GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Lisa Kuster
GSEC Practical Assignment
Version 1.4b Option 1
October 22, 2003

An Overview of Biometric Technologies

Abstract

Biometrics has been the emerging technology during the past decade. The technology appears to be the answer to the growing concern of the safety and security in both personal and public environments. Taking into consideration the tragic events of 9/11, biometrics has received a great deal of attention and recognition. As the focus on security continues to intensify, individuals, companies, and organizations are quickly trying to learn more about the "what's" and "how's" of biometrics.

In my paper, I will describe what biometrics technology is, how the technology is utilized and the different methods that are used. I will also briefly describe four existing biometrics technologies: facial recognition, fingerprint recognition, iris recognition, and signature recognition. Each of these technologies is unique in it's own way, but they all attempt to provide the same safeguards to an individual, an object(s) (i.e. a server), a room, or a building. These technologies may prove to be advantageous by eliminating security threats while optimizing the convenience to today's organizations.

Biometrics – What is it?

Biometrics refers to the automated methods of recognizing a person based on a physiological or behavioral characteristic. Physical biometrics includes fingerprints, hand or palm geometry, and retina, iris, or facial characteristics. Behavioral characteristics, traits that are learned or acquired, include signatures, voice (which is also considered a physical characteristic) and keystroke pattern.

Biometric technologies are used to verify or identify users to allow access to a variety of environments. From ATMs to logging into a network or your personal computer, biometrics is being used throughout the world. The major use of biometrics technology today is to control access for specific-authorized individuals to secure locations, rooms and/or buildings.

Biometrics can be found being utilized in federal, state and local governments, in the military, in the health field, in the banking industry, and other enterprise-wide network security infrastructures. (www.biometrics.org/html/introduction.html)

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

How many times have you forgotten your password while trying to log in to your computer at work? With the use of biometrics, you would not have to remember a password. You could simply scan one of your fingers with a fingerprint scanner or sign your name for it to be verified by signature recognition equipment.

Biometrics cannot be forgotten, lost, shared, or stolen. Biometric information is a part of each of us. Truly individual in nature, biometrics represents an optimal security solution in a world burdened with identity theft and computer hacking.

Biometric-based authentication applications in the workplace include workstation, network, and domain access, single sign-on, application logon, data protection, remote access to resources, transaction security, and web security. Whether utilized alone or integrated with other technologies such as smart cards, encryption keys or digital signatures, biometrics are set to encompass nearly all aspects of the economy and our daily lives. (www.biometrics.org/html/introduction.html)

The Cost

In 2000, expenditures for biometric authentication systems reached $66 million worldwide. According to Frost and Sullivan, a leading market research firm, a combination of finger scanning, hand geometry, iris and retina scanning, face recognition, and voice and signature verification technologies were the leading technologies responsible for the costs. The forecast through 2006 is for an overall annual growth of 54%, attaining market levels near $900 million. What is attributing to this massive growth of biometric expenditures? The events of 9/11 have helped attribute most of the growth to the expanding technology.

Identification vs. Verification Methods

The two primary uses of biometrics are identification and verification. In identification, an individual has to prove their identity (Who is this?). Verification attempts to confirm or deny the individual's identity (Is this person claims who he/she claims to be?)

Identification or recognition is the process in which the system attempts to identify a person based on biometric information when compared to biometric templates. The biometric information or identifier (i.e. a fingerprint, an iris, a person's voice) is then compared with a database in efforts to search for a match. This is known as a one-to-many comparison. At this point, the system must make a positive or negative identification.

Positive identification answers the question, "Who is this?" The response could be a name, an identification number (ID), or another unique number (e.g. social security number). The identifier is then used to search the database for a match.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Negative identification is used in the same manner except the identifier is used to ensure a person is **not** in the database.

Verification or authentication is the process used to validate the identity of an individual by comparing a verification template to an enrollment template (http://www.biometricsinfo.org/biometrics.htm). After the identity template is compared with the enrollment template, verification answers the question, "Is this person who he/she claims to be?" This is known as a one-to-one comparison.

Authentication can also be described as follows:

- Something you are – a biometric
- Something you know – a password or PIN
- Something you have – a key, token card, etc…

Accuracy

Another key importance in biometric technology is accuracy. There are three terms that are used to describe the accuracy of biometric systems. They are false acceptance rate (also referred to as "FAR" or "Type 2 Errors"), false rejection rate (also referred to as "FRR" and "Type 1 Errors"), and equal error rate. These rates are used to determine performance levels of biometric systems. The False Acceptance Rate and the False Reject Rate are the two most common criteria used on evaluating the performance of biometric systems. (http://www.htgadvancesystems.com/Advance/biometrics/science.html)

- False Acceptance Rate – percentage of an imposter being granted authorization by the biometric system.

- False Rejection Rate – percentage of a registered user being denied authorization by the biometric system.

- Equal Error Rate – the point where the False Acceptance Rate and the False Reject Rate equal each other.

Today's Uses of Biometrics

Biometric technologies are being used in a variety of different ways all over the world. The following are a few examples:

- Airports use facial scanning to recognize employees and also to try to identify known terrorists and/or criminals.
- Border crossing checkpoints use facial scanning to recognize know criminals before they enter a different country.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- Federal and local government agencies use fingerprint scanning to identify employees and prisoners.
- Airports use iris scanning to allow employees to enter and exit secured areas.
- Banks with Automatic Teller Machines (ATMs) use secured Personal Identification Numbers (PINs) and are using iris scanning to identify and verify their customers.
- Government and military sites use iris scanning for highly sensitive restrictive areas.
- Financial institutions, corporations, and government agencies use telephony applications for voice recognition to account information, service calls, and house arrests.
- Individuals may use cashless vending to prevent unauthorized uses of their credit cards. Individuals swipe their credit card then touch a fingerprint reader which then verifies the identity.

An Overview of Existing Biometrics Technologies

All biometrics consists of three basic elements: enrollment, templates, and matching. Each technology uses these elements but in their own unique way.

- Enrollment – the process where a user enrolls in the biometric system by giving a sample of their biometric(s) which can be processed and stored for later ongoing use.
- Template – a file derived from the features of a user's biometric sample, used to perform biometric matches. (http://www.biometricsinfo.org/biometric.htm)
- Matching – the comparison of biometric templates to determine the similarity or contrast of an individual's sample.

Face (or Facial) Recognition

Face recognition is one of the newer biometric technologies. The technology analyzes facial characteristics and attempts to match it to a database of digitized pictures. This technology is relatively new and has only been commercially available since the 1990's. Face recognition has received a surge of attention since the disaster of 9/11 for its ability to identify known terrorists and criminals.

Face recognition uses distinctive features of the face – including the upper outlines of the eye sockets, the areas surrounding the cheekbones, the sides of the mouth, and the location of the nose and eyes – to perform verification and identification. (http://www.biometricsinfo.org/facerecognition.htm)

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The first step in face recognition is to obtain an image of an individual and store it in a database for later use. Usually, several pictures (or video images) at different angles are taken. Individuals may also be asked to make different facial expressions for the database. Next, the images are analyzed and extracted to create a template. The last step is to verify the individual's identity by matching the images to those images that have been stored in a database.

There are four main methods being used for facial recognition: (http://www.gaits.com/biometrics_face.asp)

1. Eigenfaces – a tool developed by MIT that extracts characteristics through the use of two-dimensional grayscale imagery.
2. Feature Analysis (also know as Local Feature Analysis (LFA)) – is the most widely used technique because of its ability to accommodate for facial changes and aspect. LFA uses an algorithm to create a face print (84 bytes in size) for comparison.
3. Neural Network – a method that extracts features from the face and creates a template of contrasting elements that is then matched to a template in a database.
4. Automatic Face Processing (AFP) – a technique that looks for distances and distance ratios between certain facial features, and is more ideal for poorly lit areas.

Advantages

- High accuracy rate
- Can be performed from a distance
- Accepted by most users
- Non-intrusive
- Hands-free

Disadvantages

- Cannot always account for the effects of aging
- Sensitive to lighting conditions
- Can perform limited 1-to-many comparisons

Fingerprint Recognition

Fingerprints are unique to each individual and no two fingerprints are alike. Fingerprint recognition is the most widely accepted biometric among the technologies being used today. Fingerprints contain patterns of ridges and valleys as well as the minutiae points. Minutiae points are local ridge characteristics that occur at either the ridge bifurcation or a ridge ending. (http://www.biometricsinfo.org/fingerprintrecognition.htm).

©SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

There are three methods for scanning fingerprints: optical scanners, thermal scanners, and capacitance (solid-state) scanners. Currently, there are two accepted methods for extracting the fingerprint data: minutia-based and correlation-based.

> "Minutia-based is the more microscopic of the two. This method locates the ridge characteristics (branches and endings) and assigns them a XY-coordinate that is then stored in a file. The correlation-based method looks at the entire pattern of ridges and valleys in the fingerprint. The location of the whorls, loops, and arches and the direction that they flow in are extracted and stored. Neither method actually keeps the captured image; only the data is kept, therefore making it impossible to recreate the fingerprint." (http://www.biometricsinfo.org/fingerprintrecognition.htm).

Once the scanning is complete, the analysis is done by a comparison of several features of the fingerprint know as minutia. Investigators or systems look at where the ridgelines end or where one ridge splits in two (bifurcation). The scanning system uses complicated algorithms to recognize and analyze the minutia. If two prints have three ridge endings, two bifurcations, and form the same shape with the same dimensions, then it is likely the same persons fingerprints.

Advantages

- High accuracy rate
- Can perform 1-to-many comparisons
- Inexpensive equipment
- Easy to use (samples are easy to capture and maintain)
- Most establish and oldest of the biometrics technology

Disadvantages

- Actual finger scan images cannot be recreated from a template image
- Users relate fingerprint recognition to criminal activity

Iris Recognition

No two irises are alike, not even in one individual or in identical twins. The iris consists of over 400 distinguishing characteristics. Compared to the 40 or 50 points of distinct fingerprint characteristics, the iris has more than 250 distinct features. Therefore, iris scanning is much more accurate than fingerprints or even DNA analysis because of the analysis of the distinguishing features.

Iris scanning is executed by scanning the measures of the colored circle that surrounds the pupil. With video technology, a camera scans the iris pattern, which consists of corona, pits, filaments, crypts, striations, and radial furrows (Page). The system software then digitizes the unique information of the iris and

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

stores it for authentication at a later time. Iris scanning is painless and only takes seconds to record the iris patterns. Iris scanning is easy, accurate, and convenient. One significant downfall of iris recognition is the initial startup costs as they are extremely high.

In identifying one's iris, there are two types of methods that are used by iris identification systems, passive and active. The active iris system method requires that a user be anywhere from six to 14 inches away from the camera. It also requires the user to move back and forth so that the camera can adjust and focus in on the user's iris. (http://www.gaits.com/biometrics_retinal.asp) The passive system allows the user to be anywhere from one to three feet away from the camera(s) that locate and focus in on the iris.

This technology's main uses are for authentication, identification, and verification of an individual.

Advantages

- High accuracy rate
- Imitation is almost impossible

Disadvantages

- Perceived to be intrusive and invasive
- Can only be done from a short distance
- Optical readers are difficult to operate requiring advanced training for employees

Signature Recognition

Signature verification is the process used to recognize an individual's hand-written signature. Behavioral biometrics of a hand written signature is used to confirm the identity of a computer user. (http://www.biometricsinfo.org/signaturerecognition.htm)

During the verification process, a signature is analyzed by the shape, speed, stroke, pen pressure, and timing information as the individual is signing their name. Dynamic signature verification is a biometric technology this is used to identify a person from their hand written signature.

Dynamic signature verification looks at how the signature was actually made. It is not the shape or look of the signature that is measured but the changes in speed, pressure and timing that matter during the actual act of signing. Only the original signer can recreate the changes in pressure and timing. Even though there may be a slight variation in an individual's signature, the consistency created by natural motion and practice creates a recognizable pattern perfect for biometric identification. (http://www.biometricsinfo.org/signaturerecognition.htm)

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

A forgery of a hand written signature can easily be duplicated but it is almost impossible to duplicate the changes in pressure and timing. In simple signature comparisons, the system only verifies what the signature looks like.

Advantages

- Simple and natural
- People are receptive to signing their name
- Good for document authentication

Disadvantages

- Not widely adopted
- Low level of accuracy

New Biometric Technologies

Biometrics is not limited to the four technologies I have described. There continues to be expansion of the current technology and exploration and innovation into additional biometric security solutions. Nail bed identification and finger geometry are building on existing fingerprint technology. Advancements in security technologies have also made such identifiers as ear shape, odor, vein-scan, and gait recognition possible means of authentication. Although it has been at the forefront in personal identification, DNA matching has continued to improve and become more readily accepted.

The following is a list of newer biometric technologies and how they are obtained.

- DNA – Similar to a genetic fingerprint
- Ear Shape - Geometry of one's ear (shape, size, curves)
- Odor – Human scent of one's hand
- Vein scan – Vein pattern in the face, wrist, or hand
- Finger geometry – Shape and structure of finger or fingers
- Nail bed identification – Ridges in the fingernails
- Gait recognition – Manner of walking

Conclusion

Biometrics has become a growing technology over the past decade. Each biometric technology is unique in its own way and each has its advantages and disadvantages. Whether you are having your face, finger or iris scanned or your voice authenticated, your identity is being verified to allow access to a network, a secured environment, an account, etc…. All the technologies use the same three elements (enrollment, templates, and matching) to recognize an individual and to allow access for that individual.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Biometrics is quick, user friendly, and accurate. All individuals have biometric information whether it is a fingerprint, an iris, or their voice. How convenient is it to not worry about remembering a password? Since passwords can be forgotten, lost, shared, or stone, being your own password is definitely an advantage of biometrics.

Biometric technologies are being developed and utilized all over the world for a wide variety of reasons. The primary uses of biometrics are identification and verification. The banking industry uses iris and fingerprint scanning to identify its account holders and allows them to withdraw money. Prisons use fingerprint scanning to identify and locate inmates. Corporations use voice recognition to reset passwords and iris recognition to access secure areas.

Although the initial costs of biometrics can be quite extensive, the level of assurance attained far outweighs any dollar amount. A few perceived benefits would be more productive employees and improved morale due to an increased feeling of safety, possible insurance savings, and further automation of security procedures (i.e. fewer password resets, less opportunities for human error). One additional benefit would be how seamless and user-friendly the authentication is. Individuals simply do what comes naturally like signing a name or providing a hand or eye for scanning.

The disaster of 9/11 has made organizations, as well as individuals, more aware of the need to have a safe and secure environment in the workplace and in the home. The use of the emerging biometrics technology may well be the answer to the growing concerns of security and identity threats to our society.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

References

"An Introduction to Biometrics." Biometric Consortium. http://www.biometrics.org/html/introduction.html (14 Jul. 2003).

"Biometrics." http://www.biometricsinfo.org/biometrics.htm (23 Sep. 2003).

"Biometrics: The Anatomy Lesson." http://www.findbiometrics.com/Pages/feature%20articles/anatomy.html (9 Jul. 2003).

"Biometrics 101 – The Basics." http://www.findbiometrics.com/Pages/guide3.html (9 Jul. 2003).

"Face Recognition." http://www.gaits.com/biometrics_face.asp (23 Sep. 2003).

"Face Recognition." http://www.biometricsinfo.org/facerecognition.htm (23 Sep. 2003).

"Fingerprint Recognition." http://www.gaits.com/biometrics_fingerprint.asp (23 Sep. 2003).

"Fingerprint Recognition." http://www.biometricsinfo.org/fingerprintrecognition.htm (23 Sep. 2003).

"Iris Recognition." http://www.biometricsinfo.org/irisrecognition.htm (23 Sep. 2003).

Liu, Simon and Silverman, Mark. "A Practical Guide to Biometric Security Technology." http://www.computer.org/itpro/homepage/Jan_Feb/security3.htm (14 Jul. 2003).

Page, Douglas. "The Eyes Have It." http://www.hightechcareers.com/doc198/eyes198.html (14 Jul. 2003).

"Retinal Scanning." http://www.gaits.com/biometrics_retinal.asp (23 Sep. 2003).

"Signature Recognition." http://www.biometricsinfo.org/signaturerecognition.htm (25 Sep. 2003).

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.