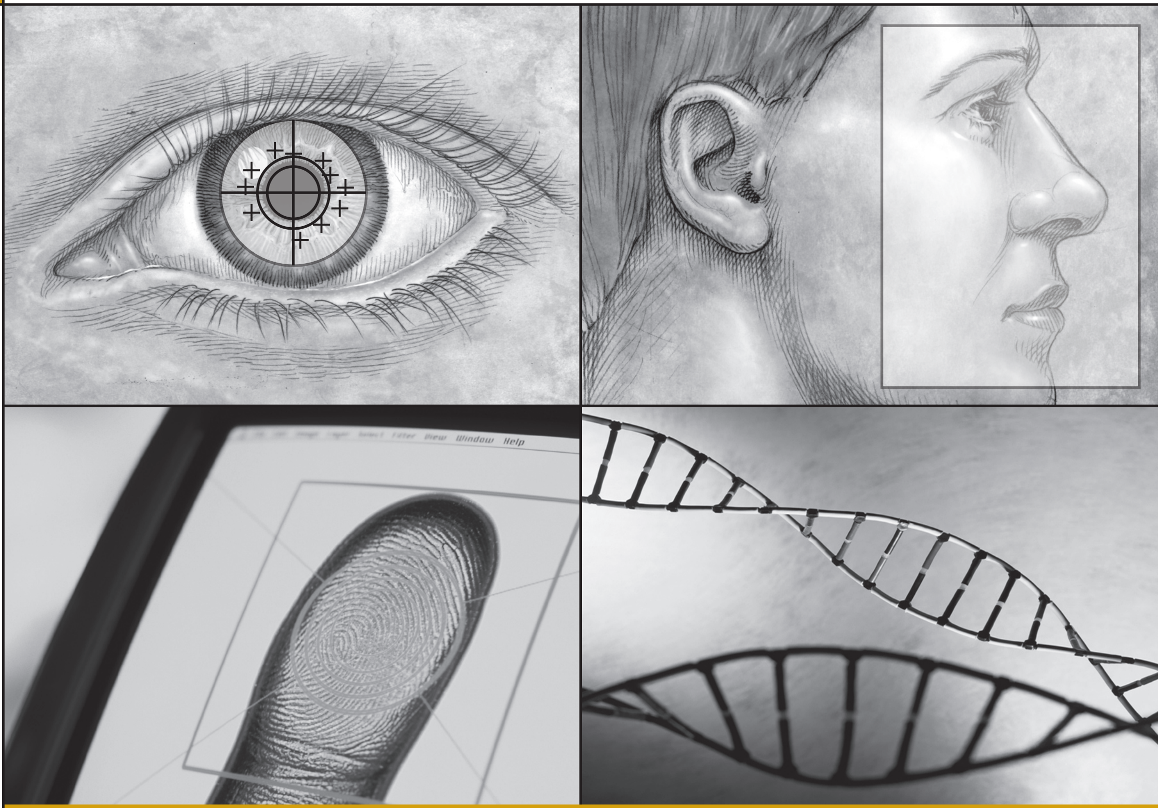
Years of 10 Research & Results 1998 - 2008

Biometrics: Enhancing Security in Organizations



E-Government/Technology Series

Babita Gupta
Professor of Information Systems
School of Business
California State University, Monterey Bay

IBM Center for
The Business of Government

2008

E-GOVERNMENT/TECHNOLOGY SERIES

Biometrics: Enhancing Security in Organizations

Babita Gupta
Professor of Information Systems
School of Business
California State University, Monterey Bay

IBM Center for
The Business of Government

TABLE OF CONTENTS

FOREWORD

On behalf of the IBM Center for The Business of Government, we are pleased to present this report, "Biometrics: Enhancing Security in Organizations," by Babita Gupta, Professor of Information Systems at the California State University School of Business at Monterey Bay.

Albert Morales

John W. Lainhart IV

Security and privacy are critical to any organization. Both business and government need to have confidence in the identity of the people doing the work of their organization. Biometrics offers a more secure means of doing this than traditional methods that depend on what a person knows (e.g., a password) or possesses (e.g., a key). Biometrics refers to the automatic identification and verification of a person based on his or her unique physical or behavioral characteristics. Using biometrics can increase confidence that the right people are doing the right work. This can increase organizational effectiveness, improve security, and reduce operational costs.

This report evaluates the use of biometrics in governmental organizations as well as the private sector. The report makes recommendations on how biometrics can be implemented effectively. One key lesson learned is that organizations need to develop a clear business case that explains the need for biometrics.

Biometrics is more secure than passwords, but it requires an investment in dollars as well as management attention that needs to be commensurate with future savings or operational improvements. Implementing biometrics usually requires changes in how organizations operate. This includes both changes to other computer systems, such as payroll, and changes in how work is done in the organization.

Successfully implementing biometrics requires organizations to work closely with their employees and other stakeholders in addressing user concerns. Without a substantial communications effort up front, organizations cannot simply "roll out" a system that requires employee fingerprints or records the patterns in their eyes. Employees need to understand the reason for the changes. Organizations need to address the concerns of employees if a transition to the use of biometrics is to succeed.

Finally, an investment in biometrics requires attention to standards. The nature of most successful new technologies is to begin as solutions to solve specific problems. The companies that field the most successful solutions grow, and the less successful ones drop out or emulate their most successful peers. Users demand standardized approaches, standards evolve, and solutions become cheaper as there is more competition. Different biometric technologies are at different points in this process, so users must balance the need to solve today's problem with an assessment of where the industry is going. The case study of the federal government's approach to employee identity cards shows one example of addressing this issue.

The use of biometrics is likely to increase greatly as the world becomes more dependent on the Internet and its attendant technologies. The recommendations in this report will help organizations use biometrics to solve today's problems while preparing for tomorrow's.

Albert Morales

Albert Morales
Managing Partner
IBM Center for The Business of Government
albert.morales@us.ibm.com

John W. Lainhart IV
Partner
IBM Global Business Services
john.w.lainhart@us.ibm.com

EXECUTIVE SUMMARY

Security of physical, financial, and information assets is emerging as a critical issue for organizations. Lapses in security such as unauthorized personnel gaining access to critical assets can have serious consequences that extend beyond the organization. Organizations need to have an absolute trust in the identity of their employees, customers, contractors, and partners; that is, that they are really who they say they are.

Usual solutions to the problem of establishing legitimate identity involve using systems that rely on what a legitimate user knows (for example, passwords or personal identification numbers) or what a legitimate user possesses (for example, ID cards or keys). However, these methods are susceptible to fraud and security threats as they do not identify the person but simply identify the information that is provided by that person. Biometric technology offers a solution to these vulnerabilities and provides a level of confidence needed for dependence on information systems and their legitimate users.

Biometrics refers to the automatic identification and verification of a person based on his or her unique physiological or behavioral characteristics, offering the promise of greater security to organizations. These characteristics can be fingerprint, face, voice, or a person's gait. Biometrics is likely to be the vital component of next-generation security systems providing greater reliability and accountability. Biometrics can be used to secure facilities, workstations, cellular phones, smart cards, online transactions, and communication networks. Technological advances in the field of biometrics and its rapid commercialization are enabling its adoption among a wide array of public and private sector organizations. Biometric technologies are experiencing high growth, with revenues likely to increase from $2.7 billion in 2007 to $7.1 billion by 2012.

This report aims to present decision makers in government and public sector organizations with a comprehensive understanding of technological, organizational, and end-user issues in adopting biometric systems; and provides best practice recommendations based on the experiences of organizations that have implemented them.

Many government organizations have already implemented biometric systems because of the derived benefits such as gaining better control of access to physical and digital facilities, managing personnel identity, enabling self-service, and fostering greater trust in e-government interactions. Some recent examples of biometric applications in government use are:

- Oklahoma City's health care management access control systems
- The federal government's Personal Identity Verification (PIV) cards for employees
- Iowa Department of Transportation to deter driver's license fraud
- Defense Department's Defense Manpower Data Center to authenticate military retirees overseas
- New York State's Social Services Department to prevent benefits fraud
- U.S. Transportation Security Administration (TSA)
- U.S. Department of Agriculture (USDA)
- California public schools

In addition, law enforcement and border control are now considering adopting biometric technologies.

The private sector is also exploring the use of biometrics. One private sector problem is what is called “buddy punching,” which is when an employee punches a timecard for another person. McDonald’s fast-food chain implemented biometrics to manage employee fraud due to buddy punching, reducing their payroll costs by 22 percent annually. Taylor Farm, a processing plant for bagging produce, was incurring 20 percent of payroll cost due to buddy punching. Taylor Farm replaced time clocks with fingerprint biometric devices to reduce fraud and high costs and was able to achieve positive return on investment within three months.

An organization evaluating the best strategy for strengthening its security systems to protect physical and digital assets and to reduce fraud needs to assess several key business factors carefully before making the decision to adopt biometrics:

- Level of security needed versus cost of potential losses due to unauthorized access and fraud
- Costs including maintenance and training, and time to receive a positive return on investment
- Integration with existing information systems and security mechanisms
- Employee attitudes and perceptions toward the new technology
- Impact on partners and other external stakeholders
- Scalability of technology as organization grows or makes the transition to e-business
- Availability of industry standards
- Costs and benefits of implementing biometric technology versus alternate technologies

It is important to note that biometric technology adoption and implementation without an integrated security infrastructure based on internal control systems and sound management policies would be inadequate. Typically, implementations of any new information system have a high failure rate. Implementation of biometric systems is a complex and costly endeavor and susceptible to failure without careful considerations. Some best practices to consider during biometric adoption and implementation are provided below.

Best Practices Related to Organizations

Organizations need to:

- Make sure that they are not using biometrics for technology’s sake but rather to solve a problem that the organization is facing.
- Have the full support and involvement of senior management, as that is likely to result in successful implementations.
- Consider carefully the added benefits of integrating a biometric system with other business systems such as payroll.
- Plan for a lengthy initial biometric enrollment process.
- Recognize that biometric systems may in fact require more processing time than traditional methods of authentication, such as passwords or smart cards.
- Plan for post-implementation support.

Best Practices Related to End Users

In order to ensure user acceptance, organizations need to:

- Assuage employee fears about biometrics by making extensive efforts to communicate with employees and educating them about the need for the technology and implementation issues.
- Inform employees about the scope of the use of biometric data collected to allay any privacy fears.
- Inform employees about the technology and the process to generate greater trust and employee buy-in. This is most effective when done by people whom employees already trust.
- Create a responsive feedback loop for employees and end users to report and fix problems associated with biometric system rollout.
- Allow for users who may be unable to present the specific biometric used by the system.

- Plan for user training in biometric enrollment and subsequent use.
- Have a process in place to ensure that enrollment takes place in a manner that does not inconvenience employees or slow down ongoing operations within the organization.

Best Practices Related to Technology Integration

To minimize technology risks, organizations need to:

- Ensure that biometrics is integrated with overall organizational security measures.
- Plan to implement biometrics initially on a small scale.
- Make sure that biometric devices in the field would be capable of operating in stand-alone mode.
- Minimize the amount of sensitive information about employees that is stored at any time in biometric devices operational in the field to protect personal biometric data against theft.
- Ensure that the biometric data capture process does not take significant amounts of time.
- Plan for biometric devices that may require special enclosure or environmental conditions to work effectively.
- Find the right balance of processing speed and accuracy trade-offs when selecting a biometric for an application.
- Make sure that the biometric selected is compliant with available industry standards to ensure interoperability and improve scalability.

Introduction: Understanding Biometrics

Biometrics such as fingerprints and handprints have been in use since ancient times. The first modern systematic use of fingerprint verification appears to have been used in India during the mid-19th century. Azizul Haque developed indexing fingerprints for Edward Henry, the inspector general of police in India. Colonial officials used this technique to stop impersonation of pensioners who had died and to prevent rich criminals from paying poor people to serve their jail sentences for them. Later in the 1900s, fingerprints passed into mainstream police use. In the 1970s, electronic readers were developed, which led to the emerging biometric technologies in use today.

In today's global economy, organizations and consumers are increasingly concerned about ensuring that entities they do transactions with are legitimate entities that can be trusted. Over the last few decades, various identity management tools to verify the identity of a legitimate user have evolved. In most organizations today, access is usually granted through the use of a personal identification number (PIN), identification (ID) card, or token at any entry point. Identity and time management systems authenticate or verify a legitimate user when the user presents at least one of the following identity authentication means to the system:

- User name, password, or PIN number—something that a user knows
- Key, token, ID card, or IP address—something that a user possesses
- Biometric behavioral or physiological characteristic such as a fingerprint, iris pattern, or voice pattern—something that is a unique part of who a user is

The problem with the first two methods is that they are inconvenient for the user (users forget passwords and ID cards), susceptible to fraud (an employee punches a timecard for an absent colleague, known as "buddy punching"), and are vulnerable to security threats (passwords or ID cards can be easily stolen or spoofed).

Using Biometrics for Identity Authentication and Identification

Among the identity authentication means discussed above, the third category deals with the concept of biometrics. Biometrics uses unique body traits or unique individual behavior as the means of identity verification.

Biometrics refers to the process of automatically recognizing a living person using his or her distinguishing, measurable traits. Biometric systems identify the person rather than what the person has (like ID cards) or what they remember (like passwords). The term *biometrics* refers to the statistical analysis of biological phenomena and measurements and has been widely used to describe technologies used for personal identity management.

Biometric systems are divided into two main categories, physiological and behavioral, based on the way the system evaluates characteristics of a living person. A physiological characteristic is a relatively stable physical feature that varies little over time, such as a fingerprint, hand structure, hand veins, retina vascular pattern, DNA, body odor, iris pattern, or other facial feature. In contrast, a behavioral characteristic reflects a person's psychological state, such as voice, signature, lip motion, gait, keystroke patterns, etc., and can be affected by influences like stress or fatigue.

Biometric systems can be used as a stand-alone system or integrated with other security technologies such as smart cards, encryption keys, and digital signatures to operate in either authentication or identification mode. Typically, most biometric systems are used for either authentication or identification purposes.

Biometric Matching Processes

Authentication or Verification

This is the process of identifying a person using *one-to-one* (1:1) matching with their stored biometric template and validating that the claimed identity belongs to the user. Authentication answers the question, “Is this person who she says she is?” This process is used in applications for authorizing legitimate users access to secure facilities, for managing time attendance, and for verifying users during financial transactions to reduce fraud.

The authentication or verification process involves a legitimate user first enrolling in the biometric system to provide her biometric template for later use. Authentication is accomplished by a user presenting a live biometric match for verification and providing some identification, such as an employee ID. This ID is used to retrieve her stored biometric template from the database, and is matched against the live biometric sample presented. The authentication or verification process results in an “accept” (for a genuine user) or a “reject” (for an impostor) decision (see Figure 1).

Biometric templates used for authentication can be stored in a central database or distributed databases such as a passport or smart card that can be carried by the user. Users have more control over their biometric template in distributed template storage than in the centrally stored templates.

Identification or Recognition

This is the *one-to-many* (1:many) matching process that establishes an unknown person’s identity by searching the database for a match. This process is used in a variety of government programs, such as identifying a criminal, checking backgrounds of people applying for citizenship, and maintaining voter registration systems. The identification process results in establishing the identity of the user, that is, answering the question, “Who is this person?” The identification or recognition process results in establishing an identity for the user or results in user identity not being found in the database (see Figure 2).

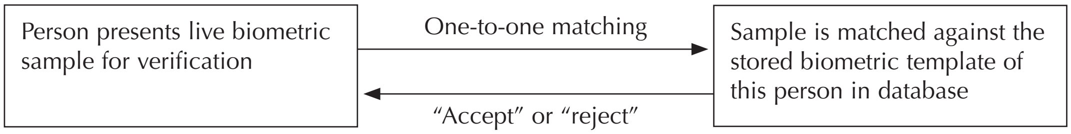
Watch Lists

Another type of biometric, a combination of the above two, is becoming popular for watch list tasks, which use the *one-to-few* (two to 10,000) matching process. Examples of such watch lists are to determine if a person checking in at the airport is on a terrorist list or if a person entering a bank is a known criminal. In these applications, individuals may not be aware that their biometric has been captured and submitted to the system for an identification and verification match.

Biometric Enrollment Process

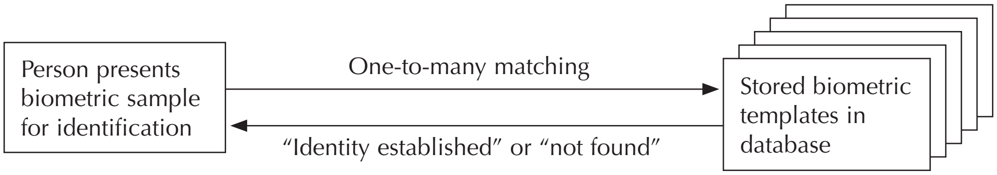
The biometric enrollment process is used to authenticate users in a biometric-enabled security system using one-to-one matching. *Enrollment* is the process in which each new user registers by providing biometric data for storage, retrieval, and matching (see Figure 3). A new user, the enrollee, provides sample readings of biometric information such as a fingerprint, hand scan, or retinal scan. Data is extracted from this sample to produce a biometric template of the enrollee by processing the biometric images through a mathematical algorithm. Because this process cannot be reversed to recreate the biometric image from the template, it is considered secure. Once the biometric template is produced, it is encrypted and stored on the desktop, in biometric

Figure 1: One-to-One Authentication Process


Person presents live biometric sample for verification
One-to-one matching
Sample is matched against the stored biometric template of this person in database
“Accept” or “reject”

Source: *Adapted from Blackburn, 2004.*

Figure 2: One-to-Many Identification Process


Person presents biometric sample for identification
One-to-many matching
"Identity established" or "not found"
Stored biometric templates in database

Source: *Adapted from Blackburn, 2004.*

reader devices, or in a central database or distributed environment for the network-based systems.

After the enrollment process is complete, a user would present her biometric characteristic to the biometric system for verification. The system would process this characteristic to compare it with the biometric template stored. If there is a match, it implies that the user is authenticated; that is, the person is who she says she is. Otherwise, no match would imply that the person may be an impostor and thus would be denied access.

The enrollment process and the resulting template quality are critical in obtaining good results during the authentication/verification process. Biometric data collected from a user during the enrollment process is considered *personally identifiable information* (PII).

Types of Biometric Systems

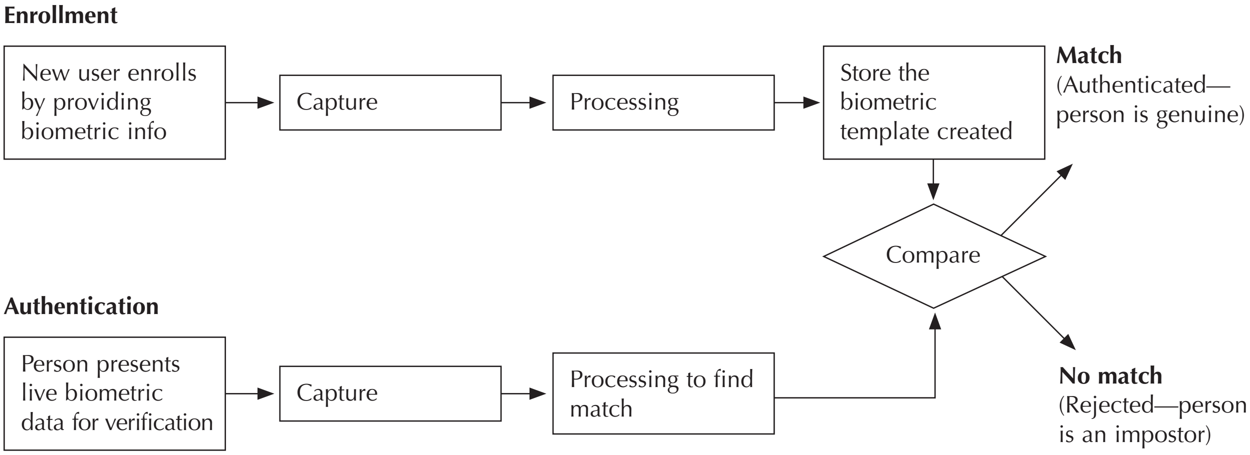
There are two main categories of biometric systems, namely, physiological and behavioral, that are used in biometric systems for authentication purposes (see Table 1 on page 12).

Physiological Biometric Systems

Fingerprint Verification

Fingerprint verification is the most popular and one of the oldest biometrics. Three main patterns make fingerprints unique: the loop, whorl, and arc. In verifying a fingerprint, many systems look at *minutiae*—the friction ridges location on a fingerprint where a friction skin ridge begins, terminates, or splits into two or more ridges. Position and orientation of these friction ridges are used as the basic attributes to describe a minutiae that cover the fingertips. The minutiae template is a list of specific characteristic data processed from a fingerprint image. Minutiae templates are more specific than general large patterns such as loops and whorls that appear on the fingerprints. A fingerprint biometric system will go further than just identifying other features such as crossovers, deltas, and pores (see Figure 4 on page 12), but it will characterize them based on the spatial frequency, orientation, curvature, etc. A positive ID will generally result if 10 to 16 of these patterns match to the print. For criminal cases, positive identification requires a minimum of 12 minutiae points matching. Fingerprint biometric readers can store more than 40 minutiae points.

Figure 3: Biometric Enrollment and Authentication Process


Enrollment
New user enrolls by providing biometric info
Capture
Processing
Store the biometric template created
Match (Authenticated—person is genuine)
Compare
Authentication
Person presents live biometric data for verification
Capture
Processing to find match
No match (Rejected—person is an impostor)

Source: *Adapted from Podio, 2001.*

Table 1: Biometric System Categories

Biometric Categories	Characteristics	Features Used for Authentication
Physiological	Unique physical features of a user that remain relatively stable over user's lifetime	Fingerprint, iris, retina, face, hand geometry, body odor, DNA, ear geometry, facial thermography
Behavioral	Reflects a user's unique psychological states	Voice, signature, gait, keystroke dynamics

Minutiae templates are preferred over the use of images for fingerprint matching because:

- Fingerprint images require more memory for storage, which can be a burden for applications that store data in a limited-size memory chip on a card.
- Larger fingerprint image data size also requires larger bandwidths and increased transmission times.
- Fingerprint images require additional processing time for repeated image compression and decompression, minutiae extraction, and other processing functions required for minutiae matching.

Hand-Geometry Verification

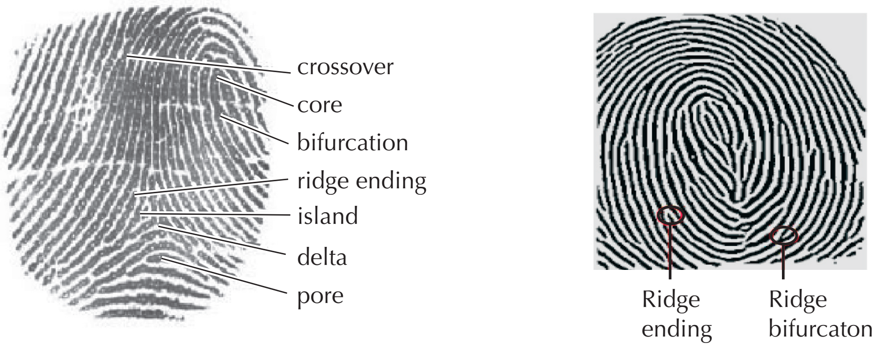
Hand geometry has been in use since the early 1970s. Dimensions of the hand such as finger length, width, and area are the major features used for analyses (see Figure 5). There are several advantages to using the three-dimensional shape of a person's hand with an identification device. First, it is reasonably fast. It takes less than two seconds to scan a hand and produce the analysis results. Second, it requires little data storage space. Third, little effort is required from the user during the verification process, and, fourth, legitimate users are rarely rejected in contrast to fingerprint biometrics, which has a very high rate of rejecting legitimate users.

Iris Recognition

Iris recognition is among the most reliable and accurate biometric technology. Every human iris is measurably unique. Iris scanning views the iris patterns around the pupil ("trabecular meshwork"), which is visible to humans. This is an elastic structure of fibers, which changes position as the pupil dilates (see Figure 6).

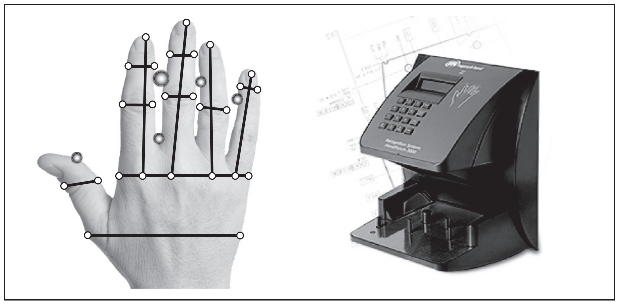
This pattern is unique even for identical twins and for two eyes of a single individual. This pattern also appears to be stable throughout the life. Iris scanners focus on the iris pattern and scan different features found on the surface of the eye such as rings, freckles, furrows, pits, etc. A 360-degree scan is performed on the retina, taking many different readings. These data are then converted into a reference point template. Iris technology has the lowest error rates among various biometrics.

Figure 4: Fingerprint Characteristics and Minutiae



Source: *Biometrics Foundation Documents, 2008.*

Figure 5: Hand Characteristics and Hand Geometry Reader



Source: *Adapted from (Left) Biometrics Foundation Documents, 2008. (Right) http://recognitionsystems.ingersollrand.com/products/.*

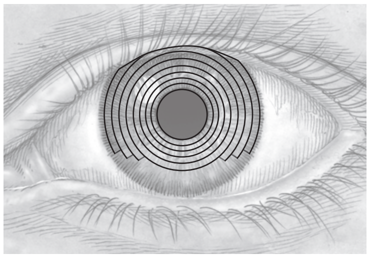
Retinal Recognition

Retinal scanners scan the inner side of the eye, which is invisible to humans. A charge-coupled device (CCD) camera scans the retinal pattern using a weak infrared light aimed through the pupil to the back of the eye. The retinal pattern is then reflected back to the camera, which scans the pattern. These data are then converted into a reference point template. This system is among the best biometric systems currently, with a low legitimate-user reject rate (false rejection rates) and virtually zero impostor pass rates (false acceptance rate).

Facial Recognition

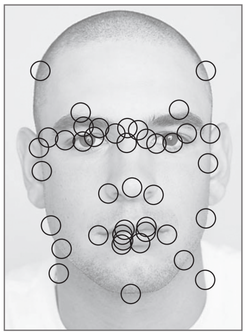
While recognizing people by their facial features is the oldest identification mechanism of all, automating this process has been technologically challenging. Facial recognition is designed primarily to find close matches of particular facial features such as eyes, nose, mouth, cheekbones, chin, and forehead (see Figure 7) against a database of static facial images.

Figure 6: Human Iris Patterns



Source: *Adapted from Biometrics big brother, 2004.*

Figure 7: Facial Features



Source: *Adapted from Who Goes There, 2004.*

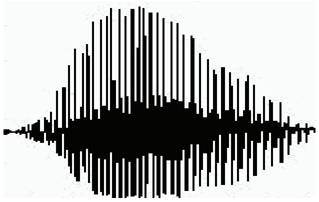
However, this technology has not proven to be reliable for one-to-one verification, due to its high legitimate-user rejection rate (20 percent), even with ideal lighting, distance, and angles. In addition, small changes in a user's appearance, including glasses, facial hair, or aging, can reduce accuracy even further.

Behavioral Biometric Systems

Voice Verification

One of the least invasive of the biometric recognition systems is to use the voice of the user to identify her uniquely (see Figure 8). All the systems that analyze voice are rooted in speech-processing technology. Most of the current systems require the user to enroll by speaking a set of sentences for creating a template. The waveform of the sentences is measured using Fourier analysis to find the frequency spectrum that characterizes the voice sample. Since people form their speech patterns through a combination of physiological and behavioral factors, imitation is virtually impossible.

Figure 8: Speech Frequency Spectrum



Source: *Biometric Measures, 2005.*

Iowa is among many states—others include Massachusetts, Oregon, Texas, Alabama, Colorado, and Kansas—using the facial-recognition-based biometric identification solution to deter driver's license fraud and identity theft. To ensure that only one license is issued to a driver, the Iowa Department of Transportation has implemented both the "one-to-one" and "one-to-many" facial recognition process.

Source: *Iowa Joins Growing, 2006.*

As voice verification relies on distinctive characteristics derived from spoken phrases, it needs as little background noise as possible to be accurate, so the technology is not well suited for use in organizations such as hospitals that are likely to be noisy. Other key factors that affect accuracy include changes in a person's speech habits due to illness, stress, or strong emotions.

Voice verification systems come in two forms. Text-dependent voice verification systems require the user to speak prepared text for verification and are considered more efficient. Text-independent voice verification systems do not rely on any specific sequence of words to verify a user's voice. These provide more flexibility, but are also more vulnerable to security threats such as spoofing.

Signature Verification

Signature verification is a measurement of how a person signs his name. There are two types of signature identification methods. One method examines the signature already written and compares it, as an image, with the signature template. The major drawback of this method is that it does not detect photocopied signatures. The other method is by the study of signature dynamics. This scheme looks at the dynamic process of making a signature—writing rhythm, contacts on the surface, total time, turning points, loops, slopes, velocity and, acceleration.

Figure 9: Signature Recognition

Source: *Biometric Measures, 2005.*

Educational institutions are using fingerprint biometrics to stop non-students from sneaking into institution premises such as dining halls and gyms. An elementary school in Rome, Georgia, has implemented fingerprint readers for students to pay for meals, avoid congestion in lunch lines, and prevent non-students from using dining hall services.

Source: *Bluestein, 2006.*

It is more likely to be used in situations that already require signature capture or those that adopt new writing practices such as pen-based computing on PDAs or tablet PCs. The main issue for signature-based applications is the need for consistency on the user's part since signatures can change over time, which creates a high legitimate-user rejection rate.

Error Rates in Biometrics

High error rates of biometric devices are one of the main challenges in the adoption of biometric technologies. The reliability of biometrics becomes a paramount issue. If not reliable, it can impede employees' ability to perform their work effectively and efficiently. This affects productivity and costs for the organization.

Biometric devices can make two kinds of errors: the false accept error and the false reject error.

- When a biometric system incorrectly rejects a legitimate user, it is called a *false reject* or *false negative* or *Type I error*. Some biometric systems have a higher false rejection rate (FRR) than others.
- When a biometric system incorrectly matches a stored biometric template with an unauthorized person or impostor, it is called a *false positive* or *false accept rate* (FAR) or *Type II error*.

A biometric application with a high FAR indicates that it would incorrectly grant a larger number of impostors access, while a low FAR implies that it would grant access to very few impostors. Usually there is a trade-off between these two errors that can affect accuracy levels, processing speeds in the verification process, and total costs (see Table 2).

Table 2: Accuracy vs. Processing Speed Trade-Offs in Biometric Systems

		Probability of Incorrectly Rejecting a Legitimate User (FRR)	
		Low FRR	**High FRR**
Probability of Incorrectly Accepting an Impostor (FAR)	**Low FAR**	High accuracy in accepting legitimate users and rejecting impostors. However, slower processing speeds and higher costs of system.	High accuracy in keeping out unauthorized users, but also slower speeds due to high numbers of legitimate users rejected by system.
	High FAR	Faster processing times as fewer legitimate users are rejected. But low accuracy since higher numbers of impostors (unauthorized users) are accepted by biometric system.	High processing speeds, but with very low accuracy in verifying legitimate users and rejecting impostors. However, biometric systems with high FRR and high FAR errors have much lower costs.

Different types of biometrics have widely differing false legitimate-user reject rates and false impostor acceptance rates. Most current biometric systems have a false legitimate-user rejection rate of 0.1 percent (a legitimate user will be rejected once out of 1,000 times on average) to 20 percent (a legitimate user will be rejected once out of five times on average).

False impostor acceptance rates of biometrics range from allowing one false authentication in 100 to one false authentication in 10 million on average.

Since each biometric application involves a trade-off between FAR and FRR, which biometric is deployed becomes a function of the security needs and cost. Ideally, a biometric system should have an extremely low FAR and extremely low FRR, but that would result in high costs for the system. Therefore, specific application requirements must be considered for a cost-effective biometric application. Table 3 provides a quick summary of these requirements with accuracy versus speed trades-offs.

Table 3: Accuracy and Processing Speed Requirements in Various Biometric Applications

Applications Using Biometric System	Speed vs. Accuracy	FAR/FRR Thresholds
Forensic applications to identify a criminal in one-to-many (1:many) match. *Example:* Law enforcement agencies, federal Registered Traveler program using multi-biometric of two fingerprints achieves FAR of 0.01 percent (i.e., one impostor falsely accepted for every 10,000 users).	High speed and higher accuracy in finding a match are a priority, even if more false positive matches are made	Low FRR/ higher FAR thresholds
Applications with high security as well high processing speed requirements. *Example:* Secure facilities such as power or nuclear plants, federal agencies.	High accuracy in keeping out unauthorized persons desired with high processing speed	Low FAR/low FRR thresholds
Applications with low costs of unauthorized access. *Example:* Libraries, authenticating online test-takers, universities.	High processing speed is a priority with trade-off of more impostors being accepted.	Very high FAR/lower FRR thresholds
Applications with high costs of unauthorized access. *Example:* Airline pilots.	Not allowing unauthorized persons access is a priority with trade-off of slower processing speed	Very low FAR/ much higher FRR thresholds

Applications of Physiological and Behavioral Biometrics

Biometrics is a rapidly evolving technology. Recent advancements in biometric sensors and matching algorithms have led to the deployment of biometric authentication in a large number of civilian applications, such as ATMs, grocery stores, airport kiosks, and driver's licenses, to prevent unauthorized access. It has been widely used in applications ranging from managing time attendance of field workers in agriculture fields to forensics applications by the Federal Bureau of Investigation for criminal identification. Fingerprint biometrics is used for log-in purposes in about 10 percent of laptops sold in the United States in 2006.

Biometric technology is used during transactions conducted via telephone and Internet (electronic commerce and electronic banking). In automobiles, biometrics can replace keys for providing secure key-less entry and key-less ignition. Due to increased security threats, many countries have started using biometrics for border control and national ID cards. Various types of biometric technologies and their applications are summarized in Table 4.

Multi-trait biometric systems are used to overcome some of the problems with single-trait or unimodal systems. Multi-trait biometric systems are essentially a combination of more than one biometric trait. The FBI's Automated Fingerprint Identification System (AFIS) uses 10 fingerprints for each individual. The US-VISIT program is also expected to move to 10 fingerprints and be integrated with AFIS system. Table 5 on page 18 provides a comparison between single-trait biometric systems and solutions using multi-biometric systems.

While multi-trait biometric systems ensure better security and accuracy by overcoming the limitations of single-trait biometrics, they are also more expensive and technically complex. Multi-trait biometric systems use various levels of information consolidation that often involve trade-offs between performance, feasibility, and costs.

Biometric System Applications in Government

Biometrics can be a viable solution to problems in verifying personal identities while protecting privacy and ensuring security. Table 6 on page 19 highlights some examples of the government's use of biometric systems. Since governments worldwide emphasize establishing the positive identity of persons in high-security areas to prevent unauthorized access, such measures are accelerating the global adoption of various biometric technologies. Sales of biometric technologies should experience rapid growth during the next six years, increasing from $1.95 billion in 2006 to an estimated $7.1 billion by 2012 (see Figure 10 on page 19). This represents significant market opportunities in many application areas such as physical access control, citizen identity, network security, financial services, and health care.

The main drivers of this growth are likely to be the public sector, comprising federal departments, law enforcement, the military, and transport and aviation markets.

Table 4: Types of Physiological and Behavioral Biometric Applications

Biometric Technology	Description	Applications
Fingerprint	Matches the minutiae, pattern, ultra-sonic or moiré fringe imprint; most common of all devices; works well in controlled environment, reliable, and cost-efficient; non-intrusive.	Most widely used in industry for a range of applications; used in biometric mouse, PDAs, and other similar devices to secure desktop and mobile computers; used for authentication in distributed networks, transportation, financial, and gaming industry; in homes for door locks, garage openers; in schools for lunch programs and library access.
Hand geometry	Uses dimensions of the hand such as finger length and width for analyses; suitable for large databases; non-intrusive.	Used at airports, legislative buildings in foreign countries, nuclear facilities, farms, day care centers, hospitals and research labs, prisons and immigration facilities, universities, fast-food retailers like McDonald's for time and attendance tracking and reporting.
Iris scan	Scans iris of the eye and digitizes a pattern for matching purposes; works well in verification mode.	Used in ATM machines; used to enable single sign-on in distributed networks; used in workforce management, immigration control, correctional facilities, airport access control, and child identification programs.
Retina scan	A digital image of the retina of the eye is created by looking at the pattern of light reflected off the retina; scanning done by a low-intensity light via an optical coupler.	Used to enable single sign-on in distributed networks; high-security and national-security applications.
Facial scan	Evaluates the shadow pattern on the face when illuminated in a specific way or takes multiple measurements at particular points around the eyes and cheekbones; operates in controlled capture (user presents biometric to facial scanner) or in random capture mode (user may be unaware of the biometric sample being collected); non-intrusive.	Used at several airports and other public locations such as casinos; banks; controlled facial scan capture is suitable for online applications such as e-commerce; random capture most suitable for law enforcement applications.
Voice scan	A behavioral technology, it uses speech-processing technology to recognize the speaker; also called speaker or voice recognition biometrics.	Used in surveillance applications; state and municipal governments; banking; e-commerce applications; vehicles for enabling ignition systems upon verification.
Signature scan	A behavioral technology, it measures writing rhythm, contacts on the surface, total time, turning points, loops, slopes, velocity, and acceleration.	A crude, non-automated version used in retailers' point-of-sale systems; also used to secure PDA devices.

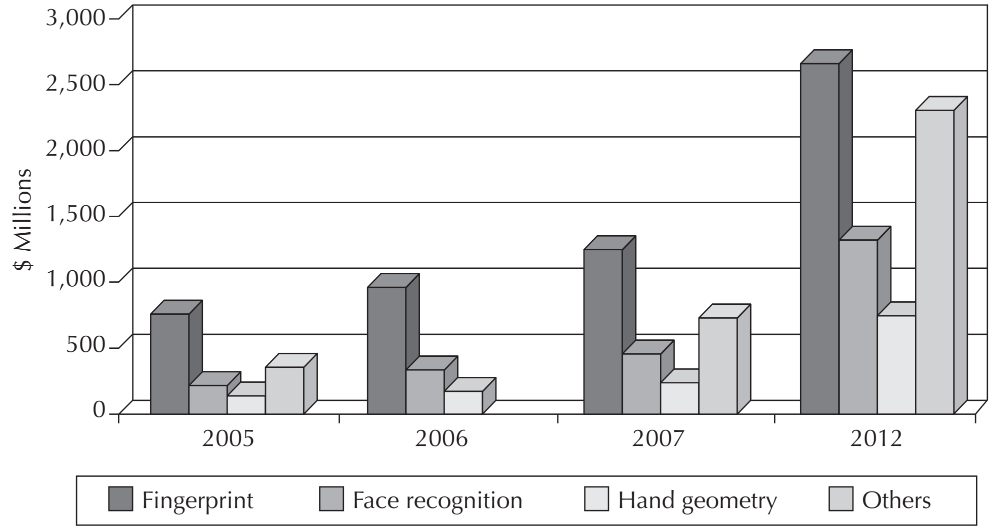
Table 5: Comparison of Single-Trait and Multi-Trait Biometric Systems

Single-Trait Biometric Limitations	What It Means	Using Multi-Trait Biometric Systems
Noisy input	Biometric system can be very sensitive to noise inputs (such as dirt, improper lighting condition, background noise) during verification process, resulting in high legitimate-user rejects.	May reduce noise sensitivity using multiple traits, some of which are less sensitive to noise.
Intra-class variations	Changes or modifications in biometric sensors used by a user to provide live data for verification may affect the matching of this data to the biometric template already stored in the database due to sensor interoperability problems.	Error probabilities in such situations are reduced with the use of multiple-trait biometrics.
Distinctiveness vs. scalability	Each biometric feature has an upper limit to how much it can discriminate among variability across individuals, and this may limit how scalable a biometric system would be as the number of users increases.	Use of multiple biometric traits increases variability distinctiveness thresholds and thus provides higher scalability.
Non-universality	For a biometric system to be operational, each user must be able to enroll successfully using the biometric trait to create her biometric template. However, some individuals may not possess the trait used to create the biometric template. For example, individuals with a speech disability may not be able to participate in biometric systems that rely only on voice scans.	Multiple traits may provide sufficient coverage points for all individuals. For example, using facial or fingerprint traits along with voice scans would increase participation.
Spoof attacks	Biometric systems, especially those that use behavioral traits, may be circumvented by an impostor to spoof the biometric trait of a legitimate user.	It is technologically much more difficult to spoof concurrently multiple biometric traits of a legitimate user.
Accuracy	Single-trait biometric systems may not be very reliable due to the trade-off between FRR and FAR error rates.	Using multiple traits lowers the error probabilities.
Cost and scalability	Single-trait biometrics that are highly accurate are also more expensive and, for the most part, less scalable.	Combining two or more biometrics that are individually less expensive may yield higher accuracy levels at lower cost and provide better scalability.

Table 6: Examples of Biometric Systems in Government

Application	Organization	Application Description
FBI's Integrated Automated Fingerprint Identification System (IAFIS)	Federal government program	Used by law enforcement agencies to identify criminals from submitted fingerprint biometrics within a 2-to-24-hour time frame.[1]
Personal Identity Verification (PIV) program	Federal program initiated by President Bush in August 2004 by issuing the Homeland Security Presidential Directive (HSPD-12) for each federal employee. To be completed by October 2008.[2]	HSPD-12 is designed to use interoperable fingerprint and facial scan-based ID cards to "enhance security, increase government efficiency, reduce identity fraud, and protect personal privacy" for all federal employees (Bush, 2004, paragraph 1).
REAL ID Law of 2005, H.R. 418	States must meet certain minimum federal ID security standards for driver's licenses and other personal state identification cards, which would be required for any federal purposes such as boarding a commercial airplane.	As per the final rule released by the Department of Homeland Security on Jan. 11, 2008, REAL ID requires name, birth date, gender, ID number, a digital photograph, address, and a "common machine-readable technology" that has yet to be finalized. The latter could be a biometric (fingerprint or retinal scan).[3]
Registered Traveler (RT) Solution—Fast Lane Option (FLO) Alliance at Huntsville International Airport initiated by Transportation Security Administration	The FLO Alliance for Registered Traveler, initially formed in 2005, brings together industry leaders in technology, finance, facilities infrastructure, security systems, consumers, and the aviation industry.	RT program is designed to allow individuals who voluntarily undergo an in-depth background check, provide biometric information (such as a fingerprint or iris scan) for enrollment, and pay an annual fee to take advantage of expedited security screening procedures at participating U.S. airports.
Transportation Worker Identification Credential (TWIC)	A federal program for specific communities like the Transportation Security Administration.	TWIC has been established to design and implement standardized issuance of fingerprint biometric security cards for unescorted physical or logical (i.e., web) access to secured areas of the nation's various modes of the transportation system, including air, rail, maritime, and mass transit.

Figure 10: Global Biometric Market Projections by Technology, 2005–2012



Source: *Dalal, 2007.*

Business Case for Biometric Systems

Biometric technology offers a more secure automated method to authenticate identity. A biometric system authenticates the user by measuring something unique to that user. Overall, use of biometrics enhances user convenience by ensuring that users no longer have to remember various passwords to gain access to premises, computers, and other sensitive information in an organization. However, this also presents challenges that must be solved for successful adoption of a biometric system for a particular application in a controlled and/or remote environment.

System designers must address many challenges and issues, both technical and managerial, in order for biometric-enabled security mechanisms to reduce risks. Biometric systems need to be integrated with other internal security mechanisms and control measures for effective implementation and timely return on investment. Biometric systems are expensive, and require substantial financial and management commitment. Addressing technical, user, and system constraints inherent to biometric technology is critical in making a convincing business case for adopting biometric technology.

Each biometric system varies widely according to the specifics of the technology used. Therefore, each biometric system needs to be carefully evaluated across business criteria of cost, accuracy, speed, security, and scalability to make sure that it would fit well within a particular organizational environment and serve the purpose (see Table 7 on pages 21–22). The main issues surrounding the use of biometrics are as follows:

- Accuracy in enrollment process
- Accuracy in verification or identification
- Speed of authentication or identification in real time for large biometric databases
- Securing the biometric systems
- Scalability of system as number of users increases
- Integration with existing legacy systems
- Consistency with standards-based application strategy and need for interoperability

Evaluating Biometric Technology Standards Availability

Since 9/11, the need for better security by government has spurred advances in biometric technology. It has led to the quest for a single standard for the interoperability of various security systems. Currently, U.S. and international data-interchange format standards exist for fingerprint, face, iris, signature, hand geometry, and vascular (vein) technologies. However, except for fingerprint biometrics, standards for most other biometrics are for raw or partially processed data, as there is yet no agreement on a single standard format at the biometric template level.

Standards related to biometric sample quality are still in their infancy, which also creates interconnectivity problems between biometric systems and existing legacy security applications. Recent implementations such as the Fast Lane Option (FLO) Solution under the Registered Traveler (RT) program by the Transportation Security Agency (TSA) require interoperability across different systems in different locations. This initiative led to the FLO Alliance between companies to address the standards and interoperability issues. Thus, travelers enrolled in the

Table 7: Evaluating Each Biometric by Business Criteria

Biometric	Strengths	Weaknesses
Fingerprint	• Good accuracy • Low impostor acceptance • Low cost • Small device size • Ease of use and integration • Non-intrusive • High scalability • High efficiency • Suitable for online transactions • Easy to maintain	• Reliability is low with large databases due to susceptibility to noisy input such as a fingerprint with a scar or dirt on the fingerprint sensor. This increases the probability that a legitimate user will be rejected (high FRR). • Lack of single standard in matching algorithms used • Estimated that 1 out of 20 adults are unable to use a fingerprint-based system for various reasons such as fingerprint degradation due to aging[4] • Some users resistant to idea of being fingerprinted, perceiving it akin to being policed
Hand geometry	• Easy to use • High accuracy is possible • Flexible performance tuning and configuration • High compatibility • Reasonably fast • Authorized users are rarely rejected • Can be used in very cold and rough environments such as construction sites • Non-intrusive • Cost savings and fraud reduction in time-attendance applications • Better suited to one-to-one verification applications	• Technology still in infancy • No single standard • Hand scanners usually bulkier than other biometric trait scanners • Low scalability • Require higher maintenance • Considered easier to spoof by an impostor since many people (less than 1 in 100) have similar hand geometry[5] • Hand size changes over a lifetime • Large data storage requirements
Retina scan	• High accuracy • Retinas alter little over a lifetime, thus yielding a stable database of high integrity	• Intrusive • Difficult to use • Problems with glasses, contacts • Costly • Technology still very new and evolving

(continued on next page)

Fast Lane Option Solution can use their RT cards using a fingerprint or iris scan at airports nationwide that have implemented the RT program.

The U.S. National Institute for Standards and Technology (NIST) has defined the Common Biometric Exchange File Format (CBEFF) to promote interoperability among biometric applications that are technology- and vendor-neutral. Other organizations such as the International Organization for Standardization (ISO), International Electrotechnical Commission Joint Technical Committee (IEC JTC) on Information Technology, InterNational Committee for Information Technology Standards (INCITS), and Organization for the Advancement of Structured Information Standards (OASIS) are creating standards for biometric interfaces, performance testing, and reporting cards for personal identification, as well as standards for securing them.

Thus, organizations should be designing biometric systems with standards-compliant products to improve interoperability. Standards-compliant biometrics also tend to be lower in cost. However, the

Table 7: Evaluating Each Biometric by Business Criteria *(continued)*

Biometric	Strengths	Weaknesses
Iris scan	• Less intrusive than retina scan • Higher matching performance • Works well with eyeglasses • Considered most accurate among all single-trait biometric applications, with reported FAR of one impostor per 1.2 million • Irises alter little over a lifetime, thus yielding a stable database of high integrity	• Intrusive • Difficult to use and integrate with other systems • Costly • Technology still very new and evolving
Facial scan	• Fairly accurate • Non-intrusive • Low cost • Easy to use • Easy to integrate with existing applications such as traffic management and public buildings that already deploy video surveillance infrastructure • Can be deployed unobtrusively (random capture) so that the user does not have to actively participate in presenting the biometric sample	• Not proven to be reliable for one-to-one verification • High legitimate-user rejection (10%) and impostor acceptance (1%) • Sensitive to small changes in user's appearance, age, lighting, angle, etc., reduces accuracy even further • Technology still in the maturing process • Unobtrusive nature raises serious privacy issues • Limited scalability
Voice scan	• Non-intrusive • Convenient for users • Useful for remote identity verification such as banking over phone • Fairly accurate	• Not well suited to populated areas such as hospitals • Variability of transducers and local acoustics • Complicated enrollment procedure • High legitimate-user rejection (10–20%) and high impostor acceptance (2–5%) • Considered easier to spoof by an impostor • Not suitable for 1:many recognition applications
Signature scan	• Fairly accurate	• Age effect changes the sign pattern • Not as accurate as other biometrics • Enrollment challenging • Does not detect photocopied signatures • Not suitable for 1:many recognition applications

reality is that while standards do exist for a few individual biometrics such as fingerprint, a single standard for most biometrics is still years away, and interoperability among different biometric scanners and readers by different vendors will continue to be an issue. Therefore, system designers need to assess an organization's biometric system needs accordingly and plan to build their biometric infrastructure in such a way that migration to a standards-based system in the future would be easy.

Evaluating Security Threats and Vulnerabilities

Most biometrics provide higher security than traditional security mechanisms but are still vulnerable to threats of spoofing, hacking, theft, tampering, legitimate template substitution, and so on. For example, fingerprint biometrics could be fooled by use of false prints, fake fingers, or the use of pattern recognition techniques such as "hill climbing attack." A criminal could forcibly get a live biometric sample from an authorized user.

Biometric technology is rapidly evolving to respond to such security threats. Commercial fingerprint sensors with improved security read a fingerprint with living tissue below the skin layer, thus reducing spoofing threats. This also enables legitimate users who may have scarred fingerprints to use fingerprint biometric technology for authentication.

One of the solutions that has been gaining support is a multiple-layer security approach to reduce these vulnerabilities. Encrypting stored biometric templates and using multi-biometrics combined with passwords or digital signatures can prevent hacking and spoofing.

Strong internal security management measures in the organization as well as network security measures such as firewalls reduce vulnerability. It is important to note that to be most effective, biometrics, whether uni- or multi-modal, should be only one component of the overall security measures, with backups and live human supervision.

Contactless biometric authentication is being used in communities such as maritime industry workers who need access to sensitive areas like ships and docks, yet may not remember their password required for contact authentication. In such communities, cost of access denial is high. For example, if workers forget their passwords routinely, it may result in significant delays in unloading a ship, which in turn leads to significant losses for the industry. Therefore, an authentication solution that does not rely on employees remembering their password is preferable, although it raises privacy issues if an employee's biometric data is siphoned off during contactless transmission by hackers.

In contactless biometrics using a radio frequency identification (RFID) chip, there are risks of "skimming" or "eavesdropping." This refers to the threat that an unauthorized electronic reader could surreptitiously read the biometric data while the ID holder is unaware. Encrypting data during contactless transmission could minimize such incidents. Recently, the U.S. backed away from issuing e-passports using RFID chips for this reason—until secure solutions to such eavesdropping threats are in place.

Contactless Biometrics Authentication Process

Contactless biometrics authentication applications are on the rise, so it is important to understand the process involved:

1. User presents his card to a contactless biometrics reader.

2. User presents his finger to the biometrics scanner for live sample.

3. Host (e.g., a server) establishes a secure session with user's card.

4. Host prepares an encrypted template of the live sample containing the fingerprint and transmits it via contactless interface to user's card.

5. The card decrypts the live sample received from host and compares it with the reference biometrics stored on the card.

6. The card returns signed result (i.e., yes/no) to the host.

Currently, the infrastructure for assuring the security and integrity of biometric enrollment processes, particularly in distributed network environments, is still not fully evolved. Before implementing biometric systems, organizations must ensure that there is a secure infrastructure to support the enrollment process. Also, expansion of the current infrastructure to business partners and customers may present major issues and challenges.

Evaluating User Acceptance

User acceptance remains a sensitive issue in biometric implementation. Many biometric security devices can be intimidating to first-time users, and people are generally uncomfortable with physically intrusive technologies. For example, most people are uneasy with the idea of having a laser-like light directed at their eye every time they need access to their place of work using iris or retina biometrics. Some users have health concerns about the transmission of infections by touching biometric sensors—for example, fingerprint or hand-geometry sensors—which may have been touched by countless other people.

For broader acceptance, biometric techniques must be physically safe, convenient to use, and as non-intrusive as possible. Most users consider biometrics such as DNA, fingerprints, and iris and retina scans more intrusive than voice and signature dynamic. Regions that have low literacy rates may not be suitable for adopting dynamic signature verification as a means of identity authentication. Also, users need to be aware of any health or privacy risks, whether real or perceived, associated with the use of biometrics. User resistance to change is another concern for the biometric system adoption. Employees may worry that even if enrollment in a biometric system in an organization is deemed voluntary, there may be repercussions to declining to enroll.

In order to use biometric devices to enhance security and identity management, provisions for adequate user awareness and training programs are crucial. Users also should have a real choice in participating in biometric systems and in the type of biometrics they choose to use.

Evaluating Implementation Cost

The advantage of integrating biometric systems with other functions within an organization such as payroll and human resources is that it enhances reporting capabilities with better data mining. An example is the agribusiness industry in California, which was able to compare data collected using biometrics to older pre-biometric system data. As a result, companies were able to identify employees who had been violating time-management union rules (taking long lunch breaks or too many breaks) and implement control measures. This integration of a biometric system with other information system applications resulted in significant payroll cost savings and improved employee morale.

Despite the high performance of biometric applications, high cost has made them a rather expensive alternative to other automated security solutions. With increasing commercialization of these technologies and increased competition, the prices of biometric devices are declining. However, not every organization can afford such an advanced security system or needs one.

Adoption and implementation of biometrics must be based on evaluating security needs, conducting cost/benefit analysis including costs of unauthorized access, and considering other cost factors such as operation and maintenance costs. For example, the use of iris scans may be more appropriate for national security applications than for authenticating users in retail financial transactions.

Other costs include the costs of incorrectly accepting impostors or rejecting legitimate users, error trade-offs versus accuracy, the costs of failure-to-enroll rates, and the costs of scaling up the system from few users to large numbers while maintaining accuracy and processing speeds. Another cost for organizations is the cost of integrating the biometric system with existing legacy systems.

Evaluating Privacy Issues

Organizations need to ensure that users have a positive attitude toward adopting biometric technologies; otherwise, they may face serious legal and ethical challenges. Biometric technologies raise difficult privacy questions with respect to surveillance[6] and personal data protection. The privacy of an individual, as advanced by Warren and Brandeis (1890), is the right of an individual to protect personal details from publication, whether obtained lawfully or unlawfully.

Individuals may have consented to provide their biometric data for a specific organization's use, and for a specific purpose only. However, users face the risk that these data may be used for other purposes without their consent or knowledge, leading to "function creep."[7] Biometric data using a facial scan, fingerprints, or DNA of an individual are especially vulnerable to secondary use including surveillance and profiling without the knowledge or consent of the user, raising transparency issues.

For example, an employee may be concerned that a fingerprint template created during the enrollment process for her employer may be shared with a different agency without her permission for a criminal background check. Another concern could be that a biometric collected for legitimate use by

Table 8: Biometric Privacy Concerns

Type of Recognition		Search Type	User Participation	Privacy Concern
Identification	Who is this person?	1:many	**Informed consent** (voluntary, with knowledge) **or Covert** (involuntary, without knowledge)	High
Verification	Is this person who she says she is?	1:1	**Informed consent** (voluntary, with knowledge)	Low

the organization may be used to extract medical information for health insurance purposes without the individual's permission. See Table 8 for privacy concerns associated with biometrics.[8]

Even though many countries recognize the value of privacy protection, privacy standards are still fragmentary and not ratified by world governments. Individual countries have adopted various strategies for achieving meaningful information privacy safeguards, but these are restricted in scope and difficult to enforce.

The security of biometric data is a critical issue, both legally and ethically, for organizations that collect and store this information. Many privacy- and data-protection-related organizations are promoting the use of privacy-enhancing technologies in biometrics to ensure the privacy of information provided by an individual. Organizations that take proactive steps to protect users' privacy concerns are likely to be more successful in their biometric implementations.

Evaluating Cultural and Social Issues

The use of biometrics affects individuals in a society, requiring, for the most part, their active cooperation for enrollment and subsequent use. Since some portion of the general population is likely to be unable to use one or more physiological or behavioral biometrics, it requires sensitivity to ensure that alternate choices are available. Some of the more contentious issues include privacy and the confidentiality of biometric databases, as well as ownership and control of biometric data. With widespread perceptions of biometrics as impinging upon the privacy of individuals, it is crucial to ensure that it is not also viewed as a discriminatory technology.

Biometrics such as DNA and retina and iris scans, which are particularly intrusive in nature, raise additional concerns about physical and health-related effects. Religious and cultural concerns of certain groups or societies may also need to be addressed. For example, individuals in some cultures may be wary of being photographed for facial scans.

The use of biometrics within organizations to manage employee record keeping and time management has led to more positive perceptions of fair and equitable employee management, as an employee can no longer "buddy-punch" for a friend. This reduces fraud and payroll costs. Biometrics also facilitates trust, which is especially helpful for electronic commerce growth and for ensuring both the individual and organization that online fraud is reduced. It is important to remember that biometrics does have the potential for a positive impact on societies by improving convenience (by not having to remember various passwords or to carry multiple identification cards), promoting fairness at the workplace and reducing fraud.

Case Study: Authenticating Federal Employees Using Personal Identity Verification Cards

Homeland Security Presidential Directive 12 (HSPD-12) was issued by President George W. Bush in August 2004, directing government agencies to ensure that only verified and authenticated personnel were able to have physical access to federally controlled government facilities and electronic access to government information systems. The goals: to enhance security and efficiency and reduce identity fraud for all federal employees.

Establishing Criteria for PIV Card Specifications

HSPD-12 mandates the development and implementation of a Personal Identity Verification (PIV) card for each federal employee and contractor that would be secure and reliable and rely on a government-wide standard to ensure interoperability. It requires that each PIV card:

a. "is issued based on sound criteria for verifying an individual employee's identity;

b. is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation;

c. can be rapidly authenticated electronically; and

d. is issued only by providers whose reliability has been established by an official accreditation process."[9]

PIV cards can be authenticated in two ways, contact and contactless authentication, although the latter is optional for agencies. To establish standards for secure and interoperable PIV cards required by HSPD-12, the National Institute of Standards and Technology was tasked with developing Federal Information Processing Standard (FIPS) 201 for granting physical and logical access to federal employees and contractors.[10] FIPS 201 establishes technical acquisition and formatting specifications; procedures for identity proofing, registration, and PIV card issuance and usage; formats for fingerprints and facial images; and cryptographic protection requirements of the biometric data to ensure high-performance and universal interoperability.

Choosing the Right Biometrics

A PIV card uses only two types of biometrics: fingerprint and facial scan. However, the PIV relies primarily on fingerprint biometrics. Digital facial-image scans are used as secondary biometrics in cases where a user is unable to provide a fingerprint during enrollment or authentication. The reasons:

- Technology for facial scans is not yet sophisticated enough to enable its use as a primary biometric in a large-scale application.
- Matching algorithms for most biometrics are still highly proprietary and technology is still nascent.
- Matching algorithms for fingerprints are technologically more viable and most likely to be compliant with FIPS 201 standards of security and interoperability within reasonable cost and effort.

For fingerprint biometrics, a minutiae template rather than fingerprint image was preferred due to the former's much smaller size, thus requiring less bandwidth and transmission time. However, there is not one standard for a minutiae template; fingerprint vendors use their own definitions to describe a minutiae and proprietary algorithms to match the same minutiae. Therefore, NIST conducted extensive research into interoperability standards and tested the performance of various algorithms against these standards to create a compliant list of products that ensure interoperability.

Facial-scan authentication technology is still in its infancy and not reliable for complete automation. Facial scans require an "attended image authentication session," that is, when a user presents a live facial sample to the biometric system for authentication, a person (rather than the automated system) then compares the live user sample with the stored facial-scan template of the user to authenticate it.

If employees need access through a remote session (e.g., using the web) and if fingerprint biometrics is not available, then employees use their PIN since a facial-scan is not possible remotely.

Establishing Technical Standards vs. Maintaining Flexibility

FIPS 201 quantifies only the minimum authentication performance standards using both the false legitimate-user reject rate (FRR) of less than or equal to 1 percent and a fixed false impostor accept rate (FAR) of 1 percent. Beyond these minimums, FIPS 201 is unique in its flexibility for agencies to:

- Establish their own error-rate specifications for field biometric systems since error rates depend on a number of factors such as sensor, number of attempts, number of fingers used, image quality, age of user, the environment, and the familiarity of users with the process.
- Allow use of multiple samples (e.g., two fingers) to substantially improve performance over single-finger authentication.

Establishing Operating Procedures for Assuring Interoperability

NIST developed FIPS 201, which specifies procedures for PIV card issuance and management. These include procedures for capturing fingerprint images using primary and secondary fingers, and formats for generating fingerprint templates stored on the PIV card. FIPS 201 specifications provide the exact procedures for agencies for retaining fingerprint images and for transforming fingerprint images into records suitable for transmission to the FBI for the employee's background check.

Once the FBI approves the federal employee or contractor for PIV card registration, to make sure that the right person is being issued the card a fingerprint template is generated. This template adheres to a specific standardized template that allows use of a PIV card in a multi-vendor product environment and across agencies, thus achieving interoperability. While the PIV card stores both the fingerprint and facial-scan biometrics for each enrolled federal employee or contractor, it primarily uses fingerprint biometrics. Digital facial-image scan is used when it is not possible for a federal employee or contactor to provide fingerprints or if there is an anomaly.

Securing PIV Cards

To secure PIV cards against various security challenges, FIPS 201 requires multiple layers of authentication of the information cryptographically protected on the PIV card:

- Digital certificate validation
- Digitally signed PIN, called a Cardholder Unique Identifier (CHUID)
- One-to-one digitally signed multi-biometrics (fingerprints and facial scan)
- Digitally signed hash table for a unique card ID

These measures make counterfeiting or spoofing of PIV cards very difficult. However, it is possible to spoof fingerprint biometrics using a cut or fake fingers. In the future, facial-scan readers could be developed for large-scale deployment, which might mitigate problems with fingerprint biometrics and make PIV cards a true multi-biometric system.

Establishing a Single Shared Service Provider for Multiple Agencies

The General Services Administration (GSA)[11] is in charge of implementing HSPD-12, which is to be completed by October 2008. GSA is designated as the *shared service provider* for federal agencies. Its role is to manage the contracts; manage all databases; and manage the issuance and management process of PIV cards, IDs, and other credentials. Choosing GSA as the shared service provider to manage the HSPD-12 compliance process for the federal government does the following:

- Makes it easier to maintain data standards and database security since all biometric data storage and maintenance is done by GSA as the service provider.
- Obviates the need for a federal agency to acquire high technical capability, experience, and resources.
- Reduces overall costs of implementation due to economies of scale since cost is spread across several agencies.
- Reduces risks for the agency, as PIV cards are compatible across all federal agencies with cross-agency readers.
- Reduces time to completion.

Currently, about 70 federal agencies use GSA as their shared service provider while 20 federal agencies have opted to store and control their own data. Agencies that had opted out of GSA as their shared service provider find that their cost of implementing HSPD-12 is higher. Most of these 20 agencies are military or international in scope.

Some agencies, such as the Treasury Department, switched back to GSA's shared service provider program after an audit report found that "the IRS was at risk of wasting taxpayer funds because the Treasury was developing its own system for issuing the cards rather than joining other agencies that had already incurred much of the upfront costs associated with this effort."[12] Other agencies, such as TSA's Transportation Worker Identification Credential (TWIC) and the Registered Traveler program, are likely to adopt FIPS 201 and will base their biometric content on the PIV specification.

HSPD-12 biometrics authenticate the employee in a 1:1 matching. This presents two main limitations: scalability and using it to recognize an employee (1:many matching). The proprietary nature of biometric-matching algorithms makes it difficult for an agency that may have adopted a 1:many matching solution to share it with other agencies. In addition, intelligence agencies may have legitimate restrictions on data sharing. Thus, different agencies may choose different proprietary solutions from multiple vendors.

Lessons Learned from the HSPD-12 Case Study

The HSPD-12 implementation case study illustrates the importance of building a strong business case using the following business criteria:

- Establishing clear goals
- Creating architecture and technical requirements using biometric data for a uniform identity credential to access federal facilities and systems
- Providing flexibility to support differing needs of various government agencies
- Choosing the appropriate biometric technology to meet goals
- Instituting organization-wide operating procedures to ensure interoperability
- Providing for evaluation of the controls within a system of record for feedback and continuous improvement
- Ensuring security using a multiple-layer solution approach
- Providing a single point of contact for various federal agencies to provide management and maintenance support of processes

HSPD-12 implementation has helped achieve various milestones in promoting the use of biometrics in government agencies to enhance security and establish common identification standards that were hitherto nonexistent. This initiative required multi-agency collaboration and information sharing at the government level as well as between the private and public sector to meet large-scale national security needs using biometrics solutions that are robust, standards based, scalable, and, most important, interoperable.

HSPD-12 implementation is also influencing the biometrics industry in an immense way as it has spurred business opportunities for companies. This has resulted in greater research and development in software and standards that combine different types of biometric data and make this information interoperable across different systems. This is leading to a trend toward systems that are less proprietary in nature and more standards-based.

Best Practices for Successful Biometric System Adoption and Implementation

Utilized alone or integrated with other technologies such as smart cards, encryption keys, and digital signatures, biometrics is set to pervade nearly all aspects of life. Utilizing biometrics for personal authentication is becoming convenient and considerably more accurate than current methods (such as passwords or PINs). As e-government applications accelerate globally, the use of biometrics will accelerate to enhance citizen trust in e-government services.

Typically, implementations of a new information system have a high failure rate because organizations do not often plan for issues and challenges associated with adopting new technology. Adopting a biometric system is no different. The much-publicized case of facial-recognition technology to scan faces in the crowd on the streets of Tampa, Florida, which was abandoned due to performance and privacy-related concerns, illustrates the challenge of biometric implementations. Based on the various biometric implementations that have taken place in government and industry, there are a number of best practices that can be useful to managers who are considering adopting biometrics as an identity and security management system in their organization.

Best Practices Related to Organizations

While biometrics offers the promise of enhanced security, not all organizations may benefit equally. For some, the cost of adoption and maintenance of these systems, coupled with privacy issues and lack of clear legal precedents, may be too high. An organization may face resistance from its partners; and, in terms of security, biometric implementation may simply make this organization a strong link among many weak links in the value chain.

Organizations need to make sure that they are not using biometrics for technology's sake but rather to solve a problem that the organization is facing. Sometimes there may be a simpler solution to enhancing an organization's security needs. Since biometric systems are generally expensive to adopt and maintain than existing systems, careful analysis based on the level of security required, cost/benefit assessment, risk analysis, organizational culture, legal aspects, in addition to other cost factors such as training, operation, and maintenance costs, is needed. Successful implementations require financial support, planning, and adequate resources.

Organizations that have the full support and involvement of senior management are likely to have successful implementations. Senior management support enables seamless technology integration and makes the implementation process manageable. Senior management can provide that support if there is a sound business case for biometric adoption using return on investment (ROI) analysis, understanding the benefits of adoption, and having a clear time frame for ROIs to be realized.

Organizations need to carefully consider the added benefits of integrating a biometric system with other business systems. For example, a biometric system for employee attendance and time management track data in real time. If this system is integrated with payroll, accounting, and human resource systems, it could lead to more accurate employee management for the organization at lower costs.

Organizations need to plan for a lengthy biometric enrollment process. It is important to recognize that the initial employee enrollment process using biometrics will be long. For fingerprint biometrics, the enrollment process can take anywhere from 30 seconds up to a few minutes per employee. This enrollment time can quickly add up if an organization has hundreds of employees.

Organizations need to recognize that a biometric system may in fact require more processing time than traditional methods of authentication such as passwords or smart cards. This may become a major issue for organizations that employ a large number of part-time, hourly, or contract workers—who will pay for the additional time needed by employees for biometric processing time?

Organizations need to plan for post-implementation support. Biometric technology is new and prone to breakdowns and other implementation problems. Biometric systems require a lot of back-end support without which their implementation would not be successful. This support is not only in terms of actual technology infrastructure but also, and equally important, in terms of support staff that can answer employee questions or solve glitches as they occur.

Best Practices Related to End Users

A user's acceptance of the biometric system is a major factor that can determine whether the implementation is successful or not. Users may be suspicious when it comes to a technology like biometrics that collects very personal data, and may worry that their biometric data may be misused for unstated purposes by organizations. One of the critical factors in technology adoption, addressing user concerns is essential for successful implementation.

Organizations need to assuage employee fears about biometrics. Organizations need to recognize that most employees are not technology savvy and may know little about biometrics. They may mistrust technology and see it as more of an impediment to their job, rather than an enabler. Employees at all levels of the organization may not be ready to embrace biometric systems. Organizations need to have an education process in place that can explain to employees why the biometric system is needed and how it could benefit their jobs.

Organizations should make extensive efforts to inform employees so they understand how their biometric data would be collected, what the data would be used for, which if any health problems may arise, and whether enrollment is voluntary or involuntary. This not only allays employees' privacy fears but also helps engender trust in biometric systems.

Employee buy-in happens if employees are informed about the technology and the process by people they trust. Agribusinesses in California successfully addressed field and plant workers' concerns by getting buy-in from supervisors (who are typically more educated and usually have had a longer tenure with the company) by explaining the need for biometrics, benefits to the employees and organization, and privacy aspects of biometric data. Supervisors then educated their crew about the need for technology and safeguards in place to protect their privacy. In this case, the crew trusted their supervisors, with whom they worked every day. If the CEO or senior management had tried to educate workers about biometric use, it would not have been as effective.

Creating a responsive feedback loop for employees and end users to report problems associated with the biometric system rollout is important for continued end-user support. Since biometrics is a relatively new technology, initial implementations usually have problems. Implementation of a fingerprint biometric system in an agribusiness organization in California was initially slow. This created clock-in problems for employees, who had to wait in long lines to start their shift and thus were concerned about losing pay through no fault of their own. Feedback from employees about these problems led the organization to get faster processing devices. This was important for the success of the biometric system in the long run as employees felt that their feedback about system usage was valued, and this in turn reinforced system usage and refinement.

Biometric systems should allow for users who may be unable to present the specific biometric used by the system. In field implementations of fingerprint biometrics, agribusiness organizations use fingerprint biometrics with all five fingers to allow for a number of field workers who either have some fingers with poor quality fingerprints or are missing some fingers. Organizations use an "any two fingerprints" match for authentication to solve this problem. Even though this is more expensive than using a single fingerprint biometric device, multi-fingerprint reader devices allow organizations to keep authentication speeds high to prevent long lines during the start of shifts.

Organizations need to plan for user training in biometric enrollment and subsequent use. Training enables users to feel more confident in their decision to accept a new technology. Employees need to understand any precautions they need to take when using biometrics. For example, training may help employees remember to remove gloves or wipe any dirt off their hands when using fingerprint readers or hand-geometry biometric readers; or to remove eyeglasses if they are using retina biometrics. This would minimize authentication problems such as legitimate users being rejected by the system, and speed up overall processing time.

Organizations need to have a process in place to ensure enrollment does not inconvenience employees or slow down ongoing operations. This is especially true for organizations that have seasonal workers and purge all biometric data at the end of the season, starting the enrollment process over again the next work season.

Best Practices Related to Technology Integration

Since the biometrics industry is still evolving and there are no common standards to ensure interoperability, organizations need to consider strategies to minimize their technology risks when adopting biometrics.

Organizations must take all appropriate technical and organizational security measures to protect personal biometric data. As noted in an earlier section (see Table 7 on pages 21–22), there are a number of ways that biometric data may be vulnerable to accidental or unlawful destruction, accidental loss, alteration, or unauthorized disclosure or access. Organizations need to secure data during storage, biometric template extraction, and transmission to central servers for authentication.

Organizations should plan initially on implementing biometrics on a small scale. Research suggests that organizations should strive for implementing biometrics as a smaller pilot program initially and then expand it throughout the organization. This would help in containing any implementation problems as well as provide important lessons for larger-scale execution. This implies that organizations need to plan for a period of time when older time management and security systems overlap with new biometric systems.

Biometric devices in the field should be capable of operating in stand-alone mode. This becomes critical when there are network breakdowns or power outages. Biometric devices with such capability would continue to operate even if these get disconnected from the network, and thus the authentication process can continue without interruption. Since this capability adds to the cost of the system, organizations need to understand the costs of productivity loss if biometric devices cannot operate during such conditions.

Organizations should minimize the amount of sensitive information about employees that is stored at any time in biometric devices operational in the field. Newer biometric devices are available with an in-built memory and operating system so that it can store data as it operates while disconnected from the network. However, this also raises privacy issues if these devices are stolen. A hacker could gain access to all sensitive data about employees, such as Social Security information, that is stored within the device's memory. This happened in Yuma, California, where someone walked away with six fingerprint devices in use at a farm that had sensitive data about employees.

Organizations need to ensure that the biometric data capture process does not take a significant amount of time. During the period of data capture by the biometric devices and data transfer to the central server for authentication, the device is essentially unable to perform any authentication. This effectively lengthens the time needed for each authentication. This can be a significant problem for organizations when there is a rush for authentication during certain times of day—for example, in the morning or at the end of lunch hour—and thus the need for faster authentication processing. Again, cost becomes the issue; the lower the cost of the biometric device, the longer the time may be needed for data capture. Therefore, organizations need to assess the frequency and consistency of data capture needs throughout the workday and balance it against cost.

Biometric devices may require special enclosure or environmental conditions to work effectively. In agribusiness, some biometric devices that were put in produce processing plants did not work when the temperature got too low; the devices got frosted. These devices are now placed in special enclosures to prevent such problems, but this adds to the initial cost estimates of biometric system implementation.

Organizations need to find the right balance of processing speed and accuracy trade-offs when selecting a biometric for an application. Some biometrics, while providing fast processing speeds, may have error rates that can create serious problems for people (see Tables 2 and 3 on page 15). For example, terrorist watch list applications rely on matching biometrics (such as facial scans) of everyone passing through a biometric scanner (in voluntary or involuntary mode) to a known terrorist in the database using one-to-many recognition. The recognition process has to be fast enough in real time and accurate in terms of making sure that a terrorist would be correctly identified by the system. However, this may involve a trade-off with a higher error rate of false positives, that is, incorrectly identifying an innocent person as a terrorist. This can have distressing social, legal, and ethical consequences for an agency if a high number of innocent people are wrongly identified as terrorists.

Organizations must make sure that the biometric selected is compliant with available industry standards to ensure interoperability and improve scalability. Designing biometric systems that are standards-compliant improves interoperability issues; in addition, they are cheaper to implement. However, as most biometrics do not yet have a single industry standard, organizations need to be mindful of creating an infrastructure and set of processes that can be readily adapted to evolving standards.

Conclusions

Government agencies are increasingly focused on protecting their physical and digital assets and protecting citizens' privacy while improving delivery and acceptance of government services, both online and offline. Currently, most access control systems for personnel identification and authentication rely on PINs, cards, passwords, or tokens. However, besides being inconvenient to the user, these solutions are easily circumvented and vulnerable to security threats and fraud.

Biometric systems offer a greater level of security for organizations. Biometric technologies can enable greater consumer trust in online transactions, thus reducing fraud and risk to buyers and sellers. However, biometric technologies are still relatively more expensive compared to existing identity and security management solutions. Organizations need to construct a business case for biometrics based on the level of security required, cost/benefit assessment, risk analysis including legal risks, and the organizational culture. When organizations are considering adopting biometrics, a process for obtaining end-user support and ensuring ease of use must be an organization-wide priority. This will lead to fewer aggravations during initial implementation and result in higher accuracy levels. Additionally, a biometrics adoption plan based on senior management support, user training, data privacy measures, and post-implementation support is likely to be successful.

Currently, a major challenge in the adoption of biometrics is the lack of a single standard across different biometrics and open standards development. Organizations need to recognize that while establishing standards are vital for ensuring interoperability among agencies, differences in operating procedures within each agency may still render interoperability objectively ineffective. Incompatibility and interoperability become even more of an issue if each organization has unique customization needs.

As biometrics adoption and use continues to grow, government agencies will play an important role in all of the following:

- Developing, testing, and adopting biometric technical standards
- Promoting investment in research and development
- Forging partnerships with the public to advance biometric technologies by demystifying biometrics
- Engaging in public debate on how and when biometric technologies should be used
- Taking the lead in setting legal and ethical guidelines for biometric data collection, storage, and use to ensure higher standards of privacy

Endnotes

1. The National Biometrics Challenge (2006) at http://www.biometrics.gov/NSTC/pubs/biochallengedoc.pdf.
2. From conversations with David Temoshok, Director of Identity Policy and Management, during January 2008.
3. http://www.news.com/FAQ-How-Real-ID-will-affect-you/2100-1028_3-5697111.html?tag=st.nl, accessed on Jan. 12, 2008.
4. http://www.gizmag.com/go/2998/, accessed on Jan. 26, 2008.
5. http://www.engr.sjsu.edu/biometrics/publications_tech.html, accessed on Jan. 17, 2008.
6. Surveillance is defined as using biometric data to answer "who is where?"
7. http://www.biometricscatalog.org/NSTCDocuments/OECD%20Biometrics%20privacy%20Jun%202004-2-4.pdf, p. 12, accessed on Feb. 8, 2008.
8. http://www.nationalbiometric.org/news/USFederalPrivacyReport0306.pdf, accessed on Feb. 8, 2008.
9. http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html, accessed on March 27, 2008.
10. http://csrc.nist.gov/groups/SNS/piv/index.html, accessed on Jan. 8, 2008.
11. The General Services Administration (GSA) Office of Governmentwide Policy provides policy and information on identity management to the federal government on issuance of ID credentials of physical and logical access for individual authentication.
12. http://www.treas.gov/tigta/auditreports/2008reports/200820030fr.pdf, accessed on Jan. 12, 2008.

References

Agnvall, E. (2007). Biometrics Clock In. *HR Magazine,* 52, 4, 103–105.

Alterman, A. (2003). A piece of yourself: Ethical issues in biometric identification. *Ethics and Information Technology,* 5, 3, 139–150.

Alvarez, L. (2008). President and CEO of Alvarez Technologies Group, Inc., Salinas, CA. Personal conversation on Feb. 19, 2008.

Anderson, R. (2001). *Security Engineering.* New York: Wiley Computer Publishing, 261–275.

Barton, B., S. Byciuk, C. Harris, D. Schumack, and K. Webster. (2005). The emerging cyber risks of biometrics. *Risk Management,* 52, 10, 26–31.

Bill, Z. (1997). Biometric shift: Integration, computer access affect uses. *Security,* 34, 45–46.

Biometric Measures. (2005). Undated. Retrieved May 2, 2005, from http://www.ece.uah.edu/biometric/biometric_measures.htm.

Biometrics, big brother and the global police state (2004). Retrieved Feb. 2, 2008, from http://www.infowars.com/archives/2004/Apr/04-13-04.htm.

Biometrics Foundation Documents (2008). National Science and Technology Council (NSTC), Committee on Technology, Committee on Homeland and National Security, Subcommittee on Biometrics Report, undated. Retrieved on Jan. 30, 2008 from http://www.biometrics.gov/Documents/biofoundationdocs.pdf.

Blackburn, D. M. (2004). Biometrics 101–version 3.1. Federal Bureau of Investigation Report. Retrieved Jan. 8, 2008, from http://www.biometricscatalog.org/biometrics/biometrics_101.pdf.

Bluestein, G. (2006). Biometric device used to pay for meals, Associated Press Writer, Oct. 25, 2006. Retrieved from Yahoo! Tech News on Oct. 26, 2006.

Bruce, S. (1999). The uses and abuses of biometrics. Association for Computing Machinery. *Communications of the ACM,* 42, 136.

Bush, G. W. (2004). Homeland Security Presidential Directive/HSPD-12. Retrieved on Jan. 10, 2008 from http://csrc.nist.gov/drivers/documents/Presidential-Directive-Hspd-12.html.

Cavoukian, A., and A. Stoianov. (2007). Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy. Retrieved on Dec. 26, 2007 from http://www.ipc.on.ca/images/Resources/up-1bio_encryp.pdf.

Chandra. A., and T. G. Calderon. (2003). Toward a biometric security layer in accounting systems. *Journal of Information Systems,* 17, 51–70.

Chandra. A., and T. G. Calderon. (2005). Challenges and constraints to the diffusion of biometrics in information systems. *Communications of the ACM,* 48, 12, 101–106.

Cooper, D., H. Dang, P. Lee, W. MacGregor, and K. Mehta. (2007). Secure Biometric Match-on-Card Feasibility Report. National Institute of Standards and Technology (NIST) Interagency Report 7452. Retrieved on Jan. 12, 2008 from http://csrc.nist.gov/publications/nistir/ir7452/NISTIR-7452.pdf.

Dalal, N. (2007). The Global Biometrics Market. Report excerpt retrieved on Jan. 8, 2008 from http://www.bccresearch.com/RepTemplate.cfm?reportID=694&RepDet=HLT&cat=ift&target=repdetail.cfm.

Dean, L. S. (2004). Transportation Security Administration (TSA) report on Privacy Impact Assessment of Transportation Worker Identification Credential (TWIC) Prototype. Retrieved on Jan. 12, 2008 from http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_twic.pdf.

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

DeQuendre, N. (2000). An eye for security. *Security Management,* 44, 22.

Dray, J., and D. Corcoran. (2006). Personal Identity Verification Card Management Report. National Institute of Standards and Technology Interagency (NISTIR) 7284 Report. Retrieved on Jan. 12, 2008 from http://csrc.nist.gov/publications/nistir/ir7284/nistir-7284.pdf.

Eugene, S. (2002). Tests of biometric devices show numerous problems. *Computers & Security,* 21, 396.

Franklin, C. (2005). Strong authentication. *Network Computing,* 16, 34.

Freschi, C. (2007). Biometrics Technology Touches the Future. *Security,* 44, 11, 94–95.

Garcia, M. J., M. M. Lee, and T. Tatelman. (2005). Immigration: Analysis of the Major Provisions of H.R. 418, the REAL ID Act of 2005. CRS Report for Congress retrieved on Jan. 12, 2008 from http://w2.eff.org/Activism/realid/analysis.pdf.

Grother, P., M. McCabe, C. Watson, M. Indovina, W. Salamon, P. Flanagan, E. Tabassi, E. Newton, and C. Wilson. (2006). Performance and Interoperability of the INCITS 378 Fingerprint Template. National Institute of Standards and Technology Interagency (NISTIR) 7296 Report. Retrieved on Jan. 12, 2008 from http://fingerprint.nist.gov/minex04/minex_report.pdf.

Harris, J. A., and D. C. Yen. (2002). Biometric authentication: Assuring access to information. *Information Management & Computer Security,* 10, 1, 12–19.

Hope-Tindall, P. (2004). Biometric-Based Technologies. Directorate for Science, Technology and Industry, Committee for Information, Computer and Communications Policy, Organisation for Economic Co-operation and Development (OECD), DSTI/ICCP/REG(2003)2/FINAL report, June 30, 2004. Retrieved on Feb. 8, 2008 from http://www.biometricscatalog.org/NSTCDocuments/OECD%20Biometrics%20privacy%20Jun%202004-2-4.pdf.

Iowa Joins Growing List of States Using Digimarc Biometric Identification (2006). FinancialWire Forest Hills: Nov. 3, 2006.

Jain, A. K., and A. Ross. (2004). Multibiometric systems. *Communications of the ACM,* 47, 1, 34–40.

Keeton, A. (2007). Fingerprints give a hand to security. *Wall Street Journal* (Eastern edition), New York, April 12, 2007, B4.

Kim, H. J. (1995). Biometrics, is it a viable proposition for identity authentication and access control. *Computers and Security,* 14, 3, 205–214.

Kleist, V. F. (2007). Building Technologically Based Online Trust: Can the Biometrics Industry Deliver the Online Trust Silver Bullet? *Information Systems Management,* 24, 4, 319–330.

Kleist, V. F., T. Pearson, and R. Riley. (2005). Evaluating biometrics as internal control solutions to organizational risk. *Journal of American Academy of Business,* 6, 339-343.

Langenderfer, J., and S. Linnhoff. (2005). The Emergence of Biometrics and its Effect on Consumers. *Journal of Consumer Affairs,* 39 (2), 314–338.

Michael, A. G. (2002). Tampa facial recognition a failure, ACLU claims. *Security Management,* 46, 10.

The National Biometrics Challenge (2006). National Science and Technology Council Subcommittee on Biometrics Report dated August 2006. Retrieved on Jan. 12. 2008 from http://www.biometrics.gov/NSTC/pubs/biochallengedoc.pdf.

Phillips, M. R. (2007). Final Audit Report–Lack of Proper IRS Oversight of the Department of the Treasury HSPD-12 Initiative Resulted in Misuse of Federal Government Resources (Audit # 200720034), Reference Number: 2008-20-030. Retrieved on Jan. 12, 2008 from http://www.treas.gov/tigta/auditreports/2008reports/200820030fr.pdf.

Podio, F. (2001). Biometrics—Technologies for Highly Secure Personal Authentication. ITL Bulletin, May 2001, published by the Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST). Retrieved on Jan. 7, 2008 from http://csrc.nist.gov/publications/nistbul/05-01.pdf.

Polk, W. T., D. F. Dodson, and W. E. Burr. (2007). Cryptographic Algorithms and Key Sizes for Personal Identity Verification. National Institute of Standards and Technology (NIST) Special Publication 800-78-1. Retrieved on Jan. 21, 2008 from http://csrc.nist.gov/publications/nistpubs/800-78-1/SP-800-78-1_final2.pdf.

Privacy and Biometrics: Building a Conceptual Framework (2006). National Science and Technology Council (NSTC), Committee on Technology, Committee on Homeland and National Security, and Subcommittee on Biometrics Report dated Sept. 15, 2006. Retrieved on Jan. 30, 2008 from http://www.biometrics.gov/Documents/privacy.pdf.

Purushothaman, M., and B. Gupta. (2005). Use of Biometrics Systems in Organizations. Proceedings of International 3rd Annual CISTM Conference, July 24–26, 2005, New Delhi, India.

Reynolds, P. (2004). The keys to identity. *Health Management Technology,* 25, 12–15.

Richard, H. (1999). An introduction to biometrics and large scale civilian identification. *International Review of Law, Computers & Technology,* 13, 337–363.

Rigelsford, J. (2003). Biometric authentication. *Sensor Review,* 23, 365.

Roberts, B. (2003). Are you ready for biometrics? *HR Magazine,* 48, 95–98.

Roger, C. (1999). Internet privacy concerns confirm the case for intervention. *Communications of the ACM,* 42, 60–67.

Ross, A., S. Prabhakar, and A. K. Jain. (2005). An overview of biometrics. Retrieved on March 7, 2007 from http://biometrics.cse.msu.edu/info.html.

Rowley, W. (2002). Surveillance society and transparent society: New challenges for society, *Spectrum,* 75, 16.

Scott, M., T. Acton, and M. Hughes. (2005). An assessment of biometric identities as a standard for e-government services. *International Journal of Services and Standards,* 1, 3, 271–286.

Temoshok, D. (2008). Director, Identity Policy and Management, Office of Government Policy, General Services Administration. Personal conversation on Jan. 10, 2008.

Tilton, C. J. (2007). Integrating Biometrics. *Appliance Design,* 55, 5, 16–18.

Toigo, J. M. (1990). Security: Biometric creep into business. *Computerworld,* 24, 75.

Trocchia, P. J., and T. L. Ainscough. (2006). Characterizing consumer concerns about identification technology. *International Journal of Retail & Distribution Management,* 34, 8, 609–620.

Warren S., and L. D. Brandeis. (1890). The right to privacy. Retrieved on Nov. 10, 2007 from http://louisville.edu/library/law/brandeis/privacy.html.

Who Goes There? A Facial Recognition Primer. (2004). Retrieved on March 2, 2007 from http://www.wpi.edu/News/Transformations/2002Spring/recognition.html.

Wilson, C., P. Grother, and R. Chandramouli. (2007). Biometric Data Specification for Personal Identity Verification. National Institute of Standards and Technology (NIST) Special Publication 800-76-1. Retrieved on Nov. 15, 2007 from http://csrc.nist.gov/publications/nistpubs/800-76-1/SP800-76-1_012407.pdf.

Zalud, B. (2007). Two 'Faces' of Biometrics. *Security,* 44, 8, 56–58.

Zetter, K. (2005). Feds rethinking RFID Passport. WIRED News. April 26, 2005. Retrieved on Jan. 4, 2008 from http://www.wired.com/politics/security/news/2005/04/67333.

Zorkadis, V., and P. Donos. (2004). On biometrics-based authentication and identification from a privacy-protection perspective: Deriving privacy-enhancing requirements. *Information Management & Computer Security,* 12, 125–137.

ABOUT THE AUTHOR

Babita Gupta is Professor of Information Systems at the School of Business, California State University, Monterey Bay. She teaches courses in electronic commerce marketing, electronic commerce business models and strategies, management information systems, database management, and computer information systems. She serves as the co-director of the E-Lab@CSUMB, an interdisciplinary research and education initiative.

Her research areas include biometrics, online consumer behavior, online security and privacy, e-government, information technology, outsourcing, and knowledge management. She has published in the *Journal of Communications of ACM, Journal of Industrial Management and Data Systems, Journal of Information Technology Cases and Applications, Computing and Information Technology, Journal of Scientific and Industrial Research*, and the Internet Encyclopedia. She is serving as a board member of the California Coastal Rural Development Corporation.

Professor Gupta holds a PhD in management sciences and information technology from the University of Georgia, Athens, an MS in industrial and management engineering from the University of Iowa, Iowa City, and a BE in electrical and electronic engineering from the Birla Institute of Technology and Science, Pilani, India.

KEY CONTACT INFORMATION

To contact the author:

Babita Gupta
Professor of Information Systems
School of Business
California State University, Monterey Bay
100 Campus Center
Seaside, CA 93955
(831) 582-4186
fax: (831) 582-4251

e-mail: babita_gupta@csumb.edu

REPORTS from
The IBM Center for The Business of Government

For a full listing of IBM Center publications,
visit the Center's website at *www.businessofgovernment.org*.

Recent reports available on the website include:

Collaboration: Networks and Partnerships

A Manager's Guide to Resolving Conflicts in Collaborative Networks by Rosemary O'Leary and Lisa Blomgren Bingham

Integrating Service Delivery Across Levels of Government: Case Studies of Canada and Other Countries by Jeffrey Roy and John Langford

Contracting

Success Factors for Implementing Shared Services in Government by Timothy J. Burns and Kathryn G. Yeaton

E-Government/Technology

The Blogging Revolution: Government in the Age of Web 2.0 by David C. Wyld

Best Practices for Implementing Agile Methods: A Guide for Department of Defense Software Developers by Ann L. Fruhling and Alvin E. Tarrell

Leveraging Web 2.0 in Government by Ai-Mei Chang and P. K. Kannan

Human Capital Management

Designing and Implementing Performance-Oriented Payband Systems by James R. Thompson

Seven Steps of Effective Workforce Planning by Ann Cotten

Innovation

Transforming Government Through Collaborative Innovation by Satish Nambisan

Managing for Performance and Results

Engaging Citizens in Measuring and Reporting Community Conditions: A Manager's Guide by Alfred T. Ho

Strategic Use of Analytics in Government by Thomas H. Davenport and Sirkka L. Jarvenpaa

Missions and Programs

Delivery of Benefits in an Emergency: Lessons from Hurricane Katrina by Thomas H. Stanton

Organizational Transformation

Improving Service Delivery in Government with Lean Six Sigma by John Maleyeff

Presidential Transition

Strengthening Homeland Security: Reforming Planning and Resource Allocation by Cindy Williams

The National Security Council: Recommendations for the New President by D. Robert Worley

About the IBM Center for The Business of Government

The IBM Center for The Business of Government connects public management research with practice. Since 1998, we have helped public sector executives improve the effectiveness of government with practical ideas and original thinking. We sponsor independent research by top minds in academe and the nonprofit sector, and we create opportunities for dialogue on a broad range of public management topics.

The Center is one of the ways that IBM seeks to advance knowledge on how to improve public sector effectiveness. The IBM Center focuses on the future of the operation and management of the public sector.

About IBM Global Business Services

With consultants and professional staff in more than 160 countries globally, IBM Global Business Services is the world's largest consulting services organization. IBM Global Business Services provides clients with business process and industry expertise, a deep understanding of technology solutions that address specific industry issues, and the ability to design, build and run those solutions in a way that delivers bottom-line business value. For more information visit www.ibm.com.

For additional information, contact:
Jonathan D. Breul
Executive Director
IBM Center for The Business of Government
1301 K Street, NW
Fourth Floor, West Tower
Washington, DC 20005
(202) 515-4504, fax: (202) 515-4375

e-mail: businessofgovernment@us.ibm.com
website: www.businessofgovernment.org