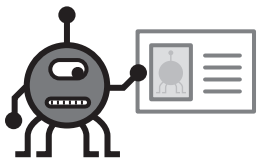
Chapter 11
Determining Identity: Biometrics



Biometrics technologies measure a particular set of a person's vital statistics in order to determine identity.

Technology Overview

The word biometrics comes from the Greek words bio and metric, directly translating into "life measurement." General science has included biometrics as a field of statistical development since the early twentieth century. An example is the statistical analysis of data from agricultural field experiments comparing the yields of different varieties of wheat. In this way, science is taking a life measurement of the agriculture to ultimately determine more efficient methods of growth.

In the most contemporary computer science applications, the term "life measurement" takes on a slightly different role. Biometrics in the high technology sector refers to a particular class of identification technologies. These technologies use an individual's unique biological traits to determine one's identity. The traits that are considered include fingerprints, retina and iris patterns, and facial characteristics. One can see that biometrics is still an appropriate title (see Figure 11-1).

The biological traits used in modern biometric applications are chosen based on our technical ability to catalogue and track them. Some traits are easier to obtain

Biometrics: Taking Life Measurements

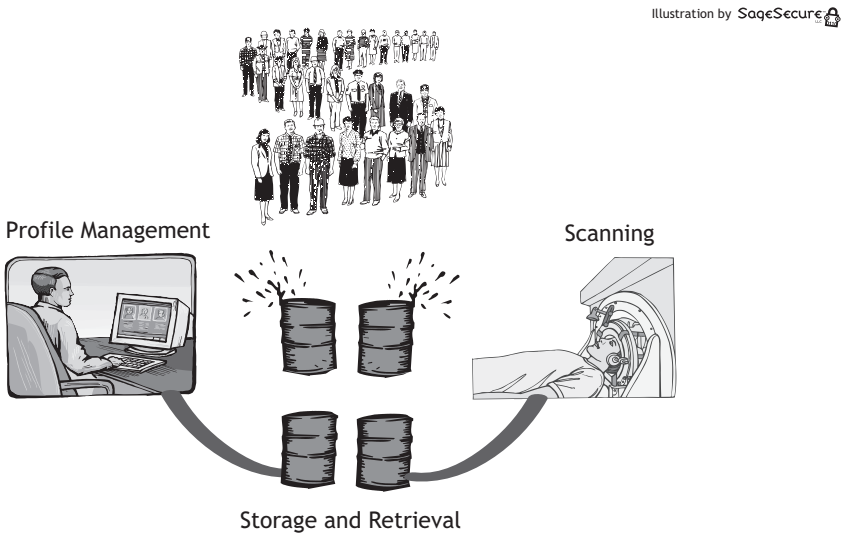


Figure 11-1

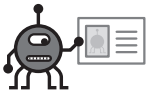
than others. Fingerprints, for example, are relatively simple to record and store in a database. They also tend to be less accurate and secure than other more complex biometrics.

Advances in biometric technology are focused on improving the accuracy and security of measurements and reducing the cost to levels appropriate for consumer applications. Simple and low cost systems available today, such as fingerprint readers, will become more reliable. High accuracy systems such as retina scanners will drop in price and will eventually supplement or replace existing systems.

As this book serves proof of, digital security is in ever-growing demand. Complex breaches of security are becoming a worldwide problem. The focus on biometric systems is an industry-wide response to the call for more effective security.

Biometrics, Past and Present

Most people have some degree of familiarity with biometrics, thanks to television and the movies. Hollywood has portrayed biometrics as futuristic technology in science fiction movies, and as elite security technology in spy movies. This has given biometric technologies an expensive and exclusive reputation. Many business owners or executives would most likely say, "We don't need that kind of security; we are not a military facility." Some people don't even think the technology is real, convinced that it's still in the realm of science fiction. As a result, biometric systems



have been unintentionally marketed as a very advanced, high-end security technology for many years now.

The difference between today and twenty years ago is seen in both the effectiveness of the technology and the greatly reduced cost. In fact, what one may have only seen in the movies may soon be seen on the front door of your home. Door locks that work using fingerprints or handprints instead of keys are already available at consumer-level cost.

In the coming years a very real and very new market for biometrics will be emerging. Hollywood may have not exaggerated the truth in their movies for a change. Biometrics is truly high tech and, when utilized, gives off an image of an expensive, extremely secure technology. If you have ever had to pass through a retina scanner to get to a meeting, you already know what we mean.

Biometrics is commonly criticized for providing more glitz than security. There can be truth to this claim, depending on how biometric systems are implemented. For example, a retina scanner provides little security if an authorized person holds the door for a stranger standing behind them. Biometrics can only provide effective security when properly combined with other identification factors. Let's take a closer look at how biometrics works to better understand how it integrates within a complete security system.

What People Think: Biometrics is for large and highly secure organizations only. They provide an unprecedented level of security. We can never afford them.

What We Think: Anybody can afford to use biometrics. They don't necessarily provide more security.

How Biometrics Work

A biometric device is a combination of a scanning interface and a software system that includes a database and measurement comparison procedures. When a user interacts with a biometric interface the software system will react positively or negatively. A positive response may give the user access to something, or just acknowledge a match in the database. A negative response may deny the person access, or simply determine that the individual has not yet been catalogued. For example, a negative response may tell administrators that the person in front of the hand scanner needs to be recorded for future access.

The first time an individual uses a biometric device, his or her measurements need to be scanned and catalogued. This process is known as enrollment, and serves two main purposes: recognition and authentication.

Recognition systems compare the incoming measurements to every measurement in the database and simply report if a match has been found. These systems are

used in numerous applications. Stand-alone fingerprint and handprint scanners check to see if the incoming print is in the "allowed" database. Voice recognition systems match incoming patterns to lists of known words and phrases.

Recognition systems can be set to automatically enroll any unrecognized measurement. They can also be set to reject already recognized measurements. This combination is useful for situations where a person can only participate a single time.

Authentication systems compare the scanned measurement to a particular expected measurement associated with a digital identity. A user first claims his or her identity by either supplying a username or a physical identifier, such as a smart card. The authentication system then retrieves the expected measurements from a database. It then compares the user's measurements to the stored values. If a match is found, the user will gain access according to the privileges specified in his or her digital identity.

There are many different types of biometric devices in use today all over the world. While the main function of all types of these systems is to identify and authenticate, they each perform the task with a unique style.

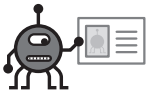
Fingerprinting has long been used to track criminal and citizens alike. The tip of every finger has a characteristic known as "friction ridges." These friction ridge patterns appear to be similar overall, but no two friction ridges are exactly the same. Police forensic teams have learned to quickly identify identical sets of prints based on patterns within the ridges.

Biometric systems have taken the concept of fingerprinting to new heights. The biometric interface specifically images the ridges of the fingertips using an especially touch-sensitive scanner. The pattern is converted to a digital file and is securely stored in a database or is compared to an already stored image. The same process used by forensic teams is performed in less than a second by a special combination of hardware and software.

Consumer biometric devices have been available to the casual user for quite some time. Fingerprint scanners for PC computers are available as stand-alone devices, and have also been built into mice and keyboards. The fingerprint scanner can be used to prevent unauthorized access to the PC. Some software also uses the fingerprint as an encryption key. This means a fingerprint can be used to protect individual files from prying eyes.

Face recognition software is one of the more recent developments in the field of biometrics. It is far more complex in function, but based on the same principles as fingerprint scanning. Face recognition works by employing a combination of scanning hardware and processing software. The hardware includes discreet high-resolution digital video cameras that can be placed virtually anywhere.

Face recognition software takes the digital image of your face provided by the camera and uses advanced statistics to identify patterns. A common technique is to break the image into a grid, and create a table (matrix) showing the average amount of darkness in each grid region. A mathematical technique called "eigenspace" is used to simplify the table, reducing the image to a set of unique equations. The



eigenspace technique essentially treats the image as a topographical map, where facial features are denoted by differences in shading. The resulting equations summarize the relationship between key facial features, such as the distance of nose tip to eyes and cheeks.

Amazingly, these relationships remain constant for any given person regardless of the camera angle, distance, or lighting conditions. Likewise, the relationships are relatively unique—the odds of two people having the same "eigenface" are very small. In many cases, a facial recognition system is more accurate than a human. These systems are far less sensitive to hairstyle, facial hair, glasses, skin tone, and other factors that might confuse a person. They can also match from images that are too small, blurry or distorted for the human eye.

Matching the face is often the easy task. In many cases, face recognition software actually has to perform the more difficult task of identifying the head in a given camera image. In all but the most controlled of environments, the task of "finding the face" is far more difficult due to complex backgrounds and other interfering factors.

One prominent example where this technology has already gone into use is Las Vegas. The phrase "Vegas, baby, Vegas" now has a whole new meaning. Casinos all over town are putting face recognition technology into their already complex and highly advanced security systems. This allows them to quickly identify burned[1] gamblers and escort them out of the casino. With face recognition technology this feat can be accomplished before the individual even gets a seat at the blackjack table.

Before identification technology could capture faces it was able to scan eyeballs. More than a fingerprint, the retina, iris, or cornea of one's eye is able to provide a completely unique pattern by which to identify an individual. The retina, which is located on the back inside of the eyeball, is made up of a series of minute capillaries, which produce a distinct pattern. The cornea and the iris are completely unique in shape and color. An eye scanner can record any combination of this information and store it in a database.

Security Considerations

Biometrics comes with its share of side effects, not all of them being negative. The problems that come with biometric technologies range from nuisances to cost. Planning ahead to incorporate the next generation of security devices is much easier when you know what surprises may lay around the corner.

Cost: As with every new toy, cost is an issue. Not only is the cost of the initial purchase a factor, but so is the cost of upkeep. With biometrics, maintenance can be a real resource problem. Upkeep of almost all biometric systems requires a consistently high level of maintenance and management. Systems that require contact

[1]The term "burned" in a gambling town like Las Vegas refers to an individual who has broken casino rules in the past and been caught for it. Once his or her face and habits are connected every casino in a gambling town will quickly ban the individual from gambling. Note the authors only know about this from reading and not direct experience.

suffer from dust accumulation as well as hand cream build up or grease on the sensors. This necessitates routine cleaning as well as diagnostic checks and sensitivity adjustments. Failure to complete the cleaning and tweaking process regularly will most often result in a high degree of system inaccuracy.

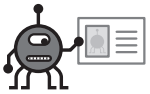
Maintenance: Technical problems also plague complex biometric systems. The fact is, they rely on large relational databases to catalogue and store the images they scan. These relational databases tend to degrade over time. They also tend to show a decrease in accuracy and response time as the data pools they store increase in size. The overall result: as the use of the biometric system increases, the overall performance of the biometric system decreases. This in turn lends itself to more maintenance and even greater upkeep costs.

Privacy: Although maintenance, technical problems, and cost may not be a surprise, the following fact is likely to catch most off guard. Biometric systems can often create an invasion of medical privacy for the people required to use them. Because of the constant accurate tracking of certain biological traits, the database is capable of detecting minor changes. These changes can often provide enough information to accurately diagnose certain medical ailments. For example, conditions like diabetes and stroke will change blood vessel patterns in the eye. A retina scanner may start rejecting a user as these conditions mature. Upon examination, the change in the eye pattern will be identified as the culprit. Many consider the capturing of information that can lead to such conclusions to be an invasion of medical privacy.

Health: Another medical related problem with using biometric security devices is the perceived health risks. Many people are not comfortable having their retina scanned, as they feel it may be doing damage to their eye. Additionally, there is the concern of such devices spreading communicable diseases. Germs that cause many ailments may be lying on the interface your body is forced to interact with each day. Whether such health risks are real or not is important in the long-term. In the short-term this may result in user resistance when trying to rollout biometric security for the first time.

Acceptance: With all these issues surrounding biometric security it becomes clear that successful corporate implementation may not be so simple. One component required to achieve success with a biometric security policy is full staff cooperation. Biometrics will only fit into your corporate culture if your employees accept it as part of their routine. People put up with many hassles on a daily basis—traffic jams, lack of parking, and so on. When they finally get to work they may not appreciate a three-tiered biometric security system. It takes the right attitude and adjusted skill level to prevent such a system from becoming a nuisance.

