Biometrics - The Wave of the Future?

By
Gary Daniel

ICTN4040
Dr. Phillip Lunsford

Will biometrics be a factor in our future? Of course it will, at least to the extent that it has been in our past history. We as citizens must decide upon the best methods to use and the best way to utilize this technology. Biometrics can be defined in several ways such as the study of measurable biological characteristics. In reference to Information Security it specifically applies to the automated use of physiological or behavioral characteristics to determine or verify identity.

Variations of biometrics have been in use for a long, long time now. One of the earliest examples of a form of biometrics could be considered to be the cave paintings where there is presumably a signature indicated by the outline of a human hand by some of the paintings. In China, biometrics were used in the 14th century to identify children to merchants, the merchants would take ink and make an impression of the child's hand print and footprint in order to distinguish among them. Facial recognition has been one of the most used biometrics throughout history. These early examples were the beginning of what we now term biometrics, when broken down to the Greek meanings, bio meaning "life" and metric being a "measurement". Other forms of biometrics were utilized throughout history to include the fingerprint technique used to identify criminals which is still in widespread use today. The fingerprint method has been used successfully in law enforcement now for many years as it is a very accurate and reliable method to determine an individuals' identity but relies on the fact that the fingerprints had to already be on file in order to provide a match. A system known as the anthropometric system was developed by a French police desk clerk named Alphonse Bertillon in 1883 to identify criminals by measuring the head and body lengths and widths (http://www.answers.com/topic/biometrics). This method was utilized until it

was discovered that there were too many inaccuracies with the methods utilized to measure and the fact that the measurements changed over time thereby not making them a unique and accurate enough symbol to provide positive identification. Biometrics are not really new technology but the manner in which we can now utilize these unique features with the aid of computers is new.

Even though biometrics have been around for a long time, the abilities to use them in the manner that we now can is the difference. In effect we are using many of the same identification means as our ancestors just in a new way. With the ever emerging technological fields we now have the capability to use them automatically. With these advances come the new horizons and responsibilities of managing that technology. The modern versions of biometrics share some of these same characteristics as there must be a "template" in a database in which to match the input data to in order to provide for identification or verification, which are the two primary objectives of biometrics. Identification is the process associated with establishing a person's identity while verification is the process of confirming or denying the identity that a person claims to be.

Biometrics as we know them have been divided into two categories, physiological and behavioral, iris, fingerprint, hand, face, voice, retina, odor, earlobe, lips are examples of the physiological means whereas signature, keystroke, voice and gait are examples of behavioral patterns that can be observed. Of these, so far the fingerprint reader appears to be the best value having the cheapest cost with a high degree of reliability. Iris scanning has the highest degree of reliability but the cost and the perceived intrusiveness of having a light scan the iris make it so far not a very accepted practice.

The systems are very hard to mimic and one of the most important reasons for biometric use is the fact that you cannot lose that biological trait as easily as you could lose a password, smartcard or authentication token. While they do not have the same vulnerabilities as their predecessors, there are disadvantages to the modern biometrics as well. People are reluctant to use anything that appears to be invasive to them such as the iris scanner which has a very high degree of accuracy but requires contact with the machine which raises concern about hygiene. Also raised are social and ethical issues as "measurements can be obtained from an individual with or without their consent and in some cases, with or without their knowledge."(Azari p112). If a password or code becomes compromised or if a key is stolen an individual has some form of recourse, however if a biometric is compromised, there is a serious problem as the individual characteristic on which the biometric is based cannot be changed (Azari p122). This is a good reason that encryption is recommended by leading industry organizations such as International Biometrics Industry Association (IBIA) and the BioAPI Consortium. The answer to a prominent issue of what if the authentication does not work is to have a backup method to utilize as well in the event that something goes wrong and you cannot be authenticated with the primary method. This method could consist of a bimodal function or using more than one metric to authenticate. Biometrics are not foolproof but as a technique to positively identify an individual they are more reliable and accurate than other forms of authentication and harder to spoof.

What is the best type of method? That depends on the proposed use. For example, some of the biometrics such as hand geometry may be perfectly suitable for small scale

use in a local area but this particular type of biometric does not scale well to a much larger database.

Concern over the use of the data continues to plague many citizens leading to a distrust that prevents wide saturation of the use of biometrics, invasion of privacy issues are big on the list. In May 2005, congress signed into law an act known as the "Real ID" Act that requires that all states by the year 2008 issue federally approved drivers licenses or id cards that will contain biometric information about you with the idea after 9/11 that it will make it more difficult for someone such as a terrorist to get on an airplane or bus. Some of the more controversial issues that are raised in this scenario are "what about homeless people?", "what about illegal immigrants". Are we not the land where the downtrodden and exploited seek refuge? While some of the reactions to using biometrics on a wide scale may be "overreacting", it is better to be safe than sorry so to that end the issues should be thoroughly investigated and resolved prior to implementation.

In order for a wide implementation of this technology, standards must be developed that will allow for their consistent use. The International Organization for Standards ISO/IEC JTC1 is the governing body of international biometric standards, but this standardization is still in progress. In the future, fixed biometric standards will be in place to guide vendors and developers in the areas of biometric application profiles, interfaces, and system performance. Along with standardization there should be certain privacy issues addressed by law such as privacy and specific use guarantees as well as checks and balances to conduct audits to ensure compliance with these guarantees. In future implementations biometric systems should contain the ability to handle exceptions as well such as an individual that does not have the required biometric. Also there are

religious confines that should be addressed as in some religions, people will not have their picture taken. Are we ready for the widespread use of this technology? That is a question that will be answered with acceptance. Only when the public deems that enough security and privacy concerns have been addressed to satisfaction will the technological benefits be realized.

Some of the current uses of this technology are the US-VISIT program that was instituted in January 2004 where the U.S. Department of Homeland Security takes photographs and digital fingerprints of some of the visitors prior to them entering the U.S. and then compares them to a database of known criminals and terrorists. Some Federal buildings and corporations are utilizing biometrics for entry to the office buildings and secure areas. There are a number of countries as well that are in the process of implementing biometrics into passports as well. Biometrics are being utilized for border security as well as at airports around the globe. With escalating world issues such as terrorism being the drivers behind the pushing for some means of figuring out who is where and what they are doing at any given moment will some of our liberties be lost? Will the methods when implemented actually make us safer? Can this technology make us more secure? These are some of the questions that people should be asking themselves.

There are many common future every day uses in which the biometric field could provide greater efficiency and enhance our lives such as the possible use to unlock and start your car, to open the doors to your home and office, to access account at a bank or Automated Teller Machine, turn on appliances or stereos, etc. There would be no access cards, no keys, just your body as the method with which to gain access. E-commerce is

one of the ways in which consumers as well as companies will find useful the biometric field as purchases online become more common and frequent.

The future of biometric use is in our hands and we must now decide what to do with it. While there are still a vast amount of issues that need to be resolved to some level of satisfaction biometrics are the wave of the future and are not going to go away so we need to decide how we are going to ride this wave. While the convenience of this technology is apparent we must address the many issues such as privacy and protection of personal information because this new way of movement throughout the world is gaining momentum and will evolve, the question is how will it evolve and how can we make maximum use of it and still maintain our anonymity. With the proper guidance mechanism in place biometric technology has the potential to improve security without seriously compromising individual privacy (Langenderfer and Linnhoff, p321).

.

References

http://www.biometricscatalog.org/biometrics/FAQDec2005.pdf

http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0525.xml

http://www.biometricsinstitute.org/displaycommon.cfm?an=1&subarticlenbr=28

*http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_7-1/lures_of_biometrics.html The Lures of Biometrics-The Internet Protocol Journal-Volume 7, Number 1-Cisco Systems, Danielyan, Edgar, Danielyan Consulting LLP

Current Security Management and Ethical Issues of Information Technology, IRM Press, edited by Azari, Rasool, University of Redlands, USA.

*http://www.blackwell-synergy.com, Journal of Consumer Affairs, Volume 39, Issue 2 Page 314-September 2005, "The Emergence of Biometrics and Its Effect on Consumers", Langenderfer, Jeff and Linnhoff, Stefan.

http://biometrics.cse.msu.edu/info.html

http://www.answers.com/topic/biometrics