Global Information Assurance Certification Paper

Bart Leonard

GSEC Practical

version 1.2d

Biometric Technologies – Evaluating the Solutions

Imagine you are a Chief Security Officer of a top-secret government agency and you realize that you need to implement some form of biometrics into your organization to further protect the nation's military secrets. Even better, you are a CSO in a Fortune 500 company that has recently seen a rash of security breaches from within and you have just attended a conference where "Defense In Depth" was the theme and you determine that biometrics is needed to further secure the physical environment.

OK, great, now what technologies are out there to choose from? Fingerprints, facial recognition, hand geometry, retinal scan, iris scan, vascular patterns, signature dynamics, voice dynamics, or one that is more interesting, odor? Yikes! Suddenly feeling overwhelmed, you think about other decisions that need to be considered including how much variance should be allowed when comparing the scan to the authentic pattern, how should you manage the organizations' reaction to this new technology, what are the support options, what procedures need to be in place if the system fails, what are the upfront and on-going costs, and what about human cloning?

According to John Woodard, University of Pittsburgh Law Review, only three of these approaches are considered to be truly consistent and unique : fingerprint scanning, retina scanning and iris scanning. However, because this is an emerging field, there are many opinions and considerations that need to be made before deciding on which biometric method is best for your organization.

In essence, biometric authentication involves, capturing a sample image, pattern or sound, extracting certain characteristics, developing a computerized template or map of those characteristics and matching against a known state. Biometric technology smartly builds a template smaller than the original capture, thereby reducing the processing overhead of matching against the known state. However, with some biometric methods, this reduction can create a scenario where two or more people pass an authorization based upon the same characteristics. For now, it seems that the methodologies that can reduce the processing overhead but still maintain a robust matching scheme, where each individual can be uniquely identified, tend to be the most expensive solutions.

The following narrative provides a brief description of a number of biometric methodologies and will hopefully allow security and business professionals to narrow their choices. One important note - before you embark on any security project including

biometrics, a business impact analysis should be performed to determine the risk to the organization of these assets being compromised. Included in this analysis should be the value of the assets that you want to protect, the impact to the organization if these assets are compromised vs. the cost of the system. From this, you can determine the appropriate dollars to allocate to a biometric or any other type of security solution.

Fingerprint Identification

Certainly the most prominent and oldest technology used in biometrics is fingerprint identification. One study, in Thieme's report rated that "public acceptance of electronic fingerprinting at 96%." The attraction for utilizing fingerprint technologies is that no two fingerprints are alike and "even if your finger is cut, the pattern grows back the same."(Featherston) However, this is not to say that fingerprints can not be permanently changed via scars, chemicals, or other means. In addition, placement of the finger on the device is crucial to the effectiveness of the authentication, and therefore detailed training should be considered.

To be clear, let's make a distinction between fingerprinting and finger-scanning. Fingerprinting is the acquisition and storage of the image of the fingerprint, usually in the form of ink on paper as seen in police stories. On the other hand (so to speak), finger scan biometrics is based on the distinctive characteristics of the fingerprint, not the fingerprint itself. A finger scan, scans the fingerprint but only extracts certain characteristics from the scan and from this a template is created for use in authenticating. This template on generally contains between 30 and 40 unique characteristics. "The Federal Bureau of Investigation has shown that no two individuals can have more than eight common minutiae (unique characteristics)." Furthermore, "the U.S. Court system has consistently allowed testimony based on twelve matching minutiae." Generally the scan device does not store the scanned information for longer than is needed to verify the person and therefore, recreation of the fingerprint would be very difficult to perform.

One of the considerations when using hand or finger-based technologies is right-handed vs. left-handed. You may want to have a requirement that the device be hand-neutral to accommodate the other-handed personnel in your organization to help ensure accuracy.

Pros

- Distinctive
- Well-known
- User acceptance is high

Cons

- Not as accurate as other biometrics
- Need for contact with a device
- Residue on scanning device may effect results
- Fingerprints can change
- Precise training is required

Vendors –

There are many vendors providing solutions for finger-scanning. The following is a partial listing but should not be taken as recommendations

SecuGen, Astro, Siemens, Ethentica, AuthenTec, BioLink, Ultra-Scan, Cross Match, Precise Biometrics, BioScrypt, Identix, Identicator, Veridicom, Sony, and Fujitsu (3)

Pricing has come down from a few years ago to a point where organizations can obtain devices for around $100 per device. Other costs that need to be considered are training as improper finger placement on device scanners can cost many man-hours providing help desk support. Expect to see this type of biometrics in keyboards, mice, PDA's, households, cars, and just about anything that needs to be protected.

Hand Scanning

Hand scanning is usually based on the height, width and length of a hand. Reliability is based upon the fact that the shape of one's hand does not change over time after reaching a certain age. However, hands are not very distinctive, in that many people have the same general shape of hand. In addition, hand geometry does not produce a large criteria set distinguishing one hand from another and therefore in organizations with large numbers of employees, multiple people may be authenticated based upon the same criteria if their hands are similar in size and shape. Therefore this type of biometric should be meticulously studied before implemented for high security applications in that you will need to develop a criteria database that is more stringent than the "out-of-the-box" capabilities. Better applications may be for time and attendance and other low-security applications.

Pros

Widely recognized

Non-intrusive

Easy to use

Low technology requirement

Cons

- Not as secure as other biometric solutions
- Higher cost (especially for high security applications)
- Injuries to hands will effect results

Prices vary however, hand-scan devices generally are more expensive than other biometric devices usually running in the $500-$1500 per device.

Vendors – the industry is dominated by Recognition Systems Inc., which is a division of Ingersoll-Rand. Other vendors include Dermalog and Biomet Partners.

Retinal Scanning

Retinal scanning (and iris scanning) is considered one of the most accurate and reliable biometric technology available in the marketplace today and therefore should be utilized in cases where significant security measures are required to protect valuable assets. Retinal scanning involves emitting a beam of light into the retina in which the eye bounces back an image of the blood vessel structure that is identified by the scanning device which then produces a map of this structure. Training is a key component in that the user must accurately position themselves in front of the retinal scanner approximately ½ inch away, while the device scans between 400 and 700 points on the retina. By contrast, finger-scanning is more user-friendly but usually only measures 30-40 points, and therefore makes retina scanning much more reliable and secure.

Pros

- Very accurate
- More secure than other biometric approaches
- Eye structure is generally constant over a person's lifetime (except in cases of disease)
- Very reliable in that it is not susceptible to fraud
- Compact storage requirements (96 bytes) as opposed to other methods (256 bytes +)

Cons

- User acceptance is lower than other more non-intrusive methods
- Training the user on positioning is key to the success of the technology
- Costly as opposed to other technologies

At this time, there is only one vendor in the marketplace, EyeDentify, however others vendors are sure to be in play soon. The cost of a single device will be in the thousands of dollars.

Iris Scan

Considered among many biometric experts as the most accurate biometric measurement for authenticating users. Iris scanning involves taking a picture of the iris and developing a 512 byte pattern based upon a variety of distinguishing visible characteristics. So much distinction is prevalent that the largest corporations do not have to worry about one iris having enough like characteristics of another that the authentication would view 2 people with the same type of iris. According to the Biometric Group, "The odds of having 2 different irises returning a 75% match is 1 in 10^{16}.

