Practical Application of Biometrics

TechRepublic

Practical Application of Biometrics

By Tom Olzak

Various sources are continually telling us that biometrics solutions are required to maintain compliance; that if we don't implement fingerprint scanning, or something less understood like facial recognition, we are negligent and headed for serious litigation. As with all security controls, there is some truth to these claims. However, what we use and where we use it--or if you use biometrics at all--is fundamentally a business decision.

Running out and purchasing a fingerprint-based authentication system, for example, without an assessment of various business needs and environmental conditions is often worse than no implementation at all. Failed sensor functionality, user frustration, and productivity losses can add up to a failed project, falling back to using passwords alone. It also builds a wall of disinterest between the security team and management that arises on the conference table whenever biometrics is mentioned. Therefore, every biometrics project should begin with an understanding about why biometrics are a useful tool, how they fit into management's vision of the business, and the questions to ask when assessing different approaches to biometrics identity verification.

This document is designed to provide a starting point for your biometrics project. In the following pages, we look at why businesses should consider this technology. We examine the nature of biometrics technology and how it relates to your existing security controls framework. Next, we explore the most successful and the most popular biometrics approaches to user identity verification. Finally, we walk through a small example of how different biometric solutions might be implemented in a single organization, depending on level of security and ease of use requirements.

The Business Case

There are two primary reasons we use biometrics: to increase the strength of authentication processes or to improve the user experience and productivity. If a business case cannot be made to support one of these, then obtaining funding for a biometrics project is not likely.

Strengthening Authentication

Internal and external forces drive the desire to strengthen authentication controls. Internal forces include:

- Management concerns about protecting intellectual property
- Management concerns about protecting financial information or internal communication
- Self-imposed ethical guidelines for protecting customer, investor, and employee information

External forces overlap in some areas. However, they usually exist because not all organizations broaden their view of ethical responsibility to include electronic information. The strongest external requirements for strong authentication are government or industry regulations or guidelines, including:

- Sarbanes-Oxley Act of 2002 (SOX). This Federal law applies to all publicly-traded organizations. Lacking specific guidelines, companies that get a large share of their income from auditing public companies worked with the SEC to create a set of controls and requirements to achieve compliance with Section 404 of the act. Material non-compliance results in a report to the board of directors and possible government sanctions. Most SOX audits, however, are only concerned with the integrity--the accuracy and believability--of financial information.
- The Gramm-Leach-Bliley Act (GLBA). The GLBA, signed into Federal law in 1999, applies

to all organizations that provide financial services. It requires access controls sufficient to prevent unauthorized release of customer personal of financial information.

- The Health Insurance Portability and Accountability Act of 1996 (HIPAA). This Federal law requires covered health care entities to safeguard patient personal and health care information. Further, it mandates that only individuals approved by the patient may have access to information, including health care professionals, family, and friends.
- The Payment Card Industry Data Security Standards (PCI DSS). The PCI DSS is not a government regulation. It was created through the collaborative efforts of all major credit card providers. The intent is to prevent the unauthorized release of customer credit card information. Failure to comply may result in the cancellation of an organization's ability to accept credit cards as payment for products and services.
- Breach Notification Laws. A majority of states now have laws in place that require organizations to take defined steps if a data breach occurs. According to a recent study by the Ponemon Institute and the PGP Corporation, the average cost of a breach in the United States is $204 per customer (Helmer, 2010).

There are other reasons for restricting access to sensitive information. However, these cover reasons why most organization should care about enhanced authentication practices.

Each of the laws and guidelines, whether affected by internal or external forces, have one thing in common; only authorized individuals may have access to certain classes of information. Historically, access controls have taken the form of user IDs and passwords. But passwords often are not enough.

Problems with Passwords

Most security managers are aware of access control problems associated with authentication via passwords, including:

- **Use of weak passwords.** Today's brute force attacks against password files use tools that allow cracking of most, if not all, passwords within a very short period. Given enough time—a few hours at most—supplementing this type of attack with a rainbow table can provide every password based on a word in a dictionary.
- **Use of strong passwords.** Requiring the use of strong passwords can deter attackers from using brute force attacks; it simply takes too long with effort exceeding the value gained. However, users tend to forget complex passwords. So, in the interest of productivity (and stress reduction) they write them down where they can find them. Documenting passwords reduces their protection to the same or lower levels as weak passwords.
- **Password sharing.** No matter how many awareness classes they attend and regardless of the number of policies provided, many users just cannot resist sharing passwords with co-workers. It is not just the business users. I have seen domain administrator account passwords shared by up to 35 people, most of whom did not actually need it. I also investigated an instance in which a database administrator gave his password to his wife so she could log in remotely to check the status of a job he was running. It doesn't matter how strong a password is if everybody knows it.
- **Weak account policies.** Some organizations still do not follow best practice for assigning and managing strong account policies, including:
    - Force a specific password length (length depends on the resources protected);

- o Track password history, denying reuse of a password for several reset cycles;
- o Force a password reset every 30, 60, or 90 days, depending on the account privileges and the data protected;
- o After a password reset, require a user to wait a certain period before resetting the password again—the waiting period should be shorter than the maximum age set above;
- o Lock an account after three to five unsuccessful login attempts; and
- o Ensure all passwords are encrypted in storage.

Passwords are not inherently bad

A reasonable, non-dictionary password is not inherently bad. A quick test is available to determine how long it would take to crack a specific password. Located at How Secure is My Password, it dismisses the possibility that a user would enter a word from the dictionary. Further, it assumes the cracking computer is executing 10 million instructions per second. It is not perfect, but it provides a general idea about how long it might take to crack certain types of passwords.

One outcome of this test is evidence that reasonable and recallable passwords can provide a good level of protection against unauthorized entry--if properly protected from friends, co-workers, and social engineers. This is a very big if…

The cost of passwords

Again, most security professionals understand these challenges at some level. However, this is not the kind of information that makes business managers sit up and say, "Fix it now!"

The use of passwords, like any control, has costs. Senior business managers do not always understand this. They often assume that setting and using passwords is a free service provided by the operating system or third-party directory service. This assumption is wrong.

There are both hard and soft costs associated with password management. According to Identity Magazine (2010) "Gartner estimates that about a third of helpdesk calls are password-related and research firm, Forrester, reckons each of these helpdesk calls costs about $70" (Passwords: the root of all evil?, para. 1). Further, business users can often take several minutes trying to remember a password for the network or application, adding productivity costs to the authentication process.

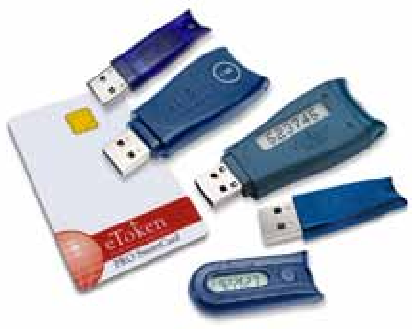
Alternative Solutions

Tossing out passwords is not always a practical way to meet security and cost challenges. Rather, supplementing them with multi-factor authentication (MFA) solutions is often a better choice.

Multi-factor authentication includes using two of the following to verify a user's identity:

- Something the person knows. Passwords and PINs are examples of this.
- Something the person has. **Figure A** depicts a collection of security tokens an organization might issue to its employees, including one-time password devices.
- Something a person is. Fingerprints, voiceprints, vein patterns, and other physical or behavioral characteristics fall into this category.

Figure A



Security Tokens (Safenet-inc.com)

Tokens are a good solution. However, they still suffer from cost and sharing/loss issues. Productivity and management costs arise as employees leave their tokens at home or lose them. Tokens are also shareable and subject to theft. Consequently, they offer additional protection but are subject to the some of the same challenges as passwords.

Biometrics, on the other hand, provides a means to reduce the risk of theft and the cost of forgetting tokens. Biometric solutions are not perfect, but as the rest of this paper demonstrates, they provide cost effective ways to streamline and strengthen identity verification processes.

Biometrics

Biometrics is the use of human physical or behavioral characteristics to verify a person's identity. This is done in one of two ways:

1. **Identification** is the process of collecting a biometric measurement (e.g. a facial scan) from a person and comparing it to a database of previously scanned data. The purpose is to determine who the person is when identity is not known.
2. **Verification** solutions collect a biometric measurement (e.g. a fingerprint) from a person and compare it to a value previously collected from that user and attached to a user account. The purpose is to verify that the users requesting access are who they say they are.

Verification, as a means to strengthen authentication processes, is the topic covered in this paper. In general, identification is used by law enforcement and physical security personnel to identify persons of interest.

Biometric Identity Verification Process

Figure B shows the identity verification process used by most biometric solutions. **Figure C** describes the enrollment process. In this example, Microsoft Active Directory® (AD) serves as the repository for fingerprint template information. Not all biometric solutions work exactly this way. However, this is a good representation of the basic process involved.

Regardless of the type of biometric used, the following components should always be present:

- Sensor for collecting physical or behavioral characteristics
- An algorithm for converting the scanned data into a value, or reference template, for later comparison
- A data store for maintaining reference templates
- An algorithm for comparing trial and reference templates
- A management interface used to enroll users and manage the acceptable level of match probability when comparing a trial template with a reference template

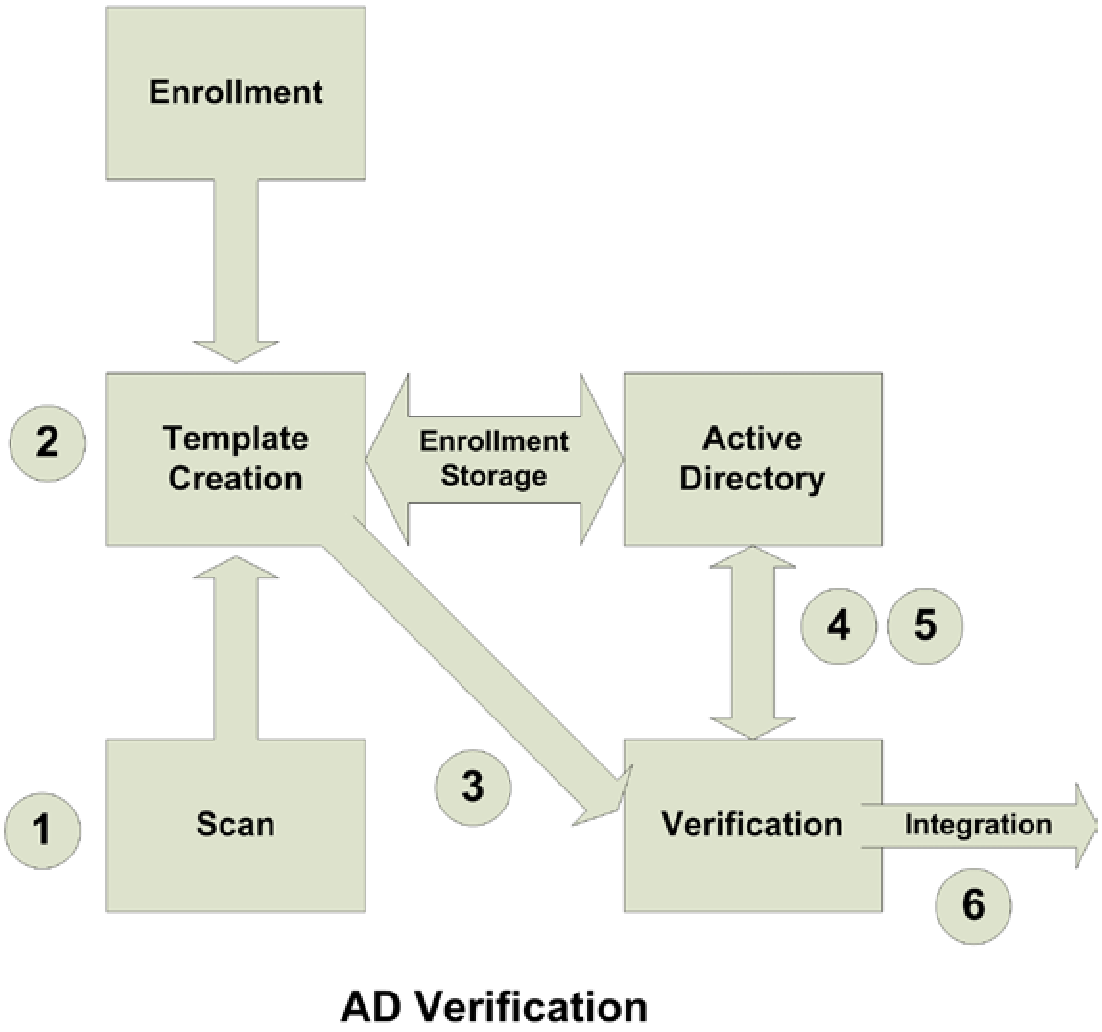
Types of Biometric Solutions

Biometric solutions fall into two general categories: physical and behavioral. Physical biometrics measures and compares characteristics of various body parts to stored information. In this paper, the physical biometrics solutions examined include:

- Fingerprints
- Vein patterns
- Iris patterns
- Voice
- Face

Behavioral biometrics measures how a user performs a task, such as writing or typing. Later in this paper, we examine one example, keystroke dynamics. Keystroke dynamics measures how a person types his or her password.