Still, there are components to biometrics that make many people feel it is worth the trouble. For one thing, company staff may feel more comfortable knowing their employer has invested in their safety. This is a big plus in the morale category. Complex-looking security systems give an extraordinary appearance of a secure environment.



Biometrics and Handguns

A company called Bioscrypt[2] has been working closely with Smith and Wesson for several years now. What do a 150-year-old gunsmith and a biometric company have in common? They forged a partnership for better gun control, which has resulted in smart guns. Guns that will actually get to know their owner, and in turn only allow their owner to use them. Supporters of this idea believe it could be the perfect solution to some of the handgun problems seen around the world. No longer will anybody be able to use any gun.

Here's how it works: When the gun is purchased a small biometric device in the handle scans the fingerprint of the owner. Before the gun is permitted to fire the handprint is scanned to determine the user's identification. If gun does not recognize the handler's fingerprint it remains locked and unable to fire. In this way, biometrics is providing a giant leap in handgun safety. If a police officer, for example, has his gun taken, the assailant will be unable to use the gun. A child will no longer be able to find and fire a handgun that was stored around the house.

In the end, you have to ask yourself if your security philosophy truly calls for biometrics. Highly effective security can be achieved without biometrics. That said, a properly implemented biometrics solution could effectively enhance both real and perceived security. As biometrics technologies drop in cost, they will become more viable for small to medium-sized business environments. If these benefits outweigh the costs and potential deterrents, biometrics may be in your organization's future.

Making the Connection

Cryptography: Biometric data is often stored in an encrypted format.

Managing Security: Biometric technologies should only be deployed in manners consistent with an organization's security philosophy. Successfully deploying biometrics requires careful thinking and organizational commitment to security.

Privacy: Biological measurements are considered highly sensitive personal information and therefore the data gathered by biometric devices must be handled delicately.

[2] Formerly Mytec technologies, changed name to Bioscrypt after acquisition and merger.

Best Practices

Biometric technology alone will only provide one-dimensional security. When it's combined with other technologies that bolster its weak points, you can have the makings of a secure environment. As we have established, wholly protecting assets always requires following the four categories of authentication methodologies. Biometrics alone only covers two of these categories, "what you are" and "what you do."

At the corporate or government level, biometrics is seen to integrate with technologies that cover the other two categories of authentication. These technologies include smart cards, passwords and *personal identification numbers* (PINs), magnetic stripes, and even physical keys. The highest level of security for these large organizations uses a minimum of three-factor authentication. That is, their security systems integrate three of the four categories of authentication methodologies.

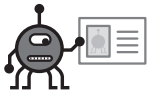
For example, let's follow a mythical employee named Steve as he tries to gain access to a completely secure area of his company. He approaches a door and the door has a complex-looking device requesting input. The device has a chin rest, a keypad, and a card-swiping receptacle that resembles those used in retail stores. Steve places his chin on the rest, at which time his retina is scanned. Upon verification of his retina pattern in the database he is then asked to swipe his magnetic smart card. If the card matches his assigned card code he is the asked by the system to enter his PIN number. With the correct input and collaboration of all three forms of authentication the door releases its lock and allows Steve access.

In this case the security system is requesting something Steve knows (the password), something he possesses (the smart card), and something he is (retinal scan). This is how three factor authentication works, and here are some of the benefits: If Steve drops his card on the ground in the cafeteria and someone else picks it up, it is completely useless. Steve's smart card on its own will not grant anyone access to anything. If someone finds a way to forge Steve's retina pattern they will still be unable to gain access without his smart card or direct knowledge of his PIN number. This offers solid protection against manyw socially engineered attacks as well.

Integrated Biometrics and You

While at one time biometrics was only used in large organizations, practical use for this technology at home has been established. Earlier in the chapter we looked at fingerprint security devices for home computers. Many devices you come into contact with on a daily basis will most likely incorporate biometrics in the years to come.

Cell phones have been a recent example. Many cell phones have voice-activated software built into the handset that allows the user to call whomever he wants by uttering a name into the phone. Voice recognition software has been available for quite some time. This software is "trained" to recognize your voice and language. The result is that it can type out on the screen whatever you say into a microphone. Its goal is to completely replace the need for a keyboard.



Biometrics: Accuracy vs. Acceptance

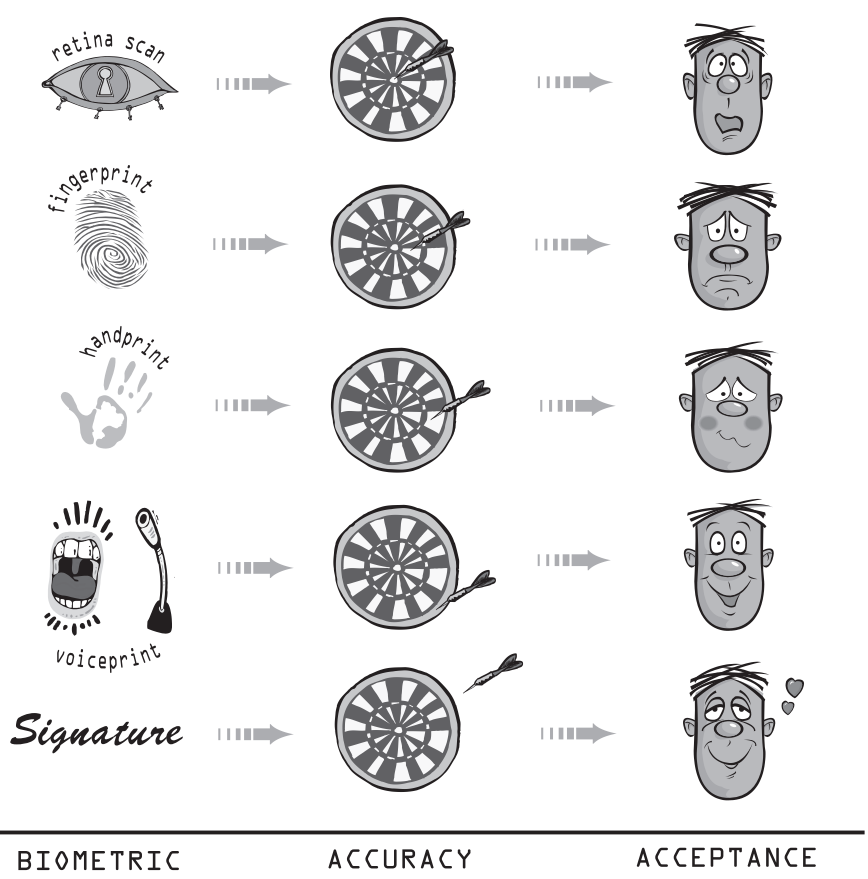


Figure 11-2

Advantages to consumer integrated biometric devices are more than just cosmetic. Ultimately, entire systems will improve and in turn make people's lives better. Medical records, financial information, and government records will all be accessible via local computer interfaces. Requests for this information will be granted based on biometric authentication. The result will be fast and deliberate access to collaborated information from anywhere in the world.

In many scenarios this type of technology could save lives. Imagine if a doctor in a California hospital could access a complete compilation of your medical history inside of one minute when you live in New York. If you were to get into a car accident

while traveling, the doctor would know about all of your pre-existing conditions and be able to administer the proper treatments in record time. This would solve massive storage problems as well, since analog records of any kind would no longer need to take up space. Biometrics provides the security necessary to make this possible (see Figure 11-2).

Ironically, when the consumers, users, and the biometric industry in general were polled an interesting discovery was made; the comfort level that people have with biometric technologies is inversely related to their effectiveness. This makes sense from a practical standpoint. People are comfortable with what they know. Most people have adjusted to giving their signature as a method of identification. On the other hand, having your retina scanned still seems a little too "Star Trek" for most people today. This information is worth serious consideration before implementing a biometric security device.

Final Thoughts

It may be frightening to realize that databases of faces are being created with each passing moment. Along with the stored faces, habits and identities can be traced over time. Now consider the real life implications of a technology this powerful. It is only a matter of time before a camera can capture your face and your motions and translate them into your identity. This could have massive implications on the future of privacy across the world.