John Bruce Wallace

Biometrics

Biometrics a paper completed as part of the requirement of IFSM 430 Information Systems and Security University of Maryland University College July 23, 2006

Abstract

Biometrics refers to the automatic identification of a person based on that person's physiological or behavioral characteristics. Biometrics identifies a person via a unique human characteristic: the size and shape of a hand, a fingerprint, one's face, or several aspects of the eye. Biometrics answers the two fundamental questions regarding an individual's identity: verification and identification. Biometrics provides answers to these two questions by establishing a pattern-recognition identity of an individual using physical/physiological characteristics, behavioral characteristics, or a combination of both. At its most simple level, biometric systems operate on a three-step process which involves the physical input of data, the verification of the input data, and finally identification -- the processing of the data.

The goal of any access control system is to let authorized people, not just their credentials, into specific places. If the goal of an access control system is to control where people, not credentials, can and cannot go, then only a biometric device truly provides this capability to the end user. Only with the use of a biometric device can this goal be achieved. Security systems use biometrics for two basic purposes: to verify or to identify users. The biometric that a security system employs depends in part on what the system is protecting and what it is trying to protect against.

Although companies are using biometrics for authentication in a variety of situations, the industry is still evolving and emerging.

Table of Contents

Biometrics In General:

Biometrics is the up and coming authentication and authorization security technologies. Although not an entirely new concept, as variations of fingerprint and foot print identification have been utilized to identify individuals for several centuries, biometrics has, with the advent of widespread globalized computerization of societies, become the focal-point of technological security, in particular where it is imperative to have security control over the individual as opposed to security control over say the company's current inventory. Biometrics refers to the automatic identification of a person based on that person's physiological or behavioral characteristics. Biometrics identifies a person via a unique human characteristic: the size and shape of a hand, a fingerprint, one's face, or several aspects of the eye. Further research in Biometrics is focused on utilizing markers in DNA as a unique and secure identifier. If the goal of an access control system is to control where people, not credentials, can and cannot go, then only a biometric device truly provides this capability to the end user. Biometrics answers the two fundamental questions regarding an individual's identity: verification and identification. Biometrics provides answers to these two questions by establishing a pattern-recognition identity of an individual using physical/physiological characteristics, behavioral characteristics, or a combination of both. Fundamentally these characteristics focus on the specific areas indicated below.

Physical biometrics include:

- Fingerprint
- Facial recognition
- Hand geometry
- Iris scan
- Retinal scan
- Vascular patterns
- DNA
- Biometric data watermarking

Behavioral biometrics include:

- Voice recognition
- Signature recognition
- Keystroke patterning

At its most simple level, biometric systems operate on a three-step process which involves the physical input of data, the verification of the input data, and finally identification -- the processing of the data. More explicitly:

