact the integrity and SNR of the signals collected. Research is necessary to correct/calibrate for these differences. Device quality and model will affect the gain, phase, SNR and frequency response—among other factors—of the signals sampled. Again, device qualification and periodic calibration will be necessary to provide the highest accuracy DBS. User health and condition (emotional state, point in diurnal cycle, etc.) must also be considered to optimize the accuracy of the DBS. Finally, powerful analytical approaches, such as task-specific spectra [7, 8] and meta-algorithmics [9], are required to limit the intrusiveness of the DBS on the users.

In many systems, the inability to ensure that knowledge, identity and possession are independent poses a significant threat to security and privacy. Converging trends in mobility, sensing, biometrics and analytical approaches, however, offer a possible path forward. Dynamic biometrics, with the advantages over "static" biometrics as described in this paper, will be a pivotal technology for architecting systems that can provide compliance for a wide array of security policies, privacy policies and levels of access to applications, services and data. The IEEE International Conference on Biometrics, Identity and Security (BIdS), is being inaugurated because of the recognition that rapid identification of individuals is of increasing importance in many areas. The DBS—while not without significant research, architectural and regulatory hurdles to overcome—builds on the rapid identification of individuals to provide a broader and potentially more robust system for security, privacy and access control.

Security is more a net than a hook. Broad, interdisciplinary approaches taking advantage of multiple technology threads are generally more robust, more scalable, and more adaptable to the changing needs of the security community. It is hoped that the DBS, in matching these qualifications, will help us provide both security and privacy in the new, sensor-rich, mobile, distributed and biometric world.

IX. Acknowledgment

Thanks to Jason Aronoff, Margaret Sturgill and the anonymous reviewers for helpful suggestions!

References

[1] S. Nanavati, M. Thieme, and R. Nanavati, *Biometrics: Identity Verification in a Networked World*. New York: John Wiley &Sons, 2002.

[2] J.C. Wells, *Accents of English*. Cambridge, U.K.: Cambridge University Press, 1982.

[3] X. Lin and S. Simske, "Phoneme-less hierarchical accent classification," HPL Technical Report HPL-2004-166, available at http://www.hpl.hp.com/techreports/2004/HPL-2004-166.html

[4] S. Vaseghi, Q. Yan, and A. Ghorshi, "Speech accent profiles: modeling and synthesis," IEEE Signal Proc Magazine, 26(3), 2009, pp. 69-74.

[5] B. Schölkopf and A.J. Smola, *Learning with Kernels.* Cambridge, MA: The MIT Press, 2002.

[6] G.J. McLachlan, *Discriminant Analysis and Statistical Pattern Recognition.Wiley Series in Probability and Mathematical Statistics: Applied Probability and Statistics*. New York: Wiley & Sons, 1992.

[7] P. Chaudhuri, A.K. Ghosh, and H. Oja, "Classification based on hybridization of parametric and nonparametric classifiers," IEEE Trans Pattern Analysis Machine Intell, 31(7), 2009, pp. 1153-1164.

[8] R.A.-H. Mohamad, L. Likforman-Sulem, and C. Mokbel, "Combining slanted-frame classifiers for improved HMM-based Arabic handwriting recognition," IEEE Trans Pattern Analysis Machine Intell, 31(7), 2009, pp. 1165-1177.

[9] S.J. Simske, D.W. Wright, and M. Sturgill, "Meta-algorithmic systems for document classification," Proc DocEng 2006, New York, NY: ACM, 2006, pp. 98-106.

[10] D.J. Levitin, "This is your brain on music," New York: Penguin Group, 2006.

[11] F. Jelinek, *Statistical Methods for Speech Recognition*. Cambridge, MA: MIT Press, 1997.

[12] D. Jurafsky and J. Martin, *Speech and Language Processing: An Introduction to Natural Language Processing, Computational Linguistics, and Speech Recognition*. Englewood Cliffs, NJ: Prentice-Hall, 2000.

[13] S. Davis and P. Mermelstein, "Comparison of parametric representations for monosyllabic word recognition in continuously spoken sentences," IEEE Trans. Acoustics Speech Signal Processing, 28(4), 1980, pp. 357-366.

[14] A. Krishnamurthy and D. Childers, "Two channel speech analysis," IEEE Trans. Acoustics Speech Signal Processing, 34(4), 1986, pp.730-743.

[15] S. Yacoub, S. Simske, X. Lin, and J. Burns, "Recognition of emotions in interactive voice response systems," HPL Technical Report HPL-2003-136, 5 pp., 2003, available at http://www.hpl.hp.com/techreports/2003/HPL-2003-136.pdf

[16] A.E. Rosenberg, C.H. Lee, and F.K.Soong, "Cepstral channel normalization techniques for HMM-based speaker verification," Proc. IEEE ICASSP, 1994, pp. 1835-1838.

[17] R. Cowie, E. Douglas-Cowie, N. Tsapatsoulis, G. Votsis, S. Kollias, W. Fellenz, and J.G. Taylor, "Emotion recognition in human-computer interaction", IEEE Signal Proc Magazine, 18(1), pp. 32-80, 2001.

[18] J.M. Baker, L. Deng, J. Glass, S. Khudanpur, C.-H. Lee, N. Morgan, and D. O'Shaughnessy, "Research developments and directions in speech recognition and understanding, part 1," IEEE Signal Proc Magazine, 26(3), 2009, pp.75-80.

[19] M. Bauer, M. Meints, M. Hansen, "Del 3.1: structured overview on prototypes and concepts of identity management systems," *FIDIS Deliverables* 3(1), 2005.

[20] A.Baldwin, M. Casassa Mont, and S. Shiu, "On identity assurance in the presence of federated identity management systems," HPL-2007-47, http://www.hpl.hp.com/techreports/2007/HPL-2007-47.html

[21] M. Casassa Mont, P. Bramhall, and J. Pato, "On adaptive identity management: the next generation of identity management technologies," HPL-2003-149, http://www.hpl.hp.com/techreports/2003/HPL-2003-149.html

[22] S. Simske, "Eye in the sky? Try crowd in the cloud," HP Communities Security Printing and Imaging Blog, April 16, 2009, http://www.communities.hp.com/online/blogs/securityprinting/archive/2009/04/16/eye-in-the-sky-try-crowd-in-the-cloud.aspx

[23] T. Narten, R. Draves and S. Krishnan, "Privacy extensions for stateless address autoconfiguration in IPv6," September 2007, http://tools.ietf.org/html/rfc4941

[24] "ATM Scam", http://www.utexas.edu/police/alerts/atm_scam/

[25] R. Lemos, "Are your 'secret questions' too easily answered?" Technology Review (web), May 18, 2009, http://www.technologyreview.com/web/22662/

[26] N. Lovering, "The impact of IPv6 on semantic interoperability," 27 April 2006, http://www.opengroup.org/projects/si/uploads/40/10346/lovering.pdf