Global Information Assurance Certification Paper

Biometrics: The Real Sentry for Protection of Information

Jesse J. Witherspoon

Introduction

Biometrics is a technology that has been in existence for a number of years and until recently was something we saw or heard about exclusively in movies or on television. However, it is now riding a new wave as it solves identity or authentication problems that have plagued system and security managers for years. It is no longer 'just' in the movies; it is being used to mitigate security risks in many business environments. For years, business and industry ignored biometrics because it was too obscure, or too esoteric. As Distributed Denial of Service (DDOS) and other network security breaches increase so is the use of biometrics.

What is Biometrics?

Biometrics technologies verify a persons' identity by analyzing human characteristics such as fingerprints, facial images, irises, heat patterns, keystroke rhythms, and voice recordings. Amazingly, it has been around in some form since the 1800's. Alphouse Bertillion invented a system in 1870 that analyzed criminals' fingerprints. Francis Galton improved the Bertillion system by proposing several biometrics indices for facial profiling. Of course, the system has been extremely enhanced since then. The most common forms of biometrics techniques are signature verification, retinal analysis, facial analysis, fingerprint verification, voice verification, and hand geometry.

Not specifically related to security is the forensic technology that we have heard about consistently since the O.J. Simpson trial, which is DNA pattern matching. Although it is not thought of as such, it is a biometrics technique. Some of the other new techniques are ear recognition, odor detection, sweat pores analysis, keystroke analysis, and head analysis. These techniques fall into two classes:

- Physiological based techniques
- Behavior based techniques

Threats

Biometrics technologies are involved in the mitigation of security risks, or threats, to network systems at whatever point an intruder may attack. They do not only come into play during the authentication mode of system access. Threats exist because of system vulnerabilities and are potential violations of security with expected or unexpected harmful results. If an unauthorized user accesses a system he/she can destroy information, operating systems, and programs. They can disclose information or they can cause disruptions or interruptions in an organization's normal operations by damaging systems or network processes.

Although, Biometrics technologies, in some form, have been around for many decades, it is still maturing. Attackers are getting smarter as time goes along and so must technology. As we venture more into the world of E-Commerce, it is critical that security technologies evolve so that it can effectively safeguard organizational assets and the privacy of data. The following sources of threats are potentially dangerous to successful operation of an organization or information processing activity:

Physical threats	Natural disasters (fire, storm, water damage) and environmental conditions (dust, moister, humidity).
Technical threats	The equipment of a system (or software) which might fail to carry out its function (failure) or it might carry them out in an appropriate way (malfunction).
Human threats	The main source of communication breaches. It includes unauthorized users who wish to damage a biometrics system, and authorized users who misuse the system either deliberately or accidentally.
Theoretical threats	The vulnerability of the algorithms, protocols, and mathematical tools used in the methods that they are implemented in the systems.

Part of the new wave that biometrics is riding is due to the successful deployment of the technology in the mitigation of the human threat risk. Human threats can be further categorized into internal and external: Internal human threats are disgruntled employees, hackers, former employees, and system/security administrators. External human threats arise from commercial espionage, vendors, manufacturers, hackers, and crackers. The specific threats are:

- Intrusions
- Denial of Service or Distributed Denial of Service
- Disclosure of Information
- Corruption of Information
- Unauthorized use of resources
- Misuse of resources
- Unauthorized Information Flow

All of the above are threats and the entity involved is referred to as an attacker who intrudes upon a system. Biometrics can prevent the intrusion attempt of an attacker to gain access to a system or a system device posing as a legitimate user.

Biometrics as a Security Resource

Biometrics as a security resource is vast and varied. There continues to be a lack of confidence in biometrics technology, in spite of the new wave that it is riding. The value in the use of biometrics will increase ten-fold if its methods are tested and standards developed. The remainder of this paragraph discusses a few of the physiological biometrics techniques that can insure that system or facility access is only provided to authorized personnel. The physiological techniques discussed are fingerprints, iris scanning, and hand geometry-vein.

The patterns and geometry of fingerprints are different for each individual and they remain unchanged as the body grows. The classifications of fingerprints are based on several characteristics such as: arch, loop, and whorls. The fingerprint systems available for recognizing these characteristics are complex and advancements in biometrics technology can now differentiate a live fingerprint from that of a cadaver.

Fingerprints and palm prints are extremely accurate since they rely on unmodifiable physical attributes, but their use for access security requires special input devices. These devices are not always compatible with standard telecommunications and computing equipment. Thus they are undesirable for remote access by traveling users. Some finger recognition systems concentrate only on the location and identification of small areas of details whether or not such areas are identical. Neural approaches allow automation of the fingerprint encoding process, which allows higher matching performance.

People with missing fingers can not use fingerprint systems. Those with injured or swollen fingers may also have a problem being verified by biometrics systems. Among the various biometrics methods investigated by the GAO (e.g., voice verification, hand geometry, signature verification, retina scanning) fingerprinting is the most viable option to use.

Iris scanning is another technique of biometrics technologies. Ophthalmologists originally proposed that the iris of the eye might be used as a kind of optical fingerprint for personal identification. Their proposal was based on clinical results that every iris is unique and remains unchanged in clinical photographs.

The iris consists of trabecular meshwork of connective tissue, collageneous stromal fibres, ciliary processes, contraction furrows, rings, colorations. All these constitute a distinctive fingerprint that can be seen from a distance. The iris trabecular meshwork ensures that a statistical test of independence in two different eyes always pass.

The properties of the iris that enhance its suitability for use in biometrics and automatic identification include:

- It is protected from the external environment
- It is impossible to surgically modify the iris without the risk of loss vision
- The iris' physiological response to light provides a natural test.

- The ease of registering its image at some distance from the subject without physical contact.

The iris recognition systems had public acceptability problems in the past because of the use of an infrared beam. Current systems register the iris image at a comfortable distance from the user but users are still skeptical of this technology. Blind people or people with severe damaged eyes (diabetics) can not use this biometrics method.

The retinal blood vessels highly characterize an individual so accuracy is one of the advantages of this method of identification. Duplicate artificial eyes are useless since they do not respond to light.

The Hand Geometry-Vein biometrics method is based on the distinct characteristics of the hands, these include external contour, internal lines, geometry of hand, length and size of fingers, palm and fingerprints, and the blood vessel pattern in the back of the hand. They compare the image of the hand with the previously enrolled sample. The user enters his identification number on a keypad and places his hand on a platter. A camera captures the image of the hand and then software analyzes it. This technology is mostly used in physical access control, law and order areas.

Hand geometry systems are reasonably fast. They require little data storage space and the smallest template. They have short verification time. A technical problem that needs enhancement is caused by the rotation of the hand where it is placed on the plate.

The physiological biometrics techniques discussed above are currently being used in numerous organizations that have critical assets to safeguard and were not afraid of trying a new and uprising technology. The remaining physiological biometrics techniques are signature verification, facial analysis, and voice verification. These techniques insure that system or facility access is only provided to authorized personnel.

Conclusion

Biometrics technologies are being adopted at an increasing pace for authentication of access rights to highly secure network systems and restricted areas (e.g., airports, laboratories). The current generation of biometrics identification devices is low cost and easy to use. Although, the security strength of the biometrics technologies must be proven by it being tested against a cryptanalytic attack, it is still considered as a premier sentry for protection of network systems. Time and space complexity analysis should be performed on successful attacks.

For the most part, the lack of confidence for biometrics technologies is caused by the lack of requirements and standards. The development of standards will demonstrate that biometrics technology is a reliable technology. Standards will also help manufacturers evaluate their products against a common set of standards. Further confidence in this technology will arise from the development of tests, in which the results would be shared

with the government and public sector. Achievement of a level of confidence will expand the biometrics market and instill trust in the capabilities of biometrics technology.

In closing, it must be said that biometrics technology is far from perfect and it faces the same challenges as all new technologies. There is also the inevitable fear of "Big Brother" lurking behind biometrics. Many people worry that governments and industry will be tempted to use the technology to monitor individual behavior.

There are few, if any ways, to fool the biometrics techniques discussed above and gain unauthorized access to a personal computer, networked environment or facility. As stated throughout this paper, biometrics is riding a new wave because more organizations are recognizing its' present asset protection value and vast potentiality. It is on the rise to being recognized as the 'real' information systems sentry.

References

Clarke, Roger. "Human Identification in Information Systems: Management Challenges and Public Policy Issues." Xamax Consultancy Pty Ltd. 1994. URL: http://www.anu.edu.au/people/Roger.Clarke/DV/HumanID.html (27 Nov 2000)

Daugman, J. "High Confidence Visual recognition of Persons by a Test of Statistical Independence" IEEE Transactions on Pattern Analysis and Machine Intelligence, v.15, n. 11 Nov 1993, pp. 1148-1161.

Deane, F., Barrelle K., Henderson R., Mahar D. " Perceived Acceptability of Biometric Security Systems" Computers & Security v.14, n.3, pp. 225-231, 1995.

Galton, G. "Personal Identification and Description" Nature pp. 173-177, June 21, 1988.

Jouce, R. and Gupta, G. "Identity Authentication Based on Keystroke Latencies" Communications of the ACM, 30, no.2, 168-176, 1990.

Phillips, Ken. "Unforgettable Biometrics." PC Labs October 29, 1997. URL: http://www.zdnet.com/eweek/reviews/1027/27/bioapp.html (27 Nov 2000)

Samal, A. and Iyenger, P.A. "Automatic Recognition Analysis of Human faces and Facial Expressions: A Survey" Pattern Recognition., vol.25, pp.65-77, 1992.

Schneier, B. "Biometrics: Users and Abuses." Inside Risks 110, Communications of the ACM, vol 42, n8, Aug 1999. URL**:** http://counterpane.com/insiderisks1.html (27 Nov 2000)

Last Updated: July 26th, 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
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 San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
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 London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS 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
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
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event