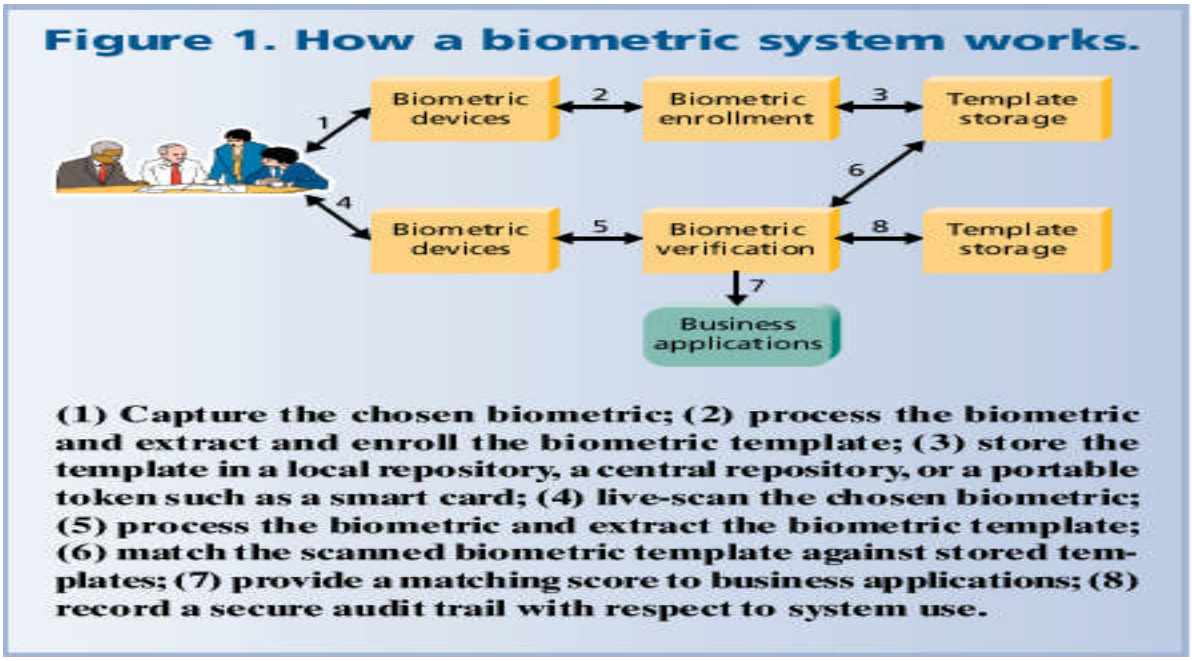
- First, Enrollment, the enrolment process is the first contact of a user with the biometric system. This process is necessary because a biometric verification system has to 'learn' to verify the identity of each user based on his biometric characteristic. During the enrolment process the system captures the biometric characteristic of a user and extracts the features it is working with. This feature vector is then combined with the identity of

the user to a Biometric Identification Record (BIR) and stored in a database. The specific biometric system recognition software configures the input data into a template that is based on mathematical algorithms that the system software processes as a series of numbers, a biometric signature. The BIR is also called template. Generally the development of the template requires that several impressions of the data object must be recorded, *i.e*., for fingerprints usually it takes at least four impressions of the fingerprint to create the template. In other words the supplicant must present their finger several times to the scanner in order for enough information to be recorded to create the template. The type of sensor and its observation will vary by biometric type. For face recognition, the sensor is usually a camera and the observation is a picture of an individual's face. More specifically the generated facial template is more like a map of the various planes, plateaus, and valleys of the face in grayscale.

- Second, Verification, The verification process is the major functionality of a biometric system. Its objective is to verify or refuse a claimed identity of a user. Therefore the user has to assert an identity to the system. The system then gets the BIR associated with this identity from the database and captures the biometric characteristic of the user. If the Biometric Live Record (BLR) that is extracted from the characteristic and the BIR from the database are similar enough, the claimed identity of the user is verified. Otherwise or if no BIR was found for the user, the claimed identity is refused. The method will again vary not only by biometric type, but also from vendor to vendor.
- Third, Identification, The objective of a biometric identification process is quite similar to a verification process. But in contrast to the verification process there is no claimed identity necessary. The system directly captures the biometric characteristic of a user and inputs the biometric signature into a comparison algorithm comparing it to one or more biometric signatures previously stored in its database. If at least one BIR is found to be similar enough, the system returns this as the found and verified identity of the user. Other system components, or a human operator, then use these result(s) for other actions such as allowing computer access, sounding an alarm, etc. Although understanding the three-step biometric process is sufficient for most users, biometric systems are in reality much more complicated and there are potentially several alternative input and processing methods for each type of biometric, *i.e.*, facial recognition may be captured via camera, or infrared camera.

(Blackburn, 2004; BSI, 2005; Chirillo, 2003)

Simon Liu and Mark Silverman in their article "A Practical Guide to Biometric Security Technology What Is A Biometric" present a very insightful diagram with explanation of how a biometric system works including the biometric capture and process procedure for creating a template. Contrasting Liu's diagram with the simplified explanation of how a biometric system works: the first step in the simple view would roughly correspond to steps 1 and 2 in Liu's diagram; the second step would roughly correspond to steps 2 and 5 in Liu's diagram; and the third step would roughly correspond to steps 4 through 8 in Liu's diagram. Liu's diagram follows as Figure 1:



(Liu, 2001)

As with all security systems, a system is only as strong as its weakest link or process. The effective quality of a biometric system's performance is evaluated based on three types of error rates:

- Type I errors also known as False Reject Rate – indicates the percentage of the rate at which supplicants who are authorized to have access to the system are denied or prevented access as a result of some failure of the biometric software or hardware. A low False Reject Rate is very important for most applications, since users will become extremely frustrated if they're denied access by a device that has previously recognized them. As a means of increasing the effectiveness of a security system, the combination of a low False Reject Rate plus a simple keypad code provides virtually unbreakable security.
- Type II errors also known as False Accept Rate – indicates the percentage of the rate at which supplicants that are not authorized users of the system are allowed access as a result of a failure in the biometric software or hardware. This figure must be sufficiently low to present a real deterrent. It's important to remember that the only way an intruder can get access is if an intruder tries. Thus, the False Accept Rate must be multiplied by the number of attempts by intruders to determine the number of possible occurrences.
- Crossover Error Rate (CER) also known as the equal error rate is the point at which the number of false rejects equals the number of false accepts. The Equal Error Rate provides a good indicator of the unit's performance. The smaller the Equal Error Rate, the better.

(Chirillo, 2003; Recognition Systems Inc.; Whitman, 2005)

Proven Biometric Technologies Currently Available:

There are a wide variety of human characteristics used by biometric devices to confirm a person's identity. The biometric industry is constantly finding new attributes and ways to measure their uniqueness. Here are the more frequently encountered biometric devices which

focus on the physical characteristics of a supplicant that are commercially available and in use in one form or another today

- Hand Geometry. The size and shape of the hand and fingers is used by a handreader to verify a person's identity. Hand geometry evaluates a three dimensional image of the fingers and part of the hand. It was the technology used for the very first commercially available biometric device, which came to market in 1976. It continues to be the most widely used biometric device for access control applications.
- Fingerprint. Law enforcement agencies have used fingerprints for decades to identify individuals, and businesses continue to do so today when undergoing background checks. However, the relatively inexpensive fingerprint access control readers that are available to the commercial market are different than these devices. The FBI system takes images of all ten fingers, while an access control fingerprint product available to the general commercial market may only capture one or two fingers for verification. Fingerprint readers create a template in a process similar to hand geometry readers for local comparison. Due to concerns regarding the total time it takes for a person to use the device (throughput), fingerprint access control may be best applied in smaller user populations. Because of cost and size, they are a perfect choice for single person verification applications, such as in logical access control, where they are used to log onto personal computers (PCs) or computer networks. In the current technological security market, there is certainly a fast growing demand for this technology.
- Facial Systems. Most facial recognition technology works by one of two methods: facial geometry or eigenface comparison. Facial geometry analysis works by taking a known reference point (for example, the distance from eye to eye), and measuring the various features of the face in their distance and angles from this reference point. Eigenface comparison uses a palette of about 150 facial abstractions, and compares the captured face with these archetypal abstract faces. In each method a template of the recorded data is created, *i.e.*, with the geometric method the shape of the face, determined by distances between the eyes, ears and nose and other facial characteristics is recorded into a template. When a person seeking access to a system or physical area is viewed via a computer connected camera, the captured image is matched against the template to verify the identity of the person. This is a technology many organizations are looking closely at for use in the fight against terrorism as the system could scan large crowds or people waiting in line for images of known and potential suspects. The system can select individuals singled out of a crowd via the review of the facial images captured in an image of a crowd that should be further scrutinized. In many instances, facial systems will be combined with another technology, for instance a facial scan may be combined with voice recognition or a password to allow access to a secure area.
- A dual biometric technology, which combines hand geometry and facial recognition technologies. The system works well in conjunction with travel documents and provides unparalleled convenience for three-factor authentication of face, card, and hand.
- Eye – Retina/Iris scans. The human eye offers two features with excellent properties for identification. Both the iris and the veins of the retina provide patterns that can uniquely identify an individual. Retinal scanning is the older technology, and requires the subject to look into a reticle and focus on a visible target while the scan is completed. With iris

scanning the scanner stores 247 traits of a person's iris into a template. The iris scanner illuminates the iris with invisible infra-red light, which shows details on darker-colored eyes that are not visible to the naked eye. The pattern of lines and colors on the eye are, as with other biometrics, analyzed, digitized, and compared against a reference sample for verification. The system functions with contact lenses and eyeglasses, but not with sunglasses. It works in an identification mode or in conjunction with Personal Identification Numbers (PINs) or cards. At a security verification/access point the user tilts the reticle unit so that his eye appears in the center of the image capture area. This image passes to a processing unit via network wiring to be compared with the iris template, otherwise known as the iris barcode, on files. When the system is used as a security verification/authentication point for access to several secured rooms or areas, several doors can be connected to the processing unit, which would grant access in instances where the supplicant's identity and authorization to access the area are verified. While the technology is quite accurate, the high cost per door limits its widespread adoption for general commercial applications.

Other biometric devices that focus on the behavioral characteristics of a supplicant emphasis keystroke, voice or speech recognition, and signature recognition have found widespread use in banking, pharmacy prescription services, virtual signatures and certificates of authenticity in e-mail and e-commerce applications.
(Abernathy; Spence; Chirillo, 2003)

The Benefits of Biometrics in Access Control: Areas of application and examples of biometrics utilized:

The goal of any access control system is to let authorized people, not just their credentials, into specific places. Only with the use of a biometric device can this goal be achieved. A card-based access system will control the access of authorized pieces of plastic, but not who is in possession of the card. Systems using PINs (personal identification numbers) require that an individual only know a specific number to gain entry. But, who actually entered the code cannot be determined. On the contrary, biometric devices verify who a person is by what they are, whether by hand, eye, fingerprint, or voice characteristic. Biometrics eliminates the need for cards. While dramatic price reductions have lowered the capital cost of the cards in recent years, the true benefit of eliminating them is realized through reduced administrative efforts. For instance, a lost card must be replaced and reissued by someone. Just as there is a price associated with the time spent to complete this seemingly simple task, when added to other system related costs, the overall administration of a card system is costly (Spence).

Security systems use biometrics for two basic purposes: to verify or to identify users. Identification tends to be the more difficult of the two uses because a system must search a database of enrolled users to find a match (a one-to-many search). The biometric that a security system employs depends in part on what the system is protecting and what it is trying to protect against.

- **Physical Access --** For decades, many highly secure environments have used biometric technology for entry access. Today, the primary application of biometrics is in physical security: to control access to secure locations (rooms or buildings). Unlike photo identification cards, which a security guard must verify, biometrics permit unmanned access control. Biometric devices, typically hand geometry readers, are

deployed in office buildings, hospitals, casinos, and health clubs. Universities are using handreader biometrics to secure access to dormitories, campus housing, and other areas where authentication of a person's identity is a priority for access to the area. Colleges and universities are also using handreaders and fingerprint readers to control and record the access to dining halls to record student meal accounts. Biometrics is useful for high-volume access control. For example, biometrics systems controlled access by people to events during the 1996 Olympic Games, and Disney World uses a fingerprint scanner to verify season-pass holders entering the theme park.

Engineers are developing several promising prototype biometric applications to support the International Air Transport Association's Simplifying Passenger Travel (SPT) initiatives. One such program EyeTicket is currently under evaluation by several airports worldwide. EyeTicket links a passenger's frequent-flyer number to an iris scan. After the passenger enrolls in the system, an unmanned kiosk performs ticketing and check-in (without luggage) functions.

The US Immigration and Naturalization Service's Passenger Accelerated Service System uses hand geometry to identify and process pre-enrolled, low-risk frequent travelers through an automated immigration system. Currently deployed in nine international airports, including Washington Dulles International, this system uses an unmanned kiosk to perform citizenship-verification functions.

- **Virtual Access --** For a long time, biometric-based network and computer access were areas often discussed but rarely implemented. Recently, however, the unit price of biometric devices has fallen dramatically, and several designs aimed squarely at this application are on the market. Analysts see virtual access as the application that will provide the critical mass to move biometrics for network and computer access from the realm of science-fiction devices to regular system components. At the same time, user demands for virtual access will raise public awareness of the security risks and lower resistance to the use of biometrics. The use of fingerprint readers built into laptop computer has become a standard security feature now built into new models coming on the market.

  In the business environment physical lock-downs can protect hardware, and passwords are currently the most popular way to protect data on a network. Biometrics, in the form of voice recognition for instance, can increase a company's ability to protect its data by implementing a more secure key than a password. Using biometrics also allows a hierarchical structure of data protection, making the data even more secure: Passwords supply a minimal level of access to network data; biometrics supplies the next level. You can even layer biometric technologies to enhance security levels, perhaps combining a hand or fingerprint reader with voice recognition in order to validate access to an organization's network and than data files.

- **E-commerce Applications --** E-commerce developers are exploring the use of biometrics and smart cards to more accurately verify a trading party's identity. For example, many banks are interested in this combination to better authenticate customers and ensure non-repudiation of online banking, trading, and purchasing

transactions. Point-of-sales (POS) system vendors are working on the cardholder verification method, which would enlist smart cards and biometrics to replace signature verification. Credit Card vendors estimate that adding smart-card-based biometric authentication to a POS credit card payment will dynamically decrease fraud.

Some e-commerce vendors are starting to using biometrics to obtain secure services over the telephone through voice authentication. Developed by Nuance Communications, voice authentication systems are currently deployed nationwide by both the Home Shopping Network and Charles Schwab.

- **Covert Surveillance --** One of the more challenging research areas involves using biometrics for covert surveillance. Using facial and body recognition technologies, researchers hope to use biometrics to automatically identify known suspects entering buildings or traversing crowded security areas such as airports. The use of biometrics for covert identification as opposed to authentication must overcome technical challenges such as simultaneously identifying multiple subjects in a crowd and working with uncooperative subjects. In these situations, devices cannot count on consistency in pose, viewing angle, or distance from the detector, essentially critical factors in assuring that an accurate image is captured for comparative purposes against a database of profiled subjects.

(Liu, 2001; Chirillo, 2003)

Integration Tailored to the Application and Organization Served:

Access control requires the ability to identify the person plus unlock a door, grant or deny access based on time restrictions, and monitor door alarms. There are a variety of ways biometrics accomplishes this task.

- Standalone Systems. Many biometric devices are available in a standalone configuration. Such devices are not only a biometric, but also a complete controller for a single door. Users are enrolled at the unit and their biometric template is stored locally for subsequent comparison. The actual comparison is accomplished within the unit and a lock output is energized depending on the outcome.
- Networked Systems. Many access control applications may be assigned to manage more than one door or access point. While multiple standalone units could be employed, a network of biometric readers is much more feasible. By networking the systems together and then connecting them to a computer, several advantages are available to users. The most obvious is centralized monitoring of the system. Alarm conditions and activity for all the doors in the system are reported back to the Centralized Control System (CCS). All transactions are stored on the CCS computer's disk drive and can be recalled for a variety of user-customized reports.
- Networked systems also provide convenient template management. Although a user enrolls at one location, his template is available at other authorized locations throughout the system. Deletion of a user or changes in his access profile is simply entered at the CCS. Some biometric systems store all information in the CCS where template comparisons are also performed. Others distribute template information to

the individual readers at each door. Either way, the net effect of template management is the same.

- Smart Card Systems. Smart cards raise the bar even higher, providing additional capabilities and flexibilities. As costs begin to come down and usage is more widespread, manufacturers of biometric devices can leverage their secure data storage to gain market share. For example, a smart card can store both the user's ID number and hand geometry template on the card. Because of this, there is no need to distribute hand templates across a network of handreaders or require the access control system to manage biometric templates. This means integration to any existing access control application is greatly simplified and additional network infrastructure costs are eliminated. Since the template only resides on the card, the solution also eases individual privacy concerns.

  Providing the best of smart cards and biometrics, the solution provides dual authentication by requesting both the right card and the right person. A smart card reader is embedded into the biometric reader. A plastic cardholder is affixed to the side of the unit where the smartcard is inserted, data read, and authorization comparison made. The verification process takes approximately one second and is virtually foolproof.

- Third Party System Integration. Manufacturers offer a variety of different methods to integrate biometrics into conventional access control systems. The most common way is card reader emulation. This method is very effective when integrating into existing card-based systems to bring extra security to the front entrance or server room. In this mode, the biometric device essentially works with the access control panel in the same way that a card reader does. The biometric device is connected to the panel's card reader port. The unit outputs the ID number of an individual if, and only if, he is verified. The format of the output is consistent with the card technology used by the access control panel. Once an ID number reaches the panel, it is handled as if it came from a card reader. The determination for granting access is made by the panel. The access control panel, not the biometric, handles door control and monitoring.

- As an alternative to a keypad, some biometric readers also have card reader input capability, the most common being proximity and smart cards, although other technologies are also supported. At the biometric unit, the user swipes their card, which contains their ID number. If verified, that card number is sent to the panel for a decision. A positive match grants the card member access.

(Spence; Chirillo, 2003)

Issues to Consider:

When considering the implementation of a biometric system there are several areas of concern that management must give consideration to. These include several human culture and comfort issues that present the possibility that a biometric system may not be received favorable. Among the areas of concern are the following:

- Acceptance. The most critical factor in the success of a biometric system is user acceptance of the device. There are several factors that impact acceptance.

- First, the device must cause no discomfort or concern for the user. This may be a subjective issue, but it is important to fully explain any concerns users may have. If people are afraid to use the device, they most likely will not use it properly, which may result in them not being granted access. Significantly many people have strong reservations about using facial and retinal image scanners, or other biometric devices in situations where physical contact is required.
- Second, it must be easy to enroll people. Many get frustrated if they have to go through the process over and over again. From the start, they are predisposed to reject the system. Significant because most biometric system capture devices require multiple readings in order to capture enough data to create a template. The requirement of multiple readings increases the human-biometric reader interface time and discomfort level if the supplicant is adverse to physical contact with the interface.
- Third, the biometric device must be easy to use. People like things that are simple and intuitive. How many times have you been frustrated at a card reader that gives no indication of which way to swipe the card? As with any well designed and user accepted Human Computer Interface simplicity of use is the driving priority.
- Fourth, the biometric device must work correctly. If working properly, it does two things: keeps bad guys out and lets good guys in. Yet, no device is perfect. In the biometric world, the two errors a unit can make are letting a bad guy in and keeping a good guy out. The probability of one of these errors happening is characterized by the false accept and false reject error rates.

- Throughput. A logistical issue that should be considered when using a biometric is the throughput, the total time it takes for a person to use the device. It is difficult for manufacturers to specify a throughput since it is application dependent. Most manufacturers specify the verification time for the reader, but that is only part of the equation.
- When a person uses a biometric reader, they typically enter an ID number on a keypad. The reader prompts them to position their face, hand, finger, or eye where the device can scan physical details. The elapsed time from presentation to identity verification is the verification time. Most biometric readers verify ID in less than two seconds.
- However, when considering the use of biometrics for access control, one must look beyond the verification time and consider the total time it takes a person to use the reader. This includes the time it takes to enter any required ID number and the time necessary to be in position to be scanned. If ID numbers must be entered, they should be kept as short as possible. If a long ID number must be used, some devices can obtain the number by reading a card that contains the ID number in the card code.
- The total time required for a person to use the reader will vary between biometric devices depending on their ease of use and verification time. A card-based access system may appear faster. The speed difference between a card and the hand reader is

about two seconds, but you make up for any latency since your hand is right in front of you, verses fumbling around looking for your card.

(Spence; Chirillo, 2003; Liu, 2001)

The Future of Biometrics:

Although companies are using biometrics for authentication in a variety of situations, the industry is still evolving and emerging. To both guide and support the growth of biometrics, the Biometric Consortium was formed in December 1995. A recent Biometric Consortium annual conference highlighted two important areas.

Standardization:

The biometrics industry includes more than 150 separate hardware and software vendors, each with their own proprietary interfaces, algorithms, and data structures. Standards are emerging to provide a common software interface, to allow sharing of biometric templates, and to permit effective comparison and evaluation of different biometric technologies. The first BioAPI standard released defined a common method for interfacing with a given biometric application. There are currently two different versions of BioAPI. One is the American National Standard (ANSI/INCITS 358-2002, also known as BioAPI 1.1). The other is the International Standard (ISO/IEC 19784-1:2005, also known as BioAPI 2.0).

BioAPI 1.1 is an open-systems standard developed by a consortium of more than 60 vendors and government agencies. It consists of a set of function calls to perform basic actions common to all biometric technologies, such as: enroll user, verify asserted identity (authentication), and discover identity. In order to accomplish the tasks of interoperability and interchangeability, BioAPI uses an instantiation of the Common Biometric Exchange Formats Framework (CBEFF). The current version is defined in NISTIR 6529A as the standard data structure/format for communicating biometric data defining a common means of exchanging and storing templates collected from a variety of biometric devices. To properly understand the specifics of the BioAPI data format, the foundations of CBEFF should be understood. In outline the main features and standards are:

Features:

- Facilitating biometric data interchange between different system components or systems
- Promoting interoperability of biometric-based application programs and systems
- Providing forward compatibility for technology improvements
- Simplifying the software and hardware integration process

CBEFF file standard sections:

- Standard Biometric Header (SBH)
- Biometric Specific Memory Block (BDB)
- Signature Block (SB) (optional)

The CBEFF data can be placed in a single file used to exchange biometric information between different system components or between systems. The result promotes interoperability of biometric-based application programs and systems developed by different

vendors by allowing biometric data interchange. CBEFF provides forward compatibility accommodating for technology improvements and allows for new formats to be created. CBEFF implementations simplify integration of software and hardware provided by different vendors.

The current BioAPI 1.1 standard contains the same text as the BioAPI 1.1 specification originally developed by the BioAPI Consortium. The BioAPI 2.0 standard is a completely new version developed by the international standards committee for biometrics within ISO (ISO/IEC JTC1 SC37).
(BioAPI Consortium; Podio A and B; Young, 2005)

Biometric assurance — confidence that a biometric device can achieve the intended level of security — is another active research area. Current metrics for comparing biometric technologies, such as the crossover error rate and the average enrollment time, are limited because they lack a standard test baseline on which to base their values. Several Governments and standardization groups, including the US Department of Defense's Biometrics Management Office, are developing standard testing methodologies. Much of this work is occurring within the contextual framework of the Common Criteria, a model that the international security community developed to standardize evaluation and comparison of all security products (BSI, 2005; CCP).

Hybrid Technology Uses:

One of the more interesting uses of biometrics involves combining biometrics with smart cards and public-key infrastructure (PKI). A major problem with biometrics is how and where to store the user's template. Because the template represents the user's personal characters, its storage introduces privacy concerns. Furthermore, storing the template in a centralized database leaves that template subject to attack and compromise. On the other hand, storing the template on a smart card enhances individual privacy and increases protection from attack, because individual users control their own templates.

Vendors enhance security by placing more biometric functions directly on the smart card. Some vendors have built a fingerprint sensor directly into the smart card reader, which in turn passes the biometric to the smart card for verification. At least one vendor, Biometric Associates, has designed a smart card that contains a fingerprint sensor directly on the card. This is a stronger secure architecture because cardholders must authenticate themselves directly to the card.

PKI uses public- and private-key cryptography for user identification and authentication. It has some advantages over biometrics: It is mathematically more secure, and it can be used across the Internet. The main drawback of PKI is the management of the user's private key. To be secure, the private key must be protected from compromise; to be useful, the private key must be portable. The solution to these problems is to store the private key on a smart card and protect it with a biometric.

In the Smart Access common government ID card program, the US General Services Administration is exploring this marriage of biometrics, smart cards, and PKI technology. The government of Finland is also considering using these technologies in deploying the Finnish National Electronic ID card.
(Liu, 2001; Chirillo, 2003)

Conclusion:

Biometrics is in its infancy, emphasis is still on the human interfacing with some external biometric device to enable a reading of data. But, as experimentation continues in the fields on biology, cognitive science, computer science, and neural-physiology the time is nearing when biometrics will entail the human utilizing an embedded interface to connect with a computer to facilitate the direct reading and processing of data The concept expressed in Star Trek of the Borg is not so far off. In fact already there are experimental, implantable interface chips that allow the human to become a Cyborg. It is but a short step from being able to interface with a mechanical arm via computer-neuron interface chips to being able to interface and authenticate via a computer-neuron interface where the verification could be facilitated via one's DNA markers. As research in Artificial Intelligence continues and the understanding of the workings of the brain are more readily modeled it will become more feasible to consider the development of neural-interface chips that could potentially allow not only authentication and verification of identity, but also, the ability to access and process data.

