Chapter 1

Understanding Biometrics

In This Chapter

- Getting a handle on biometrics
- Sampling physiological and behavioral biometrics
- Defining biometric systems
- Protecting biometric systems

Here's our "nickel tour" of biometrics — well, okay, that'd be a dollar or two in today's money — back in the day, a nickel tour meant you got a pretty good overall look at something in a short time. This chapter is like that. If you're going into a meeting about biometrics in thirty minutes, and you don't want to appear clueless about it, this chapter will show you all the basics you need. But if you're standing in the bookstore looking for more of a clue, you're much better off buying the book and taking it home where you can drill deeper into the topics you're really interested in.

What Biometrics Are and Who's Using Them

The term *biometrics* comes from the ancient Greek *bios* = "life" and *metron* = "measure." Biometrics refers to the entire class of technologies and techniques to uniquely identify humans. Though biometric technology has various uses, its primary purpose is to provide a more secure alternative to the traditional access-control systems used to protect personal or corporate assets. Many of the problems that biometrics help to solve are the weaknesses found in present access-control systems — specifically these:

- **Weak passwords:** Computer users are notoriously apt to use poor, easily guessed passwords, resulting in break-ins where intruders can guess another user's credentials and gain unauthorized access to a computer system. This could lead to a security breach where personal or business secrets are stolen by an outsider. If your password is currently *password, 123456, abc123, letmein,* or *qwerty,* please stop reading this

book long enough to change it — to the first character of each word in your favorite passage from *Moby Dick*. We'll wait.

- **Shared credentials:** In both small and large organizations, we often hear of cases like this: A computer user shares his or her password with a colleague who requires access — even though, in most organizations (and in many security-related laws and regulations), this is forbidden by policy. People by nature are willing to help a colleague in need, though, even if it means violating policy to achieve a greater purpose.
- **Lost key cards:** Many times in our careers we have both found lost key cards in parking lots and other places. Often they have the name of the organization on them, so it's like finding a key with an address on it, permitting the person who found it a free after-hours tour of some American corporation.

Biometrics can solve all these problems by requiring an additional credential — something associated with the person's own body — before granting access to a building, computer room, or computer system. An access-control system that utilizes biometrics will include an electronic device that measures some specific aspect of a person's body or behavior that positively identifies that person. The device might be a fingerprint reader, a digital camera to get a good look at an iris, or a signature pad. (We discuss all the common types of biometrics in the next section.)

Biometric technology as a means of protecting assets has been around for quite a while in some fields. Military, intelligence, and law enforcement organizations have been using biometrics to enhance physical and logical access controls for decades.

But in the past several years, there has been an uptick in the use of biometrics to protect high-value assets. Internet data centers (the kind that lease rack space and cage space to companies that prefer not to build their own fortresses) often use biometrics for admitting personnel to the data-center floor. Fingerprint-biometric devices are showing up everywhere — even built in to laptops, PDAs, and USB drives. Facial recognition is available on a few laptop models. And for protecting businesses and residences, fingerprint-biometric door-lock sets are available at your favorite big-box home-improvement center (though most of these have key-based bypass systems, reducing the *actual* security you get to the level of a key-based system).

We've also seen a grocery-store chain here in Seattle experiment with using fingerprint scanners for checkout-line payment. Walt Disney World in Orlando, Florida uses fingerprint readers for customers who purchase multi-day passes, to ensure that those who reenter the facility on subsequent days are the same people who purchased the tickets on the first day. Everyone who attended Super Bowl XXXV had their faces compared to the faces of known criminals, using biometrics. Anyone entering the United States since September 30, 2004, has submitted prints of both index fingers — and in December 2008 that will extend to all prints from both hands.

Types of Biometrics

Although there are close to a dozen more-or-less effective ways to use biometrics to identify someone, they all fall into two classes (see Figure 1-1): physiological and behavioral.

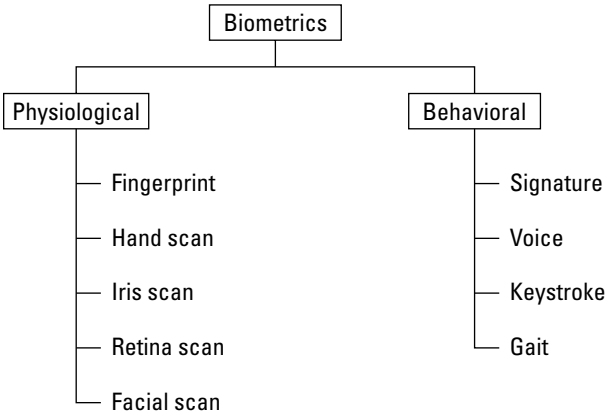

Figure 1-1: The two classes of biometrics are physiological and behavioral.

Physiological

Physiological biometrics measure a specific part of the structure or shape of a portion of a subject's body. The types of physiological biometrics include:

- **Fingerprint:** Officially established as a means of uniquely identifying people since around 1900, fingerprints are easily registered and measured — and devices for doing so are small and inexpensive. You can find them built in to laptop computers, PDAs, USB drives, door locks, and even credit cards.
- **Hand scan:** The geometry of an entire human hand is quite unique, almost as much as fingerprints themselves. Usually a hand scan does not measure the fingerprint-like patterns in the fingers and palms, but instead relies on the lengths and angles of fingers, the geometry of the entire collection of 27 bones, plus muscles, ligaments, and other tissues.
- **Hand veins:** If you shine a bright light through your hand, you can see an interesting pattern of veins — and also the bones and other elements in your hand.
- **Iris scan:** The human iris is the set of muscles that control the size of the pupil — that little hole in the middle of your eye. The human iris, when viewed up close, is the complex collection of tiny muscles that are stained various colors of brown, gray, blue, and green. When we say that

someone has blue, green, or brown "eyes," the color we're referring to is the color of the iris.

- **Retina scan:** The retina is the surface at the rear of the interior of the eye. It's not normally seen except when (say) a doctor shines a bright light through the pupil just right. But it does show up when you have a photo with "red eye" — that's the reflection of the retina. Red eye is not sufficient to identify someone; instead, it is necessary for a person to get their eye close up to a little camera that can see inside the eye.
- **Face recognition:** We recognize faces almost from birth, although *how* we recognize them is better understood now, enough that we can teach computers how to do it under certain conditions. Some laptop computers use facial recognition as a form of authentication before a subject can access the computer.

The characteristic in common with physiological biometrics is that they're more-or-less static measurements of a specific part of your body. You might have to swipe your finger, place your hand, or look at the red dot, but the biometric equipment does the rest. Just hold still . . . there, *got it*.

Physiological biometrics are discussed in detail in Part II. There you can also read about some of the unusual biometrics that may be used someday.

Behavioral

Behavioral biometrics are more concerned with how you *do* something, rather than just a static measurement of a specific body part. Some of the behavioral biometrics in use include these:

- **Handwriting:** Everyone's handwritten signature is different, probably uniquely so. Biometric systems measure signatures in a number of different ways:
  - *Static image.* This is the oldest type of handwriting recognition where we compare a stored signature image with a new sample to see if they match. Arguably, with practice, the *image* of someone's signature can be forged, although it's extremely unlikely that the forger will create the signature the same way that the original person does, which leads to the next two forms of handwriting biometrics:
  - *Signature dynamics.* Here we're measuring either (a) the motion of the stylus or pen or (b) the dynamics of how the signature image itself is created.
  - *Stylus pressure.* We can also measure the dynamics of the downward force of the stylus on the writing surface while the signature is being made.

- **Keystroke dynamics:** The rhythm of someone's typing (or *keyboarding* as we tend to call it these days) is as unique as someone's signature. The precise timing of individual keystrokes is a product of the geometry of the hand, the tone of the muscles in the hands and forearms, as well as the brain's ability to send out the right signals at the right time that result in (say) Peter typing this sentence. And one nice thing about keystroke dynamics biometrics is that it's entirely passive — a software program can continually measure keystrokes — and can, in many cases, sense whether someone walked away and someone else sat down and continued typing.
- **Voice recognition:** As with typing, the *sound* of someone's voice is the product of physical characteristics (specifically, the construction of larynx and related passageways); the brain is in control of the *linguistics* of one's voice. Some biometric systems will have the subject speak his or her name or password; better ones might have the subject read a unique phrase such as "Liberty requires virtue and mettle."
- **Gait:** The way a person walks forms a unique pattern that can be captured for biometric purposes. As with facial recognition, it's sometimes easy to recognize particular people at a distance by the way they walk.

There are stranger and more interesting behavioral biometrics that we discuss more fully in Part II.

How Biometric Systems Work

Biometric systems work through enrolling users by measuring and storing their particular biometric, and then later comparing the stored biometric data with data from unverified subjects to determine whether they should be allowed to access a system or location. Take a look at the entire process in more detail:

1. **Enrollment.**

   Before a user can begin using a biometric system, he or she must complete an enrollment process. Depending upon the biometric technology in use, the user might do this on her own, or there may be a facilitator to help. The user provides other information such as her user ID or name, and then provides initial biometric data, which could consist of (for example) swiping fingers over a fingerprint reader (for fingerprint biometrics), looking into a digital camera lens (for iris biometrics), or repeating some words or phrases (for voice biometrics). Usually the biometric system will request several samples so that the system can determine an average and deviation.

2. **Usage.**

   When the user wishes to access a system or building guarded with biometrics, the user authenticates according to procedure, which could mean swiping a finger over a biometric fingerprint reader, placing a hand over a hand scanner, or signing his name. However it's done, the biometric system will compare the sample with data stored at enrollment time, and make a go/no-go decision on whether the biometric data matches or not. If there is a match, the user is given access; if not, he is denied access and given another try.

3. **Update.**

   For the type of biometrics that change slowly over time (such as handwriting or facial recognition), the biometric system may need to update the data that was originally submitted at enrollment. The biometric system may perform this update with each subsequent measurement (thereby increasing the number of samples, with emphasis on the newer ones), or it may utilize a separate update process.

Biometric systems are generally pretty easy to use. In most cases, even enrollment takes only a minute or two, and everyday usage takes only a few seconds. Indeed, regular use may take less time than the old way of gaining access to a computer or building. This is why we usually consider biometrics a break-even in terms of the time required to use the system compared to the former way in which someone had to identify themselves.

Characteristics of Biometric Systems

Every type of biometric measurement can be classified with a number of characteristics that should be considered in a selection process. Being familiar with these characteristics will help you to better understand how to think objectively about each type. Sure, some of the available biometric technologies are cool, but it's no longer the 1990s — we have to make *rational* decisions about purchasing and using technology. Anyway, the characteristics we're talking about are

- **Universality:** This refers to whether each person has the characteristic being measured. For instance, nearly everyone in your organization will have at least one finger for fingerprint biometrics, but gait-based biometrics may be more difficult if you have any wheelchair-bound staff members.
- **Uniqueness:** How well the particular biometric distinguishes people. DNA is the best, and fingerprints and iris scans are pretty good too.
- **Permanence:** A good biometric system should measure something that changes slowly (if at all) over time. DNA and fingerprints are very good over the long term; handwriting and voice change somewhat from decade to decade.

- **Collectability:** This refers to how easily the biometric can be measured. DNA scores very low (it isn't easy to collect); fingerprint and palm-scan biometrics rate quite high. Gait requires a person to walk over a distance, which would be hard to do while sitting at a workstation. Retina scan requires the subject get really close to a digital camera.
- **Performance:** This refers to the overall technology burden: how much equipment, time, and calculation go into performing a comparison. The fingerprint method fares very well; fingerprint readers are small, compact, and accurate. DNA biometrics tend to be costly, slow, and labor-intensive.
- **Accuracy:** How well does a biometric system distinguish between subjects, and what are the false acceptance and false rejection rates?
- **Acceptability:** Will users be willing to use the biometric technology? DNA will score low because of privacy reasons. Retina scans will score low because some people will be uncomfortable putting their eye really close to something that seems intrusive. Similarly, people won't mind swiping a finger across a surface-type fingerprint scanner or getting an iris photographed from a few feet away, but some are squeamish about sticking their fingers into a device (too many "B" movies).
- **Circumvention:** This refers to how easily a forgery can be made that will fool the biometric system (early fingerprint devices, for example, could be fooled with "gummy fingers"). *Proof of life* testing — a feature that determines whether a sample comes from a *living* body part — is incorporated into many biometric systems so digital images of body parts are less likely to fool the system. But circumvention also refers to whether someone can attack a biometric system in other ways, such as replaying known good credentials through a network connection.

Benefits of Biometric Systems

The antagonists of data security generally consider any form of security as added complication at best and a violation of privacy at worst. We have instead taken the path that security should be a *business enabler* by adding value in some measurable way. Biometrics are no exception: An organization that is implementing biometrics is doing so in order to fulfill a business objective that is usually tied to the reduction of risk.

The three chief benefits that biometrics bring to an organization are

- **More reliable identification:** With biometrics in place, it's far more likely that the person logging in or entering a building is who he says he is. The risk of a lost key card, for example, is greatly reduced when a biometric is required in addition to the key card. And it's highly unlikely that you'll find a finger or eyeball in the parking lot that an intruder can use to enter a building.

- **Elimination of *password sharing*:** Because biometrics are associated with a person and cannot be separated from the person, it eliminates password sharing and that satisfies a regulatory requirement for some, and provides greater accountability for all organizations that use biometric authentication.
- **More convenient identification:** Depending upon the manner in which a biometric solution is integrated into an authentication/authorization system, the biometric solution may make identification even more convenient than before. For example, Peter can log in to his laptop computer with a swipe of his finger, which takes less time than entering a user ID and password.

Selecting a Biometric System

Different biometrics use different measuring techniques and conditions. Depending on the requirements of a specific access control situation, some biometrics will be more suited than others. For instance, DNA verification would not work well for logging in to a computer system (even one that contains *really* sensitive information), as the DNA confirmation is labor intensive and takes a few days at the very least — by that time you'll forget why you wanted to log into the system in the first place.

The point we're trying to get across here is that any initiative that considers using biometrics is to improve access control requires a *lot* of discussion — as well as the development of formal, written requirements. Failure to take those steps may result in choosing the wrong kind of solution, which can be a very costly mistake.

As with any technology-related project, the very first order of business should be the development of *formal business objectives* that are blessed or (even better) *expressed* by the executives in the organization. An example of a bottom-line objective is to *improve the company's ability to prohibit unauthorized persons from accessing valuable assets*. It's hard to find organizations that set out to acquire the latest technology just because it's cooler than the old stuff in the previous generation. Similarly, nobody adopts the newest technology just to keep the system administrators from getting bored and quitting. (Nobody reasonable, anyway.)

The steps for selecting a biometrics solution are pretty straightforward:

1. **Identify selection criteria.**

   This process includes understanding the physical and logical environments, establishing physical requirements (size, weight, and power requirements of biometric devices, for instance), determining acceptable accuracy and rates of failure (false acceptance and false rejection), and getting an accurate handle on regulatory requirements, budget, implementation effort required, and how soon you need a solution in place.

2. **Identify the field of possible solutions.**

   When selection criteria are established, it will be easier to objectively eliminate unsuitable types of solutions and get closer to a "short list" of candidates. Closer analysis of requirements, features, and budget should help you get to one or two types of biometric approaches that may work for you.

3. **Test potential solutions.**

   When you've eliminated most of the playing field and are down to a short list of specific solutions, you should consider getting hold of an actual product you can test. Most vendors will loan you a reader or two for a couple of months if they think they have a shot at selling you a *lot* of them. When you test a couple of solutions in something close to your real setting, you can see how well they really perform. Be sure you get some users involved in the testing — their observations and feedback will be more valuable than you may realize.

4. **Choose the solution.**

   After you've tested some solutions, you should be able to make a selection. The runners-up will want to know why they weren't chosen; it's best to not burn your bridges, but instead, tell them why (amiably and honestly). Who knows — you might be doing business with them in the future when your needs change.

We describe the entire process of product selection in juicy detail in Chapter 8.

Implementing Biometrics

Once you have selected a biometric system, you'll need to develop a plan to get the system installed, configured, and running. But if it were just that simple, we would not have devoted an entire chapter to the subject. The reality is that implementing biometrics is fairly complicated, not because of the technology but because of the behavioral changes that are required of the people who will be using it and the typically large impact on the organization.

Educating users must begin early and should be structured in a manner that gives them a way to ask questions and express any concerns they may have. We can guarantee that if you're implementing a fingerprint-based system, some of your users are going to express concerns regarding civil liberties and make remarks such as "I'll be damned if I'm going to hand over my fingerprints to my employer!" And we're sure you will also hear something like, "I saw someone pick his nose before using the fingerprint reader — do you think I'm stupid enough to use it too?" Our point is that user education is probably more important for biometrics than for nearly any other kind of IT project. Even switching users from Windows to Linux would be easier, in our opinion — chances are nobody will call you a fascist for doing *that*.

Aside from user education, careful planning is the most important part of successfully implementing a biometric system. If you're going to be installing biometric readers in lots of places, then you'll have the normal logistical challenges of getting equipment installed and configured properly — and making sure the red and green wires didn't get crossed (which could be a problem if your installer is color-blind).

Obviously, we've touched on only a few of the issues that crop up in biometric implementation. For the complete story, turn to Chapter 9.

Understanding Biometrics Issues

Biometric technology is nowhere near universally accepted by all users. There are a number of social and legal considerations that give every organization some pause before taking the jump headlong into implementing a biometric system. Done right, identifying and managing these implications helps an organization make a better decision — not only on the type of biometric technology used, but also on how it will be used.

Privacy

In the United States, Europe, and other regions and nations, citizens have a legal right to privacy — which at times may give the use of biometrics the appearance (if not the fact) of intrusiveness. Sometimes privacy concerns are based on misperception; at other times, they're well founded.

