# Global Information Assurance Certification Paper

# Biometrics – A Brief Overview

Denice Lauber
GIAC Security Essentials Certification
Practical Assignment
Version 1.4b

**SUMMARY**

Biometrics is a viable replacement for, or enhancement to, the use of passwords or PINs to verify the identity of a person. Each person's characteristics are unique to that individual. Even identical twins do not have the exact same characteristics. Also keep in mind that it is very hard to lose, and impossible to forget your personal characteristics, since they are a physical part of you. The use of biometrics will significantly increase the probability that the person accessing the information is actually the person they say they are. This paper will discuss the different aspects of biometric recognition with focus on the fingerprint recognition biometric.

## AUTHENTICATION

There are three different types of authentication that are in use today. They are something you know, something you have, and something you are.

The first type of authentication, something you know, has been in use for decades. This generally refers to the use of passwords or PINs (Personal Identification Number). Even though individuals are generally forced to use a password or PIN (Personal Identification Number) to access company or personal information, these passwords or PIN are generally very easy to guess or locate. Many people's passwords have a personal meaning. This makes the password or PIN easier to remember. Examples would be the name of their spouse, children, or pets. These passwords would be easy to guess given limited knowledge of the individual. If the password is difficult to remember you will find that the individual has it written on a piece of paper taped to their monitor, or somewhere near their computer. Or, if the individual believes that they are security conscience they will put the piece of paper under their keyboard.

The second type, something you have, is relatively new in the United States, but have been used to some degree in Europe. This type usually is a smart card or token. These are items that you would carry with you to use as identification, similar to a driver's license. These items do represent some type of authentication mechanism, but are relatively useless on their own, since they can be easily lost or stolen.

The third type of authentication, something you are, is generally referred to as a biometric. This is the most secure type of authentication as it cannot be easily lost, borrowed, stolen, or forgotten. It is also the most feared by the general public. Several movies have shown methods that could, in theory, be used to bypass biometric based security access. However that type of forgery is not within the scope of this paper.

## BIOMETRIC IDENTIFICATION

Biometrics can be defined as the automated used of physiological or behavioral characteristics to determine or verify identity. Physiological characteristics are based on information retrieved from a measurement of the human body. Some examples would be fingerprint recognition, facial recognition, optical recognition (iris or retina), or hand geometry recognition. Behavioral characteristics are base on information retrieved from an indirect measurement of the human body. Examples would be voice recognition, keystroke recognition and signature recognition.

## FINGERPRINT RECOGNITION VS FINGERPRINTING

Many people believe that fingerprint recognition biometrics is the same as the fingerprinting techniques that have been used for years by forensics. This is

a misconception. There are two similarities. The first is that an image of the fingerprint obtained from a scanning device. Secondly, the images are stored in a database for future reference. That is where the similarities end. In fingerprinting, a high-quality image of the entire fingerprint is taken and stored in a database. Databases that contain fingerprint images are very large since the size of the image is approximately 256 kilobytes per finger, and a single database can contain millions of fingerprints. The Automated Fingerprint Identification Systems (AFIS) databases used for fingerprint storage by police and governmental agencies can be searched for matches, but it could take hours to find a match. Even when matches are found, there is usually not an exact match, but several close matches.

In fingerprint recognition technology once the fingerprint has been scanned, a template is created that contains a small subset of the scanned data. The size of the template is usually less than 1 kilobyte. Since the size of the fingerprint recognition templates are significantly smaller than the fingerprint images, a search of the database can be completed in less than three seconds. The results of the search are in the form of a Yes/No answer. Either there is a match or there isn't. Also since only a small subset of data from the actual fingerprint image is stored, there is no way for the entire fingerprint to be recreated using the data stored in the template.

**BIOMETRIC SYSTEM**

There are generally five sub-systems in a biometric authentication system. They are data collection, transmission of data, signal processing, decision, and data storage. Each will be described briefly, to give you a general understanding of the sub-system. The fingerprint recognition system is described in greater detail after the general system is explained.

**DATA COLLECTION** - This is the beginning of the biometric authentication system. The individual's behavioral or physiological characteristic must be gathered. This generally involves the individual presenting the characteristic to be measured to a sensor.

**TRANSMISSION** – This stage involves the movement of the data gathered during data collection. Prior to the data being moved it may need to be compressed to conserve bandwidth and storage space.

**SIGNAL PROCESSING** – Feature extraction and quality control are part of this sub-system. Feature extraction involves a non-reversible compression that will ensure that the biometric image can't be reconstructed from the extracted features. Quality control verifies that the signal received from data collection is of high quality.

**DECISION** – This is the actual part of the systems that determines whether or not a match has been made. It compares the sample received against a database of templates. A accept/reject decision is made based on a system policy that has been implemented previously. This system policy determines how closely the data collected must match the data in the database before it is either accepted or rejected.

**STORAGE** – The last sub-system is the actual storage of the data collected in a database. In the instance of registration this is done automatically. Some types of biometric recognition systems will periodically update the data stored in the database, and some systems continually update the data stored.

**CHARACTERISTICS OF FINGERPRINTS**

Below is a picture of a human fingerprint. As you can see it is comprised of what looks to be lines, but are actually ridges. The Biometric Technology Overview on the International Biometric Group website describes the characteristics of a fingerprint as follows:

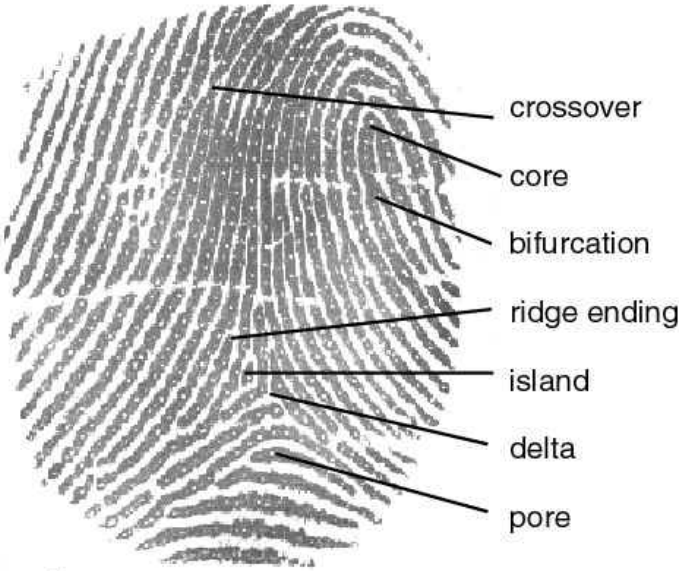


Figure 1

**Minutiae** (Figure 1), the discontinuities that interrupt the otherwise smooth flow of ridges, are the basis for most fingerprint recognition authentication. Codified in the late 1800's as Galton features, minutiae are at their most rudimentary **ridge endings**, the points at which a ridge stops, and **bifurcations**, the point at which one ridge divides into two. Many types of minutiae exist, including dots (very small ridges), islands (ridges slightly longer than dots, occupying a middle space between two temporarily

divergent ridges), ponds or lakes (empty spaces between two temporarily divergent ridges), spurs (a notch protruding from a ridge), bridges (small ridges joining two longer adjacent ridges), and crossovers (two ridges which cross each other).[1]

### EXTRACTION OF DATA

The extraction of the fingerprint data is a relatively easy and painless process. It begins with the individual placing their finger on a platen (a postage stamp size optical or silicon surface). The finger is held on the device for approximately 1 or 2 seconds. During this time the image of the fingerprint is captured. Once the image has been captured, is analyzed by a series of algorithms. These algorithms eliminate unnecessary information, such as dirt, then locate and extract the exact placement of the minutiae, and place the information into a mathematical template. The template is then encrypted and stored in the database where it will be used to authenticate the user's future access.

### AUTHENTICATION PROCESS

Once the fingerprint recognition template has been stored in the database, the user is ready to begin to use their fingerprint recognition device. The process of gaining access to information by authenticating to the database is the same as the extraction process, with one exception. Instead of storing the template in the database, the template is compared to the other templates in the database until a match is found. This process takes approximately 3 seconds. There are times when a match may not be found on the first attempt. This could occur due to the platen being smudged or being dirty. Simply cleaning the device and going through the authentication process a second time should result in a match being found.

### ACCURACY

As with all computer systems, the accuracy of the data within the system is only as good as the information that is put into the system. There are many factors that contribute to the quality and performance of the fingerprint recognition authentication process. The device that is used to obtain the fingerprint recognition must produce a high quality image. The software involved in creating and then matching templates on a large database must also be very accurate. Besides the actual device and software there are a multitude of other factors that need to be considered. These factors include, but are not limited to: environmental conditions, user training, ergonomic conditions, enrollment procedures, and demographics of the enrollees. When evaluating a biometric system there are generally three acronyms that you will see frequently. They are the FRR (False Rejection Rate), the FAR (False Acceptance Rate), and the FTE

[1] Fingerprint Feature Extraction

(Failure to Enroll Rate). These three measurements must also be taken into account when testing a fingerprint recognition system. Ideally the system used to authenticate individuals must be precise enough to reject unauthorized individuals, but must be adaptable to slight changes in the fingerprint recognition image. Such changes could include a minor cut or abrasion, dirt, high/low humidity, angle of placement on the scanning device, and many others. With the proper scanning device, software, and user training the fingerprint recognition can be a very reliable and accurate means of user authentication.

**OTHER TYPES OF BIOMETRIC RECOGNITION**

Each type of biometric registration uses a different characteristic or group of characteristics to determine a match. However they all work basically the same as the fingerprint recognition system. Below are other types of biometric recognition.

**FACIAL RECOGNITION** – The analysis of facial characteristics is the basis for this biometric. A digital camera is used to capture an image for authentication. At the present time the casino industry has been the only industry to utilize this type of biometric. They have created a database of scam artists that can be used by security personnel to quickly identify these scam artists. Facial recognition has also been used frequently by Hollywood in many futuristic movies.

**OPTICAL RECOGNITION (IRIS AND RETINA)** – This type of recognition involve the scanning of either the iris or the retina, and the characteristics are stored, and used for authentication. This type of authentication is more accurate than fingerprint or hand biometrics because there are more characteristics that can be identified. However, the general public is very protective of their eyes and very cautious when it comes to placing items close to their eyes. There are also difficulties with these devices when registering people who are blind or who have cataracts.

**HAND GEOMETRY RECOGNITION** – Measures the physical characteristics of the hand and fingers from a three dimensional perspective. This method of authentication would be a good match for a system with a large user base, or one in which the user infrequently requires access.

**VOICE RECOGNITION** – This method is not based on actual voice recognition, but on a voice-to-print authentication. This complicated technology actually transforms the voice to text. The drawback to this is that your voiceprint could vary from day to day based on many factors, such as your health. This type of recognition is not personal intrusive to the user, and as such is generally accepted. My company recently implemented a voice recognition system for verification of password resets. The system has

been in place for several months, and seems to have been accepted very well.

**KEYSTROKE RECOGNITION** – This type of recognition system is used in conjunction with a password or PIN. Not only must the individual know that password or PIN they must be able to type it at the same rate, and with the same time intervals between letters or numbers. The keystroke recognition biometric has not been widely implemented, but is one of the cheapest and easiest biometric technologies to implement.

**SIGNATURE RECOGNITION** – Signature recognition is one of the most common types of non-technologically based recognition, and has been in use for centuries. However with the use of biometric technology, not only is the actual two-dimensional signature stored, but a three-dimensional signature is stored. The third dimension is the amount of pressure applied while making the signature. This helps to reduce the possibility of forgery. A drawback to this is that you don't always make your signature exactly the same every time.

## CURRENT APPLICATIONS OF BIOMETRICS

There are numerous applications for the use of biometric recognition systems. Some of these applications include:

**PC/LAN/Application Logon** – Fingerprint recognition biometrics could be used in place of or in conjunction with the user logon procedures. The biometric device could be placed in the mouse or keyboard, and instead of entering a password to gain access to the system, the individual would simply place their finger on the scanning device. This would eliminate the need for the individuals to remember their passwords, and also reduce the cost of password reset calls to the support center.

**Single Sign On (SSO)** – This is the process by which an individual obtains access to all required resources through a single authentication process. This would eliminate the need for the user to maintain and remember multiple passwords. Since biometrics is based on physical characteristics that are almost impossible to duplicate the security concerns associated with a single Sign On system are almost eliminated.

**Website Account Access and Purchasing** – When you consider the enormous number of purchases and the amount of money that is changed hands over the internet a biometric logon is the most secure manner to handle these transactions. Not only does it eliminate multiple logons and numerous passwords, it provides non-repudiation to the sellers. With a biometric logon, the purchaser cannot deny that he or she participated in

the transaction, because the logon was accomplished with his or her fingerprint.

**National Border Crossing** – John F. Kennedy airport in New York was the first airport to use the INSPASS (Immigration and Naturalization Service Passenger Accelerated Service System). This system implemented in 1993 by the United States immigration authority used hand geometry recognition to identify and process passengers more quickly immigration. The system was completely voluntary and was used by frequent travelers. One of the conditions of use was that the individual must be a United States or Canadian national, or a national of a country involved in the United States visa waiver scheme. Individuals wishing to use the system were interviewed and their identity confirmed. They then placed their hand on the scanner, and the template was stored on a card. To use the system, the individual enters a kiosk and inserts the card into a terminal. The individual then places their hand on a scanner. The scan of the hand from the reader is then matched with the template stored on the card. If there is a match, the individual is allowed to proceed. The system is also in use at the airports in Newark, Los Angeles, Miami, and San Francisco. Our neighbors to the north also implemented a similar system in the Vancouver and Toronto airports. The Canadian systems utilize fingerprint recognition devices to allow frequent visitors to pass through inspection points rapidly.

**Drivers License Verification** – To reduce the number of counterfeit driver's licenses that are being issued, many states which are incorporating a biometric fingerprint recognition computer chip within the driver's license.

**Physical Access** – Many companies have implemented tighter security access to buildings since the terrorist attack on September 11. One of the means that some companies are employing is fingerprint recognition devices to grant access to the actual building. Furthermore, fingerprint recognition devices are being installed within the buildings to grant access to more restricted areas.

**Social Welfare** – In 1996 the Canadian province of Ontario had a population of ten million people. However there are over twelve million people receiving the benefits of the health care system. The government in that region evaluated use of biometric cards to identify the individuals that should actually be receiving the benefits of the Canadian health care system. The United States government also researched the use of biometric cards to reduce welfare fraud.

**Prison Systems** – These systems are used to verify visitors, inmates, and employees. They are most widely used to verify that the inmates are not swapping identities with either visitors or employees to gain their freedom.

**Cafeteria Administration** – Mostly used on college campuses as verification that the individual using a subsidized meal plan is actually the person requesting the service.

**Time and Attendance reporting** - Used to replace paper time cards.

**Vehicle Access and Ignition Security** – On some of the more expensive vehicle models, this is being used to replace the keypad security system. The use of biometric technology can be used reduce the number of stolen vehicles, and depending on the biometric technology used, possibly the number of individuals driving under the influence of alcohol.

**National Identity Cards** – At the present time Hong Kong is in the process of issuing "smart cards" to each of its 6.8 million citizens. This process is set to be completed by mid-2003. These cards will contain a digital photograph of the owner, their fingerprints, and such personal information as their name and date of birth. The United States would like to implement a similar "smart card", but has met substantial resistance from groups such as the American Civil Liberties Union (ACLU).

**Other** – Other applications of biometrics include, but are not limited to: ATM transaction verification, personalized firearm safety, security guard tour tracking, portable law enforcement identity checks, and secure cable TV access.

## PUBLIC ACCEPTANCE

In the past, the general public's acceptance of biometric recognition has been very low. Most individuals within the public sector view biometric recognition as a way for the government to "keep track" of an individual. Sort of a "Big Brother" type scenario. The movie industry has not been beneficial in the acceptance of biometric technology either. Many futuristic movies portray biometric technology in just that manner, as a way for anyone to know where you are at any given time.

The biggest fear among the general public in is the loss of privacy. As individuals we value our privacy very highly, and if biometric type identification and authentication systems are to gain acceptance they must be able to ensure this privacy. Many states currently have pending legislation, regulations, or other initiatives underway to ensure that an individual's privacy is protected with regard to biometric devices. Some of these states include Virginia, California, and Indiana to name a few.

Concerns over privacy and biometrics are not limited to the United States. The European Commission recently created a committee titled the "Initiative on

Privacy Standardization in Europe" (IPSE). This committee released a report that is to be used to help provide clear guidance to European businesses on how they could comply technologically with Directive 95/46/EC. This directive deals with privacy and data protection. The IPSE project team described what they termed "Privacy Enhancing Technologies" (PET). Biometric readers where the main source of "Privacy Enhancing Technologies" mentioned in the report. The reason for this is that biometric readers do not store actual images, instead they store encrypted templates of physiological features. These templates cannot be used to directly or indirectly identify an individual. In essence the biometric templates cannot be used to re-create personal information, cannot be used to access personal information, and cannot on their own be used to reveal a person's identity.

**THE FUTURE OF BIOMETRICS**

Within the next few years the use of biometrics will significantly increase. This increase in use will be due to several reasons. The first being that the size of the recognition device is small enough to be incorporated into almost any type of device. Another reason that the devices will become more common is that the cost of the technology has been, and will continue to decrease. Currently you can purchase some recognition devices and software for well under $100.00. But the most significant reason is that people will become more familiar with the technology, and will be less afraid of the technology being used to invade their privacy. Fingerprint recognition biometric devices are currently being built into keyboards, PDAs (Personal Digital Assistant), cell phones, and the computer mouse. It is speculated that by the year 2005, all computer systems sold will include some type of fingerprint recognition biometric device.

Use of biometrics will also be increased due to government legislation, both here and in Europe. In the United States, the General Accounting Office (GAO), based on advice from the National Institute of Standards and Technology (NIST) recommended the utilization of biometrics to strengthen security. This was done thru the issuance of two reports to congress that suggested the use of biometrics in travel documents and government-issued multi-purpose smart cards. In one of the reports the General Accounting Office recommended the use of finger and facial biometrics issued to all foreign nationals by the State Department and the Immigration and Naturalization Service (INS).

## GLOSSARY

**AFIS** – Automated Fingerprint Identification System

**FRR** – *(False Rejection Rates)* is the likelihood that the system will reject an enrolled user's fingerprint

**FAR –** *(False Acceptance Rates)* is the likelihood that the system will accept a non-enrolled user's fingerprint

**FTE –** *(Failure to Enroll Rate)* is the rate at which the system is unable to enroll users

**PIN** – *(Personal Identification Number)* is usually a 4-digit number assigned to an individual to allow them access to information.

**PDA** – *(Personal Digital Assistant)* is a device that is usually about the size of your hand that stores data similar to what you would normally find in a calendar or planner.

## SIMILAR TOPICS

1. Facial Recognition Biometrics
2. Optical Recognition Biometrics
3. Fingerprint Classification and Recognition

## References

1. "Fingerprint Feature Extraction" http://www.ibgweb.com/reports/public/reports/finger-scan_extraction.html (March 30, 2003)

2. Alexander, Michael, Underground Guide to Computer Security. Addison-Wesley Publishing Company, November 1995. 54-61.

3. "Finger-Scan Accuracy". http://www.finger-scan.com/finger-scan_accuracy.htm (January 19, 2002)

4. Liu, Simon and Silverman, Mark. "A Practical Guide to Biometric Security Technology". http://www.computer.org/itpro/homepage/Jan_Feb/security3.htm (January 18, 2002)

5. Biometrics Advocacy Report. http://www.ibia.org/newslett030221.htm (Volume 5, Number 3, Friday, February 21, 2003)

6. Biometric Encryption. http://www.emory.edu/BUSINESS/et/biometric/

7. "An Overview of Biometrics". http://biometrics.cse.msu.edu/info.html

8. Ashbourn, Julian. "The Biometric White Paper". http://homepage.ntlworld.com/avanti/whitepaper.htm (1999)