Biometrics: A Double Edged Sword - Security and Privacy

Wayne Penny

Wayne Penny
GSEC Certification Practical - Version 1.3
Biometrics: A Double Edged Sword - Security and Privacy

Abstract

Certainly, one cannot ignore that the events of September 11th have spurred an increased activity of private and public interest in security and especially, biometrics. This has raised concerns that reacting too quickly with rapid implementations of a technology that some are still trying to grapple with, may result in sacrificing privacy rights in the name of security. In fact, it is highly likely most people would be willing to sacrifice some degree of privacy for protection following those terrorist acts.

The individual who understands what biometrics is and how it is deployed, is provided a basis for realizing its use for security, discussing its strengths and weaknesses, and determining its perceived impact upon privacy rights of individuals.

This paper presents an overview of biometrics in general and describes some of the issues related to biometrics vulnerabilities and security, and its other side, the protection of one's privacy. It considers that for biometrics to be publicly accepted, implementations will require cooperation between organizations and individuals, working with developed open standards that meet the demand for security and demonstrate the protection of personal privacy.

A Biometrics Overview

Simply put, biometrics implements a process used to identify or authenticate an individual's identity using a physical or behavioral characteristic. The goal is to provide access control at the logical and physical levels.

An individual's voice, fingerprint, iris, and hand geometry are examples of physical characteristics. Behavioral characteristics could include signature or writing style. The Bioprivacy™ Impact Framework can assist in determining the impacts of a biometric implementation for organizations that understand the balance between effective security and privacy protection. For example, one question this framework asks is "Are users aware of the system's operation?" [1] It's a straightforward question that asks if the public is aware that a biometric system is in use for an activity. In this case, the framework indicates, not surprisingly, that the public would not approve of a security implementation that behaves in a secretive or covert manner.

---

1 "Bioprivacy™ Impact Framework." International Biometric Group.
URL: http://www.bioprivacy.org/bioprivacy_text.htm (Feb 2002)

A driving force promoting the use of biometrics for security today is protection against identity theft. A telephone number and address is enough to start someone on their way to stealing an identity. It is a predominant concern for many companies and individuals, especially considering the use of the Internet for business continues to experience rapid growth rates. Victims of identity theft know how difficult it is to prove that a theft has in fact occurred, as well. Authorities are continually frustrated with this crime, and the simple randomness of the act makes it difficult to prevent. A biometrics system would go a long way towards the prevention of identity theft because it is based on something that is specific to an individual. It is unique and cannot be duplicated. That is not to suggest however that a biometrics system is without vulnerabilities.

The implementation of a biometrics system requires coordination between the individual and the organization or business implementing the technology. During the enrollment process an individual provides a sample of a biometric: a fingerprint, an iris scan, voice recording, and so on. The sample, taken multiple times for the sake of accuracy, is averaged and stored within a database, token, or smartcard as a compressed digital representation of the sample. This is called a template.

When a live sample of a biometric is presented to the system it is compared to the recorded information, or template, provided during the enrollment process and a match is determined to within an acceptable threshold value. This response determines an individual's right to gain access to a privileged area, data, or just a PC, for example.

The threshold values used when a biometric is presented are necessary to take into account the changing characteristics of the user. Live biometrics change due to age, climate, cuts on a finger, or that stick to the face during a game of pick-up hockey. Vendors will refer to these threshold settings as False Acceptance Rates (FAR's) and False Rejection Rates (FRR's). The idea is to ensure that effective measurements exist to have the real person authenticated, and not an imposter. These settings can be adjusted based upon on the security requirements of the application.

Depending on the biometric application being used, users will present their biometrics to a system that is either identification based or authentication (sometimes called verification) based.

Biometric Identification

The identification process compares a biometric, such as a fingerprint or iris scan that is presented to the system, against all template entries in a database for a match. This is referred to as a 'one-to-many' search.

This can be compared to the mug shot search used by law enforcement. A witness, or victim, of a crime reviews a series of photographs belonging to known felons. This is a 'one-to-many' search that seeks the matching identity of the offender. Similarly, your fingerprint is presented and then compared, one by one, against a number of entries in a database. A 'one-to-many' search is used to answer the question – who are you?

The greater the number of entries in identification based systems, the greater the possibility of false positive or false negative results.

Biometric Authentication

Authentication on the other hand, is a process where a known person's live biometric is compared to a stored template of that person. For example, an individual's identity is revealed to the biometric system upon entering a PIN (Personal Identification Number). To authenticate that this is the person associated with this PIN, a live biometric is presented by the individual and compared to the template and a match is determined. This is known as a 'one to one' search. It is more accurate than the 'one to many' application and is the predominant biometric process in place today and the more privacy friendly of the two systems. This answers the question – Are you who you say you are?

Why Biometrics?

Different security methodologies exist to provide secure access to areas, services and data. Some processes are more secure than others. Something you know, such as a password or PIN, can be less secure than something you have – a token or smartcard. A password or a PIN can be forgotten, or guessed. It could be derived via brute force mechanisms. However, a token can also be lost or stolen and re-used by someone else pretending to be you.

Access to more sensitive information or locations may require a combination that provides strong two factor authentication where one uses both a password or PIN, and a token to pass security. Generally, the stronger the authentication, usually the more sensitive the information or area being accessed. While more difficult, strong two-factor can also be compromised.

Then there is something that you are. A biometric is a characteristic that is exclusively you and nobody else - your voice, your fingerprint, your iris and so on.

The advantage to a biometric is that it doesn't change. It goes where you go, so it's difficult to lose. It's also very difficult to forge or fake. In some cases, it is next to impossible. It provides a very strong access control security solution satisfying authentication, confidentiality, integrity, and non-repudiation

requirements. Growth in the Internet and its greater use for inter-business communications along with the cost benefits of implementing E-Commerce applications over the World Wide Web has raised the bar on security requirements. Logical security is just as important as physical security thanks in large part to those individuals who would do harm to the electronic worlds of organizations and individuals. And worse, as evidenced by September 11th.

Overall, biometrics technology is improving, the costs are coming down, and the public, due to recent events, seems more accepting. The following table represents a Harris Interactive Poll, taken by phone of 1,012 adults the week following the attacks of September 11th. [2]

	In Favor	Opposed	Declined To Respond
Use of facial recognition to scan for suspected terrorists at various locations and public events.	86%	11%	2%
Closer monitoring of banking and credit card transactions to trace funding sources.	81%	17%	2%
Adoption of a national ID system for all U.S. citizens.	68%	28%	4%
Expanded camera surveillance on streets and public places.	63%	35%	2%
Law-enforcement monitoring of Internet discussions in chat rooms and other forums.	63%	32%	5%
Expanded government monitoring of cell phones and e-mail to intercept messages.	54%	41%	4%

Source: Harris Interactive/Business Week

It will be interesting to observe subsequent polling of the same questions as time passes. While it is indicated that facial recognition was in high favor following the attacks, that may not be the case as time passes and a grieving nation heals. It is also interesting to note that respondents are less willing to

2 Sussis, Don "Biometrics in the Digital Realm " Insights - E-Consultant URL: http://ecommerce.internet.com/news/insights/econsultant/print/0,,10418_929651,00.html . (Feb 2002)

compromise on privacy when the questions do not imply the search for terrorists.

Biometric Applications and Implementations

Notwithstanding the law enforcement community, the largest and longest user of biometrics, there is a wider base for deployment opportunities with biometrics today than in the past due to advancements in, and the economics of, the technology. As the above table suggests, psychologically, there is probably a wider acceptance of biometrics, as well.

Interested areas of biometric use include Banks and ATM's, computers and the networks they run on, government benefit organizations, the prison system, and time and attendance applications to name a few.

Implementations can be based on:

- Challenge Response (authenticate without divulging your identity)
- Anonymous databases (separating sensitive information from the biometric templates, i.e. health records),
- Portable databases (smartcards, etc.).

Public implementations of biometric security systems tend towards identification, or one-to-many based, while private institutions tend to be more authentication, or one-to-one based systems.

Recently, an article in a Canadian news publication, the Globe and Mail, published an article specifying that the Canada Custom and Revenue Agency plans to announce in April 2002 upcoming implementations of iris scanning systems at airports in Halifax, Montreal, Ottawa, Winnipeg, Edmonton, and Calgary. These kiosks would be available to frequent fliers by the end of 2003. "Iris recognition and other biometric technologies will likely provide airport authorities with ways of improving security while speeding up clearance processes in future," says Bernie Ashe, president and chief executive officer of Ottawa-based AiT Advanced Information Technologies Corp.[3]

Biometrics Vulnerabilities

Nothing is 100% secure, not even biometrics. Nevertheless, biometrics does provide the means to present security credentials that are unique. Unlike other systems that may rely on passwords or tokens that can be vulnerable to loss or exploitation, no one is going enter your live biometric as a means of impersonation.

However, biometrics, given its infancy, does not yet eliminate passwords.

3 Marron, "Frequent flyers find fast lane." The Globe and Mail

Ideally, biometrics would seek to store a digital representation of a characteristic that cannot be reverse engineered, and can be verified without false positives thereby removing the password requirement. However, until such time, and depending on the security of the information access required, it is reasonable to assume that biometric verification may be combined with 'something you know' or 'something you have'.

Something else to keep in mind about biometric applications, security, and protection of privacy, is the lower levels of the architecture the biometric may traverse. The biometric data need not be local to the device reading the characteristic, as in the case where data is stored remotely in a central location. What then is the underlying network architecture between you and the application? It is just as important to understand and implement security along the network pathways as it is to implement security for the application itself.

There are three basic ways a biometric system can be compromised: system circumvention, verification fraud, and enrollment fraud.

The first, system circumvention, avoids using the system as it is intended. For example, the system could be bypassed for administrative purposes by using a 'backdoor' to provide easy access that also gives the hacker a vulnerability to exploit. Others include forcing exception processing built into the system that may not require using a biometric, or just blowing a door off its hinges to gain access.

Verification fraud attempts to circumvent the system during the process of verification itself. Examples include forcing an individual to verify his identity to gain access, presenting facsimile's of the actual biometric, or worse fingers or hands not attached to the owner's. In the latter case, there are biometric devices that can tell the difference between a 'live' finger and an amputated one.

Enrollment fraud goes to the basic question, "Are you who you say you are?" Obviously, some method of identity verification, proving who you are, would be required during the enrollment process of a biometric to prevent identity theft.

Different attacks can be directed at the biometric data or the biometric system itself. Biometric data attacks are typically Man in the Middle based i.e. using data playback or replay attack methods where a recording of a captured template is played back via a device tapped in to the system. Effective countermeasures to these types of attacks include cryptography and digital signatures applied to the data. A system attack example, known as the Hill Climbing Attack, employs "a pattern recognition method that allows guessing the reference data, by successively changing the input features as to provide a more

and more accurate match."[4] Once the match is good enough to fall within the threshold the system is fooled into allowing access.

Just as a firewall does not constitute a network security solution but rather a component of a defensive strategy, biometrics could be viewed in the same manner. It is not enough to assume absolute verification with biometrics alone but rather as part of a well designed security implementation that considers strong two factor authentication. Using a PIN or unique 'something you know' in conjunction with a biometric can increase the overall security of the solution. Taken further, a biometrics solution combined with cryptography and digital signature technology can make a very strong solution and provide effective countermeasures against attack and privacy invasion.

Biometrics Security and Privacy

This debate has been occurring for many years and will continue until the public is satisfied with how implementations of biometric systems affect their private lives and protect their interests. Not surprisingly, biometrics is often compared to an Orwellian process that provides more compromise of individual privacy than protection of information.

But is biometrics the culprit, the destroyer of privacy? As we have seen many times with technology, the possibility of compromise depends largely on its implementation.

For example, during Super Bowl XXXV, faces of fans were scanned and compared to mugshots of known criminals using a visual recognition technology. As you might imagine, the reactions of privacy advocates were predictable, and rightly so. But it wasn't just the scanning that was the problem. After all, if I'm sitting next to a murderer or rapist, I'm not going to be upset if this person is detained. However, the scanning was performed without the knowledge of the public, and utilized a methodology not fully understood for its impacts. Afterwards, it was evident that the public doesn't like it when systems are used in this manner, whether for their protection or not. According to Richard Norton, the executive director of the International Biometric Industry Association, "The real perception problems come from passive technologies that can be used without public knowledge. ... We haven't seen any backlash over the public hysteria but we need to make sure this technology isn't abused...if it is, the public would lose their confidence completely." [5]

Responsible vendor implementations will be concerned with informing the

4 Wirtz, p.20.
5 Scheeres, Julia. "The Positive Side of Biometrics" Wired News.
URL:http://www.wired.com/news/business/0,1367,46539,00.html (Feb 2002)

public of how the system works and will explain the system's privacy protection of the individual and the information it holds. Fundamentally, individuals, or at least those organizations that represent the interests of individuals, want to know what the system is doing and how it is doing it. The potential of unauthorized or covert collection of biometric information will not calm the outcry of civil liberty organizations and certainly the public would resist this.

How is biometric data stored? Is data stored in a central database or on a smartcard under a person's control? Is it stored on a database and linked with personal information about the individual, or stored anonymously with no link to related personal information? Data segregation of personal and biometric information should apply for biometric applications, especially those storing information in a centralized manner using an identification based system. These systems can store many records of many people. Concerns exist about how this data can be used without the consent of the individuals to whom this data is considered private and personal. Could law enforcement use it for forensics or tracking purposes, for example? Strict controls would be required for these systems to protect against unauthorized use or leakage of information to other organizations. Ask yourself, have you ever wondered why, or how, you got on so many mailing lists?

Biometric related costs are coming down and this makes the technology more attractive and will contribute to an organization's willingness to implement these systems. If the cost of implementing is less than the cost of recovering from fraudulent activity, an organization is likely to implement it. However, individuals should be aware that as costs come down and organizations can better cost justify a biometric implementation against fraudulent activity it's possible that privacy issues will not receive the attention they require.

Discussions on biometrics without discussions on privacy are highly unlikely. An effective understanding of the scanning technologies that make up biometrics (of the finger, face, iris, etc) and the inherent risks, is important for public acceptance. The Bioprivacy™ Technology Risk Ratings provides information on privacy and biometrics technologies across the following key areas of biometric deployment:

- **Verification/identification.** Technologies most capable of robust identification are rated higher; technologies only capable of verification are rated lower.
- **Overt/covert.** Technologies capable of operating without user knowledge or consent are rated higher; technologies which only operate through user consent are rated lower.
- **Behavioral/physiological.** Technologies based on unchanging

physiological characteristics are rated higher; technologies based on variable behavioral characteristics are rated lower.

- **Give/grab.** Technologies in which the system acquires ("grabs") user images without the user initiating a sequence are rated higher; technologies in which the user "gives" biometric data are rated lower. [6]

The following represents a subset of the Bioprivacy™ Technology Risk Ratings table, and displays its assessment of the Finger scanning technology where H=high, M=medium, and L=low risk. [7]

Technology	Positive Privacy Aspects	Negative Privacy Aspects	BioPrivacy Technology Risk Ratings
Finger-scan	· Can provide different fingers for different systems · Large variety of vendors with different templates and algorithms	· Storage of images in public sector applications · Use in forensic applications · Strong identification capabilities	Verification/ identification: **H** Overt/covert: **M** Behavioral/physiological: **H** Give/grab: **M** **Risk Rating: H**

Apparently, finger scanning can represent a high risk to an individual's privacy. It is important to remember that risk is relative to an effective implementation. Attention to understanding the potential risks and mitigating those risks is the key to a successful implementation and public acceptance.

Biometric Standards

Next to concern for privacy and the responsibility of organizations to support and foster privacy protection and secure access controls, are the standards that are the glue to put all this together. As is the case with encryption, biometric standards must be public to gain the trust of the users of the technology. Encryption in the business and personal domain is successful in large part thanks to the efforts of its developers who demanded cryptography be public and not hidden within the government. PKI enjoys its success because of this. If you doubt the importance of public standards, take a look back to the Clinton administration and the battle over encryption that was the Clipper Chip[8].

The BioAPI Consortium (www.bioapi.org) is a standards organization that was formed in 1998. Since then the BAPI (Biometric Application Programming Interface) and HA-API (Human Authentication-Application Programming

6 "Technology Assessment." URL: http://www.bioprivacy.org/technology_assessment.htm
7 "Technology Assessment." URL: http://www.bioprivacy.org/technology_assessment.htm
8 Levy pg 241-268

Interface) groups have merged with the BioAPI resulting in a single API industry standard. Its work concerns development of a biometric API to be used across different biometric technologies. The BioAPI Consortium's mission is to: [9]

- Work with industry biometric solution developers, software developers, and system integrators to leverage existing standards to facilitate easy adoption and implementation.
- Develop an OS independent standard.
- Make the API biometric independent.
- Support a broad range of applications.

"The BioAPI Consortium is bringing forward a high level standard to make different types of biometric devices interchangeable and interoperable," says Walter Hamilton, Vice President of Business Development with SAFLINK Corporation. "This standard has received widespread support from the industry and is on a fast track to become a recognized international standard." [10] The BioAPI Consortium released the BioAPI specification in March of 2001, which can be viewed at www.bioapi.org/BIOAPI1.1.pdf.

Other standards activities taking place in the biometric industry today can be found in organizations such as The International Biometric Industry Association (IBIA) at www.ibia.org, National Institute of Standards and Technology (www.nist.gov) and the Biometrics Consortium (www.biometrics.org).

Conclusion

The public is better educated in technology today. This is partly because technology is becoming easier to use, but also because people are understanding the wide use of the Internet for business can introduce certain risks to individual privacy. Business organizations that previously skirted around privacy issues should understand this and move towards assurance models of privacy protection for their customers. Therefore, understanding biometrics from both the individual's perspective and from the organization that is implementing it, is very important. Communicating it between the two is just as important. Two of the issues to be overcome with biometric systems and public acceptance are communications, by the vendors or implementers, and public perception of the technology. The individual must be able to understand the behavior of the system to assess its capabilities to protect information and function in an open and secure manner.