References:

Abernathy, W. and Tien, L. (n.d.) Biometrics Who's watching you? The Electronic Frontier Foundation. Retrieved July 6, 1006, from http://www.eff.org/Privacy/Surveillance/biometrics/

BioAPI™ Consortium. (n.d.). BIOAPI 2.0 — INTERNATIONAL VERSION Everything you wanted to know but were afraid to ask ... Retrieved July 18, 2006, from http://www.bioapi.org/internationalversion.html

Biometrics in the 21st Century. (n.d.). findBIOMWTRICS.com. Retrieved July 13, 2006, from http://www.findbiometrics.com/Pages/Bio21st.pdf

Blackburn, D. (March 2004). Biometrics 101, Version 3.1. Federal Bureau of Investigation. Retrieved July 6, 2006, from http://www.biometricscatalog.org/biometrics/Biometrics_101_v5.pdf

Chirillo, J. and Blaul, S. (2003). Implementing Biometric Security. Indianapolis, IN: Wiley Publishing, Inc.

Clark, A. (2003). Natural-Born Cyborgs Minds, Technologies, and the Future of Human Intelligence. New York, NY: Oxford University Press

German Federal Office for Information Security (BSI). (2005, August 17). Common Criteria Protection Profile Biometric Verification Mechanisms BSI-PP-0016 Version 1.04, 17 Approved by the Federal Ministry of the Interior. Retrieved July 18, 2006, from http://www.commoncriteriaportal.org/public/files/ppfiles/PP0016b.pdf

Liu, S. and Silverman, M. (January – February, 2001.). A Practical Guide to Biometric Security Technology What Is A Biometric. ***IT Pro* 27**-32. Retrieved July 13, 2006, from http://ccrma.stanford.edu/~jhw/bioauth/general/00899930.pdf

Podio, F., Dunn, J., Reinert, L., Tilton, C., O'Gorman, L., Collier, M., Jerde, M., Wirtz, B. (Podio A). (n.d.). The Common Biometric Exchange File Format (CBEFF) development has reached an important milestone! The National Institute of Standards and Technology (NIST). Retrieved July 18, 2006, from http://www.itl.nist.gov/div895/isis/bc/cbeff/

Podio, F., *et al.* (Podio B). (2001, January 3). NISTIR 6529 CBEFF Common Biometric Exchange File Format. Retrieved July 18, 2006, from http://www.itl.nist.gov/div895/isis/bc/cbeff/CBEFF010301web.PDF

Recognition Systems Inc. (n.d.). Convenience vs. Security: How Well Do Biometrics Work. findBIOMETRICS.com. Retrieved July 13, 2006, from http://www.findbiometrics.com/Pages/guide2.html

Spence, B. (n.d.). Biometrics Role in Physical Access Control. findBIOMETRICS.com.

Retrieved July 13, 2006, from http://www.findbiometrics.com/Pages/feature%20articles/physac.html

The Common Criteria Project (CCP). (n.d.). Common Criteria An Introduction. Retrieved July 18, 2006, from http://www.commoncriteriaportal.org/public/files/ccintroduction.pdf

Whitman, M. and Mattord, H. (2005). Principles of Information Security, second edition. Boston, MA: Thomson

Wikipedia, the free encyclopedia (2006, July 6). Biometrics. Retrieved on July 6, 2006, from http://en.wikipedia.org/wiki/Biometrics

Wikipedia, the free encyclopedia (2006, July 3). Pattern recognition. Retrieved on July 6, 2006, from http://en.wikipedia.org/wiki/Pattern_recognition

Young, M. (June 2005). BioAPI™ Consortium History of the API and Relationship To Other Standards. Retrieved July 18, 2006, from http://www.bioapi.org/history.html