Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Physical Security: A Biometric Approach

In the competitive business world today, the negative publicity and financial ramifications from an IT physical security breakage can be disastrous. An IT physical security breakage could and most likely lead to the selling of shares from stockholders, financial revenue and profit loss, numerous corporate lawsuits, disgruntled employees, corporate and brand embarrassment, and exhaustive time and effort spent on problem research and prevention. When coupled with constant September 11 terrorism concerns and the importanc...

Copyright SANS Institute
Author Retains Full Rights

AD

ForeScout

Physical Security: A Biometric Approach

Ryan Hay
SANS - GSEC Practical
Track 1C
November 12, 2003

Abstract

In the competitive business world today, the negative publicity and financial ramifications from an IT physical security breakage can be disastrous. An IT physical security breakage could and most likely lead to the selling of shares from stockholders, financial revenue and profit loss, numerous corporate lawsuits, disgruntled employees, corporate and brand embarrassment, and exhaustive time and effort spent on problem research and prevention.

When coupled with constant September 11 terrorism concerns and the importance of corporate data privacy, the need and demand for a biometric physical security solution has never been higher. This paper will address biometrics and its history, discuss and analyze various biometric techniques and products, provide advantages and disadvantages of these techniques, and conclude with a discussion on biometrics of the future.

What is biometrics?

In a formal sense, biometrics refers to any automatically measurable, robust, and distinctive physical characteristic or personal trait that can be used to identify an individual or verify the claimed identity of an individual. It is the automatic recognition of a person using distinguishing traits. (1)

From the Greek meaning life (bio) and metric (to measure), the term “biometrics” refers to technologies for measuring and analyzing a person’s physiological or behavioral characteristics. In reality, biometrics refers to protecting network and physical security through physical and behavioral biometric techniques.

The physical biometric techniques include fingerprinting, hand and finger geometry, facial recognition, iris and retinal scanning, and vascular pattern recognition. While, behavioral biometric techniques include speaker and voice recognition, signature verification, and keystroke dynamics. All of these techniques will be discussed later in the paper.

For simplicity, both biometric techniques are defined and designed for simple and streamlined identification and verification purposes of a person. In short, biometric *identification* involves determining who a person is and biometric *verification* is determining if a person is who they say they are. (2)

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

A Biometrics History

One of the first known examples of biometrics in practice, and considered the most popular form of biometrics today, was a form of finger printing used in China in the late 14th century. The fingerprinting involved Chinese merchants stamping children's palm prints and footprints on paper with ink to distinguish them from one another.

In the late Eighteenth century, body measurements were considered an alternative biometric technique. The process was designed for identifying convicted criminals of repeat offenses by measuring and recording a criminal's body, head, and limbs whenever arrested. The process was called Bertillonage. Over time the process proved very time consuming and unreliable.

Today, and mostly over the last three decades, physical security and biometrics have exploded in popularity thanks in large part to the computer revolution and the sensitivity of corporate data. Most corporations integrate a combination of physical and behavioral biometric techniques for their data centers. (Individual Biometrics 2002)

Here are some common physical security biometric techniques.

Physical Biometric Techniques

Fingerprinting

As discussed earlier, is the oldest and most popular physical technique used today. Fingerprinting takes an image (either using ink or a digital scan) of a person's fingertips and records its characteristics. The patterns are matched (ink) or encoded (digital) and then compared with other fingerprint records. Although the popularity of ink is still common, digital scanning is preferred.

With digital scanning, a user presses his or her finger gently against a small optical or silicon reader surface where fingerprint information is taken from the digital scan and sent to a database for verification and identification comparison. (Individual Biometrics 2002)

Figure A: IT Security

Figure B: Physical Security

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Companies like Precise Biometrics of Sweden, are capitalizing on the competitive and dynamic fingerprint market with the development and innovation of IT security (Figure A) and physical access (Figure B) readers. (3)

In short, fingerprint security readers provide for many advantages. Such as a piece of mind in having no passwords or PIN numbers to remember; the elimination of expensive password administration; flexibility and interoperability; an unlimited number of users; preservation of privacy (fingerprint template stored on card); ease of use; and compatibility with all major access control systems. (Precise Biometrics p6)

Conversely, the technology does pose several challenges. Scanner durability form static discharges and vandalism can be seen as a first challenge. High maintenance and cleaning of the scanners is thought of as a second challenge. And, the possibility of tricking the system with fake fingerprints is seen as a final challenge (4)

The future of fingerprinting appears to be very bright, as you will continue to see widespread usage within the law enforcement community and for personal use. Corporations have recently introduced memory stick fingerprint scanners and fingerprint mice to capitalize on the increasing market. Furthermore, a large number of banks will incorporate this as the accepted authorization at ATMs for withdrawing and depositing money and at grocery stores for fingerprint scan checkout and billing to a registered user's credit card or debit account.