Is biometrics a security solution in and of itself today? Remember that

9 Mission Statement "BioAPI Consortium" URL: www.bioapi.com
10 Armstrong, Illena. "Biometrics Technology Making Moves in the Security Game." SC Magazine March 2002 URL: http://www.scmagazine.com/index2.html (March 2002)

biometrics by themselves are not necessarily the problem. While the biometrics of an individual are unique and extremely difficult to impersonate, weaknesses or vulnerabilities can be introduced into the system based largely on how it is implemented. In the private or public sector, if an approach is haphazard, then the public will view this with doubt and deployment will experience delays. Done effectively and openly, standards based biometrics implementations can be a very secure application that will protect access to information and the privacy of individuals.

List of References

"Bioprivacy™ Impact Framework." International Biometric Group. 2001.
URL: http://www.bioprivacy.org/bioprivacy_text.htm (Jan 2002).

"Technology Assessment." International Biometric Group. 2001.
URL: http://www.bioprivacy.org/technology_assessment.htm (Jan 2002).

"IBG's Bioprivacy Initiative." International Biometric Group. 2000-2001
URL: http://www.bioprivacy.org/index.htm (Jan 2002).

Clarke, Roger. "Biometrics and Privacy" Principal, Xamax Consultancy Pty Ltd., Canberra. April 15, 2001.
URL:http://www.anu.edu.au/people/Roger.Clarke/DV/Biometrics.html (Jan 2002).

"Biometrics Explained." I/O Software Inc.
URL: http://www.iosoftware.com/biometrics/explained.htm (Feb 2002).

Mission Statement. "BioAPI Consortium." Jan 25, 2002. URL: www.bioapi.com (Feb 2002)

Sussis, Don. "Biometrics in the Digital Realm." Insights – E-Consultant. 27 November 2001.
URL:http://ecommerce.internet.com/news/insights/econsultant/print/0,,10418_929651,00.html (Feb 2002).

"Biometric Identifiers." Electronic Privacy Information Center.
URL:http://www.epic.org/privacy/biometrics/ (Feb 2002).

Plotkin, Hal. "No Silver Bullets Giving Up Privacy for Security Will Leave Us With Neither." SF Gate. Sept 2001.
URL:http://www.sfgate.com/cgi-bin/article.cgi?file=/gate/archive/2001/09/18/nosilvbullet.DTL
(Feb 2002).

D'Amour, Michael R. "World Leader in Fingerprint Authentication Technology." Veridicom Inc. Aug 30, 1999.
URL:http://www.veridicom.com/technology/privacy.htm (Feb 2002).

McCullagh, Declan. "Call It Super Bowl Face Scan I." Wired News. Feb 2002.
URL: http://www.wired.com/news/politics/0,1283,41571,00.html (Feb 2002).

Scheeres, Julia. "The Positive Side of Biometrics." Wired News. Sep 5, 2001.
URL:http://www.wired.com/news/business/0,1367,46539,00.html (Feb 2002).

Liu, Simon and Silverman, Mark. “A Practical Guide to Biometric Security Technology.” IEEE Computer Society. Jan-Feb
URL: http://www.computer.org/itpro/homepage/Jan_Feb/security3.htm (March 2002).

Armstrong, Illena. “Biometrics Technology Making Moves in the Security Game.” SC Magazine March 2002 URL: http://www.scmagazine.com/index2.html (March 2002).

Wirtz, Dr. Brigitte. "Biometric Systems 101 and Beyond." URL:http://www.silicon-trust.com/pdf/secure_PDF/Seite_12-21.pdf (Mar 2002).

Marron, Kevin. :Frequent fliers find fast lane." The Globe and Mail. March 14, 2002.
URL:http://www.globeandmail.ca/servlet/GIS.Servlets.HTMLTemplate?tf=tgam/search/tgam/SearchFullStory.html&cf=tgam/search/tgam/SearchFullStory.cfg&configFileLoc=tgam/config&encoded_keywords=biometrics&option=&start_row=1&current_row=1&start_row_offset1=&num_rows=1&search_results_start=1 (March 2002).

Nichols, Randall K., Ryan, Daniel J., Ryan, Julie J. C. H. Defending Your Digital Assets. McGraw-Hill, 2000. 358-389.

Burnett, Steve and Paine, Stephen. Cryptography. Berkeley: Osborne/McGraw-Hill. 2001. 282-291.

Levy, Stephen. Crypto. Viking, 2001. 241-268.