Chapter 1

Biometrics

IN THE REALM OF computer security, *biometrics* refers to authentication techniques that rely on measurable physiological and individual characteristics that can be automatically verified. In other words, we all have unique personal attributes that can be used for distinctive identification purposes, including a fingerprint, the pattern of a retina, and voice characteristics.

Although the field of biometrics is still in its infancy, it's inevitable that biometric systems will play a critical role in the future of security. Strong or two-factor authentication — identifying oneself by two of the three methods of something you **know** (for example, a password), **have** (for example, a swipe card), or **is** (for example, a fingerprint) — is becoming more of a de facto standard in secure computing environments. Some personal computers today can include a fingerprint scanner where you place your index finger to provide authentication. The computer analyzes your fingerprint to determine who you are and, based on your identity followed by a passcode or passphrase, allows you different levels of access. Access levels can include the ability to open sensitive files, to use credit card information to make electronic purchases, and so on.

If you've ever watched hi-tech spy movies, you've most likely seen biometric technology. Several movies have depicted biometric technologies based on one or more of the following unique identifiers:

- ✓ Face
- ✓ Fingerprint
- ✓ Handprint
- ✓ Iris
- ✓ Retina
- ✓ Signature
- ✓ Voice
- ✓ Watermarking

But how realistic are they in today's computing world, and how can they help you? This text answers these questions and provides templates for biometric applications.

Introduction

Biometrics refers to the automatic identification of a person based on his or her physiological or behavioral characteristics. This identification method is preferred over traditional methods involving passwords and PINs (personal identification numbers) for several reasons, including the person to be identified is required to be physically present at the point of identification and/or identification based on biometric techniques obviates the need to remember a password or carry a token. With the increased use of computers as vehicles of information technology, restricting access to sensitive/personal data is necessary. By replacing PINs, biometric techniques can potentially prevent unauthorized access to or fraudulent use of the following:

- ✓ ATMs
- ✓ Cellular phones
- ✓ Smart cards
- ✓ Desktop PCs
- ✓ Workstations
- ✓ Computer networks

PINs and passwords may be forgotten, and token-based identification methods such as passports and driver's licenses may be forged, stolen, or lost. Thus, biometric systems of identification are enjoying a new interest. Various types of biometric systems are being used for real-time identification. The most popular are based on face recognition and fingerprint matching; however, other biometric systems use iris and retinal scans, speech, facial feature comparisons and facial thermograms, and hand geometry.

In History

The term *biometrics* is derived from the Greek words *bio* (life) and *metric* (to measure). Among the first known examples of practiced biometrics was a form of member-printing used in China in the fourteenth century, as reported by the Portuguese historian Joao de Barros. The Chinese merchants were stamping children's palm and footprints on paper with ink to distinguish the babies from one another.

In the 1890s, an anthropologist and police desk clerk in Paris named Alphonse Bertillon sought to fix the problem of identifying convicted criminals and turned biometrics into a distinct field of study. He developed a method of multiple body measurements that was named after him (the Bertillonage technique — measuring body lengths). Police throughout the world used this system until it proved to be exceedingly prone to error as many people shared the same measurements. After this failure, the police started using fingerprinting — developed by Richard Edward Henry of Scotland Yard — after the methods used by the Chinese centuries before.

A biometric system is essentially a pattern-recognition system that makes a personal identification by determining the authenticity of a specific physiological or behavioral characteristic possessed by the user. An important issue in designing a practical system is to determine how an individual is identified. Depending on the context, a biometric system can be either a verification (authentication) or an identification system.