The privacy concern arises primarily because people believe certain biometric data that has been collected by a private organization can later be used in ways that would violate their legal rights — or even cause them more tangible harm. The classic example is fingerprint-based biometrics. When users register their fingerprints, they usually believe that the organization is collecting actual fingerprint images — but generally that's not the case. Typically a biometric system based on fingerprints *scans* the image but stores only a cryptographic hash of the data that describes the print. Hashing cannot be reversed to produce the original fingerprint. Users should feel a little better once they understand this.

Privacy laws

A number of privacy laws in the U.S. provide some vague guidance on the permitted collection and use of biometric data. We say "vague" guidance because most of these laws were written prior to the popular use of biometric technology. Some of the noteworthy laws include the following:

- **Privacy Act of 1974**, later amended by the **Computer Matching Privacy Act of 1988**. These laws define how information related to individuals can be collected and used. The long and the short of it is, federal government agencies can collect biometric information and even share it and combine it with information collected from other federal government agencies. However, every citizen has the right to know what information is stored, and must be given access to a process for correcting information that is inaccurate. These two laws don't say anything about how long federal agencies may keep this information, so it's likely they'll have it long after we die.
- **Executive Order 12333.** Signed by President Reagan in 1981, this order seeks to encourage the enhancement of biometric collection methods while still retaining privacy. Primarily the order provides guidelines regarding what situations and conditions justify the collection of biometric information, and regarding what types may be collected.

We discuss these privacy laws in more detail in Chapter 3.

Protecting Biometric Data and Infrastructure

Few will argue that biometric data, even if it's obfuscated, hashed, or encrypted, must be protected from unauthorized access, corruption, and loss. Security professionals call this the protection of CIA — the *c*onfidentiality, *i*ntegrity, and *a*vailability of data.

My fingerprints have been breached — can I get new fingers?

Unless you've been living under a rock, you've heard about the scourge of security breaches concerning credit cards, bank-account numbers, and so on. In the case of credit cards, when they're compromised, the issuing bank quickly cancels the stolen card number and issues a new number for the customer.

But what happens if a person's actual fingerprint images are compromised and published? You can't get your fingerprints replaced; they're permanent. Same goes for your iris image and your other physiological characteristics. This fact has driven the designers of most biometric systems to store biometric information in a form that can't be used to derive the original data — not even whether it's a fingerprint, an image of your iris, or a description of the way you speak.

This concern underscores the need for an organization to do an effective job of educating its personnel about the facts — making sure they know exactly how their personal information will be stored and used. Lacking this information, staff members will fear the worst, which can undermine an otherwise-well-planned biometric implementation.

Biometrics are used to protect valuable assets, whether those assets are workspaces containing expensive machinery or computer systems containing sensitive information. The measures taken to protect biometric data should be similar to those used to protect passwords and other credential data.

To understand how to protect biometric data, it is necessary to understand the types of *threats* that jeopardize it. Mostly, these are the same ones that threaten other information assets. There are quite a number of threats that we categorize as natural (such as floods, lightning, and hurricanes) and man-made (such as sabotage, communications failures, and riots).

It is also important to understand the kinds of *vulnerabilities* that may exist in biometric systems and what can be done to minimize these vulnerabilities. Some of these vulnerabilities are the same ones that other types of information systems and networks face — such as exposed cabling, missing security patches, and improper configuration.

The types of *attacks* that can take place against biometric systems include systems attacks, network attacks, application attacks, social engineering, replay attacks, faked credentials, bypass attacks, and enrollment fraud. The first four are the types of attacks that can be launched against any computing environment. The last four are types of attack specific to biometrics themselves — here's a closer look at these:

- **Replay attacks:** Here, an attacker has found a way to re-transmit known good biometric authentication data over the network in a way that can fool the system into admitting him.
- **Faked credentials:** This attack uses a forged credential in an attempt to gain access to a system or building. Examples include "gummy fingers" and images of faces or irises.
- **Bypass attacks:** An attacker may try different methods of breaking in to a system or facility by bypassing the biometric system altogether.
- **Enrollment fraud:** An intruder may attempt to enroll him or herself in place of a real individual.

For the most part, the tools and techniques used to protect typical computing environments also apply to biometric systems. For instance, all the servers, databases, and network devices that support a biometric system need to be "hardened," have current security patches installed, and have good access management controls in place.

As you might guess, we're hitting the security aspect of biometrics pretty lightly here. The heavy-duty stuff comes later: Chapter 10 has a more complete discussion of keeping biometric systems safe from harm.