JOURNAL OF INFORMATION SYSTEMS
Vol. 17, No. 2
Fall 2003
pp. 51–70

Toward a Biometric Security Layer in Accounting Systems

Akhilesh Chandra
Thomas G. Calderon
The University of Akron

ABSTRACT: This paper discusses theoretical and practical issues related to the use of a biometric-enabled security layer in accounting systems aimed at enhancing user authentication and reducing control risk. Originating in criminology, biometric technology has matured over the years with applications in diverse disciplines. However, its use in business and accounting is still in its infancy, and many issues about its role in information systems security are unresolved. The paper proposes an access decision framework that draws from the strategy and risk assessment literature to model processes where biometrics might be used to reduce control risk. Despite its potential strengths, biometric technology is not a panacea and represents one element in a portfolio of security mechanisms needed to protect information resources. The paper discusses challenges in implementing biometric technology and identifies avenues for future research.

I. INTRODUCTION

The unfortunate events of September 11, 2001 in New York City, Pennsylvania, and Washington, D.C. have forced all concerned to revisit security issues broadly, including those related to information systems. The losses resulting from these attacks will have a lasting impact. Surreptitious cyber-attacks on information resources can also have devastating consequences. The vulnerability of critical information resources to catastrophic and cascading failure makes them attractive targets for intruders and unauthorized persons with malicious intent.

Cyber-related security threats have the potential for highly debilitating consequences for business and other organizations. Yet many entities do not have effective security mechanisms in place to mitigate such threats (Scharpenberg, as quoted in Hart 2001). Cyber-fraud and lost productivity from cyber-attacks are also significant threats to economic activity (Nichols et al. 2000; Pipkin 2000). A fundamental cause of such losses is the absence or breakdown of identification and authentication[1] systems (Stallings 2000).

Sound identification and authorization mechanisms are often a necessary prerequisite for mitigating threats to other key security services such as confidentiality, non-repudiation, data integrity, and data availability. In view of recent widespread security concerns, there has been a surge of interest in biometric mechanisms as a means of strengthening identification and authentication

We thank Dan Stone, an Associate Editor, and two anonymous reviewers for their constructive and helpful feedback on earlier drafts.

[1] Identification and authentication, and the relationship between these two concepts, are discussed in a subsequent section.

services. A biometric is a distinguishable physiological or behavioral attribute that can be used to automatically verify and authenticate an individual's identity (Matyas and Stapleton 2000). Some of the popular biometrics include fingerprints, voice patterns, iris and retinal patterns, hand geometry, signature verification, and keystroke analysis.[2] Since a biometric is tied to an individual, its misuse (from loss or theft) is more difficult, although not impossible.

The accounting profession has developed various control frameworks that identify risks and security measures related to business information resources and other assets. Specifically, these control frameworks (e.g., Committee of Sponsoring Organizations [COSO] 1992; U.S. Department of Justice 1977; Canadian Institute of Chartered Accountants [CICA] 1998; SysTrust [AICPA 2002; McPhie 2000; Boritz and Mackler 1999]; CobiT 2002) challenge the accounting profession to design and maintain control systems in a manner that safeguards an enterprise's information resources. A strong security mechanism that reduces control risk and generates enhanced confidence among information systems users would be an ideal tool for accountants in the discharge of their responsibility. Biometric technology appears to be a powerful candidate. This technology can potentially reduce control risk in accounting applications and business processes, particularly when used in conjunction with traditional control measures.

In this paper, we examine the potential use of a biometric-enabled security layer in accounting systems to mitigate threats to identification and authentication services. We propose an "access decision framework" that considers both exposure and business information intensity (BII) as fundamental factors in classifying applications and business processes that might be candidates for the type of security services that biometrics can offer. The proposed framework draws from the strategy and risk assessment literature. It utilizes concepts of risk and exposure, as well as Porter and Millar's (1985) work on the interaction of information systems and strategy, to model potential accounting applications and business processes that can benefit from an application of biometrics to reduce control risk. BII refers to the level of IT content in an entity's product and value chain. BII is high when the IT content of both the product and the value chain is high. Similarly, BII is low in situations where the reverse occurs. Exposure refers to potential losses that an organization can suffer in the absence of sufficient information systems security and control (Romney and Steinbart 2003; CICA 1998).

The remainder of the paper is organized into five sections. In Section II, we provide an overview of the biometric authentication process, and discuss risk and assurance issues associated with the technology. In Section III, we analyze specific areas in accounting information systems (AIS) where biometric technologies may add value. In Section IV, we present and illustrate, with examples, an access decision framework for evaluating biometric-enabled security mechanisms in AIS and provide a decision aid for implementing the framework. In Section V, we discuss challenges and constraints in the implementation of a biometric security layer for the AIS, and identify opportunities for future research. Finally, our conclusions are presented in Section IV.

II. AUTHENTICATION AND BIOMETRICS

This section provides an overview of biometrics and discusses the biometric-enabled authentication process. It includes a discussion of the distinction between identification and authentication, an examination of factors used to authenticate information systems users, a description of the biometric authentication process, and an overview of selected issues and challenges that impact the effectiveness of biometrics as an authentication tool.

[2] Recently, there have been many publicized large-scale uses of biometrics in the federal government, state and local government, athletics, banking, construction, and retail. For more information about biometrics, see Ratha and Senior (2001), Connecticut Department of Social Services (2002), FindBiometrics.com (2003), and Biometrics Consortium (2003a and 2003b).

Identification versus Authentication

Identification is a *one-to-many* matching process that ascertains the existence of an individual in a database. This process merely determines that the person exists. If access control is predicated only on the existence of an individual, then the individual is given access to the system when the required identifier is found to exist in the access database. There is no confirmation or proof that the person who is given access is indeed the person who initiated the access procedure. Authentication, on the other hand, ascertains that the individual who is identified in the database is in fact the person whom he or she claims to be. Authentication is a *one-to-one* matching process of a claimed identity. In other words, a user who wishes to log on to a service claims a specific identity. The automated identification system searches through the entire database of users until a match is found (i.e., a *one-to-many* matching process). The authentication process, on the other hand, verifies that the claimed identity belongs to the user. The match is performed against a specific reference or authentication factor associated with the claimed identity.

Authentication Pyramid

The pyramid in Figure 1 shows three broad categories of factors that organizations use for automated authentication—possession, knowledge, and biometrics. Authentication can be predicated on a single factor (e.g., a password, a PIN, or a picture ID) or on multiple factors (e.g., password and picture ID, or PIN and picture ID). Vertical movements within the pyramid are associated with increases in the strength and focused nature of the authentication process. The likelihood that the verified identity is *not* that of the true owner also decreases with vertical movements in the pyramid.

In the first category, the user must present a physical possession (such as a token or a key) to be authenticated. Though visible and usually portable, possessions can be lost, stolen, shared, duplicated, forgotten, or destroyed. Possession-based authentication factors provide assurance that a user presents a valid token or card. Within the context of an automated authentication process, these factors do not provide direct assurance that a user who is allowed access into an information system is indeed the person he or she claims to be.

In the second category, the user provides information about his/her knowledge (such as a PIN, password, or passphrase). Passwords and other knowledge authentication factors are highly portable, invisible (unless written down), can be changed often, and can be designed to be relatively secure. However, they can be forgotten, reused, stolen, guessed, or shared. Passwords offer assurance that the person at the keyboard knows the password. They do not offer assurance that the person at the keyboard is indeed the person he/she purports to be.

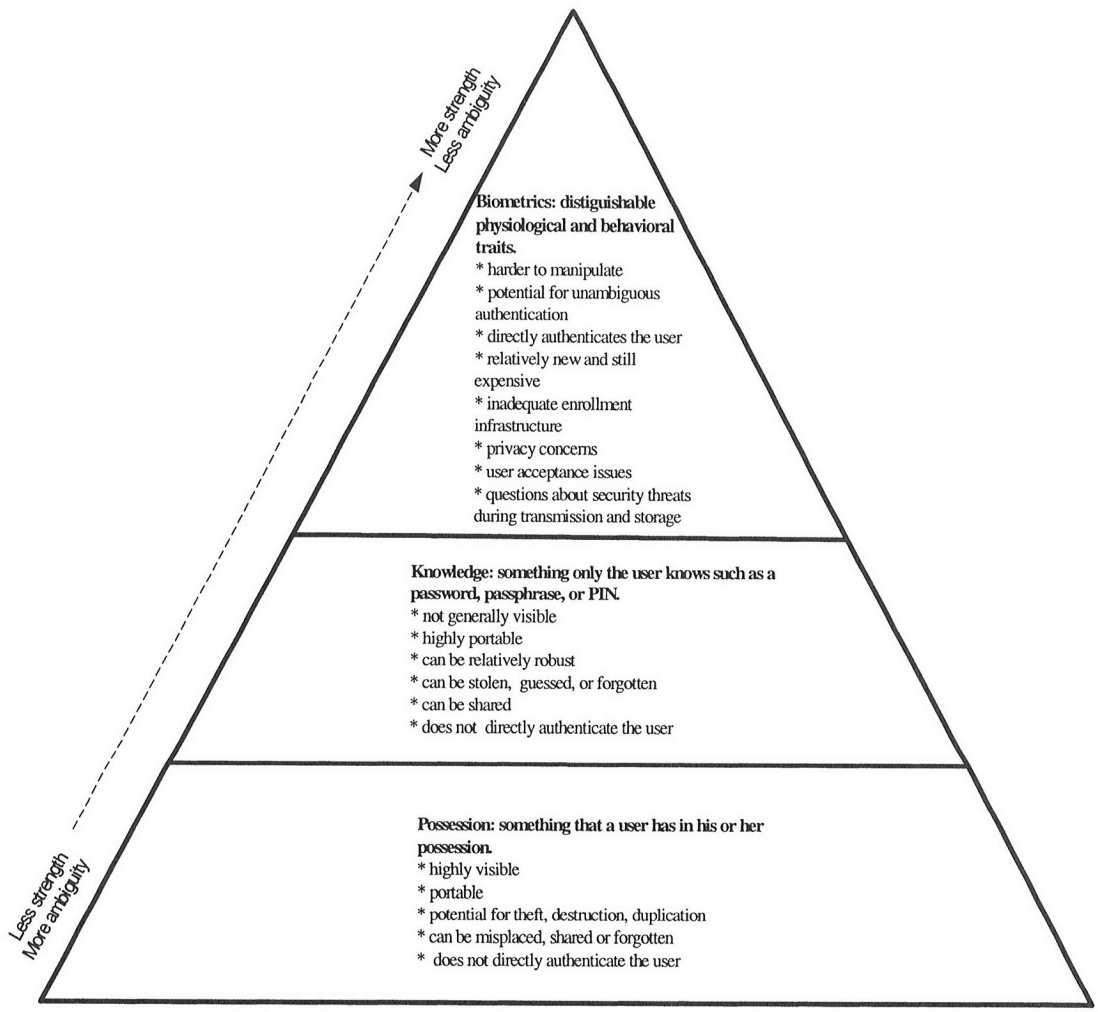
In the third category, the system employs distinguishable physiological characteristics and behavioral traits (biometrics) to authenticate the user and allow access to information resources. Biometric technology falls into this category. Biometrics are difficult to steal and directly tied to one and only one user. Furthermore, they cannot be forgotten or misplaced and, like knowledge, they are innate to the user. The nontransferability feature (except with replacement surgery) gives entities that deploy biometrics a unique advantage in building user confidence and trust in identification and authentication services. Table 1 profiles a list of various biometric tools in use, their relative features, and their strengths and weaknesses.

Biometric Authentication Process

The process used to authenticate users in a biometric-enabled security system is depicted in Figure 2. The figure also depicts several vital security and assurance issues that must be considered in the authentication process.

The process begins with user enrollment, which involves verification of a person's identity by using exogenous identifiers (such as reference letters, notarized documents, employment records,

FIGURE 1
Authentication Alternatives in a Single Factor Authentication Model



photographs, and certificates), capturing the person's biometrics, and then creating a biometric template for that user. The template is a mathematical code that contains the distinguishing features of an individual's biometrics. The template is referenced against an identifier (e.g., a name, PIN, password, token, etc.) and stored either in a database or on a portable medium such as a "smart card." The enrollment process and template quality are critical in obtaining good results during the verification process. However, effectiveness of the enrollment and subsequent verification processes can be threatened by several factors, including user awareness, acceptance, and trust in the system (Nichols et al. 2000). Factors that can impede the enrollment process as well as potential approaches to address them are identified in Figure 2.

Users must be authenticated by the biometric-enabled security system before they are granted access to a protected information system. This requires the user to present the appropriate biometric

TABLE 1
Biometric Technologies

Technology	Description
Hand Geometry	**Features**: evaluates the shape and curves of the hand, some use three dimensional perspectives, suitable for large database, infrequent usage, and less disciplined users **Pros**: easy to use, good balance of performance features, high accuracy, flexible performance tuning and configuration, ease of integration into other systems **Cons**: not many applications developed, still in infancy **Applications:** used at airports, legislative buildings in some foreign countries, daycare centers, hospitals, prisons, and immigration facilities. **Examples**: Examples can be found at the home page of The Biometric Consortium (2003b)
Signature Scan	**Features:** traditional device, a behavioral device, it checks the way a person signs his/her name, and writes letters **Pros:** fairly accurate **Cons:** age effect changes the pattern, not as accurate as other biometrics **Applications**: a crude non-automated version used in retailers' point-of-sale systems; also used to secure PDA devices **Examples**: Examples can be found at the home page of The Biometric Consortium (2003b)
Fingerprint	**Features:** matches the minutiae, pattern, ultrasonic, or moiré fringe imprint; most common of all devices, works well in controlled environment **Pros:** good accuracy, low false acceptance, low cost, small size, ease of integration **Cons:** usage errors, high false rejection with large database **Applications:** most widely used in industry for a wide range of applications; used in biometric mouse and other similar devices to secure desktop and mobile computers; used for authentication in distributed networks **Examples**: Examples can be found at the home page of The Biometric Consortium (2003b)
Voice Scan	**Features:** measures the wavelengths and frequencies of the voice **Pros:** amplitude and frequency modulations provide high accuracy **Cons:** variability of transducers and local acoustics, complicated enrollment procedure, user-unfriendly, age and hardware cause variability **Applications:** shows strong potential for use in securing mobile computers, PDAs and other similar devices; employed by many large companies to protect computer, office, lab, and vault access **Examples**: Examples can be found at the home page of The Biometric Consortium (2003b)
Iris Scan	**Features:** scans the iris of the eye and digitizes a pattern for matching purposes, works well in identification mode **Pros:** less intrusive than retina scan, higher matching performance, works well with glasses, across ethnic groups **Cons:** difficult to use and integrate with other systems **Applications:** welfare fraud prevention in Illinois; beginning to be used in ATM machines; used to enable single sign-on in distributed networks; used in smart cards, workforce management, network security and authentication **Examples**: Examples can be found at the home page of The Biometric Consortium (2003b)

(continued on next page)

TABLE 1 (continued)

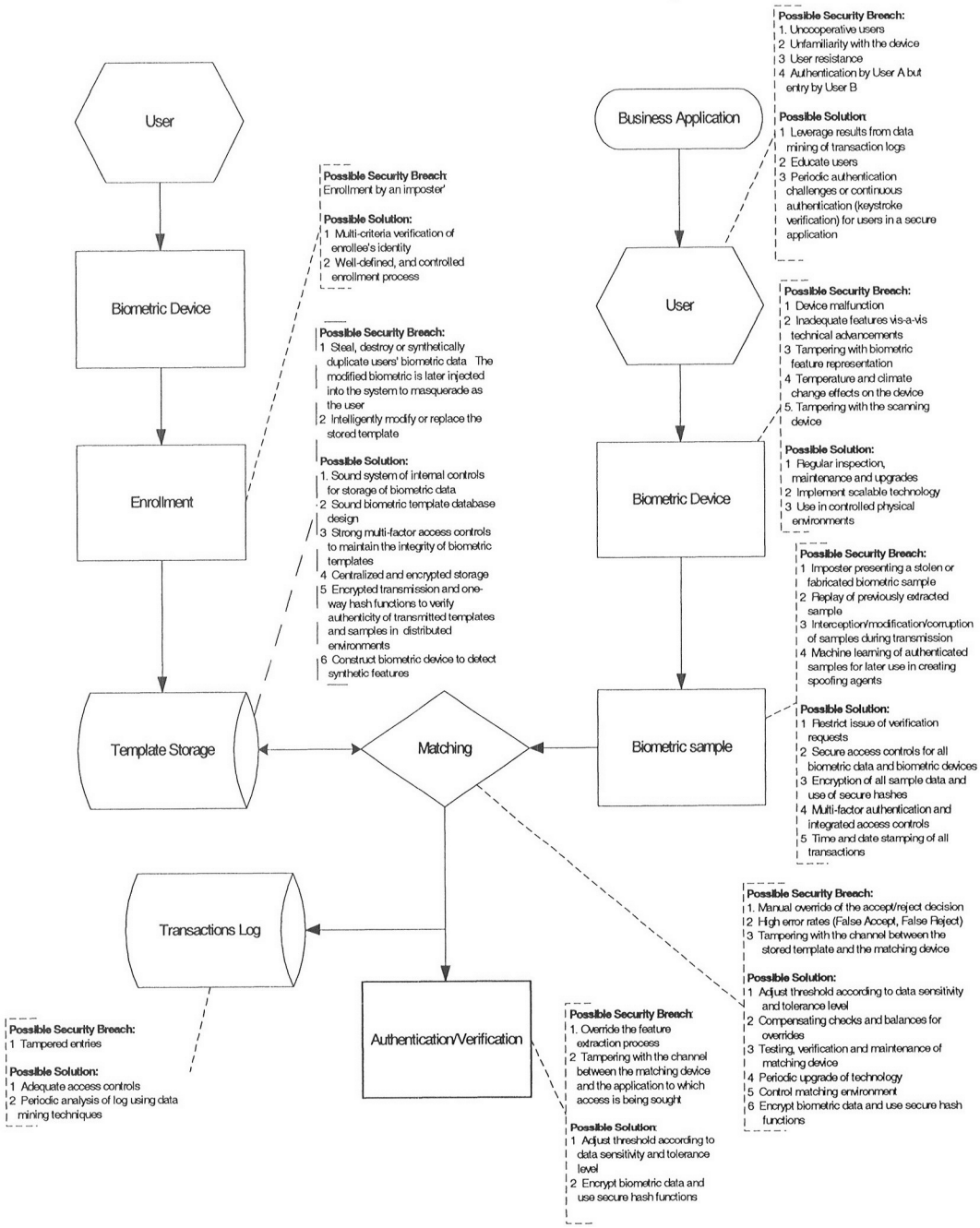
Technology	Description
Retina Scan	**Features:** a digital image of the retina of the eye is created to match the pattern against a live sample, scanning done by a low-intensity light via an optical coupler **Pros:** highly accurate **Cons:** problems with glasses, intrusive **Applications:** welfare fraud prevention in Illinois; used to enable single sign-on in distributed networks **Examples**: Examples can be found at the home page of The Biometric Consortium (2003b)
Facial Scan	**Features:** measures the curves on the cheeks and the lips to ascertain the identity **Pros:** larger number of variables can be studied **Cons:** difficult to use, limited success in applications **Applications:** used at several airports and other public locations since 09/11/01 **Examples**: Examples can be found at the home page of The Biometric Consortium (2003b)
Keystroke Scan	**Features:** A behavioral biometric device. It measures the force applied and the pattern used to push keys on a keyboard **Pros:** very convenient with little intrusion **Cons:** possible interference of noise, caused by hands movement, not associated with actual keystroke **Applications:** not widely used; has good potential for continuous authentication **Examples**: Examples can be found at Krochmal (1998), BioPassword (2001), BioChec (2003b)

for scanning. This creates a live biometric sample that is compared with the stored biometric template for that user in the biometric database. Basically, the user claims an identity by providing an identifier and follows it up by providing a live biometric sample. If the sample matches the template, a "*true*" message is generated and the user is authenticated. Like the enrollment process, there are several factors (see Figure 2) that might impede effectiveness of the matching process. Therefore, systems administrators should take appropriate steps such as those identified in Figure 2 to strengthen the integrity of the biometric system.

Effectiveness of Biometrics

Biometric technologies vary significantly in terms of effectiveness. Four factors are often used to assess effectiveness: accuracy, cost, effort, and intrusiveness. Figure 3 summarizes the performance of various biometric technologies on these four dimensions. This diagram shows that no single technology is superior across all four factors. For example, keystroke scanning is close to an ideal biometric when evaluated based on intrusiveness, cost, and effort, but its accuracy is currently very low. Similarly, iris scanning is close to ideal in terms of accuracy and effort, but cost is high and the technology is somewhat intrusive. Fingerprint scanning is the most widely used biometric technology, but it is perceived to be intrusive and carries the stigma of association with criminal identification. Facial recognition has become increasingly popular since September 11, but several field studies have produced results that call into question its reliability (Blackburn et al. 2001; Bray 2002; Stanley and Steinhardt 2002). Hence, the business process application, the desired level of security, and the fundamental security needs of a system should dictate the selection of any biometric technology. Like any technology, it should be the business process that drives investments in biometrics and not the other way around.

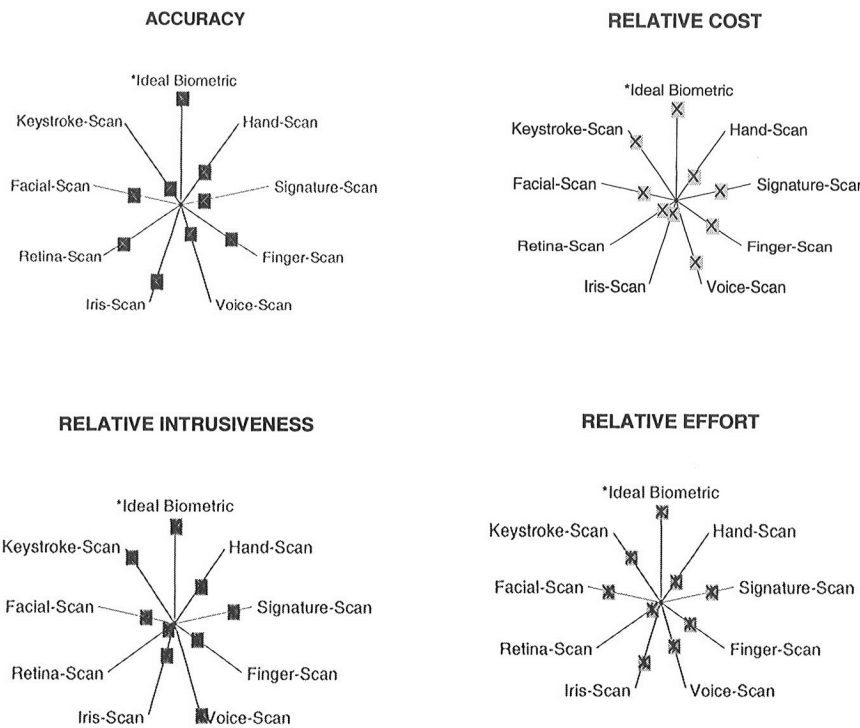
FIGURE 2
Biometric Mechanics and Associated Security Risks



An important technical issue relates to the performance of the matching process during authentication and verification. The performance of the matching process, which is typically measured by using the metrics described in Table 2, can be affected by several factors, including the deployment environment, user behavior, user discipline, user interface, user stress, familiarity with the device, condition of the biometric device, and speed of response (Nichols et al. 2000). Therefore, performance of a biometric device in the field is likely to be different from the manufacturer's rated performance. Both false acceptances and false rejections will affect user acceptance and trust in the system, and could eventually jeopardize effectiveness of the technology.

One of the benefits claimed for biometrics is more effective authentication and a higher level of confidence associated with authentication results. Confidence in the system is expected to be higher in a small local area network environment that contains both the database and the necessary matching algorithm, together with a result and "score" indicator. However, in situations where components of the complete process are split across multiple nodes in a distributed architecture (e.g., the Internet), the level of confidence might be substantially lower. Furthermore, the presence of multiple processing nodes in a distributed environment creates a perception of a complex control environment that is not trustworthy (Hall 2001; Garfinkel 1997).

FIGURE 3
Relative Accuracy, Cost, Intrusiveness, and Effort of Biometric Technologies



Source: Adapted from the International Biometric Group. (2001) Zephyr Analysis. (In reading this figure, points close to the center reflect poor performance. Points further away from the center indicate better performance. Ideal performance exists at the outer tip of a line).

TABLE 2
Biometric Performance Measures

False accept rates	(FAR): probability that an impostor may be falsely accepted by the system.
False reject rates	(FRR): probability that the genuine user may be rejected by the system.
	Both these measures are expressed in percentage (of error transactions) terms, and are designed to capture the accuracy of a biometric technology. Generally, physical biometrics is considered more accurate than behavioral biometrics.
Equal error rate:	the point of intersection between the FAR and FRR; represents a more realistic measure of performance than either FAR or FRR quoted in isolation; the threshold is plotted on the x-axis and error rate plotted on the y-axis.
ROC Curve:	Receiver Operating Characteristic (ROC) is the plot of all theoretical false accepts and false reject rates for each biometric technology. The y-axis of the graph shows the probability of verification, whereas the x-axis plots the false alarm rate.
CER:	The Crossover Error Rate is a reflection of the accuracy of the system. The lower the CER, the higher the accuracy. It is obtained by plotting the FAR and FRR. Each point on the plot denotes a hypothetical performance at various sensitivity settings.
Ease of use:	the relative user-friendly feature of biometric technology.
User acceptance:	Usually the relative intrusiveness of biometric technology will define how easily it is accepted by users.

Confidence in the authentication process is likely to be inversely associated with the probability that the "*true*" message produced in the matching process could be discovered, captured, artificially injected, or otherwise compromised. If the decision maker considers this probability to be high, then confidence and trust in the system would be low, and vice versa. Through the use of encryption and secure hash algorithms,[3] the design of the systems architecture can minimize this probability and contribute to the effectiveness of a biometric-enabled security mechanism. Biometric templates can be encrypted while in storage and/or when being transmitted over network communication channels. Similarly, a secure hash algorithm can be used to create digital signatures to authenticate the integrity of all transmitted biometric data. These processes can be employed whether the biometric matching engine resides on a back-end-server, with the client, or on an intermediary.

From the standpoint of minimizing control risk, biometrics offer a compelling choice as a security mechanism for authenticating AIS users. The value proposition offered by biometric technology is that it allows accountants and auditors to bind system access and use to specific individuals. However, there is no available evidence to indicate that biometric devices are being deployed in accounting information systems to complement existing security mechanisms. Thus, accounting-specific issues that are critical in the deployment of biometric technology merit attention. Selected issues and illustrative examples are presented in the next section.

III. ACCOUNTING ISSUES

Biometric technologies are of interest in any area where it is important to verify and authenticate the true identity of an individual. The accounting field presents a fertile domain for utilization of biometrics to reduce fraud, mistakes, errors, and control risk. The accounting function has the potential to derive benefit from biometric technologies at four distinct levels: systems design, assurance services, control integration, and data integrity at the database level.

[3] A hash algorithm produces a condensed representation of a message that cannot be reversed to produce the original message. A hash is used to verify that the message has not been intercepted and modified during transmission (Stallings 2000).

Systems Design

The design of an information system can incorporate biometric-enabled security devices in order to validate users during identification, authentication, and authorization. There are numerous accounting-related situations in which authentication and identification are needed to establish the system's privileges that should be granted to individuals. In addition, segregation of duties in AIS depends on effective authorization to access, receive, modify, process, and use information and other resources.

Assurance Services

Accountants have the expertise and training to provide assurance services to third parties. Though initially accountants may not possess the technical skills needed to provide assurance services for an entire biometric-enabled security system, their traditional strengths and reputation as assurance service providers could be readily leveraged to provide independent assessments of the trustworthiness of the enrollment process, control and supervision of biometric databases, security of communication channels, and verification that system error rates are at an acceptable level. The accounting function can also help in the development of metrics to evaluate the performance of biometric devices. Overall, assurance services offered by accountants would seek to provide confidence in the capability of a biometric device to deliver the desired level of security, particularly in distributed network environments where remote users and independent third parties are expected to rely on the system. As e-commerce grows, third parties doing business over the Internet will demand such assurance. Although the use of biometrics would reduce the level of identification and authentication errors, it might still be necessary to provide independent verification that biometric technologies are working effectively and as intended. The accounting profession is well positioned to provide such assurance services, as this is one of its traditional services.

Control Integration

The effectiveness of the organizational control environment can be enhanced by integrating biometrics with the existing set of identification and authentication mechanisms used in accounting systems. For example, biometrics can be combined with passwords to create a multifactor authentication mechanism to protect highly sensitive data and information such as employee social security numbers, customer confidential information, and proprietary business processes. Such integration will provide a highly secure mechanism to guard the safety and security of AIS. From a generic standpoint, the accounting function is often charged with the responsibility for securing organizational assets including information. This responsibility is articulated in the Treadway Commission Report (COSO 1992) and in later frameworks such as CICA's Information Technology Control Guidelines (CICA 1998), SysTrust (AICPA 2002; McPhie 2000; Boritz and Mackler 1999), and CobiT (2002).

Data Integrity

The accounting function has traditionally been the keeper of corporate data. The storage of biometric data is one of the challenges within the IT community. This presents a fertile area for accounting to seize the opportunity and help in the design and storage of a biometric database that is aligned with corporate strategy. Moreover, accountants can also provide assurance on maintaining the integrity and confidentiality of biometric databases. Like any other database, a biometric database needs supervision and control to minimize the risk of abuse, distortion, and unauthorized access.

In the remainder of this section, we provide selected examples that highlight the potential role of biometrics in accounting applications. These examples focus on enterprise resource planning, inventory fraud, and payroll.

Enterprise Resource Planning

The next frontier of enterprise resource planning (ERP) systems is the integration of information systems of an enterprise with those of its stakeholders. The goal is to achieve a seamless flow of data and to facilitate decision making in real time. When suppliers or wholesalers query a company's database, the accounting function has to ensure that only those authorized to access data are in fact interacting with the company. With the pervasive security threats that exist in distributed network environments such as the Internet, utilization of biometrics is expected to provide a higher level of security to authenticate the identity of transacting parties. Since biometric traits are relatively difficult to circumvent, integrating and streamlining a biometric-based authentication process with other security measures should enhance the trustworthiness of identification and authentication services in distributed networks. Effective authentication can strengthen other information systems security services such as confidentiality, non-repudiation, data integrity, and systems availability (Stallings 2000).

Inventory Fraud

Inventory fraud is among the most common and costly crimes in the corporate sector. Any effort to minimize the occurrence of such frauds requires establishing the identity of users accessing the system, and allowing only authorized persons to execute a business transaction. In this context, biometrics has the potential to provide a higher level of security and confidence in the internal control system. The process allows only individuals who are enrolled in the system to gain access to inventory. It provides security through the enrollment process, as illustrated in Figure 1, when authorized persons are authenticated based on exogenous information (e.g., letters of reference, pictures, certificates, and notarized documents). Security is also provided when the authorized person presents his/her biometric for scanning and matching with a valid biometric template. Thus, only persons who pass these dual authentication processes are permitted access to inventory.[4]

Payroll Accounting

Payroll accounting represents another area where authentication issues assume significance. The need for effective authentication exists in at least three processes: time-keeping and attendance records, pick-up of paychecks, and linking employees to specific tasks in job-shop environments. Biometric technology has the potential to more precisely identify and authenticate employees when they clock in and out. Biometric identification could also be effective in reducing the incidence of phantom workers as, for example, at large-scale construction sites. Finally, a combination of biometrics and bar codes could make accounting for direct labor cost in a job-shop environment seamless and precise.

In summary, biometric technology has significant appeal and potential. It is possible that the technology could be overutilized. The technology is costly, and could have unintended adverse consequences on employees, customers, business partners, and other stakeholders who interface with it. Therefore, we believe that organizations must develop appropriate models for identifying business processes where the use of biometrics would be cost effective.

IV. ACCESS DECISION FRAMEWORK

In this section, we develop an access decision framework that can assist decision makers in choosing investments in identification and authentication mechanisms. We first develop and define the concepts of business information intensity (BII) and exposure—the two key variables of the

[4] Biometrics represent only one of the new technologies that could be used to minimize inventory fraud. Using biometrics for protecting physical access to inventory, as well as other technologies (e.g., RFID tags) that limit pilfering, could strengthen controls.

access decision framework. The framework is modeled as a two-dimensional matrix, resulting in four broad quadrants with a mix of BII and exposure. Later, we provide features and examples of each of the four quadrants that have variants of BII and exposure. For each quadrant, a normative strategy is identified for the implementation of an appropriate security layer. The discussion converges on those business processes that have high BII and high exposure as the ideal candidates for the application of a biometric security layer. Since no security measure by itself is sufficient, we propose a portfolio of security measures that includes biometric technologies to strengthen authentication services, enhance trust, and promote confidence in the integrity of the AIS.

Business Information Intensity

IT is a strategic factor in competitive economies because it can alter the rules of competition, give enterprises new ways to outperform competitors, and often form the basis for whole new businesses (Porter and Millar 1985; Porter 2001). Thus, we define BII in terms of the IT content in the product and value chain of an entity. BII is high when the IT content of both the product and the value chain is high. Conversely, BII is low in situations where the reverse occurs.

An example where both product and value chain are high in BII comes from the exchange of sensitive information. This exchange may be internal or external to an entity. Internally, parties within the entity exchange proprietary and sensitive information among peers on a need-to-know basis. In modern business enterprises, this exchange process is enabled primarily through the use of IT. Thus, both the product (information) and the internal value chain are high in BII. For example, the exchange of the formulae for proprietary designs and secret recipes among authorized entities is facilitated globally through the use of information technology. The designs and recipes are information intensive and the processes used to store, modify, disseminate, and service them within the internal value chain rely heavily on information technology.

From an external perspective, information embedded in the value chain of a business-to-business (B2B) exchange firm is high in BII due to the dominance and significance of IT in its primary activities. For example, Covisint, a B2B exchange company, has to coordinate information requirements of various automobile suppliers and manufacturers. An imbalance in the information value chain would likely have a negative domino effect on the production plans of manufacturers and also cause either slow-moving inventory or a shortage of inventory in suppliers' warehouses. Thus, Covisint's value chain and products are high in BII. Information technology, particularly the Internet, is the company's primary driver of inbound logistics, operations, outbound logistics, marketing and sales, and after-sales service (Porter 2001). Furthermore, the company's infrastructure and procurement activities are inextricably linked to the Internet.

Another example comes from online banking. The services offered by an online bank are information intensive and the value chain is enabled by a distributed network infrastructure. The services offered, marketing and selling of those services, post-sale activities to support customers, and logistic systems are all based on the network infrastructure. Thus, BII is high in online banking. While a brick-and-mortar bank might also be high in BII, an online bank would be expected to utilize significantly more IT in both products and value chain. The ultimate migration toward virtual banking would make banking, in general, a high business information intensive operation. In contrast, a small landscaping business would usually have a low level of BII. Its products and services are relatively less dependent on IT and its primary value chain activities are likely to be labor intensive.

Exposure

Exposure is defined as the potential loss (in monetary terms) to the organization due to the absence or weakness of internal controls. A benefit of computerized AIS is that it reduces the number of human errors occurring during routine processing. However, this reduction in human errors is

often replaced by an increased propensity for unauthorized access to or modification of data files in computerized AIS. These problems are exacerbated in distributed network environments. The reach of the information system is global and there are more access nodes. This makes the modern distributed AIS more vulnerable to those who might misuse them than the traditional AIS. In essence, the ubiquity of computers in the AIS has increased the level of exposure in organizations. Thus, it is imperative that entities adopt enhanced security measures to control authentication and access to information resources.

If unauthorized access to information resources has severe and cascading consequences, then exposure will be high. For example, unauthorized access to the systems set-up routines[5] for a financial application could result in widespread access to the company's systems by unauthorized entities. Therefore, exposure is likely to be high because of the potential significant losses from destruction, modification, or fabrication of a company's data and information via inadequately secured set-up routines.

If information in the product and/or value chain is proprietary, highly confidential, or represents a source of competitive advantage, then the potential loss resulting from threats to that information is likely to be high. In the case of Covisint, for example, the value chain would have a high degree of exposure resulting from failures in the security of IT. Control measures that mitigate the threats to information resources used in Covisint's value chain would, therefore, translate into higher value both for the company and its stakeholders along the supply chain. Exposure would also be high in situations where organizations use computers and distributed networks to store and share proprietary designs and secret product formulae. A breach in the security of these designs and formulae could be costly for the entities involved. An online bank faces a similarly high level of exposure. Since its entire value chain is dependent on a secure IT infrastructure, security breaches would be costly and could jeopardize the bank's survival.

Two-Dimensional Framework

The transition to a knowledge-based economy makes organizations increasingly vulnerable to interception, fabrication, modification, interruption, and theft of information resources. Organizations invest countless hours and financial resources to safeguard their information and maintain data availability and integrity. Resource limitations imply that not every business process will be made impervious to abuse or misuse. A judgment has to be made with regard to the extent of investment in security measures. The access decision framework presented in Figure 4 can guide those judgments.

Figure 4 provides a two-dimensional access decision framework based on BII and exposure as described above. Business processes have different levels of BII and varying degrees of exposure. BII is measured along the horizontal axis. Exposure (to losses) is measured along the vertical axis. The interaction between the two constructs results in four broad quadrants for application of various types of security measures. Quadrant I represents those business processes where both BII and exposure is low. Business processes that have high BII but low exposure fall into Quadrant II. Quadrant III contains processes that have high exposure but low BII. Finally, Quadrant IV includes processes with high BII and high exposure.

The four quadrants of the framework highlight different degrees of vulnerability to information systems threats and can help to categorize business processes based on the extent of their vulnerability to security breaches. The placement of business processes into these four quadrants can serve as a guide to specifications of the nature and strength of security services required to protect information resources. Business processes with only low exposure cannot justify large investments in information security mechanisms. Alternately, processes that involve high levels of exposure and that are

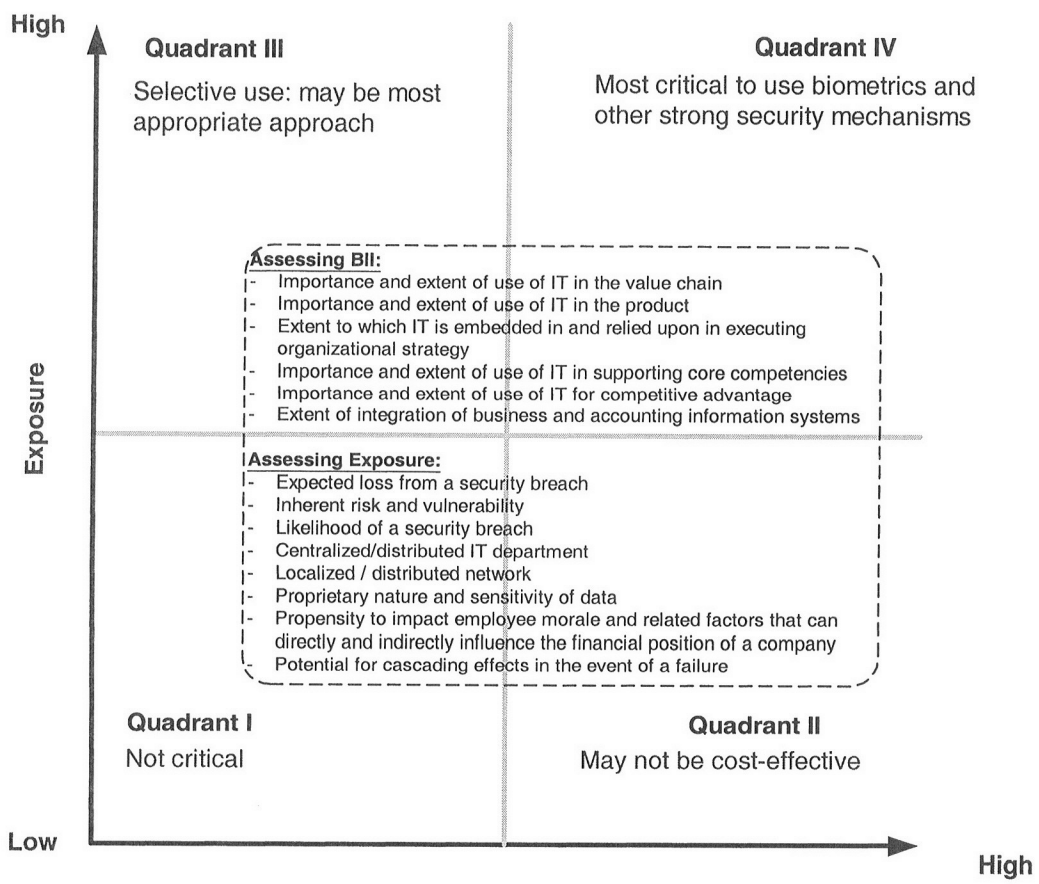
[5] Systems set-up routines are the security routines in an application where user accounts are created, user authentication requirements are indicated, and access rights, privileges, and authorizations are established.

characterized by high levels of BII should have sufficient investment in security mechanisms to mitigate threats to information resources. Thus, the framework can serve as a decision aid for identifying business and accounting applications for which adoption of a biometric security layer might be considered.

Operationalizing the Framework

The two constructs, BII and exposure, are not directly observable. Therefore, to orperationalize the framework, we propose surrogate measures that incorporate multiple factors that point to BII as well as exposure (see Figure 4).[6] The figure lists various factors for each construct. These factors can be used to classify business processes into each of the four quadrants of the access decision framework.

FIGURE 4
Access Decision Framework



[6] It should be noted that the BII construct is relatively new, and there are currently no validated instruments for measuring it. Measures to quantify BII constructs noted here are logical extensions of this study.

Quadrants I and IV

Using the two sets of factors, one can make a compelling and direct argument for placing certain business processes into Quadrants I and IV. In the case of Quadrant I, security is not critical, and therefore, we would not recommend large investments in information security for processes that fall within that quadrant. Such situations may be well suited for less intrusive traditional security measures. The low level of exposure and BII imply that losses due to compromises in access to information might not be significant. For example, nonsensitive operational reporting systems that do not make use of public communications channels would fall into this quadrant.

An illustrative case of an entity that falls into Quadrant I is a small landscaping company. This type of entity will ordinarily have limited investments in IT and will typically not make use of distributed computer networks. Vulnerability to security breaches would be relatively low since the entity's information resources would not be connected to public communication channels, and systems use can be physically restricted to only trusted persons. In such circumstances, physical protection and safeguards with traditional mechanisms, such as passwords, are likely to be adequate.

Business processes and applications that fall into Quadrant IV are likely to benefit the most from the use of biometrics. These applications have high levels of both BII and exposure. Therefore, correspondingly stronger security measures are needed to minimize the risks associated with those business activities. Examples include systems set-up, similar systems administration, database administration processes, online banking processes, exchange of sensitive and/or business critical information, point-of-sale[7] authentication for debit and credit card holders, authentication of buyers and sellers in B2B exchanges, and key authentication in a public key infrastructure (PKI). The common characteristics of these examples include the critical nature of IT in the product/service and in the value chain, the alignment of IT with the business strategy, the strong likelihood of debilitating and cascading effects of IT security breaches, IT support for core competencies, and the use of IT for competitive advantage. The distributed nature and use of public communication channels for executing most of these processes also make them vulnerable to potential security threats.

Systems set-up involves administering and maintaining security for identification, authentication, and authorization. An unauthorized user who gains access to systems set-up routines could, at least in theory, have unfettered access to all information resources throughout an entire business enterprise. Clearly, systems set-up failures could have negative consequences possibly cascading throughout the company. Integrated business information systems are often highly vulnerable to these issues.

Business-critical Internet-based processes (especially those involving B2B exchanges such as the Covisint example mentioned earlier) and online banking processes are characterized by high BII and high exposure, and thus appropriately belong to Quadrant IV. Similarly, processes that support access to sensitive information (e.g., pension and other human resources data, and communication of business strategy) in distributed network environments would fall into Quadrant IV. However, using biometric security mechanisms in such processes would invariably require third-party involvement in the enrollment process as transacting parties are likely to be scattered across the globe. Third parties would be needed to verify users' identities and privileges. In a sense, these third parties would act as certification authorities to support the biometric enrollment process and create an infrastructure for a distributed authentication system.

While certification authorities for biometric enrollment do not currently exist, we believe that as commercial applications of biometrics increase, the emergence of such trusted third parties would complement and strengthen the security of the marketplace. Further, in view of the training and preparation of accountants in verification processes, the accounting profession is ideally positioned

[7] It has been reported that Kroger, Thriftway, McDonald's, and Wal-Mart are conducting research and starting pilot programs to decide whether to deploy biometrics to authenticate customers at point-of-sale (French et al. 2003).

to add value to the marketplace by providing services as certification authorities in a distributed authentication system. Thus, accountants can have a major role in supporting the integrity of a distributed biometrics infrastructure.

Quadrants II and III

Organizations with business processes falling into Quadrants II and III must consider their needs on a case-by-case basis. For example, not all inventory control systems warrant the use of strong security mechanisms such as biometrics. Exposure associated with an inventory control system for bullion would be high but the associated BII would be low (Quadrant III). Because of the high degree of exposure, stronger biometric controls would seem to be appropriate. On the other hand, inventory control systems for low-value items such as nuts and bolts might be adequately protected with traditional security measures.

An example of an application that falls into Quadrant II is accessing read-only, low-security documents such as published quarterly financial statements, annual reports, and other publicly available types of information that are intended to reach wide cross-sections of anonymous users via a distributed network. This application involves a series of processes and a product. The processes, which constitute a value chain for the application, include the acquisition, creation, and distribution of information using the Internet and related information technologies. The product is the information that remote users can access. Defined in those terms, information technology is highly embedded in both the product and the value chain. The application is high in BII because the value chain depends on information technology and the product, as defined, is highly information intensive. However, exposure associated with services that provide access to information that is intended to be in the public domain is likely to be relatively low. Because these documents are in the public domain and will be used by anonymous persons, it would be neither cost effective nor feasible to employ biometrics to safeguard access to such documents.

In summary, a high level of IT content in the product and value chain effectively translates into high BII. Use of biometric security mechanisms is most critical in situations that are characterized by high exposure and high BII. If an application is low in both exposure and BII, then biometrics may not be a cost-effective proposition. Notwithstanding the growing popularity of biometrics, companies should not rush to use those technologies unless project sponsors can make a business case that considers both exposure and BII.

V. CHALLENGES AND FUTURE EXTENSIONS

The use of biometrics to secure information resources is new and there are many challenges and issues that systems designers must address in order for biometric-enabled security mechanisms to be a major factor in reducing control risk. These challenges and issues, which are documented in this section, provide opportunities for further research in the area.

The Business Case for Biometrics

There is often a temptation to deploy new technology based on the beliefs of key decision makers who are influenced largely by the novelty and popularity of the technology (Swan and Newell 1994; Rogers 1995). It seems intuitive that accountants and systems designers should focus on the business case and specific contextual factors that drive an organization's need for a biometric-enabled security layer as opposed to the technology itself. However, there is currently no available literature on the factors that drive adoption and facilitate effective implementation of this new technology. Research is needed to understand these issues.

Distributed Enrollment Infrastructure

Organizations that wish to use biometrics must ensure that there is a secure infrastructure to support the enrollment process. While an organization may readily create such an infrastructure

within its own boundaries, extending the infrastructure to business partners and customers presents major challenges. Currently, there is no infrastructure for assuring the security and integrity of enrollment processes, particularly in distributed network environments. The available literature offers little insight into the practical and theoretical issues involved in building such an infrastructure. Thus, further research is needed in this area.

Societal Barriers

Use of physiological and behavioral traits for security is becoming a highly contentious issue. For example, the American Civil Liberties Union (ACLU) has expressed a great deal of trepidation about the use of biometric identifiers (Stanley and Steinhardt 2002). Some of the more contentious issues include privacy and confidentiality of biometric databases, ownership and control of biometric data, and function creep (application of biometrics for purposes beyond their original purpose). Even among mainstream business entities, such as Wal-Mart, there is concern that the technology has advanced much faster than the law (International Biometric Industry Association [IBIA] 2002). These issues are prompting state and federal governments to examine privacy and security issues related to the commercial use of biometric technologies (State of New Jersey 2002).

User acceptance remains a sensitive issue in biometrics implementation (Furnell et al. 2000; Lavonne 2002; Deane et al. 1995). Factors that affect the diffusion and acceptance of biometric systems in organizations are not known. Moreover, users' concerns for privacy and the impact on biometric technologies and incident response schemes for compromised biometrics merit further attention in the AIS research literature.

Biometric Authentication as Evidence

The legal system's acceptance of distributed biometric authentication as evidence is fraught with lack of clarity and precedence. Recent court cases suggest that resolution of this uncertainty would require objective assessment of the reliability of biometric authentication systems (*Daubert v. Merrell Dow Pharmaceuticals, Inc.* 509 U.S. 579; *Kumho Tire Co. v. Carmichael* 526 U.S. 137; Harvard Law Review 2002). Yet, there is a paucity of independent evidence on the accuracy and reliability of biometric-enabled user authentication systems. There is also evidence of poor performance in certain wide-scale applications (Claburn 2002; CardTechnology.com 2002; Bray 2002; Stanley and Steinhardt 2002). Additional research is needed to explore the accuracy and reliability of biometric devices, particularly in wide-scale distributed applications.

Currently, biometric authentication systems are designed to verify the identity of an information systems user with a relatively high degree of certainty only at the start of a session (Monrose and Rubin 2000). Users are not continuously authenticated during the session, and there is no evidence that the same person who authenticated a session continued as the user after being granted initial access to the system. Further research is needed to examine the potential for using biometrics (e.g., keystroke latencies and facial recognition) as a technology for continuous authentication.

The impact of aging and other physiological changes on accuracy and reliability further complicates the use of biometric authentication as evidence. The development of robust biometric devices that can adapt to minor physiological changes would be a significant boost in this regard. Advances in biologically inspired computing algorithms such as neural networks, genetic programming, and other adaptive technologies might be used to model the aging process and distinguish between authorized and unauthorized users over time.

Precision of Biometric Identifiers

The uniqueness of the behavioral trait or physiological characteristic of information systems' users is still questionable (Jain et al. 2002). It is noteworthy that the biometrics community defines biometrics as *distinguishable* (rather than *unique*) physiological and behavioral traits that may be

used for identification and authentication. Thus, there is a presumption that biometrics are not 100 percent unique. This begs the question of the degree of similarity that should exist between a biometric sample and a user's stored biometric template in order to have a match (Granger 2001). Concerns that biometrics are not perfectly precise representations of information systems users' identities can negatively impact the public's perception of the technology, exacerbate legal issues, and undermine its potential for general acceptability. Further research is needed to explore those issues.

Spoofing

Spoofing is a distinct threat to biometric technology. Although biometric authentication systems can be protected against this threat by incorporating advanced security features (e.g., liveliness tests, random check digits, encryption of biometric templates, and secure hash algorithms), these enhancements add complexity and exacerbate issues related to cost, performance, and ease of use. Furthermore, it is not known how users might react to some of these enhancements.

Multifaceted Nature of Information Security

A biometric security layer for accounting systems is not a panacea. Information security systems must ultimately protect confidentiality, availability, integrity, authentication, and non-repudiation (Kaufman et al. 2002; Stallings 2000; AICPA 2002). Information security is multifaceted and a biometric-enabled security layer will not satisfy all the fundamental objectives for information security. Furthermore, designing a biometric-enabled security layer to protect AIS requires many trade-offs. Increasing security often involves higher costs as well as reduced ease of use and slower system performance.

Even if one should address all the preceding challenges, an organization's broad internal control system might still be weak and may not provide a good foundation for technology-based security solutions. A biometric-enabled security layer may strengthen certain general and application controls. However, the fundamental components of internal controls (COSO 1992) must still be maintained and basic control activities such as segregation of duties, supervision and authorization, approval, reconciliation, and verification of transactions and events must still be enforced.

VI. CONCLUSION

Biometrics technology holds promise for accounting applications. It can provide enhanced security for user identification and authentication, and has the potential to reduce control risk in business and AIS. Because passwords and tokens do not bind to a specific person, they are vulnerable and could result in understatement of control risk in situations where they are used. On the other hand, biometrics authenticate the actual identity of the person using a system and can, in theory, be used unambiguously to bind the use of an IT resource to a specific person. However, not all business processes and applications need to be protected with biometrics and there are many unresolved issues and challenges that need to be further researched. In this context, we proposed an access decision framework based on business information intensity and exposure to categorize business processes and applications that might benefit from the tighter security that biometrics provide. The framework is useful for guiding investments in security mechanisms, including biometrics.