Figure B: Fingerprint-based Authentication Process

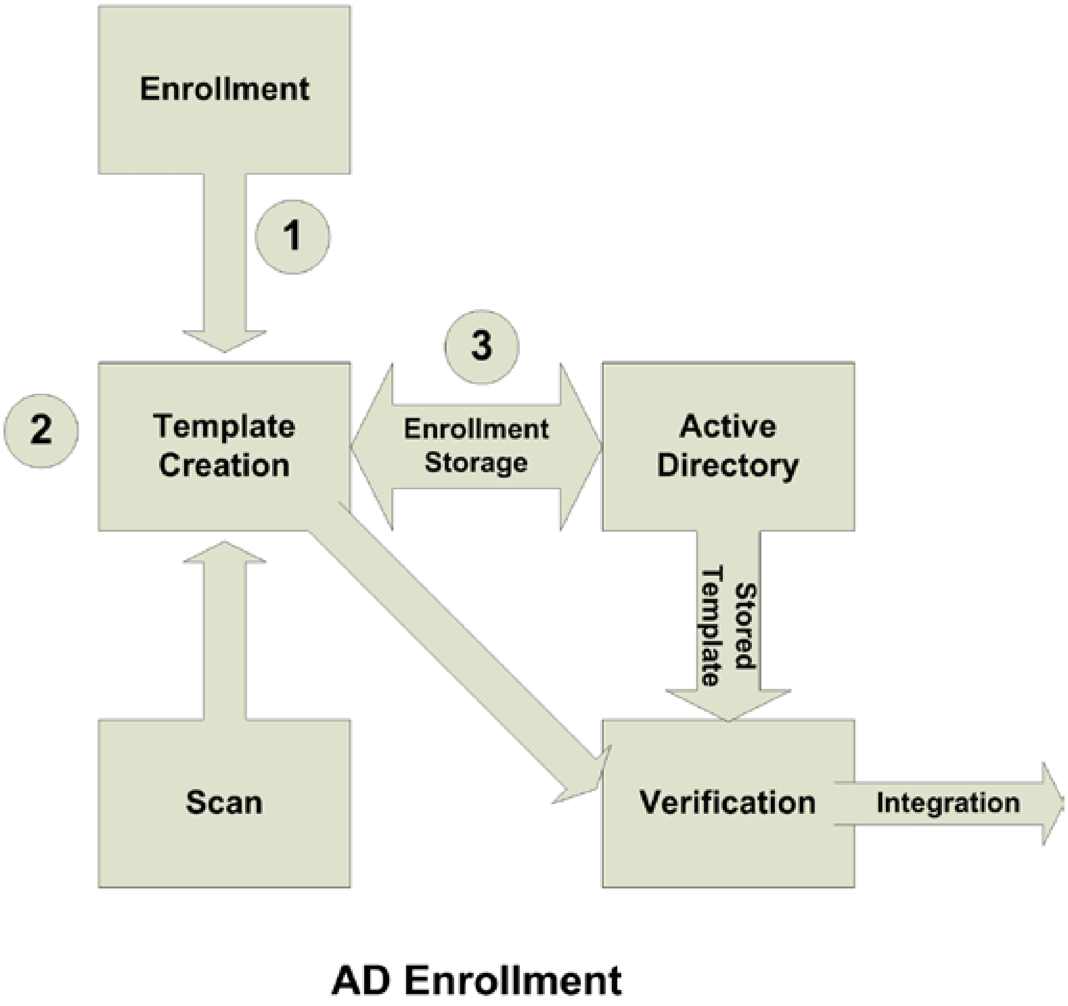


1. *Once employees enroll in the biometric application (shown in Figure C), they begin the authentication process by allowing a scanner to collect the fingerprint used during enrollment. In some cases, users must also enter their user ID. In others, enrollment may also consist of local pairing of the biometric template with user accounts. However it is done, AD needs the account information for template comparison.*
2. *The scanned information is translated by the biometrics software into a trial template.*
3. *The trial template and user ID is sent to the verification algorithm.*
4. *The verification algorithm sends a request to AD for the stored reference template associated with the user ID provided.*
5. *Once the reference template is returned, it is compared with the trial template.*
6. *If the templates match, within a reasonable margin of probability, access is granted to all applications integrated with the sign-on solution used.*

Implementation Challenges

One of the biggest mistakes made by organizations is failing to properly assess various solutions based on a clearly defined set of environmental, business, and solution management requirements. So before getting to specific solutions, it is important to spend some time learning about the potential pitfalls associated with biometrics.

Figure C: Fingerprint Enrollment Process



1. Enrollment begins with an administrator requesting the new employee to scan one or more finger prints into the biometric solution.
2. A reference template is created for each finger scanned.
3. The reference templates are stored in AD with the user ID provided for this user by the administrator.

Not all actions described to mitigate biometrics risk are necessary. However, organizations should always make a conscious and informed decision to either use them or accept the risk.

Forgery

It is not impossible to forge physical or behavioral characteristics, and some approaches to biometrics are easier to fool than others. Two ways to meet this challenge are multi-modal biometrics and interactive authentication.

Multi-modal biometrics uses two or more different characteristics to verify identity. For example, gaining access to a data center might require placing a finger on a fingerprint scanner while facing a facial recognition scanner. This may require implementation of two or more biometric authentication processes.

Interactive authentication is implementation of another factor of authentication, often with no cost above the directory services (e.g. AD) already found in most organizations. According to Microsoft MSDN (2010), "Authentication is interactive when a user is prompted to supply logon information" (para. 1). For example, a user may scan a fingerprint and then enter a PIN or password. Unlike multi-modal approaches, interactive authentication often requires implementation of a single biometric solution integrated into the organization's existing user ID and password process.

Enrollment risks

Enrollment is both a management issue and a security risk. Management expects new hires to complete first-day administrative hurdles and get to work as soon as possible. New employees often have paperwork to complete, training to attend, and orientation. Adding enrollment on top of these activities is not always popular; especially if it is cumbersome, frustrates the user, and results in error-ridden reference templates.

Security risks include errors from poor enrollment processes or questionable application algorithms. Enrollment is a vulnerable period, in which counterfeit reference templates might find their way to the data store. In addition, the administrator might inadvertently create reference templates that generate an unreasonable number of false positives or false negatives. Issues like these affect the integrity of a biometrics authentication solution and may reduce support from management and users.

Organizations should ensure technical access controls extend to the enrollment process. Implementation of least privilege, need-to-know, and segregation of duties concepts are very important. Least privilege to ensure the administrator is allowed to only perform enrollment actions; need-to-know to allow access to see only what is absolutely necessary for enrollment; and segregation of duties to validate that the documented process was followed and logs do not contain evidence of questionable behavior. These controls also help prevent contamination of the reference template data store.

Data store contamination

Data store contamination is the unauthorized modification of reference templates stored for comparison with trial templates. Reference templates are often stored in a directory service database or in general database solutions like Oracle Database® and Microsoft SQL Server®. Consequently, security best practices for highly sensitive information stored in directory services and databases apply.

Unauthorized direct access to data stores is not the only way to contaminate reference templates. Allowing unauthorized access or excessive privileges to the biometrics management applications can also cause data store integrity issues. The controls recommended in the previous section, Enrollment risks, also apply here.

Business continuity

There is a good reason AD solutions usually include more than one domain server. If one fails, users are still able to authenticate and access resources. Implementing an integrated biometrics solution with a single-point-of-failure, however, weakens any existing authentication technology redundancy.

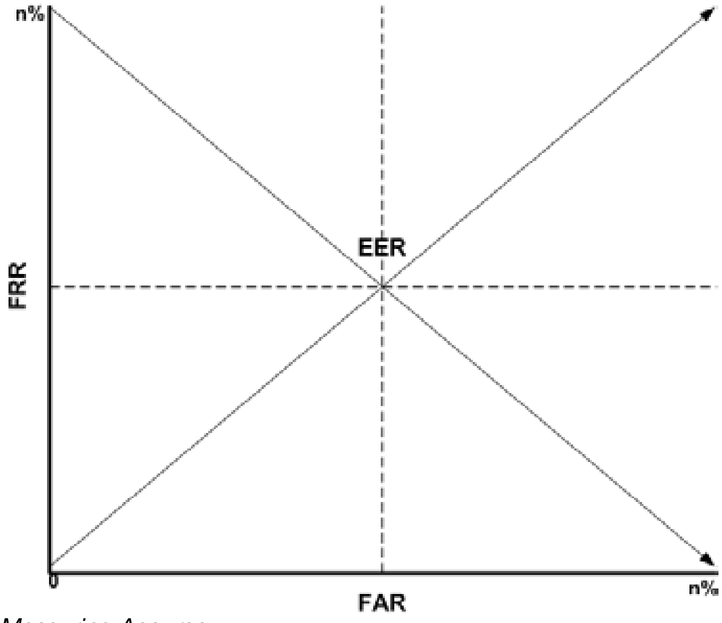
Any biometrics solution should include business continuity risk mitigation. For example, using AD to store reference templates automatically provides redundancy across all domain controllers. In addition, most cost-effective solutions include a client application for reference and trial template creation and comparison. With this type of solution, there is built-in redundancy. If not taking this approach, ensuring redundancy of scanners, software, and template storage supports continued user productivity.

Accuracy

Accuracy of biometrics is described in terms of false acceptance rate (FAR) and false rejection rate (FRR). Both rates are expressed as a percentage. FAR measures the number of unauthorized login attempts that may be approved, while FRR measures the number of authorized login attempts a specific solution might deny. The point at which both rates are equal is the equal error rate (EER), also called the crossover error rate (CER). Enterprise class solutions allow administrator accuracy adjustments necessary to reach a balance between security (FRR) and usability (FAR).

The relationship between FRR and FAR is depicted in **Figure D.** FAR and FRR are inversely related. In other words, when one increases the other decreases and vice versa. As shown in the graphic, a point exists at which both rates are equal, the EER.

Figure D



Measuring Accuracy

Achieving EER during accuracy adjustment is not always the best approach. In some cases, management might accept a higher FRR to achieve a very low FAR. The value of the assets protected might be worth the resulting frustration and productivity hits. This is a risk management decision that applies security control at the level necessary to achieve the level of protection expected.

When selecting a biometrics solution, an organization must clearly understand the related error rates, the EER, and whether they meet pre-established access control requirements. Decision makers should also be aware of how environment affects FAR and FRR.

Environmental Conditions

The quality of the surrounding area in which an organization places a scanner and the nature of the work performed can both have significant effects on error rates. For example, placing a fingerprint sensor on a manufacturing floor can result in high error rates. Contaminants in the air can settle on the sensor or material on employee fingers can result in a high FRR. Adjusting the sensor to reduce FRR results in a higher FAR. Another example is placing a fingerprint sensor at a nursing station. Nurses and aids wear gloves much of the time. How might this affect their ability to use a fingerprint sensor? Selecting the right sensor or scanner requires an understanding of where management wants it and who will use it. These are key considerations for user acceptance.

User acceptance

Lack of user acceptance is one reason biometrics projects fail, either during the project or shortly after. According to Brandel (2010), there are four reasons users may not accept the solution chosen by the organization:

- Users may resist the idea of a large, centralized repository containing information about physical or behavioral characteristics. The number of breaches reported by traditional and online media is enough to make any user question how the organization plans to protect reference templates.

- Cultural norms are also obstacles in some situations. International companies, for example, may find that a type of scanning technology accepted by American employees may not be appropriate for Asian employees.

- Health privacy concerns are another challenge to biometrics acceptance. For example, employees may believe scans of retinas or irises might reveal eye health issues that can be used against them by health insurance companies or by their employer.

- The frustration associated with errors during template comparisons or how long it takes to authenticate (especially when waiting for someone else) can kill a project. Solutions should strengthen access controls with as little impact as possible on user processes.

Casting biometrics into the workplace, hoping that employees accept it willingly, is not a good plan. O'Leary (2008) writes, "User acceptance of the access control device is one of the most critical factors in the success of a biometric-based implementation" (p. 52). Failing to manage change in the workplace may result in a large, wasted expense.

Managing change for biometrics implementation is the same for any planned process or behavior modification expected by management. It requires an understanding of the possible obstacles to change (as listed above) and a plan to mitigate their effects. According to Westover (2010),

> …it is best if the manager can describe the specific impact of the change on his or her area of responsibility and subordinates. Generally, the process is first to define the specific objective that will cause the change, then to describe the results that the change is expected to produce. The manager should then describe the impact that the change will have on the work unit or department (p.49).

Once managers understand the challenges they face, user awareness sessions regarding how the technology works, how it may change how work gets done, how the organization is managing risk, and other steps taken to address employee fears and anxieties, the implementation phase of the project can start.

Selecting the Right Solution

The one-size-fits-all approach seldom provides a cost effective security framework. Because the company down the street successfully rolled out a solution does not mean what the referred vendor representative may want you to believe; that since it worked there, it is guaranteed to work in your organization. Do not believe it without comparing the claims of success to your defined requirements and until after completion of a successful pilot.

Also consider the possibility that you may need different solutions for different access control challenges. Just because you select fingerprint scans for the accounts receivable clerks does not mean it is the right answer for the engineers responsible for product design. Keep an open mind and understand all your options.

There are various approaches to biometrics-based access control. However, the major contenders for today's solutions were listed earlier in this paper. In the following sections, we'll examine each approach as well as some advantages and disadvantages of each.

Fingerprint Scans

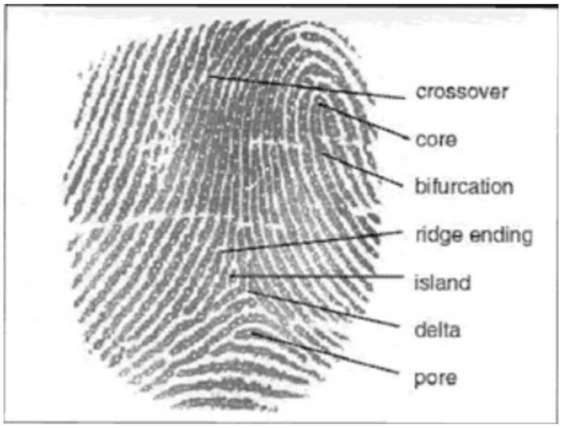
When most people hear someone speak about biometrics as an authentication factor, they immediately think about fingerprint scanning. After all, using fingerprints for identification is something they grew up with. Television police detectives solve otherwise insolvable crimes with latent prints. When MFA landed on the technology landscape, many organizations ran out and purchased it because it was the one biometrics technology widely available and familiar. Many employees are used to having their prints taken as businesses, including Disney theme parks, use prints to identify and control customers. They are simply used to it.

Although it may be the most recognized method, it is not always the best choice. For example, management might not want to protect very high value intellectual property with fingerprint biometrics when the facts about its vulnerability to forgery are explained. But before looking at the pros and cons of fingerprint biometrics, let's examine how this technology works.

How fingerprint scanning works

Figure E shows the points of interest gathered from a scanned fingerprint and converted to a reference template. Once the print is scanned, an algorithm converts the collected physical characteristics into a value—the reference or trial template. The value may differ between vendors, but the process is usually the same. This print-to-value conversion takes place during enrollment and when creating the trial template for authentication. In other words, prints are not compared. Rather, the comparison process determines if the reference template and trial template values are statistically enough alike to verify a person's identity.

Figure E



Fingerprint Characteristics

Advantages

Probably the biggest advantage is the number of solutions available for business security frameworks. Further, vendors have spent years integrating them into single sign-on (SSO) and other authentication solutions. In addition, implementers have a lot of experience working through various challenges unique to fingerprint scanning.

Another advantage is the potential for quick user acceptance. Employees do not see fingerprint scanning as an intrusive procedure. Nor does it carry with it some of the misunderstandings and fears associated with other, newer technologies.

Finally, the costs of fingerprint sensors and related implementations are usually less than those for iris scanners or vein recognition systems. However, lower cost and familiarity do not positively affect the level of security when users cannot consistently use their prints to access network resources.

Disadvantages

There are two major disadvantages associated with fingerprint biometrics: ease of forgery and sensitivity to environmental factors. Forging fingerprints to fool a biometrics sensor is not very hard. Congdon (2010) writes,

> Fingerprints are something everyone leaves behind and they can be copied by forgers using simple household items like scotch tape or gummy bears. In fact, tests have shown that fingerprints left on gummy bears are effective at fooling many fingerprint scanners (Types of Biometric Technologies, para. 1).

While some vendors may strenuously disagree with these assertions, there are plenty of examples on the Internet of tests that successfully cracked fingerprint systems.

Fingerprint sensors and the fingers scanned are all susceptible to environmental conditions. Grease and oil on fingers, machinery or paper cuts, and contaminants in the air can all cause FAR or FER challenges. In 2009, I wrote about a health club that experienced environmental issues when they tried to have their members use their prints to access the club's facilities. This was an example of poor analysis that resulted in the implementation of a technology unsuited for the application (Olzak, 2009).

Do these issues make fingerprint biometrics an unacceptable alternative? Not at all. However, use of prints is something that should be carefully reviewed with stakeholders. They should understand the risks and decide whether to move to a potentially more secure technology, like facial recognition.

Facial Scans

Face scans are not a new technology. Until recently, however, solutions using this technology were too expensive or had technical issues still to work out. Today, facial recognition and scanning technology is fast, relatively inexpensive, and very difficult to forge.

How it works

In principle, biometric authentication with facial scanning is the same as any other biometrics approach. Features of a face are scanned and a value is created by the vendor's algorithm. **Figure F** adds additional detail for this process.

Step 1 requires the facial recognition software to locate a face in the camera image. When a user gazes into the camera, the application must separate the background data from meaningful information. This is done by comparing foreground shapes with a database of general facial shapes.

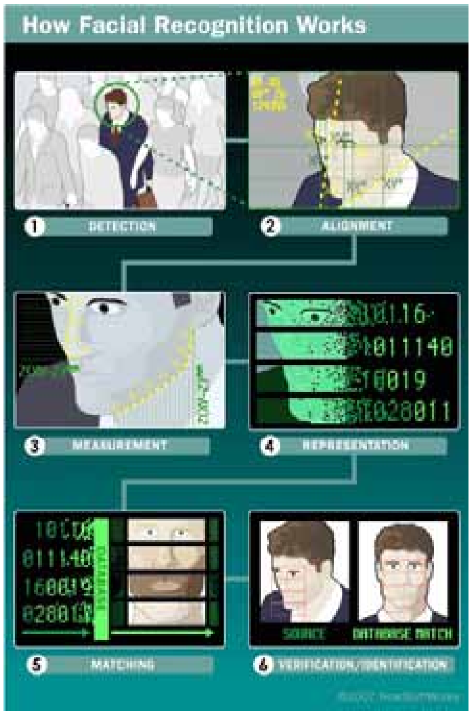
In Step 2, the application determines how the detected face presents itself to the camera. This is not usually a huge challenge with verification systems; the user is typically looking directly at the camera.

Nodal points are identified and measured in Step 3. According to Bonsor and Johnson (n.d.), there are approximately 80 points of identification, or nodal points, in the human face. Some of the most common include,

- Distance between the eyes
- Width of the nose
- Depth of the eye sockets
- The shape of the cheekbones
- The length of the jaw line

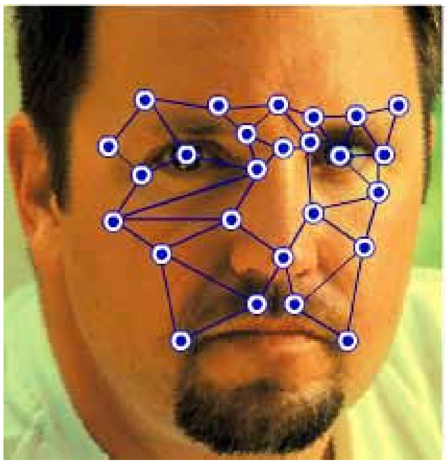
Figure G shows these and other points often used to generate a reference or trial template.

Figure F



Facial Recognition and Scanning

Figure G



Nodal Points (QuestBiometrics.com)

Steps 5 and 6 simply create a trial template, retrieve a reference template, and compare the two to verify the user's identity.

Advantages

Users may be more willing to accept this technology. Face recognition solutions are non-intrusive. No lights scan the eyes or any other part of the face. Further, the technology does not require contact with the sensor. A user sits or stands about two feet away from the camera during the verification process. This eliminates two reasons why employees might resist biometrics.

In many cases, the cost is much lower than fingerprint scanning or other scanning methods. Most biometrics solutions require the purchase of a scanner for each workstation. This is in addition to the cost of the client-side scan processing and comparison software. Solutions like FastAccess from Sensible Vision use cameras already built into laptops or monitors. This can significantly reduce the required budget if hundreds or thousands of sensors are required.

Disadvantages

As with all biometrics, face recognition solutions can be fooled. For example, latex masks can produce false approvals (Xiao, 2010). Granted, this may be much more difficult than lifting and using a fingerprint, but organizations must still consider it as a possible risk.

Multi-modal approaches defeat use of masks and other types of attacks, but the additional cost may be prohibitive. Another approach is to deploy a solution that requires the user to smile, nod the head, or that senses heat signatures of the face surface to verify that a real face is in front of the camera.

Lighting can be another challenge. Any camera needs sufficient light to produce a reasonable image. This is also true for facial recognition. Vendors like Sensible Vision cause the screen to blank into a white, bright surface. This serves as supplemental light for the camera. This may not always be an option. Again, it is important to consider environmental conditions before implementation.

Finally, face recognition technology sometimes has issues with a population containing various races (Eye Tracking, 2010). Improvements in lighting sensitivity will help remove this challenge. However, it is important to consider workforce diversity when selecting a face recognition product. Testing is crucial.

Some vendors are addressing lighting and other issues by developing 3D facial recognition systems. 3D systems use rigid, unchangeable facial characteristics, such as the contour of the eyes, nose, and chin. According to FindBiometrics.com (2010), “The advantages of 3-D facial recognition are that it is not affected by changes in lighting, and it can identify a face from a variety of angles, including profile view” (para. 7). 3D capability tends to increase the cost of facial recognition. However, if high-cost solutions with a low EER are within your budget, consider iris scans as an alternative.

Iris Scans

Iris scan solutions provide good accuracy, low possibility of forgery, and implementation flexibility. As shown in **Figure H,** iris scanners collect information about the characteristics of the colored area surrounding the pupils. This eliminates the intrusiveness of scanning the retina, located at the back of the eye.

Figure H

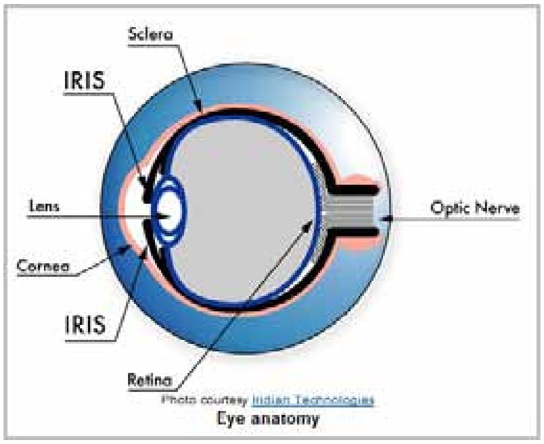


Photo courtesy Iridian Technologies

Eye anatomy

How it works

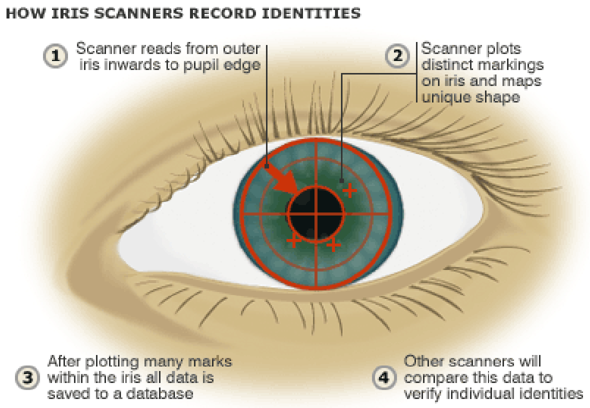
As shown in **Figure I**, the process is very simple. Starting from the outer edge of the iris, the scanner moves toward the pupil, identifies features of the iris, and records them. The final collection of characteristics is converted into a reference template and stored in AD or some other database.

Advantages

Unlike retinal scans, Iris scanning requires no contact with the scanner, and it is non-intrusive. In fact, some iris scanners work from as far as 30 feet from scanned employees in motion, reducing identity verification time and impact on employee routines (SarniffCorp, 2010). Consequently, user and management acceptance is a little easier to obtain.

The iris is a unique identification object with greater reliability than a fingerprint. For example, fingerprints are damaged by cuts, burns, or abrasions, causing fingerprint sensors to incorrectly read them. However, there is very little that can change the iris enough to cause false readings.

Figure I


HOW IRIS SCANNERS RECORD IDENTITIES
1 Scanner reads from outer iris inwards to pupil edge
2 Scanner plots distinct markings on iris and maps unique shape
3 After plotting many marks within the iris all data is saved to a database
4 Other scanners will compare this data to verify individual identities

(Baker, 2010)

Figure J

Iris Scanner

Analyzing over 200 points, use of the iris for identity verification is not affected by glasses, contact lenses, or eye surgery. It is faster than fingerprint technology and has a much lower EER. It is also more accurate than most facial recognition systems on the market today.

Finally, forgery is very difficult if an organization selects a system that adjusts light levels to ensure the pupil dilates and constricts during the scanning process. This helps ensure living tissue is in front of the scanner instead of a high resolution photograph or other forgery.

Disadvantages

The major disadvantage of iris scanning is cost. Scanners, like the one shown in **Figure J**, cost several hundred dollars to two or three thousand dollars. They are also impractical for placing at user workstations for desktop or laptop login. And although iris scanning is very resistant to false acceptance, there are instances in which it might not be useable. For example, iris scanners are typically not effective for individuals who are completely blind.

Another disadvantage lies in eye color. Because iris scans rely on locating the pupil and identification of patterns, very dark irises may cause issues for some users. Any solution should be tested to ensure it appropriately meets this challenge.

There is one emerging technology, however, that provides the accuracy and forgery resistance of iris scanning and the lower cost of fingerprint and facial recognition solutions—vein scanning.

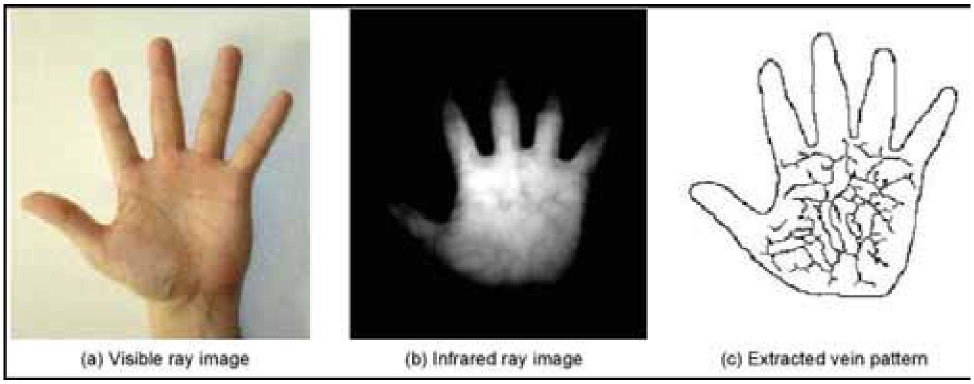
Vein Recognition

The veins of a human hand create a unique pattern suitable for identity verification. According to Shaw (n.d.) The process "…uses near-infrared light to capture a patient's palm vein pattern, generating a unique biometric template that is matched against preregistered users' vein patterns" (How it works, para. 1). Scanning is fast and requires no contact with the sensor.

How it works

Figure K (Fujitsu, Principles of vascular pattern recognition, p. 3) shows how vein recognition technology creates a reference template. Veins contain deoxidized hemoglobin that absorbs light at a wavelength of about 760 nm (near infrared). When a palm is exposed to near infrared light, the veins fail to reflect it resulting in a black vein pattern. This pattern is extracted and converted to a reference template.

Figure K

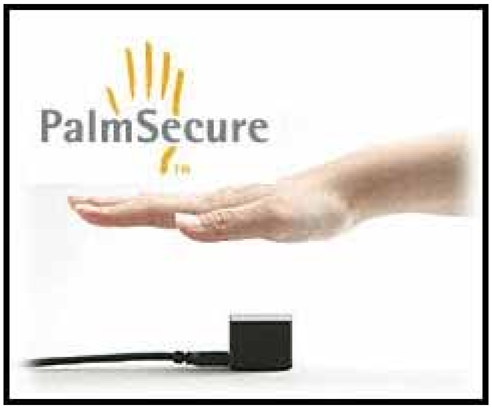


Vein Recognition Technology

Advantages

Palm scanning has several benefits for both user acceptance and business productivity. Scanning the palm, as shown in **Figure L**, is a contactless process. In addition, there are no components that would cause a user to perceive it as intrusive. Further, internal testing of Fujitsu's PalmSecure solution resulted in a FAR of less than 0.00008% and a FRR of 0.01% (Fujitsu, 2006). These results, using 140,000 palm profiles of 70,000 individuals—of various ages and vocations—demonstrate accuracy better than fingerprint technology and potentially better than any other current method.

Figure L



Fujitsu Vein Scanner

Forgery is nearly impossible. Since the palm must contain actual live hemoglobin-bearing fluid, fake or severed hands are not useful for cracking the system. Other systems that use fingers instead of the palm are just as resistant to forgery.

Finally, the cost of vein scanners is decreasing. A desktop unit is less than $200, making it possible to implement this technology for any activity requiring accurate and difficult to forge biometrics.

Disadvantages

Vein scan technology is still new and standards are still evolving. Organizations looking at this approach to biometrics-enhanced security should carefully review the potential lifespan of a product and its ability to integrate with other security solutions now and in the near future.

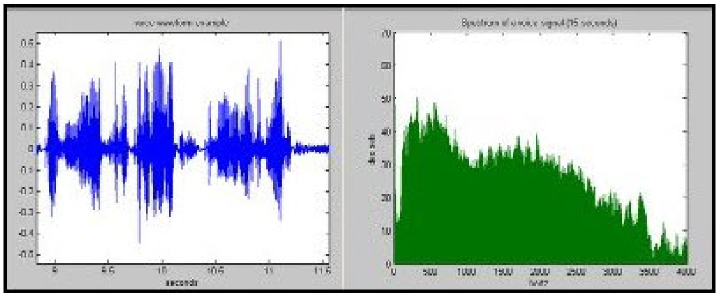
Voice Recognition

Voice recognition is included because of its increasing versatility given current and emerging telephone technology. When used in conjunction with digital phone systems, it allows both employee and customer identity verification.

How it works

Voice recognition solutions use a voiceprint to create reference and trial templates. Voiceprints, as shown in **Figure M**, consist of wave patterns produced by a human voice and certain physical characteristics (FindBiometrics.com, n.d.). Physical characteristics that affect a voiceprint include nasal passages and vocal chords. Further, the frequency, duration, and cadence of spoken words and phrases affect recorded patterns.

Figure M



Voiceprint

Voiceprints can be collected via telephone or microphone. Telephone collection is useful for customer identification. Use of microphones can supplement both physical and technical security.

Advantages

Many VoIP or other digital phone systems can act as "sensors" for voiceprint collection. This reduces costs. With the telephone, people use a nonintrusive technology with which they are already familiar. Microphones integrated into physical security systems can also leverage phone systems and share the same template database.

Another cost advantage is the ability to use PC microphones as biometrics sensors. Most laptops already have built-in recording technology and desktop microphones are very inexpensive.

Disadvantages

Voiceprints are easily forged. One way is to record the voice of a person and play it back to a voiceprint collection device. A good control to mitigate this risk is requiring a specific phrase that was spoken during enrollment instead of random speech. Although this is useful in private areas, it may not provide strong enough security in public or cubicle-rich office environments.

Voice biometrics is not as accurate as iris, vein, or fingerprint technologies. According to a article at AuthenticationWorld.com (2006), "…the equal error rate for voice was less than 1%. Also note that the Failure to Enrol [sic] Rate was 2%. This makes voice recognition biometric authentication one of the best methods for doing authentication (in low to medium risk situations)" (para. 3). Combined with the increased potential for eavesdropping, organizations considering voice recognition should seriously consider multi-modal solutions.

Keystroke Dynamics

The previous biometrics in this paper focused on physical characteristics, although voice recognition may be considered a hybrid. Keystroke dynamics, however, solely relies on user behavior. It is the least intrusive and least costly to enroll a workforce than any of the other solutions. However, it is also one of the least accurate.

How it works

As shown in **Figure N,** keystroke dynamics measures now a person types. No matter how fast a person types, the combination of dwell time—the period of key depression—and the flight time—the period required to press the next key—is reasonably unique between individuals.

Keystroke behavior is measured when a user enters his or her password. As the person types, dwell and flight time information is collected and a reference or trial template is created.

Advantages

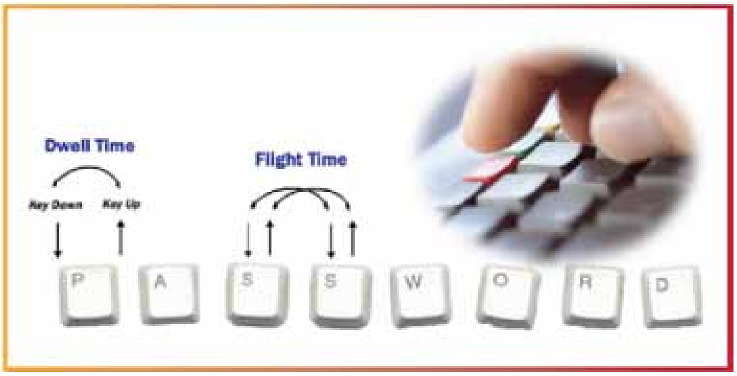
No special hardware is required. Any standard keyboard works as a biometrics "sensor." So the cost is lower than most other biometrics solutions.

Enrollment does not have to take the form of a special task. Rather, the administrator can configure the client software to simply audit keystroke information over a specified enrollment period. This activity is transparent to the user. Once sufficient information is collected, the audit or enrollment activity is transitioned to identity verification.

Specific solutions, like Sentry from AdmitOne Security, allow adjustment of verification probability based on the application the user is accessing at the time. This allows strengthening security when necessary and relaxing it when frustrating the user in the name of strong security is not necessary. This is particularly important for keystroke dynamics since it can be a weaker approach to identity verification.

It is difficult to forge. Even if a potential attacker practices, it is very difficult to achieve the same true acceptance rate of the target user.

Figure N

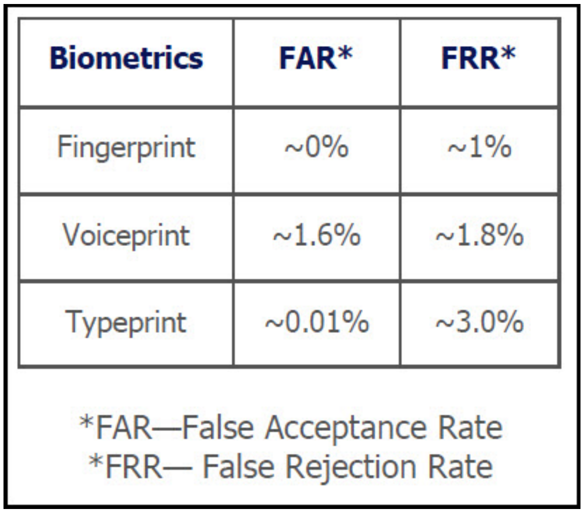


Keystroke Metrics

Disadvantages

The biggest challenge is the relatively high EER. **Figure O** lists error rates for keystroke dynamics (typeprint), fingerprint, and voice biometrics. Although not listed, the low error rates for vein and face recognition technologies were discussed earlier in this document. Although this information is four to five years old, it demonstrates the relative difference between the accuracy of keystroke dynamics and other technologies.

Figure O



Biometrics	FAR*	FRR*
Fingerprint	~0%	~1%
Voiceprint	~1.6%	~1.8%
Typeprint	~0.01%	~3.0%

*FAR—False Acceptance Rate
*FRR— False Rejection Rate

(DeepNet Security, 2006)

Another challenge to consider is the changing of passwords. The password and the way it is typed are combined into a reference template. How will this affect the organization's ability regularly to enforce password changes?

Summary

Use of biometrics as part of an overall MFA implementation is a good way to hold costs down and provide enhanced security. However, it requires a solid business case to get funding, broad stakeholder involvement to define all relevant technical and business requirements, and a lengthy vendor/solution evaluation process.

Not all biometrics solutions work under all conditions and for all members of your workforce. Understand your office and production environments and who works in them. Pilot any final solution to ensure all requirements are met and to identify unexpected obstacles to success.

Finally, this is a big change for an organization. Managing user acceptance is just as important as selecting the right technology.

To close this examination of the practical approach to deploying biometrics, we will follow a fictitious security manager as he walks through the office after the successful implementation of a biometrics framework.

Fictional Case Study

John arrived at the office early Monday morning after a long and hectic weekend. He and his team had worked with their biometrics vendors to complete the new physical and technical authentication and identity verification systems. As he promised the CIO, he was going to do a quick walk-through of the various departments as employees began arriving for work.

As he approached the front door, John looked slightly up and to the right at a small camera. After a second or two, the door lock beeped as the iris recognition system approved his access. He chose iris scanning for building access because of its accuracy at several feet, even if the employees couldn't stand still.

As he passed through the lobby, he walked to the receptionist's desk. The receptionist wasn't in yet, so he walked behind her station and pressed a button mounted under the desktop. The door beeped once more. This test confirmed that the workaround for a failed iris identification—receptionist controlled access control—was working as expected.

Next, John walked down the hall to the data center. The CIO had wanted data center access as strong as economically feasible. It also had to allow quick access when necessary. For this solution, John had chosen a multimodal approach. Since he already had an iris recognition solution, he used iris scanning as one of two identity verification methods. The second was facial recognition.

As John walked up to the data center door, he looked at a set of two cameras mounted on the wall. It took about two seconds for the two recognition systems to identify him, integrate their results, and grant him access. No problems here.

Taking the stairs to the second floor, John entered the engineering department, the brain trust of the organization. It was here that the most valuable intellectual property was created and accessed. Mary, a senior product engineer, was already working on a new design.

"Everything working OK this morning", John asked. "Any problems logging in?"

"Hey, John." Mary swiveled her chair and looked up. "No, everything worked great. I sat down in front of my computer and the camera picked up my face. I got logged in very quickly."

"Great!"

"There is one problem, I think," Mary said. "You know the timeout that locks the system if I'm away? It seems to lock me out even if I'm just turned away for a minute or so. It's a little annoying."

John thought for a moment. "OK. We designed the face recognition system to log you off if you aren't sitting in front of your screen. We can adjust the away time to help reduce the log out frequency."

Mary smiled and returned to her work. "Thanks, John. I'll let you know if I have any more problems." Because Mary had been turned away from the computer while talking to John, the face recognition system had logged her out. As soon as the camera detected her face again, it quickly logged her back on.

There was one more test before he checked in with the security team—the plant floor. John walked up to a production computer where Pete, a machine operator, was hard at work.

"Good morning, John," Pete said while taking a sip of his morning coffee. "I suppose you came out here to check on your new gizmo." Pete pointed at the camera mounted on his computer.

"Yep. How is it working for you?"

"Pretty good," Pete said. "I walked up to the computer this morning and I got logged right in. But what about the next shift? Do they have to know my password or have my picture or something?"

John smiled. "Nope. The camera on your monitor will recognize the person standing in front of the computer and log him or her in. You should already be logged out by the time you reach the time clock because the computer will see you aren't in front of it any longer. If not, the next recognized person to stand in front of the camera will cause the system to log you out and log them in."

"Sounds good," said Pete. "Now I have to get back at it. Big production run today."

Pete was feeling pretty good. Everything seemed to be working as designed. He expected one or two adjustments as the day progressed, but using the security management portal, they were easy to make and transparent to the users.

As he walked into the IS security area, he noticed one of his network security engineers reviewing a log created over the weekend. He walked over to her workstation.

"Good morning, Beth. Any trouble logging in this morning?"

"No problems at all," Beth replied. "The vein scanner for access to the password repository and the LAN/WAN management system works great."

Because of the high security required, the relatively low cost, and the small number of users, John had selected palm vein recognition for the most sensitive network security resources.

"Excellent," said John. "Hang on a second… the CEO just sent a text. The new facial recognition system doesn't recognize him this morning. Guess we can't expect everything to work day one." With a sigh, John walked to the elevator that would take him to the executive suite.

On the way up, he reviewed the morning walk-through. The iris scans for building and data center access seemed to be working OK. In addition, the facial recognition system, the primary second authentication factor, was working as designed… just needed a small adjustment. Finally, the vein recognition solution used to protect the security management tools was providing a fast and very accurate authentication method for his analysts and engineers.   Once he was done with the CEO, he would verify the database security designed for the reference template storage.

As the elevator door opened, John smiled. "Looks like it's going to be a good day."

References

AuthenticationWorld.com. (2006). *Biometric authentication - voice.* Retrieved from http://www.authenticationworld.com/Authentication-Biometrics/VoiceAuthentication.html

Baker, J. (2010). *The eyes have it at UK immigration.* Jim Baker's Ephemera. Retrieved from http://www.jnb65.com/tag/iris/

Bonsor, K. and Johnson, R. (n.d.). *How facial recognition systems work.* HowStuffWorks. Retrieved from http://electronics.howstuffworks.com/gadgets/high-tech-gadgets/facial-recognition.htm

Brandel, M. (2010). *Using biometric access systems: Dos and don'ts.* CIO Magazine Online. Retrieved from http://www.cio.com.au/article/339235/using_biometric_access_systems_dos_don_ts/

Congdon, K. (2010). *Are biometrics the key to health IT security?* Healthcare Technology Online. Retrieved from http://www.healthcaretechnologyonline.com/article.mvc/Are-Biometrics-The-Key-To-Health-IT-Security-0001?VNETCOOKIE=NO

DeepNet Security. (2006). *Keystroke biometric signature.* Retrieved from http://www.deepnetsecurity.com/products/pdf/Deepnet%20typesense.pdf

Eye Tracking. (2010). *Race presents challenge for facial and eye tracking technology*. Retrieved from http://eyetrackingupdate.com/2010/01/22/race-presents-challenge-for-facial-and-eye-tracking-technology/

FindBiometrics.com. (n.d.). *Voice/speech recognition.* Retrieved from http://www.findbiometrics.com/voice-recognition/

Fujitsu (2006). *Palm vein pattern authentication technology.* Retrieved from http://www.fujitsu.com/us/services/biometrics/palm-vein/

Helmer, G. M. (2010). *Ponemon study finds average cost of data breach was $3.4 million in 2009*. Foley Hoag LLP. Retrieved from http://www.securityprivacyandthelaw.com/2010/05/articles/cybersecurity-cybercrime/ponemon-study-finds-average-cost-of-data-breach-was-34-million-in-2009/

Identity Magazine. (2010). *The enemy within.* Retrieved from http://www.identitymag.co.za/index.php/privacy-policy/6-the-enemy-within

Microsoft MSDN. (2010). *Interactive authentication.* Retrieved from http://msdn.microsoft.com/en-us/library/aa376107(VS.85).aspx

O'Leary, T. (2008, February). Acceptance and accuracy in biometrics. *Security Dealer and Integrator,* 30(2), 52.

Olzak, T. (2009). *Implementing biometrics requires a little thought.* it.toolbox.com. Retrieved from http://it.toolbox.com/blogs/adventuresinsecurity/implementing-biometrics-requires-a-little-thought-31423

SarniffCorp. (2010, February 24). Iris on the move [Video file]. Retrieved from http://www.youtube.com/watch?v=b1uZonksCnl&feature=player_embedded#!

Shaw, G. (n.d.). *Future tense: palm vein biometric authentication.* HealthLeaders Media Magazine. Retrieved from http://www.healthleadersmedia.com/content/MAG-252325/Future-Tense-Palm-Vein-Biometric-Authentication.html##

Westover, J. H. (2010). Managing organization change: Change agent strategies and techniques to successfully managing the dynamics of stability and change in organizations. *International Journal of Management and Innovation*, 2(1), 45-50. Retrieved from http://ehis.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=6&hid=115&sid=5eaccff2-20aa-4352-8386-84d09007c1ee%40sessionmgr111

Xiao, Q. (2010). *Applying biometrics*. Defense Research and Development Canada. Retrieved from http://www.ottawa.drdc-rddc.gc.ca/html/biometrics-eng.html