Global Information Assurance Certification Paper

Information Assurance Using Biometrics

GIAC Security Essentials Certification (GSEC)

Practical Assignment v.1.4 – Option 1

Global Information Assurance Certification (GIAC) Program

Bryan Feltin

Version 1.0
June 23, 2002

TABLE OF CONTENTS

Abstract

Information Assurance refers to the processes and procedures that are implemented to keep electronic data secure and to make sure that the integrity of the information is valid. Using biometrics in information assurance is not a new concept, but with the recent events of September 11, stronger security measures are on the minds of people and corporations around the world. The following information will define what biometric technologies are and show how they can be used to increase personal, public, and corporate security. How new security technologies force hackers and crackers to try to develop methods that will circumvent these new safe guards, is also discussed. Some examples have been provided of how biometric devices have been successfully thwarted and how security professionals have enhanced systems because of hackers and their successful security breaches.

Introduction

Most organizations today have security policies in place that are designed to enforce security practices and procedures. Security vulnerabilities can stem from a multitude of factors within an organization. There are physical security concerns that deal with allowing only authorized personnel into buildings and secure areas, and there are technical security issues regarding the access authorization of personnel to appropriate electronic information. There are also telephone security vulnerabilities as well as disgruntled employee vulnerabilities. Biometrics, as it will be discussed, will focus on the physical and technical security vulnerabilities.

Many companies require employees and contractors to produce an identification badge or swipe a key-card to gain access to buildings and secure areas to address physical security concerns. Individuals that have gone through this procedure on a regular basis would probably agree that anyone could manufacture an ID card with his or her own picture on it and gain entrance to the building. ID badges and key-cards can be lost, stolen, and reproduced quite easily with inexpensive equipment. (i.e. a computer and software).

On the technical side, a security policy should reference the method required for employees to be authenticated in order to gain network access to files and confidential information. There are several methods to do this, and the most popular method is by entering a password. Depending on the requirements of the policy, the administration of passwords reflects how secure the confidential information really is. If users write their passwords down on sticky notes and attach them to their monitors because the passwords change every 30 days, anyone could read the password and logon to the network as that user. Changing user passwords on a frequent basis is a good practice in theory, but if implemented improperly (such as without the use of single sign on where a single password is required to access all systems), it can create stress for users, and increase the workload of the IT (Information Technology) department by causing an increase in calls to the IT Support Centre. One option would be the use of a secure token, which is a small electronic device that contains a six-digit display that changes every minute. The

combination of the user's private code and the secure token number creates a different password or "pass code" every minute. This is more secure than changing passwords every 30 days, and there is no real password to remember, only the private code. The flaws here are similar to physical security, in that passwords and private codes can theoretically be stolen and hacked. Secure token devices can also be stolen and used improperly, but they do make a security breach much more difficult.

Without the right security policies and procedures in place, it can be fairly simple for someone to hack into an organization. This is where biometrics can be an extremely powerful security tool. Biometrics is the science of using unique human characteristics, such as the iris, a fingerprint, or a voice to authenticate a person's identity (Rolwing, p.11). Biometric technologies are automated methods for identifying or authenticating a person based on physical attributes (Winkle, p.51). There are many possible features of the human body, both physical and behavioral, that biometric devices can use to identify or authenticate a person. The more common human features used include the face, fingerprints, a hand, handwriting, DNA, eye patterns, vein patterns, and the voice.

Two primary functions of biometric technology in the IT industry are verification and recognition of individuals. When biometric information from a known user is processed and compared one-to-one (verifies that the database contains the same information that has been presented), a verification process has taken place. When a database of biometric information is searched against an unknown sample, the recognition process has been performed. The verification process is important as it can be used to provide authentication to IT resources such as confidential files and information or even hardware such as workstations and servers. There are three primary types of authentication used to secure information:

- something you know - such as a code or a password or a PIN
- something you have - such as a key or an ID badge or a swipe card
- something you are - a biometric (such as a fingerprint, DNA, voice, etc)

Almost everyone in one way or another has used all of these methods in his or her life. Personal identification numbers (PINs) are used daily for personal banking, keys are used to lock and unlock house doors, and a signature on a credit card receipt is a form of biometric. Biometric technologies are the most secure due to the fact that there is nothing to forget or lose, and they are almost impossible to duplicate. Believe it or not, even your signature is difficult to duplicate when taking into consideration the right factors, such as pen speed, pressure, movement, and how the signature looks and reads.

Information Technology applications that use biometrics can be used to provide access to a single workstation, the entire network, a single domain, multiple domains, an application, a single file, multiple files, the Internet, and so on. As well, biometrics can be used as the key to encrypt and decrypt files and emails. Basically anytime a password or access code is required to allow access to any resource, biometrics can be used. Hollywood has been showing different uses, some possible and some not, of biometrics

for many years. In the recently released movie "Bad Company," a laptop contains the activation codes to a massive bomb, which is protected by iris scanning software that allows only Chris Rock's character, Jake Hayes, to unlock.

Using biometrics in the IT industry eliminates the need for passwords, relieves stress for the end users and lessens the amount of password resets for administrators. Biometrics help to enhance the convenience for end users by eliminating the need to carry ID cards, key-cards, or a secure token device everywhere one goes. Biometrics also increases the security of the organization because there are no passwords to steal, no ID cards to forge, and no key-cards or secure tokens that can be lost and used maliciously against the organization.

A popular saying in the security field is, "Security is not a product; it is a process." This means that the use of a biometric device alone, and relying on a single technology to protect your infrastructure, will not prevent a breach of security. By integrating multiple technologies, such as the combination of an ID card and a secure token, is a concept called "defense in depth." Defense in depth makes it more difficult, expensive and time consuming for a hacker to penetrate all aspects of well-developed security architectures. With the proper integration of technologies, hackers should get discouraged and move onto an easier target, which is after all, the end goal of security.

Biometric Technologies

How Biometric Systems Work

Figure 1 below explains the high-level process that is involved in using a biometric system. The implementation of a fingerprint scanning authentication system provides an example. Steps 1 through 3 are the initial population and the on going updating of the database that stores the records for all employees. Steps 4 through 8 are the real-time authentication process where the end goal is to grant access for authorized users and deny access for any unauthorized individuals.

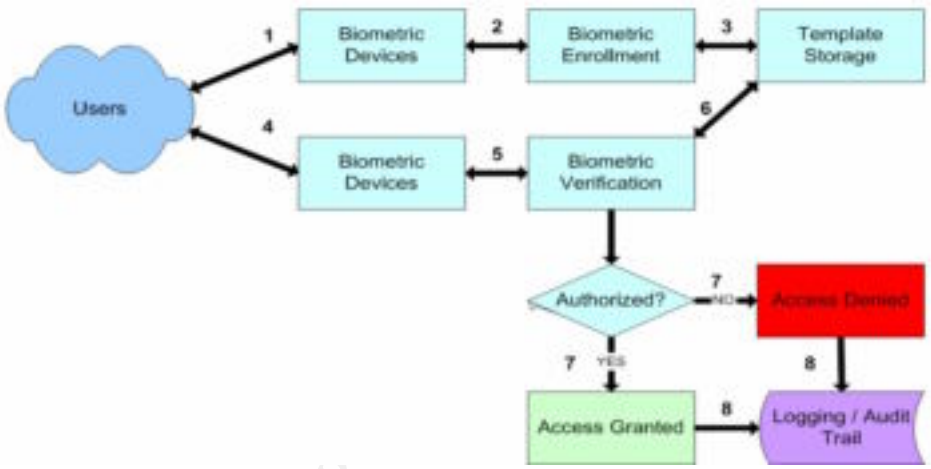

Figure 1. Biometric Systems Process

Step 1: The biometric device (fingerprint scanner) is used to collect the biometrics (fingerprints) of all employees within the organization.

Step 2: The collected biometric (fingerprint) is then processed and specific and identifiable data is formatted to fit into a template.

Step 3: The template is stored in a repository where it can be accessed to perform matching queries during a live biometric acquisition.

Step 4: The biometric acquisition (fingerprint) takes place.

Step 5: The biometric (fingerprint) is processed into its template components.

Step 6: The computer scans the database for a matching template to the live-scan.

Step 7: If a match is found and the user is authenticated, access can be granted to a computer, an application, or a location.

Step 8: The authentication or rejection is logged to provide an audit trail.

Fingerprint Recognition

Possibly considered the most popular and realistic biometric technology, fingerprint scanning has made significant strides since its inception. Simply having dirty, scarred, oily, or grimy fingers could thwart early scanners. Also, by shining a light on the residual fingerprint left behind from a previous scan, an unauthorized user could be authenticated.

There are several methods of fingerprint scanning: optical scanning, capacitive scanning, and thermal scanning. Optical scanning takes a digital picture of the fingerprint, stores the data with a certain code, and then compares it to an existing picture in the database. This is the method that can easily create false positives (authorizing non-authorized people and not authorizing authorized people) when people have dirty, scarred, or oily fingers. The measurement of how many times a biometric scanner authorizes an unauthorized user is called the false acceptance rate (FAR), and the measurement of how many times an authorized user is rejected is called the false rejection rate (FRR).

Capacitive scanning uses a "solid-state" method that gets underneath the skin by measuring electromagnetic impulses of the finger to create a more detailed fingerprint image. Thermal scanning, which is also a "solid-state" method, creates an image of a fingerprint by measuring the change in temperature from one part of the finger to the next. Since solid-state scanners are not affected by the physical appearance of the finger itself, dirty or scarred fingers do not create false positives. Basically, solid-state scanners require the finger to be alive. A dismembered finger would not be able to pass a finger print scan on a solid-state device.

There is a good chance that fingerprint biometric technology is going to become a part of everyday life. The costs involved are relatively low, the hardware required is quite reliable, and the technology is convenient for users. As a matter of fact, the use of fingerprint scanning in everyday life has already begun. In Fresno, California, a McDonald's restaurant and a company called Indivios are running a pilot program through where customer can actually pay for their order by having their fingerprints scanned. If the scanned fingerprint matches the previously acquired print stored in the database, the funds are automatically withdrawn from the user's account. This is only one example of possible applications to integrate biometric technologies into everyday life. Biometric technologies are here, but will they stay?

Hand and Palm Recognition

Hand and palm recognition involves scanning the features of an individual's complete hand to provide identification and authorization. Hand recognition can be broken down into two key identifiers: the geometry of the hand and the geometry of the fingers. Hand and finger geometry recognition uses visual and spatial characteristics, such as length and width of the fingers and hand as well as surface area, to identify an individual. Some hand and palm recognition devices can also scan the vein patterns on the back of the hand. Biometric hardware required to perform hand scanning is very reliable, easy to use, and non-obtrusive to its users.

Everyone knows how unique fingerprints are. Unfortunately, palm prints are not. However, in conjunction with hand geometry scanning, the possibility of two people having exactly the same hand/palm print is almost zero. Because of this uncertainty, it is a common practice to use a hand scanner as well as an ID card or pass code to identify an individual. This shows the "defense in depth" concept of having a layered security infrastructure, to be a good practice.

Facial Recognition

Facial recognition has been a very successful biometric practiced in the industry. It does not require users to touch any sensitive hardware or to sit perfectly still while his or her iris or retina is being scanned. It is also the most controversial for the exact reasons just mentioned.

Facial recognition works by breaking down an image of a subject's face into a database of predefined traits, such as the distance between the eyes, the size of the nose, the size of the mouth, plus many more facial features and measurements. For an optimal scan of a person's face, the individual should be directly facing the camera in a well-lit area. Head movement and tilt should be minimal. Facial recognition software is said to able to scan large crowds and compare the faces it scans to faces in a database to identify people. How accurate is this method if the optimal scan requires so many variables to be present for a quality result?

The hardware used to perform facial recognition does not need to be state of the art. In fact, there is software that can be purchased today, that with the assistance of a web cam can be connected to a personal computer. Facial recognition software can then be used to logon to the computer. This is where the controversy arises. Video cameras today are getting smaller and smaller and can be concealed in almost anything, even a wristwatch. This can and has led to many privacy concerns. For example, at the 2001 Super Bowl, the Tampa Police Department installed video cameras throughout the stadium to try to detect known criminals. The system did not match any faces to terrorists, only those of pickpockets and scalpers. It was not disclosed where the cameras were located but they could have been anywhere, even in the washrooms. This proves the point that people

will not know when or where they are being watched. They will not know what kind of information is being gathered on their habits or what that information is being used for.

Voice Authentication

Voice authentication is commonly referred to as voice recognition but the distinction between the two must be made. Voice recognition implies recognizing the sound of one's speech. Voice authentication is based on voice-to-print authentication, where technology converts voice to text by scanning the vocal pattern of the user's speech.

There are many comedians that make impressions a part of their standup act. Some even have an uncanny resemblance in speech to the person that they are impersonating, but they cannot defeat a voice authentication device. The human voice has many unique and distinctive characteristics, which enable it to be used as an identifying tool. As somewhat of a precaution, voice recognition devices will prompt a user to speak a random phase or some type of pass code to eliminate the possibility of a user's voice being recorded and played back. Two of the key identifiers in a voice sample that makes up the voice pattern are the pitch and the resonating frequency.

The main components of a voice recognition system are the microphone, the recognition software, and the computer. Microphones of high quality are relatively inexpensive. With the abundance of personal computers in homes and businesses everywhere, voice recognition is a viable option.

Retinal Scanning

Retinal and iris scanning are similar in that they both involve the scanning of the eye, yet they are quite different in how and what they scan. Eye scanning technologies are some of the most powerful, accurate, and reliable biometric devices in use today. However, they are also very expensive and very obtrusive.

Over time, retinal recognition is said to provide the most stable means of biometric identification. Retinal scanners scan the blood vessel pattern in the back of a person's eye. These patterns remain the same throughout the life of a human, which makes it a good long-term technology. Only in cases where a person suffers a serious head injury can the blood vessel pattern be altered. Orientation problems are minimized because the eye automatically aligns itself as it focuses on an illuminated target. One downfall, however, is that comparisons of a live sample to the records in the database can take much longer than other biometric systems due to the size of each record which results in an increase in time for the system to find a record that matches.

One issue with retinal scanners is that they are quite sensitive and they require a high level of cooperation from its users. A user must sit extremely still while focusing on a

specific target as the scanner moves very close to the eye. Because of these issues, many users are quite leery about using systems that have the scanning mechanism come so close to their eye. This is also why retinal scanners are not widely found in the industry except in cases of extremely high security.

Iris Scanning

No two irises are the same, not even in your right and left eye or the irises of identical twins. Iris scanning does not have as many issues as retinal scanning due to the fact that the user's eye can be a few feet away from the scanning device. Also, users do not have to focus on a specific point during the scan. Unlike retinal scanners, the wearing of eyeglasses does not hinder the effectiveness of an iris scan.

Iris scanning involves analyzing features found in the coloured ring of tissue that surrounds the pupil of the eye. When an iris is scanned, the position and shape of the iris and eyelid, light reflection, and moisture found in the eye are some factors that are taken into consideration. The image is then sectored for analysis and the data is generated with a complex algorithm and stored in code. There is a multitude of characteristics in a single iris, which makes it the best identifying feature of the human body. Each iris is so individually unique that iris scanning is one of the most accurate and reliable biometric technologies.

Defeating Biometrics

Just like every other aspect of the Information Technology industry, hackers are everywhere and they love a challenge. As new technology emerges, be it a new audio or video format such as DVD, a new encryption format, or even a new biometric technology, there are people out there who are going to hack it and propagate it throughout the Internet community. Many of these hackers do it for the thrill of the challenge, while others do it for personal gain.

Security professionals are taught that the best way to implement and administer a secure infrastructure is to learn and understand previously successful attacks. By understanding successful attacks, new safeguards can be put in place to prevent the same attack from happening again. There are some known hacks and attacks that have successfully fooled biometric systems. As biometric companies learn from these hacks they can begin to address the downfalls and improve the technology by predicting what the hackers will try next. Security professionals must stay current with the latest technologies, apply any fixes as they are released, and remove any vulnerabilities whenever possible, to reduce the risk.

For one that follows technology closely, one would think that fingerprint scanning is the new wave for security. Instead of using the wonderfully popular ID badge, it would be quite convenient to have a fingerprint scanned that logs one into his or her computer or unlocks secure areas in the corporation. There are numerous companies that have marketed mice and keyboards that have thumb and fingerprint scanning devices built into them to do exactly this. Is this a secure system?

Mathematician Tsutomu Matsumoto claims that he has defeated eleven fingerprint scanners available today, 80 per cent of the time using a technique that costs less than ten dollars. (Leyden). He has successfully fooled optical and capacitive scanners as well as "live finger detection" devices. In fact, he has written a paper on it. Have you heard about the Gummy Finger? The basics behind it are that by using gelatin, as found in most gummy candies, and a mold, he can create a fake gummy finger that has fooled many sensors. The beauty is that the gummy finger, and therefore the evidence, can be eaten after it is used to thwart a system. Fingerprint scanning companies have been claiming for years that what Matsumoto has accomplished was impossible. They know better today. They know what they need to fix, and its back to the development stages for most of the fingerprint scanning companies.

This is only one example of thwarting fingerprint scanners. Think of the different types of scanners mentioned and what their "kryptonite" would be. Take the thermal fingerprint scanner for example. What is the key difference between it and other fingerprint scanners? It requires changes in temperature to develop a print. Several thermal fingerprint scanners have been fooled simply by breathing on the device or by

placing a plastic bag filled with warm water on the sensor that contains the residual fingerprint from a previous user. Now how good of an idea is it to replace your ATM PIN with a fingerprint?

Facial recognition programs have not faired much better than fingerprints. Since the attacks of September 11, 2001, organizations and airports have been looking for ways to better identify people and pick out certain individuals in a crowd. The Palm Beach airport tested a popular facial recognition package for eight weeks, and the results were far less than astounding. Several employees had their faces entered into the system and the recognition software was to scan for them as they moved throughout the terminal during their daily activities. The system was fooled if the person was wearing glasses (the glare most likely threw off the sensors), if the lighting was wrong, or if the person's head moved too much. The program successfully identified the employees less than 50 per cent of the time. This is not acceptable when searching for terrorists.

There is facial recognition software commercially available that allows a user to logon to his or her computer simply by sitting in front of a web cam that is connected to the workstation. Facial recognition software has successfully been fooled quite easily by placing a picture of an authorized user in front of the camera when prompted to logon to the system. The more advanced systems require a person to smile or blink, but these have been fooled by holding a laptop up to the camera with a short video of the user. Getting an up-close digital picture or a short video of an authorized user blinking or smiling can be quite difficult for a hacker. Nonetheless, once the image or video is captured, it can be reused over and over again. Think of what the consequences would be if your facial recognition software failed to authorize you access to your computer, or for that matter, your company's mission critical system because the lighting was not right.

Eye scanners, too, have been successfully fooled, though not as easily. A digital image on a laptop did not fool the iris scanner, nor did the high quality printed image of the user. When the printed image had a hole cut in the middle of the eye and a real human peered through the picture to the camera, the system authorized the user.

Only a few examples have been given to show how current biometric systems have been fooled. When new technologies are released, there will be different ways around them. This shows that hackers are out there, and they have been quite successful breaching security in the past. Some of the technologies are extremely difficult and time-consuming to thwart, but once a method is found to circumvent a security measure, it can be exploited repeatedly until the vulnerability is removed.

Final Thoughts

Biometric are the oldest form of recognition and authentication. Humans have been recognizing individual faces and voices since the beginning of time. Mankind is not alone when it comes to biometrics. Animals also have their own unique sounds, smells, iris patterns, DNA, and so on. It is possible that someday, instead of tagging or branding cattle, an iris scanner could be used. So what is all the fuss with biometrics today?

With today's technology, we have the ability to store biometric data in databases, which allows us to authorize users that we do not know and cannot recognize. For example, the only reason someone can recognize another person's face or voice and correlate it to a name is because he or she already knows that person. There is now way to verify who a stranger is, especially over the phone.

As shown, biometric devices must improve, and they will. The key behind a good biometric device is not secrecy, but rather to determine or detect the liveness of a biometric sample. It appears that devices on the market today are performing the detection poorly. This is rather ironic when considering the breakdown of the word biometric: "bio" means living and "metric" means measure. The whole purpose of a biometric device is to correctly identify a person. When that doesn't work 100 per cent of time, it increases the chance of identities being stolen and lost. Identity theft is not new, but think of the implications of having a biometric stolen. Devices today have unacceptable False Rejection Rates and False Acceptance Rates. They cannot be solely relied on for security.

Consider this: "Biometrics as explained is a set of unique identifiers, but they are not keys." When one loses his or her wallet or the wallet gets stolen, what happens? The individual will call the credit card company and report the theft, and the company will put a freeze on the card, so no one can spend his or her money. What would happen if everything was paid for with a simple scan of the finger and a hacker was able to successfully lift and recreate one's fingerprint? Now that hacker can keep the print and have access to everything that the individual had access to. In a world that is run by technology, the possibilities are endless. If a credit card gets lost, it is not a big deal. The credit card company will issue a new card. It is much more difficult to get new fingerprints.

Biometric identifiers are very powerful and useful in the right situation and under the right circumstances. They are useful as an identifier, but they are not useful as a securing mechanism, such as a key. A key represents secrecy, randomness, and the ability to be destroyed and replaced with something new. Biometrics are unique identifiers, but they are definitely not secret.

Security is not a product; it is a process. Having a good security policy is the first step to Information Assurance. The policy must be adhered to, reviewed regularly, and updated

when needed. Following the "defense in depth" concept by integrating multiple technologies will greatly decrease the chance of a disaster occurring. Just like in the movie "Bad Company." The bad guys eventually get Jake Hayes' eye open for the computer to scan, and they gain access to the bomb's codes. Since they do not need Jake anymore, they are about to kill him until he fools them into thinking that there is also a password required to activate the bomb. His quick thinking keeps him alive just long enough to escape. Of course!

References

Denning, Dorothy. "Security Strategies for E-companies." January 2001.
URL: http://www.infosecuritymag.com/articles/january01/columns_logoff.shtml.

Leyden, John. "Biometric sensors beaten senseless in tests." The Register Newsletter.
May 22, 2002. URL: http://www.theregister.co.uk/content/55/25400.html.

Leyden, John. "Gummi bears defeat fingerprint sensors." The Register Newsletter.
May 16, 2002. URL: http://www.theregister.co.uk/content/55/25300.html.

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

McCullagh, Declan and Zarate, Robert. "Scanning Tech a Blurry Picture." Wired News.
February 16, 2002. URL: http://www.wired.com/news/politics/0,1283,50470,00.html.

Rolwing, Rebecca. "Don't See The Password, Be The Password." Smart Computing Learning Series - Computer Privacy & Security. Volume 8 Issue 4 (2002): 11-14

Schneier, Bruce. "Biometrics: Truths and Fictions." CRYPTO-GRAM Newsletter.
August 15, 1998.
URL: http://www.counterpane.com/crypto-gram-9808.html#biometrics.

Schneier, Bruce. "Biometrics: Uses and Abuses." CRYPTO-GRAM Newsletter.
August 1999. URL: http://www.counterpane.com/insiderisks1.html.

Thalheim, Lisa and Krissler, Jan and Ziegler, Peter-Michael. "Biometric Access Protection Devices and their Programs Put to the Test." Body Check. November 2002.
URL: http://www.heise.de/ct/english/02/11/114/.

Winkle, William. "Security, Convenience & Abuse – Biometrics Arrive." Computer Power User. May 2002 (2002): 50-54

Related URLs

http://members.aol.com/MonT714/tutorial/the_eye/

http://www.aimglobal.org/technologies/othertechnologies/biometric_retinalscan.htm

http://www.biomet.org/hand.html

http://www.biometricgroup.com

http://www.biometrics.org/html/introduction.html

http://www.biometrika.it/eng/wp_biointro.html

http://www.eyeticket.com

http://www.facial-scan.com/facial-scan_vendors_and_links.htm

http://www.finger-scan.com/finger-scan_technology.htm

http://www.finger-scan.com/finger-scan_vendors.htm

http://www.hand-scan.com/hand_scan_vendors.htm

http://www.indivos.com

http://www.iris-scan.com/iris_recognition_vendors.htm

http://www.retina-scan.com/retina_scan_vendors_and_products.htm

http://www.signature-scan.com/signature_scan_vendors.htm

http://www.viisage.com

http://www.visionics.com

http://www.voice-scan.com/vendors.htm