In order to design and build an effective biometric-enabled security layer for AIS, several theoretical and implementation issues need to be addressed from both an academic and a practical standpoint. The interaction among technological, cognitive, behavioral, and legal factors must be examined in the implementation of biometric enabled systems and processes. Both practitioners and accounting professionals need to walk a fine line. The claimed promise of biometrics rests on the assumption that a sound business case is made, the system is correctly implemented and used, and it

performs effectively in the field. The success of biometrics in AIS requires due consideration of assumptions, challenges, and constraints applicable to this technology in its current state. We recommend further research to explore such issues.

REFERENCES

American Institute of Certified Public Accountants (AICPA). 2002. *Trust Services Principles & Criteria.* Incorporating SysTrust & WebTrust, Exposure Draft. Available at: http://www.aicpa.org/download/trust_services/ed_princ_criteria.pdf (Accessed March 3, 2003).

BioChec. 2003. *Keystroke Heuristics.* Available at: http://www.biochec.com/keystroke/ (Accessed March 3, 2003).

Biometrics Consortium. 2003a. *Research and Databases.* Available at: http://www.biometrics.org/html/research.html (Accessed March 3, 2003).

———. 2003b. *Examples of Biometric Systems.* Available at: http://www.biometrics.org/html/examples/examples.html (Accessed March 3, 2003).

BioPassword. 2001. *Technical Report: BioPassword Keystroke Dynamics.* October 18. Available at: http://www.biopassword.com/home/technology/BP%204.5%20Technical%20Paper.pdf (Accessed March 3, 2003).

Blackburn, D. M., M. Bone, and P. J. Phillips. 2001. *Facial Recognition Vendor Test 2000—Evaluation Report.* DoD Counterdrug Technology Development Program Office, February 16. Washington, D.C.: Government Printing Office.

Boritz, E., and E. Mackler. 1999. Reporting on systems reliability. *Journal of Accountancy* 188 (5): 75–87.

Bray, H. 2002. Face testing at Logan is found lacking. *Boston Globe* (July 17).

Canadian Institute of Chartered Accountants (CICA). 1998. *Information Technology Control Guidelines.* Toronto, Ontario: CICA.

CardTechnology.com. 2002. German savings banks reject biometrics at ATMs. *Card Technology Magazine.* Available at: http://www.cardtechnology.com/ (Accessed September 19, 2002).

Claburn, T. 2002. Man vs. machine. *Smart Business* 15 (4): 34.

CobiT. 2002. *Control Objectives for Information and Related Technology.* Available at: http://www.isaca.org/cobit.htm (Accessed September 14, 2002).

Committee of Sponsoring Organizations (COSO). 1992. *The Committee of Sponsoring Organizations of the Treadway Commission.* Available at: http://www.coso.org/ (Accessed September 14, 2001).

Connecticut Department of Social Services. 2002. *DSS's Biometric ID Project.* Available at: http://www.dss.state.ct.us/digital/ditutor.htm (Accessed March 3, 2003).

Deane, F., K. Barrelle, R. Henderson, and D. Mahar. 1995. Perceived acceptability of biometric security systems. *Computers and Security* 14: 225–231.

FindBiometrics.com. 2003. Available at: http://www.findbiometrics.com (Accessed March 3, 2003).

French, V. O., R. R. Norton, and R. A. Dornbusch. 2003. *Biometric Advocacy Report.* V (3): February 21. Available at: http://www.ibia.org/newslett030221.htm. (Accessed March 3, 2003).

Furnell, S. M., P. S. Dowland, H. M. Illingworth, and P. L. Reynolds. 2000. Authentication and supervision: A survey of user attitudes. *Computers and Security* 19: 529–539.

Garfinkel, S. 1997. *Web Security & Commerce.* Cambridge, MA: O'Reilly & Associates.

Granger, G. 2001. *Authentication Confidences.* White paper, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA.

Hall, J. A. 2001. *Accounting Information Systems.* Cincinnati, OH: South-West Publishing.

Hart, P. 2001. National commission warned of country's vulnerability to attacks, lecturer here says. *University Times* 34 (7). Available at: www.pitt.edu/utimes/issues/34/011121/08.html (Accessed April 26, 2002).

Harvard Law Review. 2002. Evidence—Fingerprint Experts—Seventh Circuit upholds reliability of expert testimony regarding the source of latent fingerprint—*United States v. Havvard,* 260 F.3d 597. *Harvard Law Review* 115 (8): 2349–2356.

International Biometric Group. 2001. *Zephyr Analysis*. Available at: http://www.biometricgroup.com (Accessed September 14, 2001).

International Biometric Industry Association (IBIA). 2002. *Biometric Advocacy Report*. IV (14, August 2). Available at: http://www.ibia.org/newslett020208.htm (Accessed August 30, 2002).

Jain, A. K., S. Prabhakar, and S. Pankanti. 2002. On the similarity of identical twin fingerprints. *Pattern Recognition* 35: 2653–2663.

Kaufman, C., R. Perlman, and M. Spencer. 2002. *Network Security: Private Communication in a Public World*. Upper Saddle River, NJ: Prentice Hall.

Krochmal, M. 1998. Tool monitors keystroke rhythms for ID. *TechWeb*: October 7. Available at: http://www.techweb.com/wire/story/TWB19981007S0012 (Accessed March 3, 2003).

Lavonne, K. 2002. Grocer seeks loyalty boosts through biometrics. *American Banker* 167 (87): 13.

Matyas, S. M., Jr., and J. Stapleton. 2000. A biometric standard for information management and security. *Computers & Security* 19: 428–441.

McPhie, D. 2000. AICPA/CICA SysTrust principles and criteria. *Journal of Information Systems* 14: 1–7.

Monrose, F., and A. D. Rubin. 2000. Keystroke dynamics as a biometric for authentication. *Future Generation Computer Systems* 16: 351–359.

Nichols, R. K., D. J. Ryan, and J. J. C. H. Ryan. 2000. *Defending Your Assets*. New York, NY: McGraw-Hill.

Pipkin, D. 2000. *Information Security*. Upper Saddle River, NJ: Prentice Hall.

Porter, M. E., and V. E. Millar. 1985. How information gives you a competitive advantage. *Harvard Business Review* 63: 149–160.

———. 2001. Strategy & the Internet. *Harvard Business Review* 69: 63–78.

Ratha, N. K., and A. Senior. 2001. *ICAPR Tutorial on Automated Biometrics*. Hawthorne, NY: IBM T. J. Watson Research Center. Available at: http://www.research.ibm.com/people/a/aws/icapr.html (Accessed March 3, 2003).

Rogers, E. M. 1995. *The Diffusion of Innovations*. New York, NY: Free Press.

Romney, M. B., and P. J. Steinbart. 2003. *Accounting Information Systems*. Upper Saddle River, NJ: Prentice Hall.

Stallings, W. 2000. *Network Security Essentials: Application & Standards*. Upper Saddle River, NJ: Prentice Hall.

Stanley, J., and B. Steinhardt. 2002. *Drawing a Blank: The Failure of Facial Recognition Technology in Tampa, Florida*. An ACLU Special Report. Available at: http://archive.aclu.org/issues/privacy/drawing_blank.pdf (Accessed August 20, 2002).

State of New Jersey. 2002. Biometric Identifier Privacy Act. Assembly No. 2448. State of New Jersey. 210th Legislature. Introduced June 13, 2002 by Joan M. Quigley, Trenton, NJ.

Swan, J. A., and S. Newell. 1994. Managers' beliefs about factors affecting the adoption of technological innovation: A study using cognitive maps. *Journal of Managerial Psychology* 9 (2): 3–11.

U.S. Department of Justice. 1977. *Foreign Corrupt Practices Act*. Available at: http://www.usdoj.gov/criminal/fraud/fcpa.html (Accessed September 14, 2001).