Pros

Highly accurate and reliable

Eye mapping is mostly in place from birth and is generally consistent over time

Scalable across the entire organization without losing accuracy or reliability

Non-intrusive biometric technique as the user does not have to physically touch a device

Cons

Cost

Iridian is currently the only vendor to date that has this technology www.iridian.com

Facial Scanning

There are generally four types of facial scan authentication, eigenfaces, feature analysis, neural network, and automatic face processing. Eigenfaces uses a grayscale methodology to highlight facial characteristics. Feature analysis is similar to eigenfaces, but it is more accommodating for other characteristics like smiling and frowning. Neural network methods use an algorithm for authentication that compares known features to captured features. Automatic face processing uses physical measurements for authenticating users such as distances between eyes, mouth and nose. Each method has it's own strengths and weaknesses in that facial changes, hair changes, light and darkness, smiles and frowns, hats and glasses all effect the reliability of the authentication. No one method of facial scanning can accommodate for all variables so additional study should be taken if facial scanning is utilized.

One of the advantages of facial scanning is it can provide periodic monitoring as opposed to one-time authorizations of other biometric methods. For example, if utilized on a PC, if an authorized user moves away from their computer and someone else sits in the chair to try and compromise the unit, the facial scanning device can recognize that a non-authorized user is present and shut down access privileges on that computer.

Pros

Non-intrusive as the user does not have to physically touch the device

User acceptance is generally high

A face picture provides the best audit trail of all methods

Cons

Similar appearances or changes in appearance can effect the accuracy

Speed of processing can be an issue for large organizations

Not as precise or reliable as other methods

The following are some of the vendors of facial scanning solution: BioID, Biometrica, eTrue, Viisage, Visionics, Imagis, AcSys, Digitech. Pricing varies among the different providers and solutions.

Signature Dynamics and Voice Dynamics

Generally considered to be the least effective means of biometric authentication, due to the fact that behavioral influences also effect the results in that fluctuations in signature writing and voice inflections are common from day to day die to mood, health, dryness, etc.

Crossover Accuracy Chart

The following chart, from the Ruggles report, depicts the crossover accuracy of the different biometric methods available today. There are two types of measurements, the rate of false acceptance, where a user is authorized incorrectly, and the rate of false rejections, where a valid user is not authorized. These two measurements are calculated to provide a result that is depicted below. The higher the 2nd number in the chart, the more accurate the method and generally the higher cost.

Biometric	Crossover Accuracy

Retinal Scan	1:10,000,000+
Iris Scan	1:131,000
Fingerprints	1:500
Hand Geometry	1:500
Signature Dynamics	1:50
Voice Dynamics	1:50
Facial Recognition	no data
Vascular Patterns	no data

Conclusion

Biometric technology is emerging, improving and not foolproof. If used, it should be one component of a "Defense In Depth" strategy. As noted, each method has its' own unique strengths and weaknesses, which means that studying the risk analysis, the end user community, the environmental factors, integration issues, and support and maintenance costs should all be taken into consideration before a choice is made. Compounding the issue is the fact that standards are still being developed and cross-integration among different vendors is not a cost-effective option. As with any security solution, the balance between ensuring the security of assets, vs. the cost of solution, and user acceptance is one that will continue stir debate among decision-makers.

(1) Featherston, Cutler, Researchers Seek New Methods of Identification, 12 April 2001, URL: http://www.statenews.com/article.phtml?pk=3704

(2) International Biometric Group, Biometric Technology Overview, URL: http://www.biometricgroup.com/a_bio1/technology/research_a_technology.htm

(3) Ruggles, Thomas, Comparison of Biometric Techniques, 15 March 1998, URL: http://biometric-consulting.com/bio.htm

(4) Woodard, John D., Biometric Scanning, Law and Policy: Identifying the Concerns—Drafting the Biometric Blueprint, 1997 University of Pittsburgh Law Review, URL: http://www.pitt.edu/~lawrev/59-1/woodward.htm

(5) San Jose State University, Biometrics Publications, URL: http://www.engr.sjsu.edu/biometrics/publications_tech.html

(6) Theime, Michael, Mapping Form to Function, Information Security Magazine, March 2000, URL: http://www.infosecuritymag.com/articles/march00/features1.shtml

Last Updated: July 27th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
Community SANS Indianapolis SEC401	Indianapolis, IN	Oct 09, 2017 - Oct 14, 2017	Community SANS