Verification versus Identification

Today, wehave the technology and processing power to employ advanced, cost-effective, and much more accurate biometric identification systems. There are two different ways to resolve a person's identity: verification and identification. Verification (am I whom I claim to be?) involves confirming or denying a person's claimed identity. In identification, one has to establish a person's identity (who am I?). Each approach has its own complexities and could probably be solved best by a specific biometric system, including the following:

- ✓ Physical biometrics:
  - Fingerprint — Analyzing fingertip patterns (see Figure 1-1)
  - Facial recognition/face location — Measuring facial characteristics
  - Hand geometry — Measuring the shape of the hand
  - Iris scan — Analyzing features of colored ring of the eye (see Figure 1-2)
  - Retinal scan — Analyzing blood vessels in the eye
  - Vascular patterns — Analyzing vein patterns

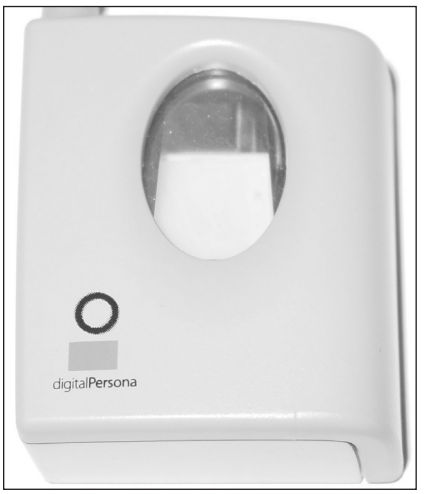

Figure 1-1: Fingerprint biometric system for logon identification and authentication

- DNA — Analyzing genetic makeup
- Biometric data watermarking (which is really a method rather than a physical attribute) is used to store/hide biometric information.

✓ Behavioral biometrics:

- Speaker/voice recognition — Analyzing vocal behavior
- Signature/handwriting — Analyzing signature dynamics
- Keystroke/patterning — Measuring the time spacing of typed words

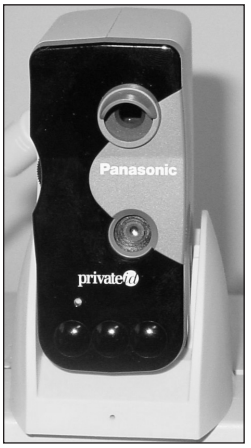

Figure 1-2: Iris recognition biometric system

bio fact

Fingerprint recognition is one of the oldest biometric technologies, and its application in criminal identification, using eyesight, has been in use for more than 100 years. Today, computer software and hardware can perform the identification significantly more accurately and rapidly. Fingerprint technology is among the most developed biometric technologies, and its price is cost-effective enough to make its way into public use.

Facial recognition is among the newer technologies for commercial applications. Two-dimensional face recognition systems impose a high misidentification rate; however, newer three-dimensional facial recognition is showing significant improvements and much better accuracy.

note

Iris scanning is among the most accurate of all biometric technologies with very little overlap between acceptance and rejection curves. This system type is expensive and is recommended for very high security requirements.

Signature recognition is becoming increasingly popular, and the dynamic recognition of relative pen speeds and pressures has significantly improved the accuracy of this system. This technology is also cost-effective for smaller budgets.

Table 1-1 illustrates the most common biometric systems in use today and their characteristics with regard to accuracy, user-friendliness, and user acceptance.

TABLE 1-1: Common Biometric Report by the University of Athens

Biometric System	Accuracy	Ease of Use
Fingerprint	High	Medium
Hand Geometry	Medium	High
Voice	Medium	High
Retina	High	Low
Iris	Medium	Medium
Signature	Medium	Medium
Face	Low	High

User acceptance is also an important issue to consider when selecting a biometric system for employees to use on a regular basis. The following is a general user acceptance list in descending order, from the most accepted to the least accepted:

1. Iris scan
2. Keystroke/patterning
3. Signature/handwriting
4. Speaker/voice recognition
5. Facial recognition/face location
6. Fingerprint
7. Hand geometry
8. Retinal scan

You should consider three factors when designing a biometric solution: *Type I errors, Type II errors,* and *crossover error rate (CER)*. When an authorized individual is rejected by a biometric system — termed *false reject* — this is a Type I error. When an intruder is falsely accepted by a biometric system — termed *false accept* — this is a Type II error. The CER is a percentage rating of Type I versus Type II errors. A lower CER rate means better accuracy.

The following is a general CER list in descending order of accuracy, from the most effective to the least effective:

1. Hand geometry
2. Iris scan
3. Retinal scan
4. Fingerprint
5. Speaker/voice recognition
6. Facial recognition/face location
7. Signature/handwriting
8. Keystroke/patterning

Applications

Biometrics is a rapidly evolving technology that is being widely used in forensics, such as criminal identification and prison security, and that has the potential to be used in a large range of civilian application areas. Biometrics can be used to prevent unauthorized access to ATMs, cellular phones, smart cards, desktop PCs, workstations, and computer networks. It can be used during transactions conducted by telephone and Internet (electronic commerce and electronic banking). In automobiles, biometrics can replace keys with keyless entry devices.

APPLIED BIOMETRICS

This book covers the hottest topics in biometrics development for applications, including the following in regards to applied methodology and program development:

- ✓ Fingerprint identification
- ✓ Hand geometry
- ✓ DNA analysis
- ✓ Speaker recognition
- ✓ Face location
- ✓ Retina scanning
- ✓ Iris scanning
- ✓ Keyboard recognition
- ✓ Multibiometrics
- ✓ Data hiding
- ✓ Sample solutions

It also provides a sample installation and usage of each biometric technology in the data arena where it's most practical. During the sample installation and usage specific features of the product being used are noted. This becomes an important factor in determining which product is right for you. For example, one product may provide good protection and make accessing Web sites easier, while another product may allow access to specific applications to be controlled.

The text also shows how the biometric technology is used to control logon access and, where possible, how it can be used for items such as e-mail and file encryption. For executive and information technology (IT) managers, the following biometric concerns are also covered:

- ✓ What form of device is most appropriate for your use?
- ✓ Should the devices be shared or used individually?
- ✓ How large and how skilled a support staff is needed?
- ✓ Should users be coming in from multiple places? Over multiple channels, such as a *local area network (LAN),* Web, wireless, or *virtual private network (VPN)*?
- ✓ What other forms of IT security should be in place (*Public Key Infrastructure [PKI]*, security portal, firewall, and so on)? How will they interact?
- ✓ Will users be switching access modes?
- ✓ Will different users and groups require different security policies for different applications and transactions?
- ✓ How should all this be administered?
- ✓ Is this for inside the firewall, outside the firewall, or mixed use?

If you have decided to invest in biometrics, you'll find some tips to help you leverage your investment. Can the biometric product(s) be used for multiple purposes, such as the following?

- ✓ Site identification/access
- ✓ Building identification/access
- ✓ Secured location identification/access
- ✓ Equipment identification/access
- ✓ Mobile device protection

PRACTICAL USAGES

Throughout this book, you'll find example scenarios in which biometrics is both a sound practice and a solid investment that can ultimately help ensure security while reducing cost. Additionally, you'll find some futuristic examples of how biometrics may be used to provide new services while maintaining high security.

According to Charles Lynch, Jr. (Vice President of Sales and Marketing for Datastrip, Inc.), vertical markets using biometrics include the following:

- ✓ **Government** — Passports, national identification (ID) cards, voter cards, driver's licenses, social services, and so on
- ✓ **Transportation** — Airport security, boarding passes, and commercial driver's licenses
- ✓ **Healthcare** — Medical insurance cards, patient/employee identity cards
- ✓ **Financial** — Bankcards, ATM cards, credit cards, and debit cards
- ✓ **Retail and gaming** — Retail programs, such as check cashing, loyalty rewards and promotional cards, and gaming systems for access management and VIP programs
- ✓ **Security** — Access control and identity verifications, including time and attendance
- ✓ **Public justice and safety** — Prison IDs, county probation offices' use for identification of parolees, county courthouses' use for ID systems
- ✓ **Education** — Student/teacher identity verification and access control. Biometrics are now being implemented in large-scale ID systems around the globe. Many new passport and national ID card systems use some type of biometric encoded in a bar code or smart chip.
- ✓ **Driver's licenses** — Technologies being recommended by American Association of Motor Vehicle Administrators (AAMVA), the organization that oversees DMV standards, include biometrics and two-dimensional bar codes. Georgia, North Carolina, Kentucky, and others already utilize biometrics on their respective state driver's licenses.

Outside of the government and military arena, corporate America is stepping up to biometrics for applications ranging from employee IDs to time and attendance. The bulk of the biometrics marketplace still consists of traditional systems used to compare fingerprints to vast, centralized databases of criminals' fingerprints.

Where possible, this text also depicts some potential future developments for the technologies discussed.

Facts, Characteristics, and How Biometrics Can Work for You

The most popular use of biometrics for network security is for secure workstation logons. Each workstation requires software support for biometric identification of the user, as well as a hardware device, depending on the biometric being used. The cost of hardware devices is one factor

that may lead to the widespread use of voice biometric security identification that can leverage common sound cards and microphones, especially among companies and organizations on a low budget. Hardware devices such as computer mice with built-in thumbprint readers will be the next step. These devices will be more expensive to implement on several computers, because each machine would require its own hardware device. A biometric mouse, with the software to support it, is available in the United States for approximately $120. The advantage of voice recognition software is that it can be centralized, reducing the cost of implementation per machine. At the top of the price range, a centralized voice biometric package can cost up to $50,000 but may be able to manage the secure logon of up to 5000 machines.

According to the International Biometric Industry Association (IBIA), the following are important details about current biometrics and the industry:

- ✓ **The public, opinion leaders, regulators, and legislators need the facts about biometric technology.** During the past decade, the science of biometrics has matured into an industry that offers real-world solutions to serious problems faced by businesses, schools, and government agencies. Hardware and software produced by biometric manufacturers offer a safe and reliable means to ensure privacy, protect assets, confirm identity, and guard against unauthorized access. Clearly, the marketplace has begun to accept biometrics as a better alternative to less-secure screening and identity verification processes. This success has not yet led to broad public awareness about what biometrics do and how they work. At best, this means that consumers might resist using the technologies in place of more antiquated, but familiar, processes. At worst, regulators and legislators will make ill-informed decisions that will stifle the use of biometrics on identity documents, in banking, and in benefits administration. The lack of common and clearly articulated industry positions on issues such as safety, privacy, and standards further increase the odds that governments might react rashly to unfounded accusations about the functions and uses of biometric technology.
- ✓ **Biometric technology serves as the gatekeeper of confidential personal information.** Biometric technology is used to erect a barrier between personal data and unauthorized access. Technically speaking, the devices create electronic digital templates that are stored and compared to "live" images when there is a need to verify the identity of an individual. The templates use proprietary and carefully guarded algorithms to secure the record and protect it from disclosure. Standing alone, these templates are of no use; they cannot be reconstructed, decrypted, or otherwise manipulated to reveal a person's identity to someone else. Used this way, biometrics can be thought of as a very secure key, but one that cannot be passed on to someone else. Unless this biometric gate is unlocked by the proper key bearer, no one can gain access to that person's information. Compared to other methods of proving identity — producing a driver's license, showing a birth certificate, or revealing one's family history — biometrics are the only currently known tools that can enhance personal privacy and still deliver effective solutions in situations that require confirmation of identity
- ✓ **Biometric technology is a major defense against identity theft.** Identity theft — using stolen credit cards, phony checks, benefits fraud, network hacking, and other impostor scams to defraud businesses, government agencies, and consumers — costs billions of

dollars per year. It is a problem that drives up prices of goods, increases taxes, complicates routine transactions, and strains law enforcement resources. Until recently, the only way to attack the problem has been to add expensive screening and administration procedures; however, steps such as hiring security guards, maintaining accurate databases, reviewing identity documents, administering password systems, and asking personal questions have proven to be costly, stopgap measures that can be defeated by enterprising crooks. Biometric technologies offer effective, low-cost solutions that streamline these traditional, labor-intensive processes. Biometric devices are an effective substitute because they create highly accurate digital records of a person's physiological features. These records can be safely stored for later comparison against a live image that is captured from the user at the time the service or benefit is demanded. All of the devices are nonintrusive, user-friendly units that recognize features such as an iris, a voice, a signature, a fingerprint, a hand, or a face. This gives end users such as banks, merchants, government agencies, and employers extraordinary control over transactions without inconveniencing or embarrassing the customer.

- ✓ **Biometrics are safe.** Biometric devices and software are nonintrusive technologies that are designed to work effectively under variable and demanding conditions. These products do not present health or safety risks to either users or operators. They don't leave marks, don't take physical samples, and require minimal or no contact by the user.
- ✓ **Biometrics are reliable technologies that deliver effective solutions.** Although biometric technologies are relatively new to the marketplace, they have already earned a reputation for effectiveness in a variety of demanding environments that require high levels of accuracy, robust security, and solid customer service. The results produced by these solutions have been well documented. For example, several banks in Texas report that check fraud plummeted by more than 50 percent when biometrics were used; employers cite savings of millions of dollars by using the devices to eliminate time and attendance abuse; and a state government agency says that fraudulent welfare claims declined more than 25 percent when a biometric verification process was introduced. On the customer service side, users have repeatedly expressed complete satisfaction with biometric solutions that expedite border clearance formalities, replace network passwords, and authorize financial transactions.
- ✓ **Biometric manufacturers and developers deliver what they promise.** The devices on the market offer refined, durable, and accurate solutions that have undergone rigorous evaluations and been put through exhaustive trials by end users. As further assurance that the devices work as promised, each member adheres to a strict International Biometric Industry Association (IBIA) code of ethics and attests that any stated product performance claims are accurate and can be independently verified by a competent authority.
- ✓ **Biometric technology is user friendly.** Biometric devices are engineered and developed with the user in mind. The convenient designs have intuitive interfaces that make them easy to operate whether they are used every day, or just now and then. In most cases, biometric processes are quicker and simpler than those that they replace, and can be set up to function reliably even if the user has forgotten a personal identification number.

In a recent trial in the United Kingdom, a bank reported that 91 percent of all users preferred biometrics to PINs and signatures as a means of identification at ATMs and teller windows.

- ✓ **Biometric solutions mean lower costs.** The savings from converting manual processes to those driven by biometric devices can be significant. This is especially true in circumstances where safety and security is important, and customer service and accessibility are essential. In the past, maintaining security and controlling transactions meant using labor-intensive screening methods or administering password/PIN systems — often both. Biometrics offers an effective alternative by automating these processes for a fraction of what the other approaches cost. Businesses, schools, and government agencies have found that the return on investment from biometric solutions is high when they are used to deter identity theft and preserve resources at the same time. There are many examples of how biometrics can improve efficiency. Until recently, network security could only be protected by passwords; now, biometric peripherals can be used to automatically identify the user. Financial transactions, particularly those conducted at ATMs, are protected by PINs; biometric technology can replace this vulnerable system with a process that gets high marks from consumers. Going through border controls has always meant waiting in lines, but where biometric devices are in use, travelers are able to move seamlessly through inspection processes. Biometrics can be used in similar ways to stop losses due to payroll fraud and save time in trying to resolve questions of eligibility for benefits.

Other Common Biometric Characteristics

In general terms, biometric technologies do not actually compare the physical traits that they are designed to use as a unique identifier; rather, they create templates for comparison. The initial comparison templates are created during an enrollment process. This enrollment process may require the individual to provide multiple instances of the biometric trait. For example, a fingerprint enrollment process may require the individual to place a given finger on the fingerprint scanner four times. Depending on the device and the comparison technology, four actual comparison templates may be stored, or the four copies may be used to create a composite comparison template.

Template creation and comparison processes are described throughout this text. However, each manufacturer of biometric technologies often incorporates its own unique method of accomplishing the comparison, and, in most cases, the method is patented.

Finally, the book discusses both the general strengths and weaknesses of biometric technologies. There are many rumors, myths, and misconceptions concerning biometric technology when compared to its much more widely accepted "password protection" counterpart. You will see how biometric technology can provide the next level of security protection when selected and used appropriately.

Summary

Many forms of biometric systems exist for identification and verification purposes; each has a different price range with associated crossover error rates and user-acceptance levels. This book dissects these systems and formulates a cookbook-style template for your own applications. In addition, it formulates methodologies and examines object-oriented source code for strong authentication solutions. Finally, it looks at the weaknesses of each solution and how to mitigate those weaknesses to enhance security and risk acceptance in your environment — whether it is a small home office, a medium-sized infrastructure, or a vast enterprise.