Global Information Assurance Certification Paper

Overview of Biometric Encryption

Mark Wood

April 26, 2001

Version 1.2c

Introduction

So how do we protect access to our information systems from theft and malicious attackers? Remember those sci-fi or spy movie filled with high-tech security devices that operate or activate by voice, fingerprint, handprint, eye, or face recognition. Now that technology is becoming a reality. Imagine going to work and accessing the building by the sound of your voice, then getting on the computer, which uses a fingerprint scanner built into the mouse to give you access your companies LAN. Technology is moving at an alarming pace producing another revolutionary technology known as biometric encryption. "As information system professionals, we should be aware of technologies that help enhance network security measures."(1) The purpose of this document is to prepare and inform people of the new technology known as biometric encryption.

What is Biometric Encryption?

Biometric Encryption uses the physical characteristics of an individual as a way to code/ decode or provide/ deny access to a computer system. Some of the characteristics that are currently being researched are fingerprinting, palm/ handprints, retina and iris, facial recognition, and voice authentication. Since these physical characteristics are unique to each individual biometrics is seen as a way to fight fraud and theft. The technology is viewed as superior to that of current password and personal identification number (PIN) systems. The reason behind it is that there is no smart card, key card, post-it note, or password to lose. In addition to that you also ensure that the person accessing the system is actually an authorized user. A few additional reason that biometrics are better is convenience to the customer (no password to remember), and reduces time IT department spend on lost cards or forgotten passwords.

History of Biometrics

The link of biometrics can be traced back to the ancient times of Babylonia and early China who used fingerprinting to sign and seal documents. More recently fingerprinting is being used by federal government and law enforcement agencies involved in security activities, criminals and personnel identification. "Ben Miller remarks, 'the first application of biometrics here was in 1968: a Wall Street brokerage used fingerprints to open the vault where the stock certificates were held. That application cost $20,000 in 1968. It would probably cost $1,700 today, and by the year 200, it'll probably cost just $300.' "(2)

How Biometric Encryption works

So how does it work? As with any other encryption system were you take plaintext put it through an algorithm, which is encoded with a single key or multiple keys to get encrypted. Today we use passwords or PIN numbers as our keys. The problem with today's encryption keys is the safe storage of this key. These keys are a high vulnerability to encryption system because they can be lost, stolen, and hard to remember.

Biometric Encryption uses a physical characteristic of an individual as the key to encrypt the plaintext or information you wish to encode. So the only thing that has really changed is that instead of trying to memorize that big long password your IT department has implemented you just have to bring yourself. This eliminates the chances you loose, forget or the key from getting lost. It is also hard to impersonate another person in trying to access the system. Let take a look at some of the possible keys that a biometric encryption system might use.

Fingerprint Recognition

This is the most widely used and developed of the technologies. Fingerprint recognition is not the same as fingerprinting. Fingerprinting is used by law enforcement who record your fingerprint. In biometrics they use finger-scan, which take a high-quality picture (250 kb per finger) of your fingers and stores a template (250-1000 bytes) of key unique features on your finger. The template is the key, which cannot be used to reconstruct your fingerprint and only stores a small amount of unique patterns on your finger.

There are three technologies used to get good images and these are Optical, Silicon, and Ultrasound. Optical is the oldest and most widely used providing resolution of up to 500 dpi. The weakness of this technology is size and latency prints (leftover prints of users). Identix and Motorola are the two prominent companies using this technology. Silicon, which most companies are moving towards today is gaining ground. The pros of this technology are less surface area and a better image. Weaknesses include durability and enrollment (getting print into the system). Ultrasound is considered the most accurate of the technologies, but it popularity and use have not caught on. Ultrasound uses acoustic waves and measures the distance based on impedance of the finger, platen, and air. This technology combines the strength of the other two with no real weakness other than it is not widely used. In Figure 1 you can see some of the unique features in your finger that this technology looking for.

Figure 1

Face Recognition

This technology is just like other biometric encryption techniques using various methods, but in recognizing a persons face. The technology focuses on parts of the face that are less susceptible to change or alteration. Primary areas that a facial system would look for are the outline of the eye sockets, cheekbone structure, and around the mouth. There are two different approaches to this technology, which are Local Feature Analysis (LFA) and Automatic Face Processing (AFP). LFA uses dozens of features of the face and also incorporates the location of these facial features. Enabling the system to accommodate changes in the face. AFP uses ratios of distance and the distance between easily acquired features of the eyes, nose, and mouth. This method is more effective in frontal or dimly lit area of capture. Facial images require between 150-300kb and templates are about 1300kb. For a facial recognition system you need a quality video card, camera, and processor speed.

Optical Recognition

There are two types of optical recognition using the iris or the retina. The iris has 266 unique features as opposed to around 13-60 for other biometric technologies. Making optical verification one of the most accurate of the biometric schemes. The characteristics of the iris are converted into a 512-byte template. Iris technology can also scan the iris while an individual still has glasses on and is less intrusive. The error rate of this system is very low for example IriScan's Equal Error Rate is 1 in 1.2 million attempts. The odds that two different irises will return the same identification are 1 in 10 to the 52nd. A system like this costs $6,500, which includes the reader, software, and a PC with frame grabber.

Retina technology has the same attributes with a few exceptions. The system is more intrusive when scanning the individual has to focus on a point and has to have glasses off. Take a look at Figure 2 below to see the location of the iris and retina.

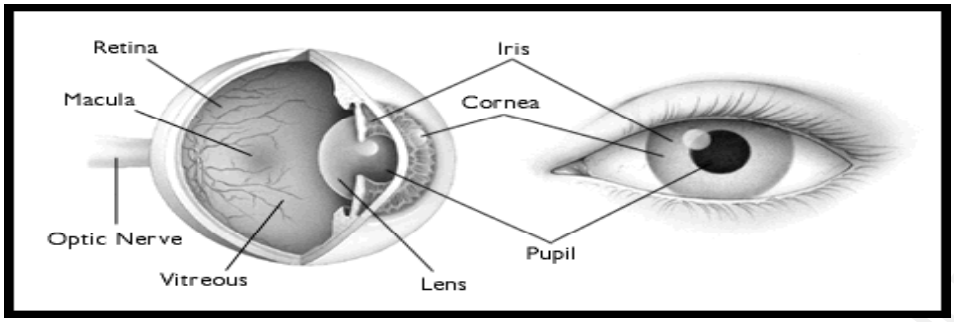


Figure 2

Voice and Key Stroke Recognition

Voice recognition is very appealing to the telecommunications industry. Reason being that most of the technology is already on most PC's today reducing the cost to implement this technology. Issues in this area are changes in a persons voice throughout the day making verification difficult at times.

Key Stroke recognition is another of the many new ways biometric companies are trying to increase the security of passwords by adding the way in which you enter the password. Another biometric technology I would like to mention is signature, which is just like that of Key Stroke recognition.

Government and Biometrics

The U.S. government is looking into the future of biometric technology to evaluate this new technology and it's many uses. The government thinks this technology is so important that it has formed the Biometric Consortium Charter. This organization was formed out of the 1992 working group known as the Biometric Consortium, which had been sharing information between the six executive branches and the each of the military services. "The National Security Agency initiated the formation of this consortium as part of the Information Systems Security mission."(3) The charter was formally approved on December 7, 1995 by the Facilities Protection Committee and reports to the Security Policy Board through the Security Policy Forum.

There are several government and state pilot program out there today. These are only a few examples of the program being used today.

- Federal Bureau of Prisons – Currently using hand geometry biometric systems to monitor prisoners, visitors, and guards. By the end of 1995 30 prisons were to have this system installed.
- Automated Fingerprint Image Reporting and Match (AFIRM) – In July of 1991, Los Angeles California installed the first AFIRM system. The system was put in

place to reduce fraudulent and duplicate welfare check claims. California is expecting the statewide implementation of the AFIRM by the end of 1997.

- California, Colorado, Florida, and Texas Department of Motor Vehicles – Working to establish a fingerprint biometric system for drivers licenses and record data.
- FBI Integrated Automated Fingerprint Identification System (IAFIS) – To replace the manual method used today.
- Immigration and Naturalization Service (INS) Passenger Accelerated Service System (INPASS) – Again the use of hand geometry for verification. Canada has a similar system called CANPASS, which uses fingerprint recognition instead of hand geometry.

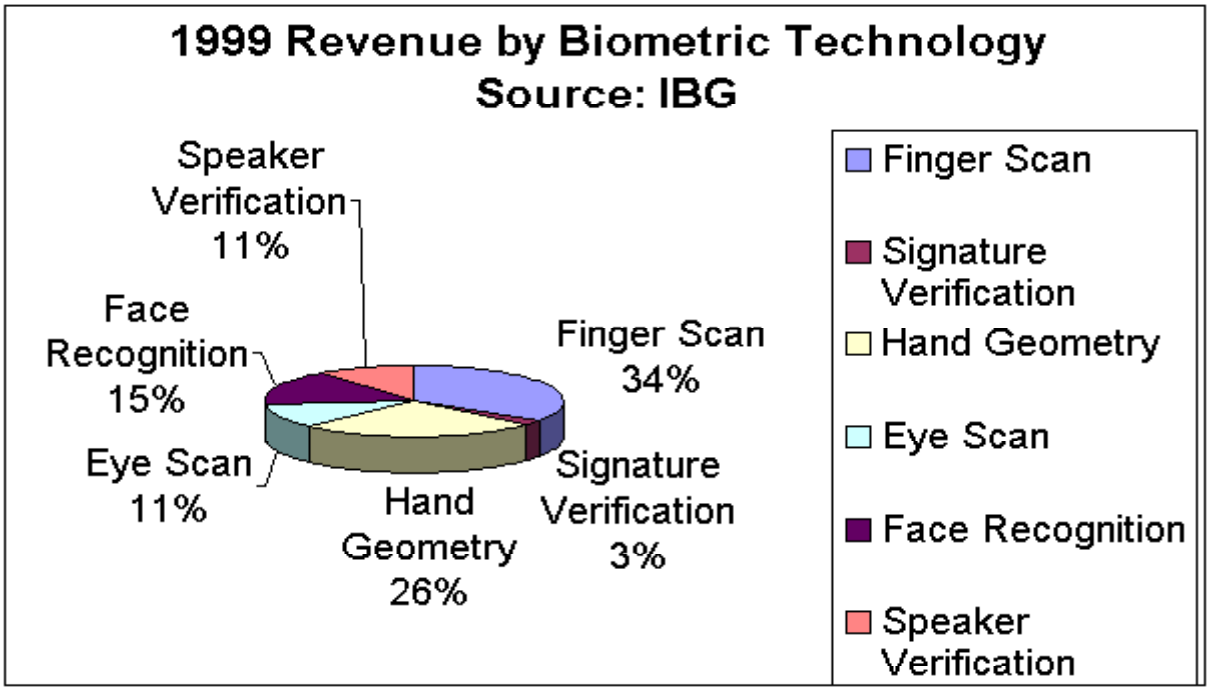
Conclusion

As you can see Biometric Encryption is an emerging technology. By no means does Biometric Encryption solve all of our security problems, but it could be a piece of the puzzle. Biometric Encryption is in the early stages of development so there are problems with the technology. There are people and groups that think this a way big brother (Government) to keep more information about each of us. Biometric Encryption has its uses but like any other technology you have to look at both the benefits and the drawbacks. The figure below is from IBG on Biometric and its projected revenue take a look. I hope this overview gave you some insight to this emerging technology.

Finger-Scan Market Report

For companies or agencies interested in facts, figures, and research on the finger-scan market, we recommend International Biometric Group's **Biometric Market Report 2000**. You'll receive the same report available on www.biometricgroup.com, but purchasers from Finger-Scan.com also receive expanded sections on "*Growth and Risk Factors in the Finger-Scan Market*" and IBG's "*Finger-Scan Market Executive Summary*".

Sample Chart from Biometric Market Report 2000



Total 1999 revenue of non-AFIS biometric disciplines: $58.4 million

Estimated annual revenues of non-AFIS biometric disciplines by 2003: $594 million

Works Cited

1. Esser, Mishelle. "Biometric Authentication". http://faculty.ed.umuc.edu/~meinkej/inss690/messer/Paper.htm

2. O'Sullivan, Orla. "Biometrics comes to life".http://www.banking.com/aba/cover_0197.htm(3/31/01)

3. Joseph P. Campbell, Jr., Lisa A. Alyea, and Jeffery S. Dunn. "Government Applications and Operations". www.biometrics.org/REPORTS/CTSTG96/

References

Esser, Mishelle. "Biometric Authentication". http://faculty.ed.umuc.edu/~meinkej/inss690/messer/Paper.htm(3/31/01)

O'Sullivan, Orla. "Biometrics comes to life".http://www.banking.com/aba/cover_0197.htm(3/14/01)

Joseph P. Campbell, Jr., Lisa A. Alyea, and Jeffery S. Dunn. "Government Applications and Operations". www.biometrics.org/REPORTS/CTSTG96/ (3/21/01)

Ashbourn, Julian. "The Biometric White Paper". http://homepage.ntlworld.com/avanti/whitepaper.htm(3/21/01)

Gunnerson, Gary. "Are You Ready for Biometrics? Biometric ID systems bring tighter security to networks and greater convenience to users". http://www.zdnet.com/pcmag/features/biometrics/intro.html (3/22/01)

Rae, David. "Sci-fi security for the next generation". http://www.vnunet.com/Features/1113471 (3/9/01)

Phillips, Ken. "Unforgettable biometrics' Your body is your key(Just try not to lose it)'". http://www.zdnet.com/eweek/reviews/1027/27bioapp.html (3/22/01)

"Sample Chart from IBG's Biometric Market Report 2000". http://www.biometricgroup.com/a_shared/market_size.htm (3/9/01)

Mendell, Ronald L. "Biometrics: The Tightrope". http://security portal.com/articles/biometrics20010220.html (3/14/01)

O'Shea, Timothy m. and Mike Lee. " Biometric Authentication Management". http://www.networkcomputing.com/1026/1026f2.html (3/9/01)

"Hand Scan.com". http://www.hand-scan.com (3/21/01)

"Facial Scan.com". http://www.facial-scan.com (3/21/01)

"Finger-Scan.com". http://www.hand-scan.com (3/21/01)

"Hand Scan.com". http://www.hand-scan.com (3/21/01)

Last Updated: September 22nd, 2017

Upcoming Training

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 Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	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 Summit & Training 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
SANS Tokyo Autumn 2017	Tokyo, Japan	Oct 16, 2017 - Oct 28, 2017	Live Event
CCB Private SEC401 Oct 17	Brussels, Belgium	Oct 16, 2017 - Oct 21, 2017	
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
Community SANS Colorado Springs SEC401~	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS Vancouver SEC401^	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive