Interested in learning more about security?

SANS Institute InfoSec Reading Room

Biometrics: An In Depth Examination

The purpose of this paper is to give the reader a good foundational understanding of biometric security systems. The intent is not to make the reader an expert in any one system. Therefore, it will not focus on any one specific type of biometric. Rather it will look at the biometric process as a whole giving a brief overview of the types of biometrics available. Problems and issues as well as current applications of biometrics will also be discussed.

Biometrics: An In Depth Examination

Kyle Cherry
GIAC Security Essentials Certification
Version 1.4b, Option 1
November 2003

Abstract

The purpose of this paper is to give the reader a good foundational understanding of biometric security systems. The intent is not to make the reader an expert in any one system. Therefore, it will not focus on any one specific type of biometric. Rather it will look at the biometric process as a whole giving a brief overview of the types of biometrics available. Problems and issues as well as current applications of biometrics will also be discussed.

1. What are Biometrics

Explained simply, biometrics is the statistical analysis and measurement of human traits or characteristics. Once these measurements have been taken, they may then be used to authenticate an individual or user. This is done by comparing the sampled biometric against a template taken earlier. This process will be discussed in further detail below.

Although biometrics is viewed as an emerging technology, in reality, their use has been documented throughout the history of mankind. In Egypt, thousands of years ago, it was common for individuals to use physical traits or characteristics such as scars, eye and hair color, height, etc., to identify individuals for business transactions. (7) The Old Testament cites the use of a biometric in the Book of Judges 12:5-6. It states:

"Then said the men of Gilead unto him, Say now Shibboleth: and he said Sibboleth: for he could not frame to pronounce it right, Then they took him and slew him at the passages of Jordan…." The Old Testament *(11)*

In this example, the pronunciation of the individual was used to identify or authenticate who they were. His repercussions for failing the authentication test were quite a bit more drastic than simply not being granted access, but it was a biometric in use nonetheless.

Biometrics can be easily segregated into two main categories:

1. Phenotypic or Behavioral - The use of pronunciation above is an example of phenotypic or behavioral identification. Phenotypic traits are ones that we develop or acquire over time through our own individual experiences. Further examples of these besides voice recognition would be such things as signature verification or gait examination. (11)

2. Genotypic (genetic) or Physical – Genotypic identification is the use of individual genetic traits to identify a person. This would include such things as fingerprint analysis, facial recognition and vein patter analysis. (11)

Either sub-category of biometrics may be used for authentication although the choice may depend on the application or use. It has been suggested that the use of physical biometrics is more appropriate when using medium-to-high security applications while behavioral biometrics may be sufficient when working with low-to-medium security applications. (12) The perceived difference here is that theoretically, physical biometrics will never change and cannot be copied. And although it may be difficult, it could be possible to, for example, replicate an individual's signature pattern.

A Word On Authentication

An essential aspect of security is the ideology of authentication – the ability to prove that someone or something is what it claims to be. In the systems' security realm there are three commonly accepted types of user authentication:

1. Something you have – digital certificates, tokens, smart cards and keys

2. Something you know – passwords, personal identification numbers (PIN), or some other piece of personal information such as your pet's name or mother's maiden name

3. Something you are – a biological trait (a biometric) (10)

At first glance, biometrics appears to be the most secure and appealing of the three options. It is nearly impossible to steal or forge one's genetic traits. It is far more difficult than stealing a password or other personal information such as a PIN. They cannot be lent to another user, and they cannot be forgotten. In most cases, they are not intrusive and are convenient to the end user.

But they do pose some interesting challenges as well. For example, if a user's fingerprint pattern is stolen, what can you do? The user can't just simply change their fingerprint like they could a password. A new fingerprint cannot be issued like a certificate could. Recent tests of biometric systems have demonstrated that they are not hack proof. This is interesting food for thought and should be considered when a decision is made to implement any type of authentication system. I will discuss the benefits and concerns in further detail throughout the paper.

2. How Do They Work

The Biometric Process

The process model behind a biometric system is generally the same regardless of the biometric being used. While there will be obvious differences in how measurements are collected, stored, etc., depending on the biometric chosen or the specific product, the theoretical model remains the same across all types. Following is a brief summary of the processes utilized in most biometrics systems.

Collection and Enrollment
The first step in any biometric system is collection of the biometric being used. The device used to capture the initial sample will vary depending on the type of physical trait being collected. This could be a reader or sensor used to scan a fingerprint or palm or a camera to capture facial images or certain aspects of the retina or iris. In any event, before using the system for the first time for authentication the user must enroll their biometric sample. This entails the user presenting a "live" biometric sample of the chosen trait a requisite numbers of times, usually at least three, so that the system may produce/build a template. In most cases, this template is then matched with another identifier or reference id, such as a PIN. Going forward, the user will then enter their PIN, which will tell the system which template to use when comparing against for authentication. (7)

The task of building the template is also sometimes referred to as extraction of the biometric. This is due to the fact that most biometric systems do not store full images of the biometric in the way that law enforcement agencies store fingerprints. Rather, certain aspects or points of the biometric are "extracted", and converted into a mathematical code. (5) The attribute extracted depends on the type of biometric you are working with and will be examined more closely when the individual types are reviewed.

As noted above, multiple samples of a trait are taken in an attempt to produce the best quality template possible. This will allow or take into consideration the subtle differences in such things as speech inflection or varying degrees of pressure when a palm or finger is pressed against a reader. (5) It may also include such things as having users present different facial expressions or using varying degrees of light when taking samples. Collecting a quality sample and building a good template may be the most crucial part of the process. A poor quality template could result in false rejection and require re-enrollment into the system. A stronger template will also help make the system more secure. (7)

Template Storage
After a user has enrolled in the system and their template has been extracted, that template must be stored so that it may be retrieved later for comparison. There are three main options for template storage, each with its advantages and disadvantages. The options are:

1. Store the template at the biometric reading device

2. Store the template remotely in a centralized database

3. Store the template on a portable token (smart card) (1)

The main advantage to storing the templates within the biometric reading device is faster response time. If your templates are stored at the reader you will not

have to wait on other system or network resources. Most systems can effectively handle the storage and retrieval of a small amount of templates. But if you have several thousand users, this may pose a problem. If that is the case, you may be better off storing your templates in a centralized database. Additionally, if something were to happen to the reader/system you could potentially completely lose all of your templates. Then re-enrollment of all of your users would be required. (7)

Storing your templates in a centralized database makes the most sense if you have many users or multiple systems. It also allows the use of more layers of security to be applied to the process. The main disadvantages would be the additional resources needed to maintain the additional system and the network traffic created between the biometric reader and the database. Additionally, if the network were to be down for some reason, the biometric readers would be useless. (7)

Storing the template on a smart card has the main advantage that the user will have sole possession of their trait. They may also then use the card at any number of readers or devices, making it more convenient for the organization to position readers at different locations. Although this storage technique may make the end user feel more comfortable it may not be in the best interest of the organization. Issuing cards to all users may become cost prohibitive. In addition, it may become more costly if the user were to lose their card and re-enrollment plus re-issuing of a card became required. (7)

The best storage solution for an organization may be the implementation of multiple storage systems. This will allow the organization to combine the benefits of the solutions and at the same time negate some of the potential disadvantages. Again, the main disadvantage here would be the prohibitive cost. But for organizations that are able to justify the cost, it would be beneficial to store the template at both the device level as well as at a central database. The increased response time could be utilized and the templates would not be lost if there was a failure at either level individually.

Comparison and Matching

Each time a user attempts to authenticate against the system, another “live” biometric sample is taken. Much the same as in the enrollment, the sample is then extracted producing another mathematical code or template. This template is then compared to the previous template stored in the system. If the specified requirements for a match are met, the user is authenticated. If the template taken is not within the successful parameters, the result is a non-match. (5)

Some biometric devices will allow the organization to set the number of attempts allowed for successful authentication. Although you will want to allow a reasonable number of attempts in order to let genuine users authenticate, you do not want to allow so many attempts that it may comprise the secure-ness of the

system. Meaning you don't want to give a hacker an exorbitant amount of tries at defeating the system. Additionally, some biometric systems may update the stored template each time a live sample is taken. This will help update the template with any changes that may have occurred to the biometric over time. This could include minor cuts and scrapes, aging, etc. Of course any major change to the biometric should result in a non-authentication and re-enrollment may be required. (7)

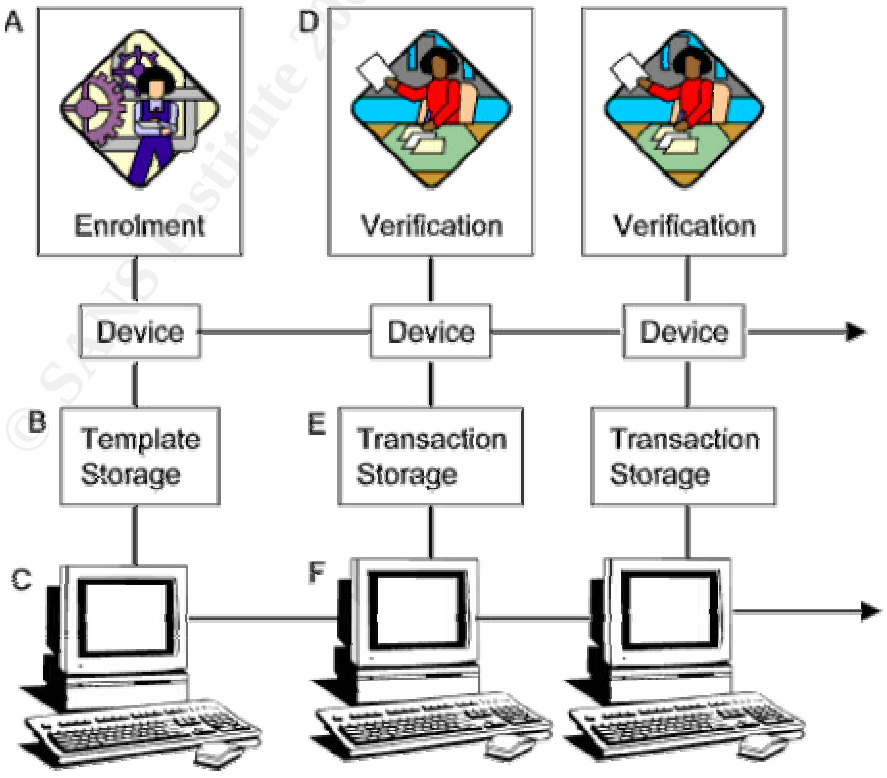
Audit Trail

The final step in the biometric process is the storage of the transactional data or audit trail. Audit information can prove to be a very valuable source of information. It will show you who has successfully authenticated as well has who has tried and has been unsuccessful. This may help you pinpoint security problems or issues. You will be able to determine how many attempts at authentication are usually required to successfully authenticate. This can help you fine-tune your system.

Again, this information can be stored locally on the device or centrally depending on your preference. Either way, a scheduled review of logs for any unusual discrepancies is always a good security practice.

Following are two examples taken from other sources of what the process flow for a biometric system may look like:

1. From "The Biometric Whitepaper" by Julian Ashbourn (7):



Device – The biometric system/device
A – Live sample is presented for collection and enrollment
B – Template is built and stored on the Network (C represents the Network)
D – Live sample is presented for comparison and matching
E – Transaction data or audit trail is stored after verification (with F again representing the Network)
Process is repeated

2. From “A Practical Guide to Biometric Security Technology” by Simon Liu and Mark Silverman [10]:

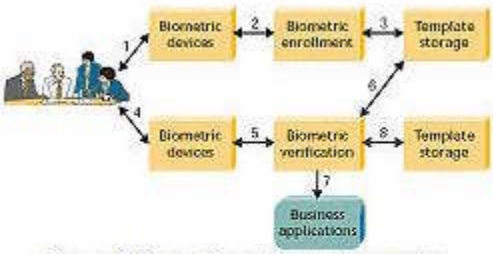


Figure 1. How a biometric system works.
(1) Capture the chosen biometric; (2) process the biometric and extract and enroll the biometric template; (3) store the template in a local repository, a central repository, or a portable token such as a smart card; (4) live-scan the chosen biometric; (5) process the biometric and extract the biometric template; (6) match the scanned biometric against stored templates; (7) provide a matching score to business applications; (8) record a secure audit trail with respect to system use.

Identification vs. Verification

Any time you discuss biometrics it is important to make sure that the distinction of Identification vs. Verification is understood. At first glance they may seem like they are very similar principles, but in actually they are very different. Most biometric devices authenticate users using the verification method. As noted in the process above, during the Collection and Extraction phase, often a PIN is entered so that it may be used to reference the stored template. When a user would attempt to authenticate they would first be required to enter their PIN, which would in turn let the system know which template to retrieve for comparison. The live sample would then be compared against the retrieved template and a match or no-match would result. In this way the system is really just “verifying” that you are who you claim to be. This is often referred to as a one-to-one match.

Identification on the other hand is more detailed and complex. Rather than entering a PIN for reference purposes you just merely present your live sample. The system then takes the template and compares it to all that it has stored in its database. It keeps checking until it finds a match and is able to declare that it has “identified” you. This is referred to as a one-to-many match. And in some

cases it may actually produce many results. Depending on how "strong" the parameters of your system are, it is possible that a live sample may match many stored templates. Although the ability to identify a user is appealing, especially at larger organizations, this is something that should be considered with caution. In many instances it may not be as secure as a verification model is.

Performance Measurements

When evaluating biometric systems there are four main performance measurements that should be considered. The first three deal with the accuracy of the system. Accuracy is the most important aspect of any authentication system. If the system cannot accurately perform its tasks, then security is compromised. The fourth measurement deals with the speed of the system. Although not as important for authentication purposes, the speed of the system is very important to the end user.

False Rejection Rate

The false rejection rate, usually expressed as a percentage, is the rate at which the biometric system wrongly denies access to legitimate, enrolled users. False rejection is sometimes referred to as a Type I Error. [(13)] How important this error rate is to an organization implementing a biometric solution is dependent on the role of the system. If the main purpose of the system is to limit access from unwanted intruders this error may be less important. If, however, the system is used to authenticate customers, such as at an ATM or retail store, the error may be more important. If the customer is unable to authenticate they will be unhappy and possible revenue may be lost.

A distinction should also be made between False Rejection and the Failure to Acquire by the system. These are often confused or considered to be the same. A failure to acquire results when the system is not presented with enough biometric information to enable it to build a suitable template for comparison. This may be caused by such things as smudges on a fingerprint reader, low light levels for a facial recognition camera, or not speaking clearly into a voice verification system. In all cases, it is the user and not the system that is responsible for a failure to acquire. This could be done accidentally or on purpose. [(13)]

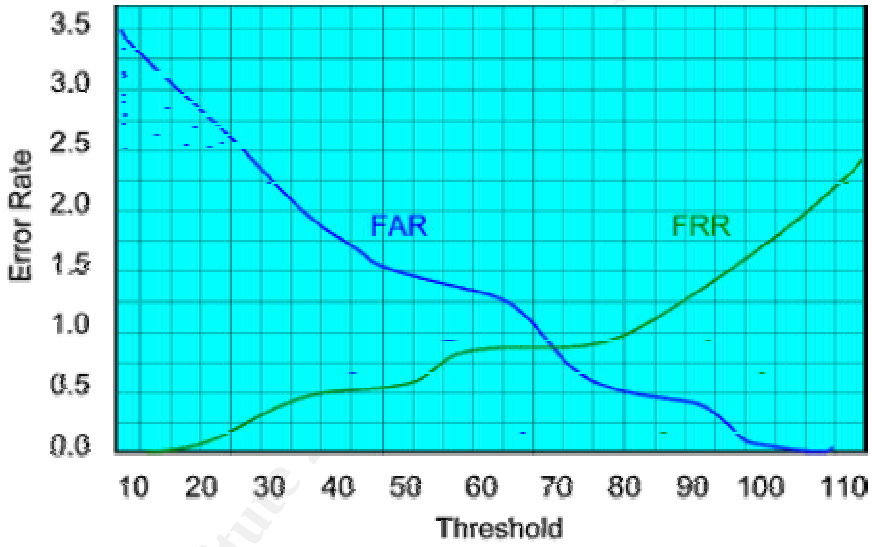
False Acceptance Rate

Also expressed as a percentage, the false acceptance rate is the rate at which the system wrongly authenticates an un-enrolled intruder. This may commonly be referred to as a Type II Error. [(13)] For obvious reasons, false acceptance is usually the most important error to consider when implementing a biometric solution. A higher false acceptance rate means an increase in the likelihood that an impostor will be able to authenticate with the system.

Crossover Error Rate

Also referred to as the Equal Error Point, the crossover error rate is the point where the false acceptance rate and the false rejection rate are equal. It is commonly considered the most realistic and reasonable rate to use when comparing biometric systems.

Although false acceptance and rejection are independent measures, they do have an affect on one another. The sensitivity of most biometric systems can be adjusted. Therefore, if an organization decides that false acceptance is most important, they may fine-tune their system so that only near perfect matches are accepted. The downside to this however, is that the rate of false rejection will most likely increase, and vice versa. The crossover error rate is the middle ground, optimizing both rates for the system. The following diagram from "The Biometric Whitepaper" by Julian Ashbourn [7] illustrates this point. The equal error point is the point where the FRR and FAR cross:



Speed and Throughput Rate

Last but not least, the final performance measurement to be considered when implementing a biometric system is the speed and throughput rate. The speed of a biometric system is not solely related to the speed or power of the data processing aspect of the system. Rather, it relates to the process flow in its entirety. The speed from beginning to end needs to be considered. It really does not matter how fast the data can be handled if the rest of the process is cumbersome and too time consuming. For example, this means that everything from presenting the finger for the sample to opening and closing the door, if required, should be considered when calculating the speed of the system.

3. Commonly Used Biometrics

For the purpose of this paper, I will be subdividing the types of biometrics into two main categories. The first, commonly used biometrics, are those that are frequently put to use today. The second category, developing biometrics, are up

and coming technologies that are either in research stages or just beginning to be utilized for security authentication. It should also be mentioned that just because these are commonly used biometrics does not mean that they are static and immune to change. On the contrary, advancements are being made all the time making them more secure and easier to use.

Fingerprint Verification

Fingerprints have certain natural traits that make them ideal for use in biometric systems. Fingerprints are developed between the first and second trimester and remain unchanged (barring any damage or scarring) until death. Fingerprints are unique. No two people on record have been found to have the same fingerprints. Fingerprint identification has been used by law enforcement agencies for many years. But this type of one-to-many match is seldom used for commercial purposes. Most fingerprint systems operate in authentication, rather than identification, mode.

Fingerprint scanning can be done in several different ways. Some systems scan the distinct marks on the finger called minutiae points (similar to the traditionally used police method). Others analyze the distance between ridge endings and ridge burifications on the finger. The positioning of pores and straight pattern matching may also be used. More recent developments include the use of moiré fringe patterns (superimposing of lines and grids to capture three-dimensional surface shape) as well as ultrasound. Fingerprint systems should be kept clean as smudges or dirt and grime may cause problems for the reader.

Hand Geometry

Hand geometry involves the analysis and measuring of the hand and fingers. The user places their hand on the reader with their fingers in designated positions. A camera is then used to capture both a top view, which gives the length and width, as well as a side view, which gives the thickness. Hand geometry is one of the most established uses of biometrics today. It is accurate and fast.

Retinal Scanning

Retinal scanning involves using a low intensity light to scan the unique pattern found in the retina portion of the eye. An optical coupler is used to produce the light, which analyzes the layer of blood vessels found at the back of the eye. It requires the user to position their eye at the reader and focus on a central point. This is not always convenient for those who wear glasses and some find the idea of a light scanning their eye intrusive, although it is not painful and poses no known danger. Retinal scanning devices are often used in areas where high security is needed and where less consideration is given to convenience and comfort of the user.

Iris Scanning

Iris scanning technology is commonly thought of as the most secure or strong biometric system. This is due to the fact that the iris contains a very complex pattern and large number of measurable characteristics that make it practically impossible to replicate. Even a person's right and left iris patterns are different. For iris scanning, a camera is used to record a digital image of the user's iris. Contact lenses and glasses do not interfere with the scan. And unlike retinal scanning, there is no intrusive light beamed into the individual's eye. Of all biometric technologies, iris scanning has the most potential for further development.

Voice Verification

Voice verification uses a microphone-recording device to capture a sample of a user's voiceprint. Measurements of a number of characteristics are taken, including cadence, pitch, and tone. (5) Voice verification is considered to be a hybrid of physical and behavioral biometric types. (5) On the physical side, the shape of your throat and larynx helps to predetermine your voiceprint. But then again, your experiences help influence such things as inflect and dialect. And although difficult to do, it is possible that one could alter their voiceprint. Additionally, it is important to make sure that the distinction between voice verification and voice recognition is understood. Voice recognition is software that is able to decipher words that are spoken, and is not an authentication technique.

Voice verification is fairly simple to implement. Because most workstations come with a microphone of some sort pre-installed, new hardware is usually not needed. It may also be implemented using current telephone systems. Voice verification has run into some opposition and has been accused of being hard to use from an end user perspective. At times it is difficult to enroll in the system as background noises, and static as well as the common cold can cause problems at enrollment and during verification.

Signature Verification

Signature verification involves the use of a special pen, tablet, or both to capture the way a person signs their name. Although the final appearance of the signature is important, a number of other attributes are captured as well. These include speed, velocity, pressure, angle of the pen as well as the number of times the pen is lifted from the pad. Signature verification is considered to be very accurate. Additionally, most users will not object to providing their signature for verification, as they are use to identifying themselves by signature all the time (i.e. credit card slips, checks, etc.).

Facial Recognition

Facial recognition utilizes distinctive features of the face to authenticate users. A camera of some sort (digital, video or thermal) is used to capture the features. This includes such things as the upper outlines of the eye sockets, the cheekbones, the sides of the mouth, and the location of the nose and eyes. (14)

Video facial recognition maps out a number of points on the face or creates a three-dimensional image to be used for comparison. The user is usually required to stand a few feet away and most systems are capable of compensating for expressions, glasses, hats and beards. Poor lighting can cause problems so most systems will need to be placed in well-lit areas.

Thermal recognition systems use an infrared camera to scan faces and create a digital map of their thermal patterns. This digital image is known as a thermogram. Branching blood vessels under the skin, which are hotter than the surrounding tissue, are responsible for creating the "hot" spots that the infrared camera picks up. Much like fingerprints, no two people are known to have the same thermogram.

4. Developing Biometrics

The following developing biometric systems are either emerging technologies that have not been fully explored or are systems that are just now beginning to gain acceptance.

Palm Print
Similar to fingerprinting, palm print biometrics is a system that measures the physical characteristics of an individual's palm. The specified palm is placed on a reader where the measurements are taken. Not enough data has been collected yet to determine if palm prints are as unique as fingerprints.

Vein Pattern
Vein pattern matching involves scanning the vein patterns on the back of a user's hand. The user places their hand into a reader. Inside a small black and white camera and LED array are used to capture the digital image. The LED array, combined with filters also inside the reader, is used to magnify the contrast of the veins under the skin. This results in a vein distribution pattern that may be used for authentication. Certain vein aspects or points, as well as the whole distribution, are used for verification. (11)

Like finger and palm prints, vein distributions are unique, making them an attractive biometric for use. The right and left hand of an individual do not exhibit the same vein distribution pattern. They can also be expensive to implement and are not as convenient as fingerprint readers. There is also the question of how vein patterns change over time. It is unknown whether there is significant change in the vein pattern over long periods of time and how this could possibly affect authentication.

Ear Shape, Body Odor and Gait Analysis
Ear shape is a physical biometric that measures the shape of the outer ear, lobes and bone structure. Done much in the same manner as facial recognition, a two or three-dimensional picture may be taken.

Body odor is a system that analyzed the natural body odor given off by an individual. Electronic sensors are used to gather the odor, usually from the least intrusive area as possible, such as the back of the hand.

Gait analysis is the analysis of the way an individual walks. This usually includes some sort of mat with sensors that an individual will then walk across. Measurements of the speed, pressure applied by the foot, manner in which steps are taken as well as the number of steps required are taken and used for verification.

5. Applications and Considerations

As stated previously, the use of biometrics is an emerging technology. Because of this, it is likely that most of us have not worked with security systems that utilize them. There are a relatively few number of vendors that manufacture these specialized products and costs at times have been prohibitive. But like most technologies, costs will decline as manufacturing and research processes improve. And as user acceptance increases, it is more likely that biometrics authentication will become a part of our everyday lives. Since the purpose of any authentication system is to prove the identity of the user, biometrics can be incorporated into any number of situations where this security requirement exists. The sky really is the limit for biometrics use. Following are some examples of how biometrics are being utilized at this time.

Financial Transactions
Almost all financial institutions have researched using biometrics at one point or another. The benefits are obvious. One of the greatest advantages would be the ability to replace a PIN number with a secure biometric. This would greatly reduce the chance that an ATM card could be used maliciously. The implementation of a biometric with the use of checks and credit cards would also have a huge impact on identity theft, a growing problem of concern. Loyalty and rewards programs could be setup to require a biometric any time a transaction is processed. They could also be set up to control access to safety deposit boxes and vaults.

Access Control
Biometrics can also be utilized any time that access control is a requirement. This could be general physical access to a building as well as access to a workstation, computer system or network. Theoretically a biometric could be used to delineate access control to the lowest levels such as access to a particular file or computer application. Building security systems, especially in areas where confidential or classified information needs to be stored. Such would be the case in many government buildings.

Identity Verification

Again, at the simplest level, biometrics is about identity authentication. This opens up a wide area of suitable applications for the technology. Any time you are looking for a convenient, accurate and quick method of identifying or verifying an individual, a biometric solution could be a good choice. Some common uses throughout the world include such things as time card or attendance systems. Employees can be required to quickly check in and out of work with the scan of a finger or the eye. This helps keep an accurate record of hours worked and makes it impossible to forget to "punch" in. Public welfare programs utilize biometrics to make sure benefits are received, as well as used, by the correct individuals. Biometrics are used for patient management in hospitals and clinics to keep track of individuals for billing purposes as well as medical charts and to make sure that patients receive the correct medications.

Law Enforcement

Although biometrics have been used by police agencies for some time on a limited basis (fingerprinting, etc.) the tragedy of 9/11 helped bring to light the many hypothetical benefits of biometric systems to law enforcement areas. The ability to do such things as facial recognition scans to look for potential terrorists or criminals in airports or other high profile public places can be a great benefit to security personnel and systems. Unfortunately, in reality many of these systems have not been able to live up to the standards they claim to accomplish. False identifications (i.e. false rejections) occur frequently and slow down check in times, angering customers. However, as technologies progress these will be very viable uses. In addition, biometric systems are currently used with great success in such areas as immigration checks and individual movement control. They have been implemented to help move law enforcement criminal records into the digital age. Digital fingerprint scans have replaced the traditional ink system.

Considerations

How well a system performs its stated purpose is probably the most important fact to consider when looking at any authentication solution. For example, does it have a suitable and realistic false acceptance rate that meets your organization's needs? These performance measurements were discussed in detail earlier. However, when an organization is making the decision on whether to use biometrics or not, there are some additional considerations that should be made.

Some of these considerations may be more or less important depending on the need of the organization. Additionally, there may be other facts not listed here that need to be taken into account when implementing a biometric solution. In general, the following should be considered any time it is decided that biometrics are a viable solution for your organization.

1. User Acceptability – Next to performance, and in some cases before, this is usually the main concern of users. Is the system intrusive and hard

to use? Will users feel that their privacy is being violated or will they feel like criminals (e.g. fingerprinting)? Will the users feel that they are potentially exposing themselves to harm (e.g. light scanning their retina)? In most cases user acceptability can be increased in some degree by education and information.

2. Uniqueness of the Biometric – The key to the strength and security of any biometric is its uniqueness. Fingerprinting and iris and retinal scans are typically considered the most unique. This does not necessarily mean that they cannot be replicated; rather it means that they have a sufficient number of complex patterns or traits that can be used to build a strong template for authentication.

3. Resistance to Counterfeiting – Can the biometric be easily replicated by an intruder? Again, this is different from #2 above. Fingerprints, for example, are very unique. However, there have been many detailed successful attempts at replicating fingerprints. Iris scans on the other hand, are considered to be almost impossible to replicate as well as extremely unique.

4. Reliability – The system should experience minimal downtime. If the system where to go down, it should be fairly easy to bring it back up with minimal loss of productivity and data. In order for a biometric system to perform its stated purpose it is imperative that it be reliable. If users cannot authenticate or gain access, they most likely will be unable to do their jobs. If consumers or customers are unable to authenticate they will be angry and revenue and faith may be lost.

5. Data Storage Requirements – How big are the templates being stored on the system? New hardware may be required if there is not sufficient storage space. This may also have an impact on processing speeds and network traffic.

6. Enrollment Time – How long will it take the organization to enroll its users? Some systems make require several hours. An organization will have to look at this lost “productivity” and see if it is justified.

5. Problems and Issues

The benefits of a biometric system are fairly obvious and straightforward. Since they are an intrinsic part of the user, they do not require the user to remember a password or pin. At first glance, they are very secure. An impostor will not have much success randomly generating a fingerprint to gain access. But because they are an intrinsic part of the user, they pose some interesting problems that other systems do not have. Also, since most biometric systems are not completely isolated, they are exposed to the same risks that the rest of the

network or other applications are. Following are some of the main problems and issues surrounding biometric systems.

User Acceptability

This was mentioned earlier under considerations but is important enough to be mentioned again. User acceptability may be the biggest issue facing biometrics for a number of reasons. First and foremost, users are concerned about their privacy. Many view the use of biometrics as an intrusion into their personal life. They are unsure how this information might be used in the future. Is it possible that the government could get a hold of such information and use it to keep track of what someone does without his or her consent? Will banks and retailers be able to sell such information much like e-mail addresses? It sounds like a conspiracy theory, but it really is possible.

There is also the issue of being able to possibly gather medical information from some biometric templates. Scans of the iris and retina may possibly indicate drug use or even medical conditions and diseases as blood vessel patterns may change due to health related events. Does this violate HIPPA laws and statutes? It is most certainly not the purpose of any system to be detecting such things at this time, but what if the information falls into the wrong hands or is used improperly. Most people would not want their management or employer having this information without their consent.

Finally, many users also fear that use of a biometric system may result in some harm to them. This may be as simple as fearing that the light shown into their eyes during a retinal scan could cause damage to their vision. This is not the case, but it is easy to see where this fear comes from. There is also the issue of possibly spreading contagious diseases through the use of scanners by many individuals. Many contagious diseases can be spread by simple contact so this is a possibility.

With all of this being said, user acceptability has actually started to increase. Education of the user base has been the main reason for this. Users are beginning to understand the potentially devastating financial problems caused by such things as identity theft. And the tragedy of 9/11 has proven that there is a need for enhanced security which biometrics can help provide.

A recent survey conducted by Privacy & American Business (P&AB) and funded by the US Bureau of Justice Statistics showed that many American consumers felt that it was appropriate for the private sector to require biometrics for certain transactions [(16)]. This included such things as:

- Verifying the identity of a gun purchaser against a database of convicted felons (91% agreed)
- Verifying the identity of credit card purchasers (85%)
- Withdrawing funds form an ATM (78%)

- Accessing medical or financial records (77%)
- Conducting background checks (76%) [16]

Technical Problems

System cost and accuracy are two of the biggest technical problems associated with biometrics. In most cases, new hardware and software will be required to implement a biometric solution. Depending on the type of system used, for example iris scanning, the cost may become prohibitive to install scanners at all desired locations. Fingerprint scanners, on the other hand, have become more affordable. As time goes on, most systems will become cheaper and more efficient.

Accuracy may pose a problem if false acceptance and rejection rates are not acceptable for an organization. As mentioned earlier, these usually may be fine tuned, but in some instances biometrics may still not be able to offer the same false acceptance and rejection rates as a cryptographic token solution.

As mentioned above, most biometric systems are part of a bigger security or technical infrastructure. They often rely heavily on other parts of that infrastructure to perform effectively. A good example would be the storage of templates. If these are stored on a central database or server you have another possible point of entry for an intruder. Typical precautions would need to be taken to make sure that your network was secure. Although an impostor may not be able to easily replicate a fingerprint, you need to remember that a fingerprint is translated by an algorithm into a mathematical code or string of bits. If an intruder is able to hack into the network and retrieve and decipher that code, they may be able to circumvent the system and use the digital fingerprint. [3]

The physical security of the biometric device needs to be considered as well. If an intruder had access to the wiring of a voice recognition system, it may be possible for them alter the wiring and play a recorded voice into the microphone. [2] This may seem far-fetched, but it should be considered a possibility. An organization can evaluate how likely, or unlikely, such events are and plan accordingly.

Intrinsic Problems

As mentioned previously, biometrics have the advantage that they are an inherent biological trait, and as such, cannot be lost. But this also poses an interesting dilemma at times. What can you do if your trait happens to be stolen? Fingerprints, for example, are unique but they are not secrets. We leave them everywhere with everything we touch. Voices may be recorded and replayed at any time. Once your biometric is stolen, you have some serious issues. Re-enrollment is not possible. Unlike resetting or changing your password you cannot simple reset your fingerprint. [17]

There is no simple or correct solution for this problem. The use of multifactor authentication can help insure the security of the system if a biometric is stolen but will not resolve the problem completely. Multifactor authentication is the use of two or more authentication techniques such as requiring a PIN or password to be used with a fingerprint scan. An impostor would not only need to steal the fingerprint, but would have to know the password as well. It is possible to combine as many authentication techniques as desired. For highly classified systems, for example, it would be possible to require a PIN, a smart card, a fingerprint scan and an iris scan. Of course most organizations, besides governmental agencies, would be unable to afford such a system. In any event, special consideration should be given to how a stolen biometric would be handled if it did occur.

Are They Really Secure

Recently there have been some well-documented successful attempts at replicating fingerprints. The first major break through came in January of 2002 when Japanese Cryptographer Tsutomu Matsumoto was able to create a fake finger using a plastic mould and gelatin. Matsumoto found that he was able to fool four out of five fingerprint systems using his fake finger. (9)

To take his test a step further, Matsumoto recovered latent fingerprints from a glass, enhancing them with a cyanoacrylate adhesive (super-glue fumes) and photographing them with a digital camera. He then used PhotoShop to improve the image contrast and printed the image onto a transparency sheet. From there Matsumoto took a photosensitive printed circuit board and used the transparency to etch the fingerprint into the copper. The circuit board was then used to produce a more detailed mold. Gelatin was used again, along with the new mold, to produce another fake finger. He tested this fake finger on 11 commercially available fingerprint systems and found that he was able to fool each about 80% of the time. The materials used were not particularly expensive or hard to acquire, and the process was not especially hard to complete. (9)

In November of 2002, two German hackers known as Starbug and Lisa tested and were able to trick several commonly available biometric systems. They found that they were able fool normal facial recognition systems using still photos and were able to fool one live-check system using a recorded video of the individual. Once the system detected the head movement of an enrolled user it granted access. In addition they were able to fool a fingerprint scanner by simply breathing lightly on it until latent fingerprint images left on the system were exposed. Latent fingerprints were also exposed and re-used using a simple plastic bag with water and pressing gently against the sensor. They also found that they were able to use tape and graphite powder to pick up the latent fingerprint and then if the tape were gently pressed against the reader, they were again granted access. (8)

The real shocker was their ability to fool an iris recognition system, supposedly the most secure biometric. Using a digital image of a human eye that had been sprayed onto mat inkjet paper with a resolution of 2400 X 1200 dpi, and including a small hole for one's pupil to look through, they were easily able to fool the iris recognition software. (8) Again, the materials for all of these "tricks" were not very hard to come by and were not expensive.

In August of 2003 Starbug and Lisa presented additional attacks at the Chaos Computer Camp. They made some additional enhancements to their earlier attacks using a digital camera to retrieve the latent image and using latex to create the final product similar to Matsumoto's fake finger. They claim the additional attacks were made in response to criticism they received from the vendors used for initial testing. Several of the vendors claimed that only in a laboratory setting would these attacks be viable. Starbug and Lisa plan to do additional field-testing to prove the vendors wrong. (18)

The ease at which these hackers were able to defeat the systems should be of great concern. Taken at face value, biometric systems may not be as secure as they claim. But testing/hacking projects like this will only serve to improve the future products that come to market.

7. Conclusion

Biometric systems have made leaps and bounds in the last 30 years since their inception. It is estimated that global biometric sales will rise more than 500% by 2007 reaching revenues of $4 billion. While there are obvious advantages to these systems, there are also certain considerations that organizations need to think about when deciding whether or not to implement a biometric solution. They are not for everyone. Further testing is needed to make sure that they are as secure as they claim to be. But in the coming years, it will be hard to deny the advantages that they offer. I expect that in the future, biometrics will become a basic fundamental of everyday life. It may not be exactly like the movies, but then again, it might be close.

References

1. King, Todd. Security+ Training Guide. Indianapolis: Que Certification, 2003.

2. Garfinkel, Simson. Web Security, Privacy & Commerce, 2nd Edition. Sebastopol: O'Reilly, 2001.

3. Cheswick, William R., Steven M. Bellovin, Aviel D. Rubin. Firewalls and Internet Security: Repelling the Wily Hacker, Second Edition. Boston: Addison Wesley, 2003.

4. Pfleeger, Charles P., Shari Lawrence Pfleeger. Security in Computing, Third Edition. Indianapolis: Prentice Hall PTR, 2002.

5. Vacca, John. "Biometric Security Solutions." 25 October 2002. URL: http://www.informit.com/isapi/product_id~%7BC3A2803B-7E73-4341-AB9F-BC91D275E970%7D/content/index.asp (12 October 2003).

6. "Biometrics." Network Security Technology. URL: http://www.cs.usask.ca/undergrads/der850/project/biometrics/index.shtml (30 October 2003).

7. Ashbourn, Julian. "The Biometric Whitepaper." URL: http://www.biometricsinfo.org/whitepaper4.htm (12 October 2003).

8. Thalheim, Lisa, Jan Krissler, Peter-Michael Ziegler. "Body Check – Biometric Access Protection Devices and their Programs Put to the Test." c't Online. November 2002. URL: http://heise.de/ct/english/02/11/114/ (30 October 2003).

9. Matsumoto, Tsutomu, Hiroyuki Matsumoto, Koji Yamada, Satoshi Hoshino. "Impact of Artificial "Gummy" Fingers on Fingerprint Systems." 28 May 2002. URL: http://cryptome.org/gummy.htm (30 October 2003).

10. Liu, Simon, Mark Silverman. "A Practical Guide to Biometric Security Technology." 2000. URL: http://www.computer.org/itpro/homepage/Jan_Feb/security3.htm (5 November 2003).

11. Lindup, Alastair. "Vein Pattern Analysis." 2003. URL: http://www.cems.uwe.ac.uk/~jgilliga/UQI133H3/digsig/Vein.htm (5 November 2003).

12. Behrens, Laura. "What You Need To Do: Planning a Biometrics Security Rollout." The Key to Confidentiality. January 2002. URL: http://security1.gartner.com/story.php.id.115.s.1.jsp (12 October 2003).

13. Richards, Donald R. "Biometric Identification." Access Control Issues. URL: http://www.cccure.org/Documents/HISM/033-037.html#Heading3 (12 October 2003).

14. "Face Recognition." BiometricsInfo.org – Biometrics Information Resource. URL: http://www.biometricsinfo.org/facerecognition.htm (15 November 2003).

15. Wildes, Richard P. "Iris Recognition: An Emerging Biometric Technology." September 1997. URL: http://www.cs.yorku.ca/~wildes/wildesPIEEE1997.pdf (15 November 2003).

16. Leyden, John. "Americans give thumbs up to biometrics." The Register. 1 August 2003. URL: http://www.theregister.co.uk/content/55/28782.html (11 November 2003).

17. Bar-El, Hagai. "When To Use Biometrics." 8 October 2003. URL: http://downloads.securityfocus.com/library/When_To_Use_Biometrics.pdf (11 November 2003).

18. Harrison, Ann. "Hackers Claim New Fingerprint Biometric Attack." 13 August 2003. URL: http://www.securityfocus.com/news/6717 (11 November 2003).

Last Updated: February 24th, 2018

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

CyberThreat Summit 2018	London, GB	Feb 27, 2018 - Feb 28, 2018	Live Event
SANS London March 2018	London, GB	Mar 05, 2018 - Mar 10, 2018	Live Event
SANS Secure Osaka 2018	Osaka, JP	Mar 12, 2018 - Mar 17, 2018	Live Event
SANS San Francisco Spring 2018	San Francisco, CAUS	Mar 12, 2018 - Mar 17, 2018	Live Event
SANS Paris March 2018	Paris, FR	Mar 12, 2018 - Mar 17, 2018	Live Event
SANS Secure Singapore 2018	Singapore, SG	Mar 12, 2018 - Mar 24, 2018	Live Event
SANS Northern VA Spring - Tysons 2018	McLean, VAUS	Mar 17, 2018 - Mar 24, 2018	Live Event
ICS Security Summit & Training 2018	Orlando, FLUS	Mar 18, 2018 - Mar 26, 2018	Live Event
SANS Munich March 2018	Munich, DE	Mar 19, 2018 - Mar 24, 2018	Live Event
SEC487: Open-Source Intel Beta One	McLean, VAUS	Mar 19, 2018 - Mar 24, 2018	Live Event
SANS Pen Test Austin 2018	Austin, TXUS	Mar 19, 2018 - Mar 24, 2018	Live Event
SANS Secure Canberra 2018	Canberra, AU	Mar 19, 2018 - Mar 24, 2018	Live Event
SANS Boston Spring 2018	Boston, MAUS	Mar 25, 2018 - Mar 30, 2018	Live Event
SANS 2018	Orlando, FLUS	Apr 03, 2018 - Apr 10, 2018	Live Event
SANS Abu Dhabi 2018	Abu Dhabi, AE	Apr 07, 2018 - Apr 12, 2018	Live Event
Pre-RSA® Conference Training	San Francisco, CAUS	Apr 11, 2018 - Apr 16, 2018	Live Event
SANS Zurich 2018	Zurich, CH	Apr 16, 2018 - Apr 21, 2018	Live Event
SANS London April 2018	London, GB	Apr 16, 2018 - Apr 21, 2018	Live Event
SANS Baltimore Spring 2018	Baltimore, MDUS	Apr 21, 2018 - Apr 28, 2018	Live Event
SANS Seattle Spring 2018	Seattle, WAUS	Apr 23, 2018 - Apr 28, 2018	Live Event
Blue Team Summit & Training 2018	Louisville, KYUS	Apr 23, 2018 - Apr 30, 2018	Live Event
SANS Riyadh April 2018	Riyadh, SA	Apr 28, 2018 - May 03, 2018	Live Event
SANS Doha 2018	Doha, QA	Apr 28, 2018 - May 03, 2018	Live Event
SANS SEC460: Enterprise Threat Beta Two	Crystal City, VAUS	Apr 30, 2018 - May 05, 2018	Live Event
Automotive Cybersecurity Summit & Training 2018	Chicago, ILUS	May 01, 2018 - May 08, 2018	Live Event
SANS SEC504 in Thai 2018	Bangkok, TH	May 07, 2018 - May 12, 2018	Live Event
SANS Security West 2018	San Diego, CAUS	May 11, 2018 - May 18, 2018	Live Event
SANS Melbourne 2018	Melbourne, AU	May 14, 2018 - May 26, 2018	Live Event
SANS Northern VA Reston Spring 2018	Reston, VAUS	May 20, 2018 - May 25, 2018	Live Event
SANS New York City Winter 2018	OnlineNYUS	Feb 26, 2018 - Mar 03, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced