List of Figures

Synopsis

Biometrics is the theory and practice of recognizing an individual based on biological and behavioral traits.

Biometric systems are not like other authentication technologies. Biometric authentication is not based on a subject's establishing that his or her mind is the only mind that knows a particular secret; instead, biometric authentication is based on a subject's establishing that his or her body is the only body that exhibits a particular trait. Biometric traits, unlike passwords and cryptographic keys, are not secret and cannot, in principle, be made secret. Biometric authentication systems therefore do not and cannot depend on the secrecy of biometric traits for their proper functioning. They rely instead on the presumed difficulty of impersonating a living person who is presenting an actual physical trait to a biometric system's sensor.

System designers who use biometrics need to understand the unique properties of biometric technologies, the statistics supporting the use of biometrics, and the characteristics and motivations of the population which will be exposed to the biometric system in order to design effective systems.

If they're deployed as a "magic bullet," without proper thought to their inherent properties and limitations, biometric technologies can weaken authentication, create serious operational problems, alienate users, and infringe privacy rights. But if they're used in the context of a carefully designed identification or authentication system, biometrics can perform better than alternative technologies.

Analysis

Interest in biometric authentication and identification has increased over the past decade in response to: weaknesses in other widely deployed authentication systems (including passwords), improvements in biometric sensor and matching technology, and heightened focus on strong authentication following the terrorist attacks on the United States in 2001.

When used in the context of a carefully designed identification or authentication system, biometrics can perform better than alternative technologies. When deployed as a "magic bullet," without proper thought to their inherent properties and limitations, biometric technologies can weaken authentication, create serious operational problems, alienate users, and infringe privacy rights.

Proper use of biometrics requires an understanding of how biometric matching relates to identification and authentication, how biometrics differ from other authentication technologies, how the statistics of biometric matching depend on both the characteristics of the population which will use the biometric system and on the system's objectives, how environmental factors affect the performance of biometric sensors, and how biometric systems can fail.

Careful design of the entire system of which biometrics is a part can produce robust, effective authentication and identification. Neglecting the properties which make biometrics different from more-traditional authentication technologies can create spectacular failures.

Biometrics

Biometrics is the theory and practice of automatically recognizing an individual based on biological and behavioral traits. Biometrics has a long history, starting in the 1880's with the Bertillon system of body measurements and the fingerprint identification system of Henry Faulds.

Biometric Traits

Today's biometric systems measure a broad range of physical and behavioral traits including fingerprints, iris characteristics, vein patterns of the retina, geometry of the hand, facial geometry, characteristics of selected locations of DNA, dynamics of typed keystrokes, dynamics of movement when signing, dynamics of gait when walking, and acoustics of the voice.

A biometric system which relies on measuring a single biometric trait is said to be "unimodal." A biometric system which measures several biometric traits is said to be "multimodal."

Biometric traits are selected on the basis of two properties: *distinctiveness* and *stability*.

If two individuals are very likely to be distinguishable on the basis of a particular trait, that trait is said to be highly distinctive.

Hand geometry is not especially distinctive; that is, it's somewhat likely that two individuals selected at random will have hands of similar size and shape. Fingerprints are fairly distinctive; that is, it's fairly unlikely that two individuals selected at random will have very similar patterns of friction ridges on the surfaces of all 10 fingers. DNA profiles are extremely distinctive; the probability that two individuals selected at random will have the same DNA subsequences at a standard collection of probe locations is extremely small.

Rigorous scientific studies have quantified the distinctiveness of DNA profiles; most other biometric modalities have not been subjected to similarly rigorous studies, and as a result the distinctiveness of those modalities is much less well established. Fingerprints, surprisingly, have not been subjected to extensive distinctiveness studies, although their use in identification dates back more than a century.

If a particular biometric trait does not change or changes very slowly over an individual's lifetime, the trait is said to be stable.

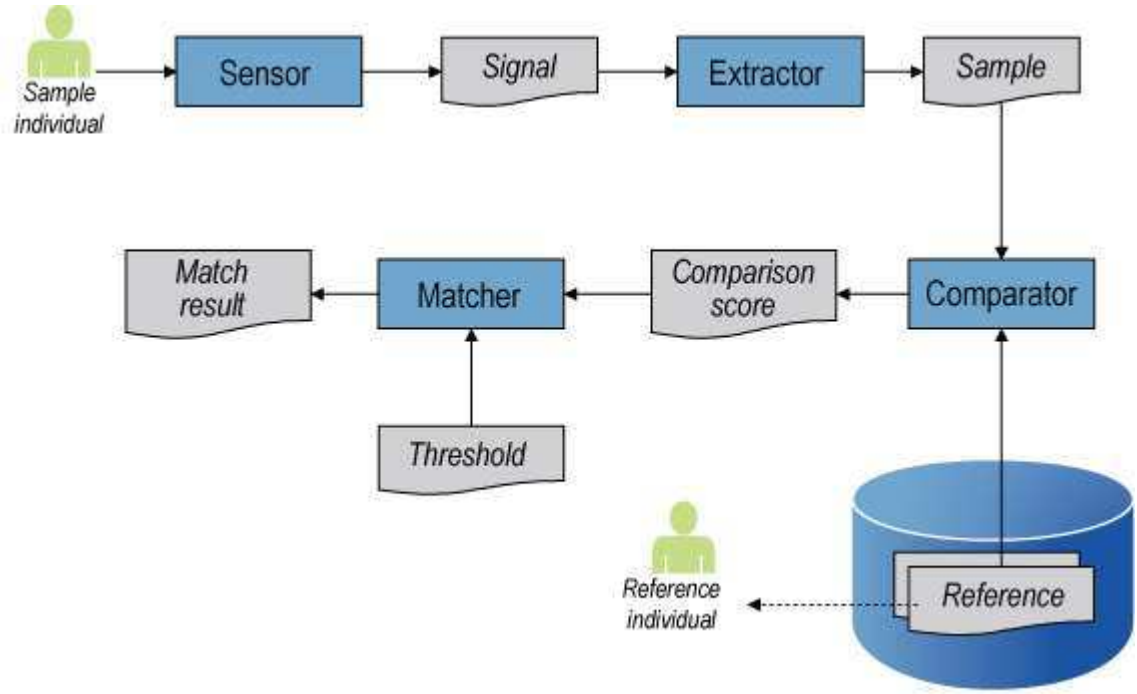
Some traits are not very stable. The geometry of faces and hands changes over time, especially among young subjects. Voice dynamics can change as a result of colds, injuries, neurological disorders, strokes, or other events. Keystroke dynamics can change as a result of training, keyboard differences, or other factors. Gait can change as a result of injuries, pain, or new shoes.

Other traits are very stable. DNA subsequences at locations probed by DNA profiling systems do not change over an individual's lifetime.

The Structure of a Biometric System

The structure of a biometric system is illustrated in Figure 1.

Figure 1. The Structure of a Biometric System



A biometric system has a *front end* consisting of a sensor and some associated logic and a *back end* consisting of a feature extractor, a sample comparator, a database of biometric references against which samples collected by the sensor are compared, and a matcher, which determines whether the output of the comparator should be considered a match or a non-match.

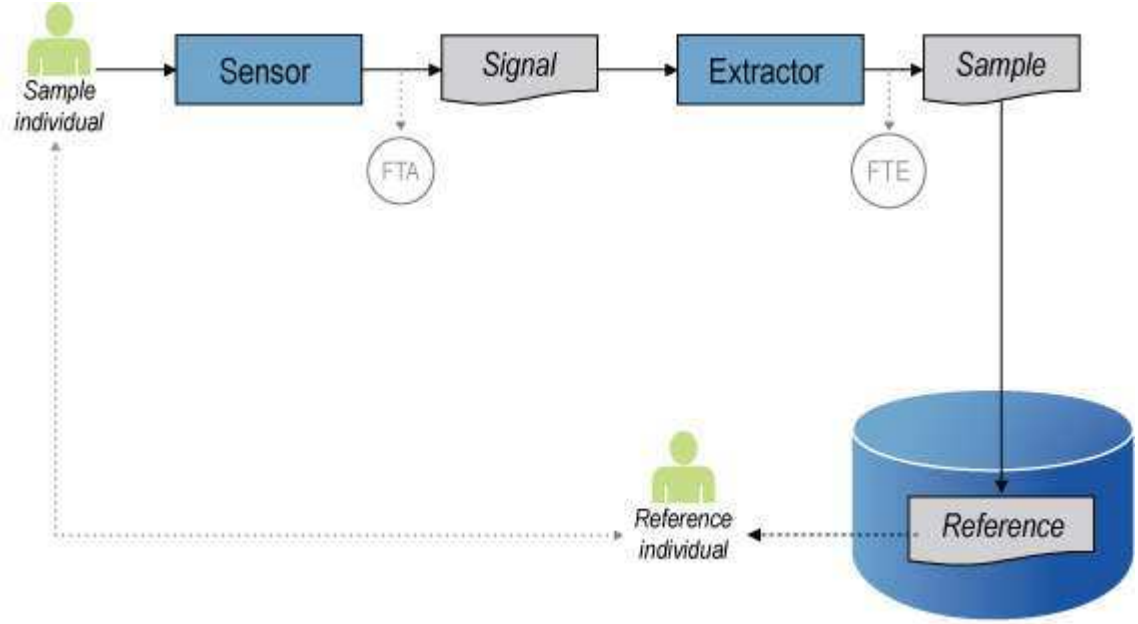
The Biometric Process

Biometric systems are used as part of a process of generating matches between samples observed by biometric sensors and references representing individuals who have previously been enrolled in the system.

Enrollment

The process of biometric matching begins with enrollment. Enrollment is illustrated in Figure 2. Each subject who needs to be recognized by the biometric system must be enrolled in the system and associated with a "reference." The reference is the system's baseline measurement of the subject's biometric traits of interest.

Figure 2. Biometric System Enrollment



Two types of failures are possible during enrollment. The first is failure to acquire (FTA). This failure occurs when the sensor is unable to detect the trait which it is designed to

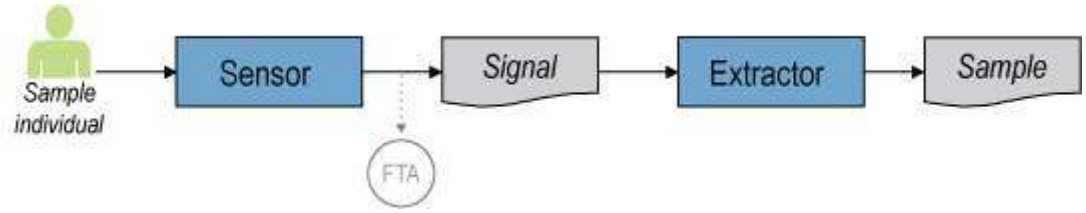
recognize. This can happen for a variety of reasons, including the absence of the trait (for example, when a fingerprint detector is used to image the finger of a subject whose fingerprints have been worn off through manual labor) and presence of environmental factors such as dirt which degrade the signal received by the sensor.

The second type of failure is failure to enroll (FTE). This failure occurs when the sensor generates a signal, but the quality of the signal is not sufficient to generate a valid biometric reference. In the case of fingerprints, this can happen when the sensor detects a finger image but cannot recognize the minimum number of minutiae—the characteristics of the patterns of friction ridges which are used as the basis for comparing fingerprints—necessary to create a reference. Biometric modalities other than DNA all have FTE rates larger than zero because some individuals do not display the trait recognized by the sensor for that modality (e.g., people without fingers do not have fingerprints; people without eyes don't have irises or retinal veins; mutes do not have voices to recognize; paraplegics do not walk and so do not have gait dynamics, and so on).

Sampling

Once a set of references has been generated by enrolling all the subjects in the population of interest, a biometric system can be used to recognize individuals in that population. The process of recognition starts with sampling, which is illustrated in Figure 3.

Figure 3. Biometric Sampling



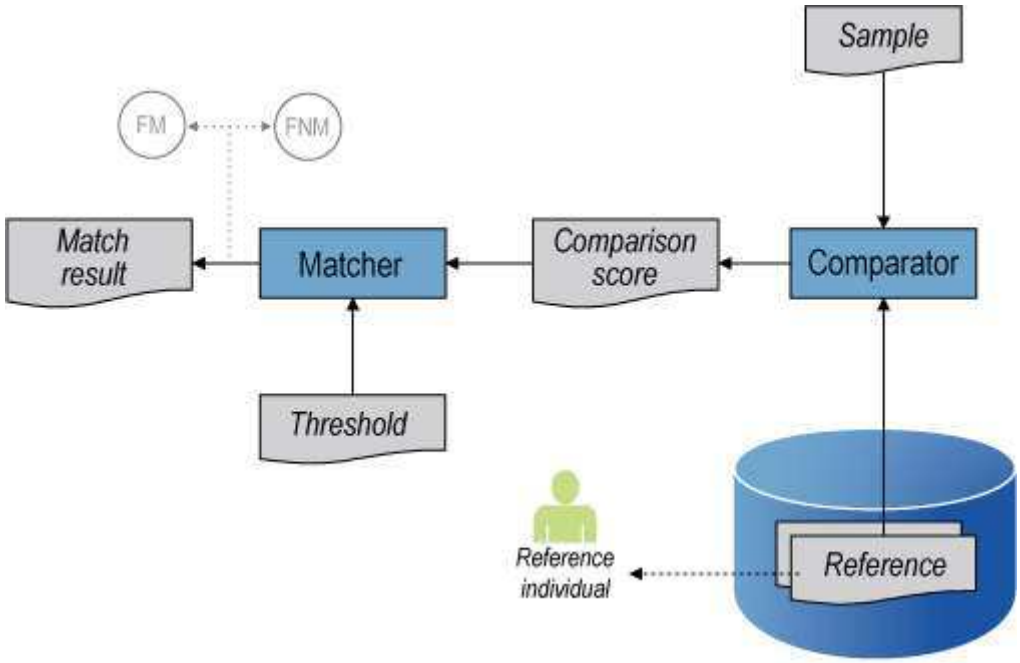
A sample is generated by extracting *features* from the signal generated when a biometric sensor observes a subject's biometric traits. In a fingerprint-recognition system, the trait is the pattern of friction ridges on the surface of the subject's fingers; the signal is a picture of the subject's fingertip which has been converted to a digital format by an analog-to-digital converter. The features are "minutiae" (loops, whorls, ridge endings, bifurcations, and so on) which are used to distinguish one fingerprint from another. Minutiae are extracted from the signal by an "extractor" algorithm which creates a "sample" by arranging the list of extracted features (minutiae) in a standard format.

Sampling can fail due to an FTA. As in the enrollment process, this can occur either because the sampled subject does not display the trait the sensor is designed to detect or because environmental factors degrade the signal.

Matching

Once a sample has been generated, the biometric system's back end attempts to match the sample to one or more references representing subjects who have been enrolled in the system. The matching process is illustrated in Figure 4.

Figure 4. Biometric Matching



Matching starts with a comparison of the sample against one or more references from the biometric system's database. When a biometric system is used to verify a subject's claimed identity, the comparator compares the sample against the reference representing the identity claimed by the subject. When the biometric system is used to try to identify an individual who has not claimed any particular identity, the system may compare the sample against several references or even against all the references in its database.

Each comparison of a sample against a reference generates a *comparison score*. The comparison score is a measurement of how similar the features in the sample are to those in the reference. The more similar the sample is to the reference, the more likely it is that the sample and the reference represent the same individual.

It is extremely important to recognize that biometric systems do not establish identity in an absolute sense. Instead, biometric systems provide an estimate of the probability that a sample and a reference resulted from two different observations of the same individual. For some biometric modalities, some individuals, and some pairs of observations, this probability may be very high, so that the probability that the individual has not been correctly identified by the system is only one in millions or billions, but it is never a certainty. In other words, the comparison score—expressed as a probability—is always less than 1.0.

Because the comparison score is always less than 1.0, the designer of a biometric system must choose a *threshold*. A comparison score at or above the threshold will be considered a *match* between a sample and a reference, while a comparison score below the threshold will be considered a *non-match*. The biometric system uses a matcher to apply the threshold to comparison scores and declare *match results* (i.e., to declare that a comparison has resulted in a match or in a non-match).

Because comparisons are probabilistic and thresholds are set arbitrarily, two kinds of failures can occur during matching: a *false match* (FM) and a *false non-match* (FNM). A false match occurs when a sample taken from one subject and a reference taken from a different subject are similar enough that the comparison score exceeds the matcher's threshold. A false non-match occurs when a sample taken from an individual and a reference taken from the same individual are different enough that the comparison score is lower than the matcher's threshold.

Applications of Matching

Biometric matching can be used to achieve a variety of identification and authentication goals.

Verification

The biometric literature uses the term "verification" to refer to the same process security professionals call "authentication." A biometric system is said to "verify" a subject's

claimed identity when the subject's biometric sample is compared against the reference sample for the claimed identity and a match is declared.

A false match (FM) in a verification application incorrectly recognizes an impostor as the subject whose identity he claims. A false non-match (FNM) in a verification application incorrectly rejects an enrolled subject's claim to the identity she enrolled.

An FM in a verification application incorrectly recognizes an impostor as the subject whose identity he claims. An FNM in a verification application incorrectly rejects an enrolled subject's claim to the identity he enrolled.

Like authentication, verification requires the subject to claim an identity in advance. It's easy to draw analogies between biometric systems and other authentication systems, but these analogies are misleading in one important respect. While biometric verification is similar to other authentication processes in that it compares evidence gathered from the subject after the subject claims an identity against a piece of evidence created at the time the subject was enrolled, there is a crucial difference. Most authentication systems depend for their security on maintaining the secrecy of the sample and reference evidence (the "authentication data"); passwords and cryptographic keys, for example, must be secret if an authentication system which relies on them is to function securely.

Biometric traits, on the other hand, are not secret and cannot, in principle, be made secret. The appearance of your face is visible to (and photographable by) the public. The sound of your voice can be recorded. Your gait can be modeled using a videotape of you walking. The pattern of tissue in your iris can be photographed; even a 35mm film picture of your face and upper body contains enough iris detail to identify you biometrically. Steve McCurry and *National Geographic* demonstrated this when they used McCurry's famous "Afghan Girl" cover photograph to locate and identify Sharbat Gula 17 years after the original picture was taken.[1]

Biometric verification systems do not and cannot depend on the secrecy of biometric traits for their proper functioning. They rely instead on the presumed difficulty of impersonating a living person who is presenting an actual physical trait to the biometric system's sensor. For this reason, unattended biometric sensors and sensors with weak presence and liveness detection capabilities are significantly more susceptible to impersonation attacks than are attended systems with robust presence and liveness detection.

Identification

A biometric system is said to *identify* a subject when the system compares the subject's biometric sample to a reference sample, a match is declared, and the identity of the subject corresponding to the matched reference is associated with the sampled subject.

Biometric identification can be divided into two cases: *closed-set identification* and *open-set identification*.

In the case of closed-set identification, the sampled subject is known or assumed to be represented by a reference in the system's database; the problem in this case is to determine which subject's reference most closely matches the sample. An FM in a closed-set identification application falsely recognizes one enrolled subject as a different subject. An FNM in a closed-set identification application incorrectly classifies a known subject as unknown.

In the case of open-set identification, it is not known whether the sampled subject is represented by a reference in the system's database. In this case, the problem is more complicated; the system has to determine whether the sample matches any subject in the database, and if so, which subject it matches most closely. An FM in an open-set identification application falsely recognizes one enrolled subject as another enrolled subject, or falsely recognizes an unknown subject as an enrolled subject. An FNM in an open-set identification application falsely classifies a known subject as unknown.

Screening

A biometric system is said to "screen" subjects when it checks to see whether a subject's sample matches any reference in the system's database.

A biometric system implements *whitelist screening* when it requires a subject's sample to match a previously enrolled reference before granting the subject access or privilege. In whitelist screening, subjects on the whitelist are enrolled in the biometric database.

An FM in a whitelist screening application grants an unauthorized subject access; an FNM denies an authorized subject access.

A biometric system implements *blacklist screening* when it denies a subject access or privilege because the subject's sample matches a previously enrolled reference. In blacklist screening, subjects on the blacklist are enrolled in the biometric database.

Measuring the Accuracy of Biometric Matching

Vendors and researchers use a variety of metrics to describe the accuracy of biometric systems. Some of these metrics are more useful than others.

In general, the least ambiguous and most useful metrics are the match and non-match rates: true match rate (TMR), false match rate (FMR), true non-match rate (TNMR), and false non-match rate (FNMR).

"False accept rate" (FAR) and "false reject rate" (FRR) are difficult to interpret because "accept" and "reject" have different definitions in different applications. When a whitelist screening application "rejects" a subject, it does so because it has *failed* to match the subject. But when a blacklist screening application "rejects" a subject, it does so because it has *succeeded* in matching the subject. A single biometric (that is, a system with identical sensors, comparators, databases, and matchers) may therefore have different FAR and FRR values when it is used for whitelist screening than it does when it is used for blacklist screening.

When a biometric system is tuned so that its FMR is equal to its FNMR, the common value of both these rates is called the "equal error rate" (EER). The problem with this metric is that it measures the system in a configuration which is almost certain not to be the configuration of use. Almost all biometric systems are tuned to avoid either FMs or FNMs—a system which is tuned to make the FM and FNM probabilities equal is rarely practically useful.

Plotting a biometric system's True Positive Rate (TPR) against its false positive rate (FPR) results in a graph called a receiver operating characteristic (ROC) curve. Interpretation of ROC curves requires some experience, but ROC curves do provide useful information in choosing thresholds for the system's matcher. Plotting ROC curves requires careful attention to the definition of "positive"—because a biometric match may be either a positive or a negative, depending on the application to which biometrics is applied.

When predicting the performance of a biometric system, it is important to understand the statistical properties of the population to which the system will be exposed. Error rates are easier to estimate in a closed population (i.e., a population all of whose members are enrolled in the biometric system) than in an open population (i.e., a population in which some individuals who try to access the system have not been enrolled). It's easy to see why this is so. In a closed population, we can in principle compare every subject's reference against every other subject's reference and determine the comparison score of the two most similar references; this helps to set a match threshold which balances FMR and FNMR optimally. In an open population, on the other hand, we cannot estimate in advance how similar the next unenrolled subject might be to a randomly selected enrolled subject.

The Base Rate Fallacy

A problem which illustrates the importance of understanding population statistics occurs when implementing blacklist screening in a large, open population. If the population has a million subjects and half of them are on the blacklist, and the biometric system in question has been tuned to have FMR and FNMR of 0.01%, and if 100,000 randomly selected subjects a year present themselves to the biometric system, the system will see 50,000 people on the blacklist and 50,000 "innocents." This will result in the following statistics:

49,995 true blacklist matches (= suspects arrested)
5 false blacklist matches (= innocents arrested)
49,995 true blacklist non-matches (= innocents allowed to pass)
5 false blacklist non-matches (= suspects allowed to pass)

This is pretty good performance; almost all the arrested subjects are suspects, and almost all those allowed to pass are innocents. But if the 100,000 subject population includes five people on the blacklist and 99,995 innocents, the statistics look very different:

5 true blacklist matches (= suspects arrested)
10 false blacklist matches (= innocents arrested)
99,985 true blacklist non-matches (= innocents allowed to pass)
0 false blacklist non-matches (= suspects allowed to pass)

In this case, all those allowed to pass are innocents, but two-thirds of those arrested are also innocents. As the population gets larger, this problem, which is called the "base rate fallacy," gets worse. Screening applications generate many more false positives than true positives in large populations which contain very small numbers of suspects. A system designer who is not aware of the population statistics—or who does not understand how population statistics influence system performance—will not design an appropriate secondary screening mechanism and will subject large numbers of innocents to investigation and other costs and inconveniences. Over time, this will undermine confidence in the system.

Design Criteria Other Than Matching Accuracy

Designers of biometric systems must make many engineering tradeoffs between conflicting requirements.

Biometric systems modalities which have low error rates often have slow sensors or matchers (DNA profiling, for example, is much more accurate than face recognition but also much slower). But many biometric systems have high throughput requirements—they must process large numbers of subjects in a fairly small interval of time. Some tradeoff between throughput and accuracy of matching may be required.

Some biometric modalities are highly sensitive to environmental factors. Face-recognition systems are sensitive to lighting conditions, presence or absence of facial hair and sunglasses, and so on. DNA sensors are sensitive to the presence of tissue from individuals other than the subject being presented to the sensor. Voice recognition systems are sensitive to ambient noise. Controlling environmental factors may be difficult in some settings, and environmental controls may also reduce system throughput.

Uncooperative users can significantly degrade the performance of a biometric system by creating environmental conditions which are not conducive to recognition (e.g., by concealing traits from the sensor). Designers of biometric systems must take care to create conditions which encourage users to cooperate with the system.

Even cooperative users may not be adept at using biometric systems. A field trial of a fingerprint system in the United States showed that even users who had used the system successfully at enrollment time found a surprising number of ways to present themselves to the sensor incorrectly when it came time to be recognized. Users presented the wrong finger, the wrong surface of the finger, the wrong part of the hand, or the wrong finger orientation (e.g., sideways). They tapped or swiped the sensor rather than pressing the finger down on it. Some users even attempted to present their eyes to the fingerprint sensor. Effective training and education of users, coupled with intuitive design of sensors, is important for successful deployment of a biometric system.

Unattended sensors present attackers more opportunities for spoofing and subversion than attended sensors. An attendant can check to see whether the user is avoiding presentation of a trait to the sensor, sabotaging the sensor, or presenting some sort of picture or model to the sensor instead of an actual body part. Unattended sensors have to rely on less-flexible and less-effective automated presence and liveness detection algorithms to detect these types of attacks.

Sensors which are physically remote from comparators and matchers often present exposed network connections to attackers who may try to prevent legitimate traffic from reaching the comparator, or who may try to inject replays or synthetic data into the data stream received by the comparator.

All biometric systems generate FMs and FNMs. All biometric systems (with the possible exception of DNA) fail to enroll some subjects. For these reasons, biometric systems must incorporate secondary screening procedures and backup identification or authentication processes. If these secondary and backup processes are less reliable and less secure than the biometric components of the system, attackers will exploit the situation by preventing the biometric system from acquiring a sample in order to force the larger system, of which biometrics are a component, into one of its less-reliable alternate modes.

Recommendations

Biometric systems are not drop-in replacements for other types of authentication systems. They present designers with different opportunities and problems, and they require different user behavior. A deployment of biometrics for authentication or identification will be successful only if designers understand and exploit the strengths of biometrics while avoiding the weaknesses.

Get User Buy-In

Biometrics require subjects to expose themselves in some way to a sensor. Subjects who are aware that biometrics are in use and object to that use can easily hide their traits from the system's sensors. It's critical, therefore, to get users to buy in before deploying a biometric system. Various objections may be raised to the use of biometrics, including:

- Biometrics will invade my privacy
- Biometrics will be used to track my behavior and punish me
- Biometrics are "creepy"
- Biometrics violate my religious beliefs
- Biometrics will be used to enroll me in a government database

These objections must be taken seriously and addressed in a fair, respectful, and transparent way. The designers of the system must be made available for conversations with future users of the system and must make the system's goals and non-goals clear. System designers must also respond constructively to user objections and communicate clearly about changes they make in response to those objections.

Know What Application You're Implementing

As noted in the "Applications of Matching" section of this overview, design criteria for biometric systems will vary widely depending on the application that biometrics are deployed to support. System designers must be clear about their goals; they must decide whether they want:

- A verification (i.e., authentication) system
- A closed-set identification system
- An open-set identification system
- A closed-set whitelist screening system
- An open-set whitelist screening system
- A closed-set blacklist screening system
- An open-set blacklist screening system

Decisions about FMR/FNMR tradeoffs, secondary screening procedures, backup authentication processes, attended versus unattended operation, and system throughput goals need to be made based on the required operational characteristics of the system and on the known properties of the population which will be exposed to the system after it is deployed.

Focus on the System, Not the Sensor

Too many biometrics requests for proposal (RFPs) focus on the FMR and FNMR of the sensor to the exclusion of most other concerns. System concerns are much more important than sensor concerns in real systems. System concerns which should be considered include:

- Mean-time-to-failure of system components including sensors
- Time to recognize a single user
- Sensitivity of the system to environmental factors
- Percentage of population which does not display the traits recognized by the system
- Percentage of the population which is expected to present themselves to a sensor before they have enrolled
- Ease of use of sensors
- Ease of enrollment
- Time and cost to enroll a user
- FTE rate
- Scalability of the reference database, including the rate at which response time degrades as the population grows
- Distinctiveness and stability of the chosen biometric traits
- Cost, performance, and reliability of secondary screening process
- Cost, performance, and reliability of backup authentication process
- Cost of operating sensors in attended mode
- Security requirements for enabling use of unattended sensors

- Security requirements for enabling use of remote sensors
- Separation of communications between biometric system components and other network traffic
- "Future-proofness" of the biometric reference format
- Process for responding to subpoenas
- Process and infrastructure for testing and auditing the operation of the biometric system
- Process for generating alerts if the system becomes inactive or senses an attack
- Threat model (who is likely to attack the system, and what are the likely attackers' motivations?)
- Vulnerability assessment (what attacks on the system are likely to succeed, and what are the consequences of a successful attack?)

Understand the Statistics and Design the System Around Them

Biometrics don't identify people with certainty; they identify people probabilistically. This means that every biometric match carries with it a usually small but always nonzero probability of falsehood. The designers of a biometric system must understand both the population statistics and the system performance statistics in order to analyze how often an FM or FNM will occur in actual use. Once the FM and FNM rates are understood, a careful risk analysis should be conducted to determine how effectively a proposed biometric system addresses the risks it is designed to control.

Pay Attention to Throughput

Biometric systems are often used to control access to facilities. Most access situations have throughput requirements; building entry control systems, for example, must usually perform efficiently enough to allow most of the inhabitants of a building to enter during the half-hour before a work shift begins. A biometric building access control system must be designed with enough sensors to support this volume of traffic. Throughput restrictions can result from sensors which are slow to acquire signals, from environmental interference with the ability of sensors to acquire signals, from communications bottlenecks between sensors and back-end elements of the biometric system, and from insufficiently scalable databases or comparators. A significant number of biometric system failures have been attributable to inability to support throughput requirements. Biometric system designers should model throughput carefully during the design phase and should stress-test the system prior to deployment.

Control the Sensor Environment

Many biometric sensors perform poorly in "noisy" environments. Voice-recognition sensors have trouble with certain kinds of ambient noise; face- and iris-recognition systems have trouble in poor lighting; fingerprint-sensor performance can be degraded by dirt and oil on the sensor's surface. The environment surrounding biometric system sensors should be designed to be "sensor friendly" and should be examined periodically to ensure that system performance isn't being compromised by environmental conditions.

Prefer Local and Attended Sensors

The use of sensors which are located far from the biometric system's back-end elements exposes the biometric system to additional risks. Remote sensors require transmission of sensor signal data across a network. They also require physical security measures to protect against sensor tampering, and they are susceptible to spoofing attacks in which a fake sensor is positioned in front of the real sensor in an attempt to capture and duplicate user traits.

Unattended sensors also create risks. Attackers can more easily fool sensors with images or models of authorized users' biometric traits if they do not also have to fool a human attendant. Unattended sensors can be physically attacked for extended periods of time or attacked using sophisticated tools.

Systems which use attended sensors close to the biometric system back end create fewer risks and thus present system designers with less-complicated problems.

Design a Robust Backup System

Attackers don't have to defeat biometrics if they can confuse a biometric system and force a larger system within which a biometric subsystem operates into a weaker backup mode. If, for example, a fingerprint sensor is used to control the operation of a gate leading into a facility, but users whose fingerprints aren't recognized are allowed to enter a pin code

into a keypad to gain access—and if all users are given the same four-digit pin— then there is a good chance that the pin will fall into an attacker's hands, and the attacker will simply bypass the fingerprint check and use the pin to open the gate.

Mechanisms used as backups for biometrics should generally be designed to assume that a failure of the biometric system to make an access decision about a subject is a suspicious event; the backup procedure probably should be manually attended and involve some sort of strong authentication. In the gate-control example (see previous paragraph), a reasonable backup procedure might be to require any subject not recognized by the fingerprint sensor to display a high-quality photo ID to a human guard, who would then call a manager to verify the right of the subject to enter the facility.

Do Not Assume That Biometric Traits Are Secrets

Biometric traits are not secret. They cannot be secret. If you ever find yourself thinking that (1) you need to encrypt biometric samples on the wire to keep them secret [as opposed to, for example, applying a keyed hash to them to keep an attacker from modifying them in transit], (2) you need to encrypt biometric references in the database, (3) you need to "reissue" a biometric to a user because the contents of the database have been publicized, or (4) you need to "reissue" a biometric because someone has captured user traits by subverting a sensor or putting up a counterfeit sensor—STOP! THINK AGAIN!

These groundless fears arise from one of three mistaken assumptions:

1. The assumption that because passwords used to authenticate subjects must be kept secret, biometric traits used to authenticate subjects must also be kept secret. This assumption is false because biometric authentication is not based on a subject establishing that his mind is the only mind that knows a particular secret; biometric authentication is based on a subject establishing that his body is the only body that exhibits a particular trait. Biometric traits are chosen for distinctiveness; the only way an attacker can fool a biometric sensor is by tricking it into thinking that an image of someone else's body is actually part of the attacker's body. Defeating the attacker is not accomplished by covering the legitimate subject's body to prevent the attacker from observing it. Defeating the attacker is accomplished by revealing the attacker's body so that the biometric sensor can sense its true traits rather than the disguises the attacker tries to use to fool the sensor. Automated methods for revealing the attacker's body are called "presence and liveness" tests. Manual methods, however, are more effective than automated methods. When criminal suspects are fingerprinted in police stations, a trained booking officer (not the suspect) cleans and inspects the suspect's finger and then places the suspect's finger on the sensor in the correct orientation. This process is extremely reliable; and it's very hard for suspects to fool the sensor.
2. The assumption that possession of an image of a subject's biometric trait enables an attacker to impersonate the subject by presenting that image to a biometric sensor. Here again, the solution is not to cover the legitimate subject's body; it is to reveal the attacker's body either by supervision or by presence and liveness testing.
3. The assumption that possession of a digitized copy of a subject's biometric sample enables an attacker to impersonate the subject by bypassing a biometric sensor and presenting the digitized sample directly to a comparator. This is true only if the communications system has been designed in a way that leaves it open to active or passive wiretapping attacks or replays. The solution to these problems is to ensure that attackers cannot access the network segments carrying traffic between components of the biometric system. This can be done either by isolating the network segment in question or by cryptographically authenticating system components to one another and using strong cryptographic protocols to protect the integrity (not the secrecy!) of intra-system communications.

Pay Attention to Presence and Liveness

Presence and liveness tests protect biometric systems against impersonation of subjects by attackers who have acquired images of a legitimate subject's traits, as explained in the previous recommendation. System designers need to ensure that presence and liveness tests are effective in preventing impersonation attacks on sensors.

Protect Communications Against Spoofing

Protecting communications integrity and ensuring that biometric system components are strongly authenticated to one another protects the system against active and passive wiretapping and against replay attacks, as noted above.

Educate and Train the Users

Many people are confused by biometric sensors; their confusion causes them to behave in ways which make it difficult for a biometric sensor to acquire a usable image of their biometric traits. People present the wrong body part to the sensor, or they present the right body part in the wrong orientation, or they don't stand still long enough for the sensor to acquire an image, or they do any number of other amusing and confounding things.

Training users to properly present themselves to a sensor, what to expect after they have presented themselves to the sensor, and teaching them what to do if the sensor fails to recognize them, can substantially improve both a biometric system's accuracy of identification and its throughput.

Test Before Going Live

Biometric systems are sensitive to environmental factors and user behavior. Laboratory models of biometric system performance seldom accurately reflect performance in the field under operational conditions. Leave ample time for field testing of the system before it is put into production. Make sure you test the system under a variety of environmental conditions (e.g., rain, wind, darkness, direct sunlight, dust, high and low humidity) and at scales which resemble the load the system will encounter at peak times during operation. Test both success conditions (e.g., legitimate subjects presenting themselves to the system) and failure conditions (e.g., attackers trying to subvert the system or innocent but unauthorized users presenting themselves to the system). Test enrollment and disenrollment procedures. Test backup authentication methods and secondary screening processes. Test using a population which resembles (statistically, physically, and in terms of system training) the population the system will encounter when it is operational.

The Details

A wide variety of biometric sensors are now available; these sensors recognize different biometric traits and have different operational parameters.

Biometric Modalities

A biometric modality is a biometric system which recognizes a specific biometric trait. Fingerprint identification is one modality; voice recognition is another. Some biometric systems are multimodal; that is, they declare a match only when a subject matches references in two or more modalities. Multimodal systems are usually deployed either because the match rate achievable using a single modality is deemed to be insufficient for the intended application or because forcing an attacker to spoof the system in two modalities simultaneously presents the attacker with a harder problem than attacking a single modality.

The most-commonly used biometric today is fingerprints. The population statistics of fingerprint identification have not been subjected to extensive scientific study, but fingerprints appear to be quite distinctive and fairly stable (absent injuries, occupational wear, or loss of fingers). Acquisition of finger images is fast and not very invasive. Fingerprints have some "creepiness" and user opposition issues, most of which stem from the fact that local, state, national, and international criminal justice organizations maintain extensive databases of fingerprint images, and people (rightly or wrongly) fear that images captured by a biometric sensor in the workplace or elsewhere will find their way into, or will be matched against, criminal justice databases.

Hand geometry (i.e., measurement of the shape and size of the hand and fingers) is less distinctive than fingerprints and is only moderately stable. Hand-geometry sensors are not very invasive, but they often take longer to acquire an image than do fingerprint sensors. Training users to properly present their hands to a hand-geometry sensor can be difficult. Hand-geometry sensors are not especially creepy, but subjects may have concerns about hygiene.

Until recently, face-recognition systems have not been very accurate, but they can acquire images very quickly and with minimal user cooperation. The fact that a face-recognition sensor can acquire an image stealthily and without user consent contributes to a degree of creepiness. Two-dimensional face images are not highly distinctive. Faces are also less stable than many other biometric traits in part because of the ability of subjects to cover or disguise parts of their faces. New face-recognition systems which capture three-

dimensional images appear to be capable of more accurate recognition than older, two-dimensional face-recognition technologies.

Iris-recognition systems capture images reasonably quickly, though when compared to some other biometrics, their performance is more affected by lighting conditions and subject position and orientation. Collection of iris images is minimally intrusive and images can be captured at a distance without shining bright lights into a subject's eyes. Iris-recognition systems are moderately creepy; sensors which require subjects to bring their eyes close to an imager are often mistaken for retinal scanners, and subjects worry that lasers will be shone into their eyes. Sensors which capture iris images remotely are subject to objections based on lack of use consent. Iris structures recognized by iris-recognition sensors appear to be quite stable and quite distinctive.

Retina scanners are rarely used today. They recognize patterns of veins in a subject's retinas by shining a laser or other bright light onto the retina through the pupil. Subjects find this imaging technique creepy, scary, and sometimes painful. The collection of retinal images is slow compared to face recognition and fingerprint imaging, and collection is quite sensitive to environmental conditions, including subject positioning. Retinal vein patterns are only moderately stable and, furthermore, sometimes change because of disease conditions; this raises privacy concerns.

Voice samples can be collected noninvasively, though signal quality can be degraded by environmental noise. Voice dynamics are only moderately stable and moderately distinctive, and a voice is easier to spoof (using, for example, a high-fidelity recording) than some other biometric traits. Collection of voice samples is not especially quick, as a reasonably lengthy sample may be necessary for good identification performance. On the other hand, voice samples can be collected in parallel with performance of a transaction (especially over voice channels such as telephones) in a way which is minimally disruptive. Recording voice information over telecommunications channels is often subject to legal restrictions, including requirements to obtain consent. Voice recognition is not especially creepy.

Gait dynamics measures the motion of subjects as they walk. Gait dynamics are not especially distinctive and also not especially stable. Environmental factors like surface texture and footwear can influence gait dynamics. Collection of gait dynamics samples is relatively slow as subjects have to be observed taking several steps. On the other hand, collection can be minimally invasive or even stealthy, which gives rise to some level of creepiness.

DNA profiles are extremely distinctive and extremely stable. Collection of DNA samples is very slow and somewhat invasive compared to other biometrics. DNA is considered a quite creepy biometric, in part because of the invasiveness of collection, in part because of its association with criminal forensics (criminal justice organizations in many countries maintain large databases of criminal convict and sometimes suspect DNA profiles), and in part because of a largely (but not entirely) unfounded belief that disease status and heredity can be inferred from DNA profiles. DNA as a biometric is quite sensitive to environmental conditions; contamination of a subject sample with even a small amount of tissue from other individuals (including individuals who collect the sample) or from the natural environment, which contains a lot of DNA, can destroy the usefulness of the sample.

Attacks on Biometric Systems

Biometric systems can be attacked at a variety of points to achieve a variety of attacker goals.

Attack Goals

Attacks on biometric systems aim to achieve one or more of three goals: impersonation, evasion, and degradation.

Impersonation attacks aim to fool the system into falsely declaring a match between an attacker and some other individual represented by a reference in the database.

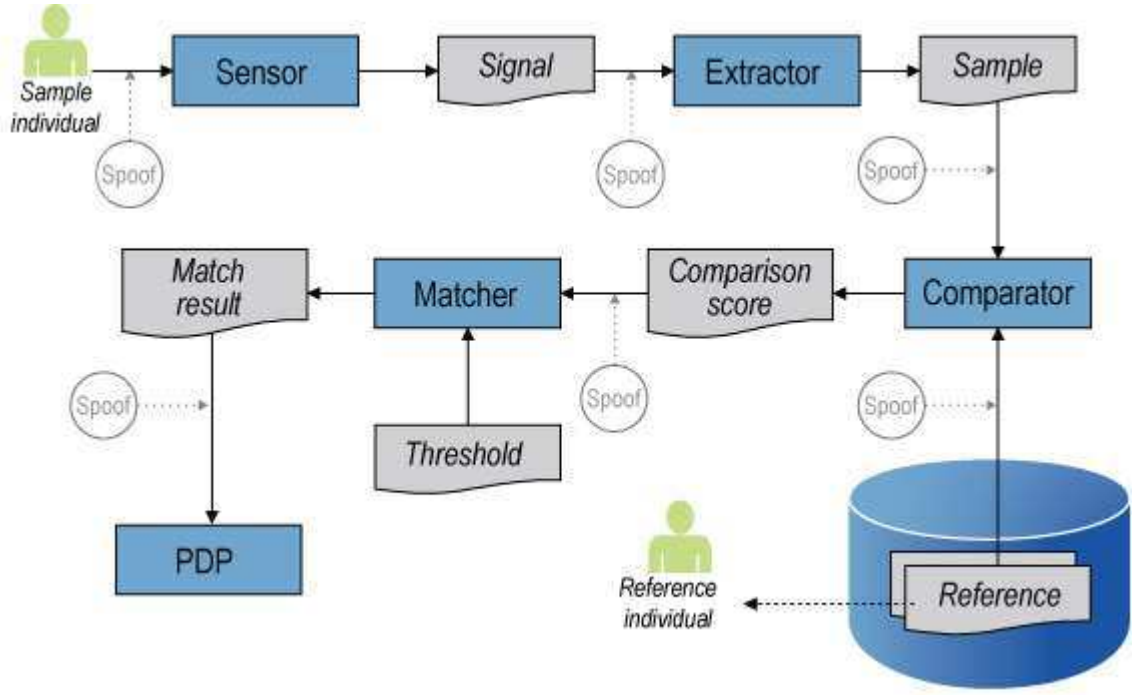
Evasion attacks aim to fool the system into falsely declaring a non-match when, in fact, the attacker is represented by a reference in the database.

Degradation attacks aim to impair the system's performance to a degree which either forces the system's operators to stop using it and switch to a presumably less-accurate or more-easily circumvented backup system or denies access to some resource by degrading the system's performance to an extent which prevents legitimate users from being authenticated and allowed to use the system.

Attack Points

Figure 5 illustrates the points in a biometric system which might be attacked.

Figure 5. Locations of Attacks on Biometric Systems



Spoofing the sensor is achieved by presenting something which is not actually a trait of the attacker's own body to the sensor, or attempting to replace the sensor with a subverted sensor which will send a signal chosen by the attacker to the biometric system's back end, or attempting to interpose a rogue sensor between legitimate subjects and the real sensor with the intent of performing a session-splicing attack and piggybacking attacker traffic on the legitimate subject's biometric authentication, or by introducing environmental noise intended to prevent the sensor from acquiring a usable image of the attacker's biometric trait.

Spoofing the extractor is achieved by corrupting the data stream sent from the sensor to the extractor either to replay an image of a legitimate subject's biometric trait or to transmit an unrecognizable image in place of an actual image of the attacker's biometric trait.

Spoofing the comparator is achieved by corrupting the data stream sent from the extractor to the comparator to replay a sample representing a legitimate subject or to transmit a sample which is unlikely to match any reference in the database in place of the attacker's sample.

Spoofing the database is achieved by corrupting the contents of the database to introduce or remove references which will match attackers or by corrupting the data stream sent from the database to the comparator to replay a reference which will match the attacker's sample or to replay a reference which is unlikely to match the attacker's sample.

Spoofing the comparator is achieved by corrupting the data stream between the comparator and the matcher to replay a score which will be declared a match, or to replay a score which will be declared a non-match.

Spoofing the matcher is achieved by corrupting the data stream between the matcher and the application's Policy Decision Point (PDP) to replay a match or non-match decision.

Conclusion

Biometrics differ in important ways from other authentication technologies. System designers who use biometrics to authenticate, identify, or screen users in order to achieve identity and security goals need to understand the properties of biometric systems, the statistics supporting the use of biometrics, and the characteristics and motivations of the population which will be exposed to the biometric system. Careful design of the entire system of which biometrics is a part can produce robust, effective authentication and

identification. Neglecting the properties which make biometrics different from more-traditional authentication technologies can create spectacular failures.

Notes

[1] David Braun. "How They Found National Geographic's 'Afghan Girl.'" *National Geographic*. 7 Mar 2003. http://news.nationalgeographic.com/news/2002/03/0311_020312_sharbat.html