Fingerprinting Examples:

Casio Computer and Alps Electric have developed a small fingerprint scanner (Figure C) built into a short, thin cylinder for use in cellular telephones and other portable devices for use in Fall 2003. The cylinder, 0.2 inches in diameter and 0.6 inches long, contains a sensor, light, and lens. When users roll their fingers over the device, it can produce an 8-level monochrome fingerprint image at 600 dots per inch resolution. (5)

Figure C: Casio Cellular Scanner

Figure D: HP IPAQ H5450

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Hewlett-Packard (Figure D) became the first manufacturer to add biometric identity checking to a mass-market consumer portable electronics device last year, when it built a small fingerprint scanner into its HP IPAQ H5450 PDA (Williams p1)

Hand Geometry

As you guessed, hand geometry is a biometric solution that reads a persons hand and/or fingers for access.

Hand geometry may be familiar to you if you have ever been to a Walt Disney World theme park. Prior to entering the theme park, a user aligns the palm of his or her hand and fingers onto a metal surface with guidance pegs that read the hand and finger attributes of that person. In conjunction with your paid admission ticket, the device then records the users hand information and sends it to its database for identification and verification for entering and reentering the park. Like fingerprinting, this is usually a 5 second process. (Individual Biometrics 2002)

Hand geometry offers many advantages similar to the other technologies such as ease of use, small data collection, resistant to attempt to fool a system, difficult technology to emulate a fake hand, and provides for the elimination of buddy punching in workforce management solutions.

There are however several challenges to the technology. Besides high proprietary hardware costs and size, the aging of the hands and fingers of individuals poses a challenge. The inability of the machines to cater to those with hand injuries is a second challenge; the lack of accuracy of the technology can be seen as a third challenge, and the final challenge deals with the biometrics inability to not recognize a fake hand. If the right pressure is applied to the surface correctly, this can be done with relative ease. As mentioned, this has proven to be extremely difficult. (Individual Biometrics 2002)

The future of hand scanning appears to be static. From a cost standpoint, is more expensive then fingerprint technology and just as effective. In the case of a workforce management solution, hand punch terminals are not as reliable since hand scanners are predominantly used for verification purposes only. If used in conjunction with other techniques, passwords, and smart card and tokens then it could prove to be a viable method.

A Hand Geometry Example:

Corporations such as Time Masters, Inc, out of Los Angeles, California, have specialized in this technology and have marketed hand and finger geometry as a part of a workforce management solution for companies. The Time Masters Hand Punch (Figures E and F) captures a three-dimensional accurate image of an

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

employee's hand each time an employee punches in and out with green and red lights notifying the employee of the status of each punch. (6)

Figure E: Time Masters Hand Punch

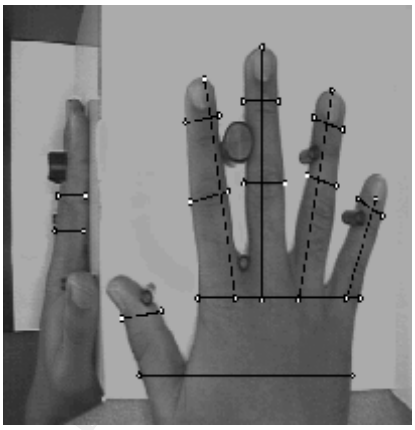


Figure F: HP Hand Position

Facial Recognition

As gathered from the name, facial recognition analyzes the characteristics of a person's face. Access is permitted only if a match is found. The process works when a user faces a digital video camera, usually standing about two feet from it, where the overall facial structure, including distances between eyes, nose, mouth, and jaw edges are measured. These measurements are retained in a database and used as a comparison when a user stands before the camera again. (Individual Biometrics 2002)

Facial recognition has many advantages such as easy integration into existing access control or time and attendance systems; verification and/or identification being accomplished in a short time period; flexible communication interfaces that enable terminals to be networked together; and a non-intrusive technology.

Facial recognition technology does have its challenges. Today's IT and Security professional will have to deal with the frustration of verification reattempts. Changes in lighting, objects in the background distorting a reading, imprecise facial positioning, and expressions of the user can all contribute to verification reattempts. A second challenge is the scanners inability to recognize countermeasures against a clean photo such as beards, mustaches, and disguises. A third challenge is the possibility of fake faces or molds affecting a reading. Legal and privacy issues can be seen as final challenges. (7)

The future of facial recognition remains uncertain due to the difficulties in making a positive identification of a person and with this biometric being a verification-only type of system. Since its inception, facial recognition has been touted as a fantastic system for recognizing potential threats (whether terrorist, scam artist,

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

or known criminal) but so far has been unproven in high-level usage. The technology has proven to have more problems than successes.

A Facial Recognition Example:

Cognitec Corporation's FaceVACS-Entry technology facial recognition scanner (Figure G) showcases a facial recognition example. Here the technology is used for allowing this flight attendant airport access and verification. Notice the distance (2 ft) from the machine to the user. (8)

Figure G: Cognitec FaceVacs

Iris Scanning

Iris scans analyze the features that exist in the colored tissue surrounding the pupil of an eye – the iris. It involves a user, as close as a couple of inches and up to 2 feet away, looking into a device where their iris is scanned and compared. The comparison is conducted at more than 200 points and checked for similar rings, furrows and freckles of the eye. (Individual Biometrics 2002)

The main advantage of iris scanning involves the extreme accuracy of the technology. Since no two irises are alike, identification and verification are done with confidence. Iris scanning also involves non-invasive technology; an ease of use since irises cannot be stolen, unlike keys, access cards, and password systems; and eliminates the frustration for users to have to remember passwords. In addition, and unlike the other techniques learned thus far, will recognize a fake eye from a real one by varying the light shone into the eye and watching for pupil dilation. (Individual Biometrics 2002)

The main challenge of iris scanning involves its high cost. Over time, this should come down in price. Additional challenges involve the potential difficulty in getting someone to hold their head in the right spot for a scan, bad readings due to poor

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

conditions such as lighting, surface positioning if behind a curved, wet, or reflecting surface; and the possibility of obscured irises due to eyelashes or drooping eyelids. (Biometric security systems p 20)

The future of iris scanning appears to be very bright as the ease of use and accuracy of the technology will open the doors for iris scanning in correctional facilities, county jails, airports, banks, and police stations around the country. It is very possible that in the near future everyday people will use iris scanners on a daily basis for entering the office and logging onto corporate networks. Parole officers can use the technology for verifying their paroles; government officials can use it to prevent welfare recipients from using different names and receiving twice the allotted welfare; and ordinary people can use it as a means of an electronic signature for online purchases and business documents. (9)

An Iris Scanning Example:

Corporations such as Iridian Technologies have taken advantage of iris scanning with the development of their very own proprietary architecture and camera software. The Iridian iris recognition technology reaches the marketplace in cooperation with iris-enabled camera (Figures 2,3,4) manufacturers and distribution with licensees such as Panasonic, Oki, and LG. (10)

Figure 2.

Figure 3.

Figure 4.

Iridian Technology Iris Scanners (Figure 2 – Windows based Workstation iris scanner, Figure 3 – Physical access reader, Figure 4 – ATM machine, where an iris is used in place of a PIN number) (Chang p3)

Retinal Scanning

Retinal scanning devices are the most accurate physical biometric available today since there is no known way to replicate a retina. Similar to iris scanning, retinal scanning analyzes the layer of blood vessels at the back of the eye. The scanning involves using a low-intensity light source and an optical coupler that reads the patterns of a person's retina.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Still relatively new and primarily used for high-risk security areas, its popularity is gaining acceptance. Retinal scanning has a user look through a small opening in the device at a small green light. The user must keep their head still and eye focused on the light for several seconds during which time the device will verify his or her identity. This process takes about 10 to 15 seconds total. (Individual Biometrics 2002)

Besides being the most accurate biometric technique available, retinal scanning provides for several additional advantages. The first advantage is the capability of providing viewing assistance to those who are visually impaired (Figure H); a second advantage is providing a piece of mind in knowing the technology is 100% accurate, and the final advantage of the technology being seen as a great long term cost alternative to some other biometric techniques. (Biometric Security Systems web p23)

Besides cost, several challenges to this technology exist. They include the invasive screening process and user discomfort. For example, it requires a user to stand within inches of a device to get an accurate reading, it requires a user to remove glasses if they wear them, it requires a user to place their eye close to the retinal scanning device, and it requires a user to focus on a certain point for a certain period of time.

The future of retinal scanning appears bright. However, it needs to be more refined, non-intrusive, and cost effective for acceptance. I think over time you will see a decrease in the costs and more marketing of the products and technology.

Retinal Scanning Examples:

Corporations like Microvision (11) have capitalized on retinal technology and specifically in offering it as an alternative to helping those who are visually impaired (Figure H). Through a small device called Nomad (Figure I), people will be able to read information from a small, wearable computer that projects an image over their normal vision. The display is a red, transparent computer screen, but, in fact, is no screen at all. The device shoots a tiny laser beam that draws patterns onto the retina so that only the wearer sees the images. (12)

Figure H: Microvision

Figure I: Nomad User

Figure J: Retinal Tech

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

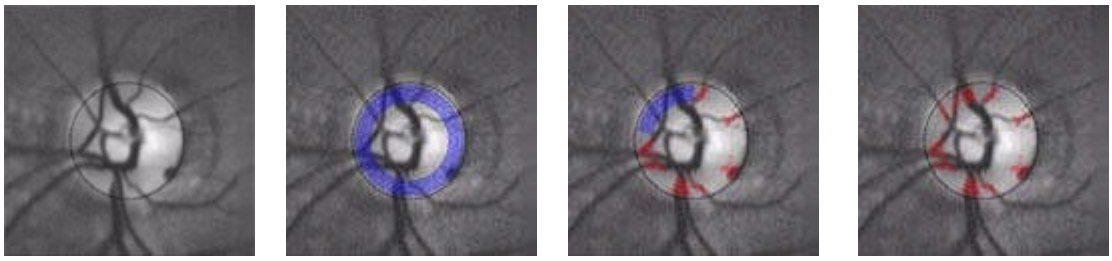


Figure K: Retinal Tech scanning process

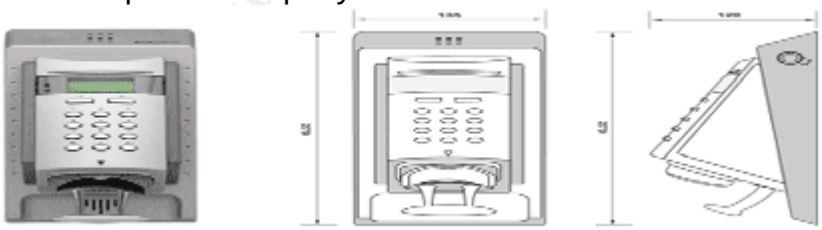
To illustrate the retinal scanning process, Retinal Tech Corporation offers a retinal scanning device (Figure J) that scans a person's retina in four distinct and different phases (Figure K). This technology is designed to be extremely versatile for attachment to a door for physical access, incorporation into a wand, kiosk, or ATM machine, and for connection to a computer. It also works outdoors, in low lighting, and is hands free. (13)

Vascular Patterns

Vascular patterns are best described as a picture of the veins in a person's hand or face. The thickness and location of these veins are believed to be unique enough to an individual to be used to verify a person's identity. (Individual biometrics 2002)

The most common form of vascular pattern readers are hand-based such as Techsphere Corporation (Figures L and M), in requiring the user to place their hand on or in a curved reader that takes an infrared scan of their veins. This scan creates a picture that can then be compared to a database to verify a user's identity. (14)

Figure L: Techsphere Company Scanner



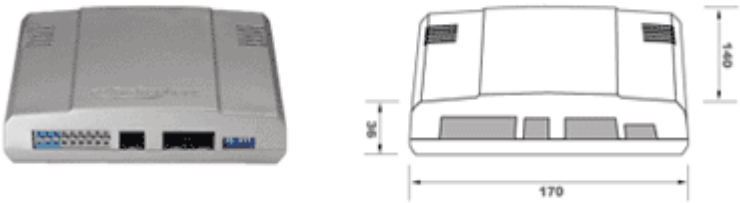


Figure M – Techsphere Company Reader

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Too new to have much data, vascular pattern technology does seem to have a few advantages over its counterparts, including the great difficulty in emulating another person's vein structure, and not having to worry about rain, glasses, or external injuries. (Individual Biometrics 2002)

Challenges do exist in the medical community. Medical testing such as the effects of aging, heart attacks, and medical problems with one's arteries on the scans has yet to be determined fully. It also requires a large amount of space to mount the device so that the entire hand can be scanned; which may restrict its usability. (15)

The future of vascular pattern recognition appears to be very bright. Though minimally used at the moment, vascular pattern scanners can be found at major military installations, some multi-outlet retailers, and currently as a means of gun control. The scanner is built into the guns handle so when an authorized person grabs the handle the firing mechanism is automatically unlocked enabling them to shoot. (Biometric Security Systems p24)

A Vascular Pattern Example:

UK researchers have developed the SIA scope (Figure N) for vascular recognition technology to help aid in the early detection of skin cancer - the first noninvasive system to be able to "look" beneath the surface of the skin. By using it, doctors can rapidly tell the difference between skin cancer and other types of skin damage. This allows the cancer to be identified earlier and treated more quickly, and with greater success.

Figure N: the SIA scope

Based on a scanning technique using harmless light, in a sequence of visible (red, green and blue) and infrared wavelengths from 400 to 1,000 nanometers, light interacts with tissue in different ways depending on the composition of the tissue.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

The SIA scope measures the amounts of the different frequencies of light that are absorbed, scattered and reflected by skin.

Computer software uses a mathematical model to compare the reflectance properties with the results expected from normal skin tissue. Subsequently, it constructs images that show the tissue composition at more than 350,000 points in the skin within a scan area of 11-millimeter diameter to a depth of about 1,000 nanometers (one micro-meter), enabling a doctor to detect early signs of cancer or recognize other skin complaints.

The system completes a scan in under five seconds and processes the data to create a series of images in about 10 seconds. These SIA graphs as they are known (which can also include 3D representations) image the concentrations of melanin, dermal melanin, blood and collagen in the scanned area. (16)

Here are some behavioral biometric techniques.

Behavioral Biometric Techniques

Speaker Recognition Software

Speaker recognition software has been around for quite a while and is beneficial for those utilizing speech and voice as a means of authentication. Speaker recognition involves a user speaking into a microphone with his or her password or access phrase. Here, systems are able to filter out background noise and take into account microphone variances. Verification is confirmed via a database from a previously recorded voice and takes approximately 5 seconds to complete. (Individual Biometrics 2002)

There are several speaker recognition verification systems to consider. They include Fixed Phrase Verification (subject uses the same phrase to access a system), Fixed Vocabulary Verification (designed to prevent the recording of passwords, incorporates a limited vocabulary often using PIN numbers for access), and Flexible Vocabulary Verification (fixed or prompted strings of words can be used as pass phrases). (Biometric Security Systems p24)

To prevent recorded voice use, most devices require the high and low frequencies of the sound to match, which is difficult for many recording instruments to recreate well.

Advantages of speech recognition technology include the flexibility to record and accept multiple verifications, speech, and multiple languages; the inexpensive cost and implementation (easily deployable since a telephone and microphone are used); ease of use, and its acceptance. The challenges of this technology deal with it being unaccommodating to the hearing impaired, as well as, the potential of using recorded voices as a breach of access. (Woodward p4)

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

The future of speaker recognition continues to be bright. You will see more and more applications for controlling access to computer networks (add this to usual password, token, or smart card authentication) or websites; automated password reset services; transaction authentication for telephone banking, and electronic and mobile commerce; for home parole monitoring and prison call monitoring; in voicemail browsing for labeling incoming voicemail with speaker name; and for personalization of voice-web or device customization. (17)

A Speaker Recognition Example:

The Scan Soft TTS-2500 is part of the Scan Soft Corporation Speech Solutions product range and is a high-quality solution to enable speech to virtually any device through the integration of a broad range of features onto a single chip.

The product allows developers to speech enable devices for talking clocks, household appliances, navigation aids, talking books, answering machines and voicemail systems, talking dictionaries, language translators, security system monitors, and cell phones to industrial warning system controls and educational electronic learning aids.

All devices allow for very competitive prices with applications providing multilingual (available in 5 languages: American English, French, German, Spanish, and Mandarin Chinese) options and unlimited system vocabulary in selectable male, female, and customized voices. As well as, providing high accuracy, advanced speech algorithms, low cost, and superior quality. (18)

Signature Recognition

Is an automated method of measuring an individual's signature by having a user sign on a tablet or on paper that is lying over a sensor tablet. The device records the signature and compares it to its database. (Individual Biometrics 2002)

The technology examines such dynamics as speed, directions, and pressure of writing; the time that the pen or stylus is in and out of contact with the paper, the total time taken to make the signature; and where the stylus is raised and lowered on the paper. (Woodward p4)

The advantages of signature recognition include being able to accommodate to those who have trouble speaking, ease of use, easily deployable, and low development and application costs.

It does have several challenges. The obvious choice involves the inability of the technology to cater to those with difficulty writing and the inability of adjusting the technology to cater to those using foreign languages. Because of this, the future of signature recognition remains static. If you are a global corporation, you may want to opt for other biometric alternatives.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

A Signature Recognition Example:

Companies such as Automated Signature Technology have revolutionized signature recognition with several customized products.

They have developed signature recognition automatic pen and ink signature machines that alleviate the task of signing letters. In addition, they allow you to sign your name with any kind of pen desired.

Here, Figures O and P showcase two Automated Signature Technology signature recognition types. (19)

Figure O: AST SR #1

Figure P: AST SR #2

Keystroke Recognition - 9

Involves a user typing his or her password or phrase on a keyboard. The system then records the timing of the typing and compares the password itself and the timing to its database. Verification takes less than 5 seconds. (Individual Biometrics 2002)

This technology examines such dynamics as speed and pressure, total time taken to type certain words, and the time elapsed between hitting keys. It also involves measuring successive keystrokes, keystroke durations, finger placement and applied pressure on the keys from that user. (Woodward p5)

The advantages of keystroke dynamics in the computer environment are obvious. Neither enrollment nor verification disturbs the regular workflow because the user would be tapping the keys anyway. And unlike other biometrics systems, keystroke dynamics is almost free. The only hardware required is the keyboard and using the software is no more difficult than typing ordinary passwords. (20)

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Analysts who follow the biometrics industry say the keystroke technology is less accurate than other technologies such as fingerprinting or retinal scans and has gained little acceptance. Thus, the future of keystroke recognition remains uncertain.

A Keystroke Recognition Example:

This keystroke recognition technology has recently gained notoriety in the music industry. Start-up Musicrypt.com and Net Nanny Software said they are joining forces to create software that can identify individual music listeners by the way they tap out letters on computer keyboards. This information would be used to protect songs against unauthorized distribution and use.

The companies want music labels or online retailers to insert the technology into downloaded music, so that only a person who buys a given song would be able to play it on a computer. Identifying the buyer by these keystroke patterns is far more secure than using passwords, which can be passed on to thousands of people. (21)

Biometrics of the Future

Are infinite in their possibilities. Many of the technologies discussed thus far are paving the way of the future. However, newer technologies (gait recognition, lip print identification, body odor) are gaining more and more acceptance.

In the medical world, gait recognition, which measures body gestures and movements, is being used by physical therapists to help detect and remedy human movement patterns. It may someday revolutionize the way we are allowed access to places. This behavioral biometric technique recognizes the uniqueness in the ways people walk by scanning human movement, then digitalizing (via binary transfer) the data, and storing the data for a match. It can detect, classify, and identify humans from distances up to 500 feet away and under all weather conditions in both day and evening. Its accuracy remains a current drawback. (Shen p11)

In the forensic science community, the use of Lip Print identification is gaining more acceptances. Similar in the logic of fingerprinting, lip prints provide an alternative form of identification. The hassle of reading ones lips and piercing issues prove to be challenges. The main drawback is the user effort required for authentication. (Shen p14)

Body odor recognition (also called chemical odor analysis) is seen as another biometric. Yet still unproven, we know that certain breeds of dogs excel at using their sense of smell to track humans. At least one company is working on a device to identify people based on body odors. The scientific basis of the work is that the chemical composition of odors can be identified using special sensors.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

The University of Leeds has pioneered similar research that has application to drug and bomb detection technologies. The disadvantages of this technology include inconsistencies in chemical composition resulting from hormonal or emotional changes. (22)

The main obstacles of biometrics will continue to involve complexity and privacy issues surrounding information abuse. Biometric information abuse has caused some civil libertarians to be incensed by the risks posed by the personal nature of biometric information and how this information can be manipulated or misused for unimaginably evil purposes by other people, employers, and governments. Additional concerns center around biometric accuracy and performance – vendors need to be able to commit to a 100% accuracy of their technologies, something that they do not want to do at this time; many of the biometric techniques are easy to fool such as the case of a fingerprint saved on a piece of candy; and systematic bypass of determined and creative hackers. In other words, today's hacker is becoming smarter than ever. (23)

Physiological biometric technology and finger scan technology (36%) will continue to dominate the biometric market. However, other technologies such as hand 27%, signature 5%, iris 16%, voice 6%, and facial 11% recognition are all gaining popularity. And handwriting technology is becoming popular with banks and credit card authorizations. (Shen p6)

The future of biometrics depends upon its industry. The biometric industry must first shed the negative media perceptions of the technologies. It must change the perceptions of an immature and standards developing market. It must improve the engineering of biometric applications and show a better return on investment to corporations. And most importantly, it must improve its growth by eliminating the privacy perceptions and legal issues that exist. (24)

Biometrics usage will continue to work in conjunction with security software (firewalls, antivirus, encryption) and security hardware (token and smart cards, and firewall/VPN devices); in security sensitive environments such as airports and casinos; with law enforcement; prisons, jails, amusement and theme parks, corporate time systems, in assisting the disabled and mentally challenged; with new technologies for laptops not communicating with a corporate network; on desktops communicating with a corporate network; and more vendor product and service line expansion. The popularity of e-business will continue to be the driving force behind advanced security needs. (Shen p6)

When choosing a biometric system, the following items should be considered when deciding. Characteristics such as speed, accuracy, user-friendliness, low-cost, public acceptability, reliability, resistance to counterfeiting, acceptable storage requirements, and fast enrollment times should all be considered. (Network Security 2003)

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Overall, I hope this paper has exposed you to a vast future of opportunity that exists in physical security and biometrics. The intent was to showcase and discuss the myriad biometric techniques available today and tomorrow, highlight the advantages and disadvantages of these techniques, illustrate key company and contact information if interested in implementing them, and to provide you with assistance and considerations with choosing the right biometric solution.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Bibliography

1. Woodward, John. "Biometrics: A look at Facial Recognition"; October 2003. http://www.rand.org/publications/DB/DB396/DB396.pdf

2. Individual Biometrics. "An Overview of Biometrics", June 2002 http://ctl.ncsc.dni.us/biomet%20web/BMIndex.html,

3. Precise Biometrics. "Personal Proof: Knowing who's who when security really counts", November 2003. http://www.precisebiometrics.com/data/content/DOCUMENTS/200359141913709Personal_Proof_2003.pdf

4. Biometric Security Systems. "Biometric Technologies", November 2003. http://www.biometricsecurity.com.au/technologies/technologies.htm

5. Williams, Martyn. "Casio Unveils Better Cell Phone Security", http://pcworld.shopping.yahoo.com/yahoo/article/0,aid,109597,00.asp, Yahoo; Feb 28, 2003.

6. Time Masters Corporation website. Product Family. October 2003. http://www.time-masters.com/jjj.php?family=100

7. Penman, Richard. "The Role of Facial Recognition: Biometrics in the Security Industry", Geocities, July 6, 2002. http://www.geocities.com/penmanre/Research/FacialRecognitionBiometrics.htm

8. Cognitec Systems. Product Family. November 2003. http://www.cognitec-systems.de/products-entry.htm

9. Chang, Ellen. "Iris Scanning", Research Paper, Dec 8, 2000. http://www.stanford.edu/~ellenc/cs147/IrisScanning.htm

10. Iridian Technologies. Product Family. November 2003. http://www.iridiantech.com/products.php?page=4

11. Microvision Corporation. Home Page. November 2003 http://www.microvision.com

12. Heckman, Candace. "Eyesight of the future is here". June 18, 2001. http://seattlepi.nwsource.com/business/27731_retina18.shtml

13. Retinal Technologies. Technology. November 2003. http://www.retinaltech.com/technology.html

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

14. Techsphere Corporation. Products. November 2003. http://www.tech-sphere.com/english/system.htm

15. Shen, Michelle M. "The Promise of Future Technologies", June 26, 2003. BiometriTech: 2003 NY Conference and Exposition. http://www.epolymath.com/futuretechnologies.pdf

16. Welsh, David. "Non-Invasive technology looks beneath the skin", October 25,2003. Dawn weblink, http://www.dawn.com/2003/10/25/index.htm

17. Reynolds, Douglas "An Overview of Automatic Speaker Recognition Technology", Applications. July 10, 2002 http://www.clsp.jhu.edu/ws2002/preworkshop/reynolds.pdf,

18. Scansoft Corporation. Real Speak TTS-2500 Product Information. November 2003. http://www.scansoft.com/realspeak/tts2500/

19. Automated Signature Technology. Products. November 2003. http://www.signaturemachine.com/products/products.html

20. Schaup, Sonja "Computer user verification based on keystroke dynamics", Cryptology and Data Security. November 2003. http://cs.fernuni-hagen.de/researchAreas/cryptology/main_Computer_User.html

21. Borland, John. "The latest in anti-piracy efforts: Keystroke Recognition", news.com, June 13, 2000. http://news.com.com/2100-1023-241792.html?legacy=cnet

22. Network Security Technologies. Presentation. November 2003 http://www.cs.usask.ca/undergrads/der850/project/biometrics/methodologies.shtml

23. Yudkowsky, Chaim. "Body of evidence suggests increased use of biometrics", Triangle Business Journal, October 2003 http://triangle.bizjournals.com/triangle/stories/2003/10/06/smallb3.html,

24. Huddart, Martin. IBIA: Biometrics Advocacy Report. October 3, 2003. http://www.ibia.org/newslett031003.htm

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Last Updated: March 10th, 2014

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Northern Virginia 2014	Reston, VAUS	Mar 17, 2014 - Mar 22, 2014	Live Event
Secure Canberra 2014	Canberra, AU	Mar 17, 2014 - Mar 22, 2014	Live Event
ICS 410@ Sydney 2014	Sydney, AU	Mar 24, 2014 - Mar 28, 2014	Live Event
SANS Munich 2014	Munich, DE	Mar 31, 2014 - Apr 05, 2014	Live Event
SANS 2014	Orlando, FLUS	Apr 05, 2014 - Apr 14, 2014	Live Event
FOR518 Mac Forensic Analysis	Vienna, VAUS	Apr 22, 2014 - Apr 27, 2014	Live Event
SANS Abu Dhabi 2014	Abu Dhabi, AE	Apr 26, 2014 - May 04, 2014	Live Event
US Cyber Crime Conference	Leesburg, VAUS	Apr 27, 2014 - Apr 28, 2014	Live Event
SANS Austin 2014	Austin, TXUS	Apr 28, 2014 - May 03, 2014	Live Event
Security Leadership Summit 2014	Boston, MAUS	Apr 29, 2014 - May 07, 2014	Live Event
SANS Security West 2014	San Diego, CAUS	May 08, 2014 - May 17, 2014	Live Event
SANS Secure Europe 2014	Amsterdam, NL	May 10, 2014 - May 24, 2014	Live Event
SANS Melbourne 2014	Melbourne, AU	May 12, 2014 - May 17, 2014	Live Event
SANS ICS410 London 2014	London, GB	May 12, 2014 - May 16, 2014	Live Event
SANS Malaysia @MCMC 2014	Cyberjaya, MY	May 12, 2014 - May 24, 2014	Live Event
SANS Bahrain May 2014	Manama, BH	May 17, 2014 - May 22, 2014	Live Event
SANS Delhi 2014	New Delhi, IN	May 19, 2014 - May 31, 2014	Live Event
SANS Secure Thailand	Bangkok, TH	May 26, 2014 - May 31, 2014	Live Event
Digital Forensics & Incident Response Summit	Austin, TXUS	Jun 03, 2014 - Jun 10, 2014	Live Event
SANS Rocky Mountain 2014	Denver, COUS	Jun 09, 2014 - Jun 14, 2014	Live Event
9th Annual ICS Security Summit	OnlineFLUS	Mar 12, 2014 - Mar 23, 2014	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced