Global Information Assurance Certification Paper

Something You Are: Biometrics versus Privacy

Jim McDowell

GIAC Security Essentials Project

Version 1.4b

Abstract

Biometrics involves collecting, storing, and using our unique physiological and/or behavioral characteristics for some purpose. In the field of computer security, the purpose is usually twofold, identification and authentication. In this paper, I will discuss some of the present and possible future uses of biometrics. I will also discuss the dangers of storing and using biometric data.

For biometric information to be useful for comparison, a sample of the data must be on file in advance. Privacy rights advocates claim that inadequate controls exist to protect people from the misuse of biometric data. They fear that the wrong people may gain access to the databases that store biometric data, or that the data may be used in ways that were not originally intended. Although their fears are not ungrounded, biometrics appears to have a promising future in computer security. It is imperative that lawmakers act now, while biometric methods are in their infancy, to legislate how biometric data will be collected, stored, accessed, and used.

Introduction

What is all this talk about biometrics? Biometrics are best defined as measurable, physiological, and/or behavioral characteristics that can be utilized to verify the identity of an individual. Biometrics can include unique, physical characteristics of the body, such as the eyes, fingers, hands or face. Biometrics can also include unique voice patterns and even brainwaves. Since your biometric information is unique to you, it can be used to positively identify you. Biometrics can also be used to provide confidentiality, integrity, and availability for the sensitive data that you, and others, work with on a daily basis. But some people question whether collecting, storing, and using biometric information is an invasion of your privacy. In this paper I intend to discuss some of the possible uses, and dangers, of biometrics.

Background

The word “biometrics” is derived from the Greek words "bio", for "life", and "metric", for "to measure”. The use of biometrics for identification and authorization is not a new concept. People have used biometrics for identification of others since the beginning of time. Merchants and armies have used hair color, eye color, skin color, scars, and other identifying characteristics as a way to identify friends, enemies, and trading partners. Fingerprints were used for identification in 14th century China. During the late 19th century, a Parisian policeman named Bertillion developed a method of positive prisoner identification involving measuring certain parts of the body and positively identifying individuals based on those measurements. Bertillion’s method involved eleven different body measurements and included such measurements as head diameter, length of the right ear, length of the left forearm, and the breath of the arms when fully extended to the sides of the body. Bertillion argued that the probability of two people having exactly the same measurements was one in four million. As you would expect, when Bertillion’s method failed, it did so in a big way. In 1903 a newly admitted Ft Leavenworth prisoner was measured using Bertillion’s method. The clerk seemed to remember another prisoner with the same name and similar measurements. Sure enough, Will West's measurements were a perfect match to those of another Leavenworth prisoner, one William West.

At about the same time that Bertillion was developing his system for biometric identification, Edward Henry, a British citizen, was developing a biometric identification system based on fingerprints. Henry’s methodology quickly spread throughout the world as a forensic tool. Despite the modern trend towards DNS as a forensic tool for positive identification, Henry’s fingerprinting system is still the most preferred method of biometric identification in the world.

Due to our inability to store information so that it could be retrieved in a meaningful way, the full impact of biometric identification methods was not seen

until recent years. For example, in 1911 when the Mona Lisa went missing, French authorities collected a thumbprint left at the scene. But because of the chaotic filing system that the authorities were using, they were unable to make a positive identification even though the print was on file in their records.

Modern Biometrics

Modern biometric methods are classified as either physiological or behavioral. Physiological biometric methods are the most popular and include fingerprinting, hand scanning, retina scanning, and facial feature measuring. Behavioral biometric methods include voice recognition/verification and signature verification.

Hand Scanning uses the measurements and contours of the hand and fingers. Measurements include hand thickness, length, width; finger height, length, and width; and the distance between the joints. "The U.S. Justice Department is installing hand-geometry identification equipment in all federal prisons—the same equipment used by Olympic Village officials in Atlanta in 1996 to track athletes and staff (Page 2002)."

Fingerprinting is the most well-known and used biometric method of identification in the world. Normally associated with criminal forensics, fingerprinting has many other uses. "In 1995, New York became the first state to implement a state-wide, automated, fingerprinting system to identify its 750,000 public assistance recipients—resulting in a net closing of 30,234 fraud cases and an estimated cost savings of $256.2 million (Page 2002)."

Retinal Scanning is intrusive and has not gained much public acceptance. Retinal scanning devices point a low intensity light beam at the center of the eye and record the pattern of the blood vessels in the eye. Iris Identification, another biometric method that measures unique characteristics of the eye, uses a non-intrusive camera to photograph and catalog the eye.

Facial Feature Measurement is one of the fastest growing areas of biometrics. Like Bertillion's measurement methodology, facial feature measurement is not as accurate as other biometric methodologies, so it is usually used as a second method in conjunction with some other means of identification. Facial feature measurement uses computer vision, which is the science of extracting information from computer images. A camera is used to take a photograph of someone's face. Biometric software is then used to analyze certain facial aspects, such as face size, mouth width, eye separation, face shape, etc. Casinos use this as a method of identifying scam artists.

No two voices are the same. In fact, the same sounds produced from the same vocal tract at different times are not identical. Voice Recognition systems convert speech into text and use stochastic methods to build a model that represents these variations. The pattern matching process can then compare a given voice pattern to the speaker model for the claimed identity.

Conventional signature verification is widely used to confirm or deny the validity of written documents. Your checkbook is a good example. Biometric signature verification methods typically make a bitmap of the signature. That signature bitmap file, in conjunction with pen pressure and pen angle, is compared with a database entry to verify identity. In their paper entitled "Online Signature Verification Based on Altitude and Direction of Pen Movement", the authors claim that the altitude and azimuth of the gripped pen, under signing, have an individuality reflecting the shape of the writer's hand and the habit of writing (Hangai, S. and S. Yamanaki 2002). According to Yamanaka and Hangai, pen azimuth and pen pressure "would be effective writer verification parameters", when combined with other signature verification methods, like signature bitmaps (Hangai, S. and S. Yamanaki 2002).

Privacy

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated (Constitution of the United States 1791)." Privacy advocates claim that taking biometric data from an individual without the express consent of the individual is a violation of the Fourth Amendment to the US Constitution. It seems reasonable to assume that future privacy rulings will fall under laws associated with searches and seizures, and therefore the Fourth Amendment. The Congress of the United States has, over the last 35 years, has enacted some privacy laws that detail the manner in which an agency of the federal government must maintain records that it collects on its citizens. For the most part however, the job of ensuring the confidentiality and integrity of personal data in the commercial marketplace is left to each state. A summary of state privacy laws is beyond the scope of this paper, however they can be found at the Electronic Privacy Information Center website at http://www.epic.org/privacy/consumer/states.html.

The Federal Privacy Act of 1974 prohibits an agency of the US Government from providing citizen's records to a third party without the individual's consent, allows a person to correct erroneous information about himself or herself, and legislates that all information about an individual must be made available to that individual. In other words, there can be no secret, and possibly incorrect, information about us in a US Government database.

The Driver's Privacy Protection Act of 1994 places restrictions on the disclosure of driving records by the state Departments of Motor Vehicles. However, subsequent to this act the US Supreme Court ruled that driver's license information can be regulated by the US Congress as an interstate commerce commodity. The Court intended for Congress to have the authority to regulate commercial truck drivers who engage in interstate commerce.

The Communications Assistance For Law Enforcement Act of 1994 allows US Government agencies to tap into, and intercept, communications channels if they have court authorization.

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 laid the groundwork for the privacy of health records. Although lacking in specific details, HIPAA mandated the development of standards for the exchange and release of patient health records. The Clinton-Gore Initiative of 1999, as a part of those mandated standards, required that a medical facility get an individual's consent prior to sharing a patient's health record. The Bush Administration has loosened these restrictions to requiring a "good faith" attempt to get a patient's consent prior to releasing his or her health records.

Analysis

Oracle CEO Larry Ellison has been pushing for a national identification card as a way to thwart terrorism. Others have suggested that the national ID database include biometric data as proof of identity. I cannot imagine a more lucrative target for abuse than a database containing personal and biometric information. What safeguards would prevent this data from being misused? The Privacy act of 1974 was a good start at controlling access to sensitive information, however more controls are needed if we are to trust governments and commercial companies with our most private information. A good example of "usage creep" and misuse can be found with Social Security Numbers. The US Congress' original intent for the Social Security Number was that it be used for the purpose of reporting income to the Internal revenue service. When was the last time you applied for credit that your SSN wasn't required? Social Security Numbers are now standard, required, fare for credit applications, driver's licenses, most identification requirements, and many authentication requirements.

Biometrics has privacy advocates scared. This is particularly true in light of the fallout from the events of September 11, 2001. Changes ordered by the US Attorney General allow the FBI to use commercial databases to freely gather information about people. Under the new guidelines, FBI agents don't need probable cause in order to collect and analyze data from commercial sources. According to the ACLU, the new FBI guidelines "reversed many self-imposed restraints the Justice Department adopted in the 1970s after revelations of illegal spying (Bigelow A5)." The revised FBI guidelines are the result of the events of September 11, 2001 as well as the USA Patriot Act. The Patriot Act makes it

easier for prosecutors to use information gathered from intelligence wiretaps. Privacy advocates such as the ACLU and the Electronic Privacy Information Center (EPIC) fear that if biometric data is included into commercial databases that government agents will be able to track every movement we make. They also fear that government agencies may use biometric data, such as facial features, to categorize people as likely terrorists.

How data is used and by whom are important. Just as who has access to commercial databases is very important. In 1995, Lawrence Poneman provided information about his family to a Jewish organization for the purported purpose of uniting Holocaust victims with their families. A couple of years later Poneman discovered that the organization had sold its database to a direct marketing group. That information was subsequently sold numerous times and ended up in the hands of a neo-Nazi group in Idaho.

Medical records are the most sensitive of any data stored anywhere. Clearly, biometric methods could be used to authenticate medical staffs that need access to patient medical records. But what if future biometric data could be used to predict susceptibility of an individual to certain diseases or to help predict a person's lifespan. How valuable would such information be to a life insurance company? How much would it pay to get such data?

Los Angeles County, California, estimates that it has saved $55 million in fraud during the last 8 years by using fingerprint identification to positively identify recipients. New York State claims to have saved an estimated $314 million since 1995 by using biometric identification methods. Texas, and Pennsylvania are considering following suit. Biometrics appears to be a no-brainer for welfare programs, however biometric methods have not really caught on in most states. Perhaps this is due to the stigma normally attached to the use of fingerprinting in criminal forensics. The appearance of making recipients feel like criminals may be keeping more states from adopting biometric identification methods.

In her written testimony to the United States Senate Judiciary Subcommittee on Technology, Terrorism, and Government Information, Michelle Brown described a series of events in which her name and personal identification records were used to buy goods and services, to rent property, and to engage in criminal activity. According to Ms. Brown, reclaiming her identity has cost her about 500 hours of time spent writing letters and making calls to creditors and to the authorities. The entire transcript of Ms. brown's testimony can be read at http://www.privacyrights.org/victim8.htm and is recommended reading for readers of this paper (Brown 2000). While biometrics might not have saved Ms. Brown a great deal of time, having such data on file with a recognized agency would certainly help prevent such occurrences. Such information could be used for credit card transactions in the same manner that a digital signature is used for online e-commerce transactions.

The most prevalent tool in use today for ensuring the confidentiality, integrity, and availability of computer systems and data is the password. However passwords are often misused and abused. System administrators who require strong passwords run the risk of having users write the passwords on post-its and stick them in plain sight on their monitors. Easy passwords do little for security, but they make the system administrator popular with users. Authentication is a clear use for biometric tools. Imagine using a thumbprint reader to login to your network, or a facial scanner to enter your locked, workplace door. No more carrying those little magnetic access cards around!

Replacing PINs may be the biggest single use for biometrics. According to John Parselle, of FingerScan Pty Ltd., Sydney, Australia, "There is a huge amount of interest by banks around the world in biometrics right now (O'Sullivan)." FingerScan produces a scanning device which plugs into an ATM machine and connects to the bank. Technically, biometrics are a good replacement for PINs because they are unique to the individual and they cannot be lost or stolen.

The American Association of Motor Vehicle Administrators (AAMVA) has proposed that congress enact a uniform driver's license system for all US drivers. AAMVA also is calling for legislation that would require states to make biometric information part of the driver records. Under the proposal, a state would use biometric data to create a driver's license that provides "irrefutable identification." The American civil Liberties Union (ACLU) has called on the Congress to reject the plan as "just a nation ID card by another name (Thibodeau 2002)."

As a result of the Daniel Van Dam murder case in San Diego, California, California authorities are now providing a fingerprinting service for parents of small children. Parents may have their children's fingerprints stored in a police database. Unfortunately, the use fingerprinting will only be valuable in victim identification after a crime has been committed, however fingerprints might be helpful in locating a victim that is being transported or has been kept somewhere. However, organizations like the ACLU have expressed fear that such biometric information on file may, at some future time, be used for other than it's intended purpose.

There are many examples of DNA used in forensics to convict or exonerate someone suspected of a crime. In June 2002, DNA tests linked a man to the slaying of three Louisiana women. This has prompted Louisiana authorities to reopen the unsolved cases of 37 other murder cases. But the investigation has been hampered by the fact that Louisiana has not had a DNA database until recently and their database is not been fully developed yet. DNA evidence is "one of the most significant law enforcement breakthroughs in the past century" according to William Gore, the agent in charge of San Diego's FBI office (Taylor A18).

According to an article from the San Diego Union-Tribune dated Saturday, August 31, 2002, "Prison and probation officials have begun collecting DNA samples from people convicted of federal crimes, renewing a national debate over whether the gathering of DNA evidence infringes on privacy rights (Taylor A18) ." A convicted bank robber who is serving time in a prison in San Diego has refused to submit his DNA. Federal authorities have accused him of violating the terms of his release. The San Diego case is one of only a few such prosecutions in the nation. The convicted felon's attorney claims that collecting DNA without permission violates the Fourth Amendment to the Constitution. Remember that the Fourth Amendment is part of the Bill of Rights and that it guards against unreasonable searches and seizures by government agencies.

Conclusion

The effects of September 11, 2001, have accelerated the pace of development for the field of biometrics. Biometric devices are unique to the individual and make good identification and authentication devices.

Biometrics is already being used in criminal forensics, public assistance recipient authentication, and in the prison system to positively identify detainees. Future uses could include PIN and password replacement, authentication to sensitive data, and as a means to combat identity theft. But developing databases storing a myriad of biometric data is not without its hazards. There are scant few privacy laws at the federal government level. There are no federal government laws that pertain specifically to the collection, storage, and authorized use of biometric data. “It’s great when the state proposes using biometric information to track down deadbeat parents and make them pay child support”, says John Woodward, a senior policy analyst at RAND, an Arlington Virginia-based think tank, “but it is not so great when you think about somebody selling your digital photo (Winter 2000).” Biometrics isn't failsafe either. If someone stole your digital certificate you would notify the Certificate Authority (CA), ask the CA to revoke the certificate, and then have the CA issue you a new certificate. Now suppose someone has stolen your retina scan. What do you do?

Biometrics appears to be a growth industry of the near future. However, until lawmakers are willing to tackle the privacy aspects of biometrics, there will be tremendous opportunity for the misuse of biometric data. At a minimum, lawmakers at the federal and local level should try to gain an understanding of biometric technology. They should act now to strengthen the various privacy statutes while still allowing the U.S. Government the leeway to protect it’s citizenry from terrorism. Unfortunately, in the words of Barry Steinhart of the ACLU, “The technology is moving at the speed of light, and the law is moving at the speed of a tortoise (Winter 2000).”

References

Brown, M. 2000. Identity Theft: How to Protect and Restore Your Good Name. *U.S. Senate Committee Hearing on the Judiciary Subcommittee on Technology, Terrorism, and Government Information.* Retrieved from the World Wide Web: http://www.privacyrights.org/victim8.htm

"Biometrics: The basics". Retrieved 27 August 2002 from the World Wide Web: http://www.mckinnonsc.vic.edu.au/la/it/ipmnotes/biometrics/biobasics.htm

Bigelow, B.V. 2002. FBI will tap into personal profiles. San Diego Union-Tribune, 3 September 2002, sec. A, 4.

Hangai, S. and S. Yamanaka. On-Line Signature Verification Based on Altitude and Direction of Pen Movement. Retrieved 21 August 2002 from the World Wide Web: http://www.hanlab.ee.kagu.sut.ac.jp/~yamanaka/contents/study/icme2k

McCullagh, D. The Oracle of National ID Cards. *wired.com.* Retrieved 30 August 2002 from the World Wide Web:http://www.wired.com/news/conflict/0,2100,47788,00.html

"Overview of Biometrics". Retrieved 30 August 2002 from the World Wide Web: http://developer.novell.com/research/appnotes/2001/july/01/A0107013.htm

O'Sullivan, O. Fingers, hands, eyes, face, voice, all are in use and could relegate PIN-based security to history. *banking.com.* Retrieved from the World Wide Web: http://www.banking.com/aba/cover_0197.htm

Page, D. Biometrics: Facing Down the Identity Crisis. *hightechcareers.com.* Retrieved 10 September 2002 from the World Wide Web: http://www.hightechcareers.com/doc198/biometrics198.html

Privacy Laws by State. *epic.org.* Retrieved 9 September 2002 from the World Wide Web: http://www.epic.org/privacy/consumer/states.html

Speaker verification. *biometrics.cse.msu.edu.* Retrieved 21 August 2002 from the World Wide Web: http://biometrics.cse.msu.edu/speaker.html

Taylor, M. 2002. DNA from prisoners, parolees collected. San Diego Union-Tribune, 31 August 2002, sec. A 1.

The Communications Assistance to Law Enforcement Act of 1994. United States Code Title 47 Chapter 1001. Retrieved 28 August 2002 from the World Wide Web: http://www.eff.org/pub/privacy/Surveillance/CALEA

The Driver's Privacy Protection Act of 1994. United States Code Title 18 Chapter 123. Retrieved 28 August 2002 from the World Wide Web: http://www.hdr.com/dppa.html

The Health Insurance Portability and Accountability Act of 1996. 67 Fed.Reg. 53181. Retrieved 3 September 2002 from the World Wide Web: http://www.mbf-law.com/pubs/client/rules_cor.pdf

The Privacy Act of 1974. United States Code Title 5 Chapter 552a as Amended. Retrieved 28 August 2002 from the World Wide Web: http://www.usdoj.gov/foia/privstat.htm

Thibodeau, P. 2002. National driver's license system plan comes under fire. *computerworld.com.* Retrieved 6 September 2002 from the World Wide Web: http://www.computerworld.com/databasetopics/data/story/0,10801,67385,00.html

Winter, C. 2000. Biometrics: Safeguard or Invasion of Privacy? Ft Lauderdale Sun-Sentinel, 29 October 2000. *biometricgroup.com.* Retrieved 7 September 2002 from the World Wide Web: http://www.biometricgroup.com/a_press/sunsentinelarticle_oct2000.htm

Last Updated: July 22nd, 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
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
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
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
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
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 Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CA	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
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
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
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 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
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