


Fall 2006

Biometric Security: Are Inexpensive Biometric Devices Reliable Enough to Gain Wide-Spread Security Usage?

Brian Thanh Tran

University of Arkansas, Fayetteville

Follow this and additional works at: <http://scholarworks.uark.edu/inquiry>

 Part of the [Information Security Commons](#), and the [Management Information Systems Commons](#)

Recommended Citation

Tran, Brian Thanh (2006) "Biometric Security: Are Inexpensive Biometric Devices Reliable Enough to Gain Wide-Spread Security Usage?," *Inquiry: The University of Arkansas Undergraduate Research Journal*: Vol. 7 , Article 11.

Available at: <http://scholarworks.uark.edu/inquiry/vol7/iss1/11>

This Article is brought to you for free and open access by ScholarWorks@UARK. It has been accepted for inclusion in Inquiry: The University of Arkansas Undergraduate Research Journal by an authorized editor of ScholarWorks@UARK. For more information, please contact scholar@uark.edu.

BIOMETRIC SECURITY: ARE INEXPENSIVE BIOMETRIC DEVICES RELIABLE ENOUGH TO GAIN WIDE-SPREAD SECURITY USAGE?

By Brian Thanh Tran
Department of Information Systems

Advisor: Dr. David E. Douglas
Department of Information Systems

Abstract:

The ever growing need for security in today's world requires exploring the feasibility of various security methods to ensure the safety of the world's population. With the tremendous growth of technology, e-commerce, and business globalization, society implements new methods to try to battle security problems. Technology advances has resulted in a number of inexpensive biometric devices to the marketplace. Two questions surface regarding this devices—are they reliable enough for general usage and will people be willing to use them?

This research conducted a repeated design experiment to determine the effectiveness of four inexpensive biometric devices—three fingerprint readers and an iris scanner. Further, a questionnaire was designed to gain insights to the views of subjects using these biometric devices. On average, all the devices performed well for identification purposes—the fingerprint readers performing better than the iris scanner. The questionnaire revealed that most people prefer fingerprint readers over that of iris scanners and that although 60% of the people surveyed had heard of biometrics, only 21% of those surveyed had ever used a biometric device. The public does not feel that these devices provide complete security, but does provide a reliable means for identification.

Introduction

Biometrics is the study of biological characteristics and behaviors for the purpose of verifying identity. With the tremendous growth of technology to try to battle security problems, the reoccurring question often becomes “is this a reliable security method?”

Methods used by forensic teams such as latent fingerprints, DNA, hair samples, or fiber analyses are not considered to be in the field of biometrics. Biometrics has a key advantage over traditional methods such as tokens (smartcards, keycards, etc) and passwords because they are measurable and use physiological and/or behavioral characteristics to verify the identity of an individual. Tokens can be lost, stolen, forgotten, and in some

cases be duplicated. Passwords have the problems of being stolen, broken, shared, or forgotten.

With the continuation of corporate globalization, events such as 9/11 and the London bombings of July 2005, and identity theft, the need for better security measures have become more prominent and necessary. Recently, biometric technologies are becoming security options in everyday use for businesses and organizations. Trying to take a leap into the biometrics market, Accenture was given a \$10 billion contract in 2004 to incorporate biometric identification measures for the U. S. Visitor and Immigration Status Indicator Technology program, which allows for the tracking of foreigners entering the United States. With the growing importance of e-commerce and online transaction processing the security of IT infrastructure has never been as critical as it is now.

In the midst of the technology age, we are trying to find more methods in which to solve the problems of identity theft and verification to allow for a safer society. This project will provide reliable insights into using inexpensive biometric devices for identity and authentication. In analyzing the collected data, the wealth of information derived from the primary research will allow for a better understanding of how effective current biometric technology really is and what impact it could possible make in the present and future.

New technologies open a world of opportunities. Having an accurate identification and authentication process will help deter crimes, fraud, and save critical resources that can be used to advance the efficiency of society. Currently, the United States has about \$1 billion dollars in welfare benefits that are claimed by individuals who are double dipping with fake identities. Companies such as Mastercard estimate their credit card fraud to be approximately \$450 million annually, and ATM cards have a fraud worth of approximately \$3 billion annually {{Jain, A. 1999; 2}}. According to Erik Bowman from CardTech/ SecurTech, the growing demand for network security industry will increase the market for biometric applications from \$24 million in 1997 to \$60 in 1999 {{Lawton, George 1998; 17}}.

These facts demonstrate that the opportunities for biometric devices to enter the market and make a direct impact are very high.

However, the possibility for so many variables such as age, ethnicity, different body states such as sickness or allergies, or even medical solutions such as contact lenses and Lasik eye surgery, challenges using biometrics to verify identity in everyday life. The technology, if in fact successful, should provide improvements for identity theft and fraud problems. If properly designed, biometric devices could allow for technological advances to improve efficiency and productivity of society as a whole. Nevertheless, this technology also raises a number of questions, some of which are listed below.

- Who uses biometrics?
- How does biometrics work?
- How does biometrics NOT work?
- How effective are these technologies?
- How will these technologies affect private lives?

Purpose of Study:

The research will attempt to answer these questions by use of biometric products that can be purchased by the everyday consumer. Multiple devices testing the same biometric variable were purchased to confirm the reliability of the device and the variable they are testing. Biometric devices considered for the research project included those manufactured by companies such as BioCert, Microsoft, Panasonic, and APC. Through surveys, we hope to gain insight on how people view these devices and do a comparison on whether or not people find these devices as privacy’s enemy or privacy’s friend. This study and the survey focus on the inexpensive biometric devices and do not incorporate all biometrics.

The first research question addresses the accuracy of inexpensive biometric devices. The research question is answered via the three hypotheses in the next section. A questionnaire was developed to help answer the second research question.

To answer the first research question required taking multiple measurements on the same subject with each biometric device. In this research, each subject was identified at six different times with each of the four biometric devices. Thus, it is a repeated measures design model. In addition, age and gender were used as factors. The repeated design research model is shown below as Diagram 1.

Diagram 1. Diagram of Research Design.

ID #	Age	Sex		Run 1	Run 2	Run 3	Run 4	Run 5	Run 6
------	-----	-----	--	-------	-------	-------	-------	-------	-------

The Repeated Measures Design and Hypothesis:

The repeated measures design applies when the values of the dependent variable(s) represent repeated measures on the same subject. The repeated measures are taken at different times on the same subject. This model is used extensively in medical research but also applies to this research.

The model allows testing of hypotheses about measurement factors – referred to as within-subject factors and includes interactions of within-subject factors with independent variables often called between-subject factors. In this model the between-subject effects represent the different biometric devices and the with-in subject effects are the effects over time. The model also includes interactions.

The following hypotheses are used to test the major research question relating to inexpensive biometric devices:

- H₁:** Fingerprint readers and iris scanners accurately identify people on the first try.
- H₂:** The effectiveness of fingerprint readers and iris scanners do not change over time.
- H₃:** Age and gender have no impact on fingerprint readers and iris scanner accuracy.

Fingerprint Recognition Devices:

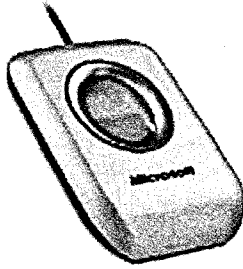
Fingerprints have long been known to be unique to every person. This being so, many places have used fingerprints as a way to identify individuals. As security concerns continue to grow, so does the number of passwords. Personal computers today often store sensitive and confidential data. They are also the access point to corporate networks. As systems become smaller and more mobile, they are more at risk of being lost or stolen. Biometrics provides users a convenient and secure way to manage and access multiple security phrases and codes.

Today’s fingerprint recognition and identification systems work by taking a digital scan of a person’s fingertips and then records the finger’s unique physical characteristics. The fingerprint data will either be stored as an image or encoded as a character string, depending on the developer. The advancement of fingerprint identification has made it the technology of choice in today’s consumer products, such as computer keyboards, cell phones, door locks and employee time clocks. Relative to other biometric choices, fingerprint recognition is cheaper, faster and accurate enough for most applications in which it is used. To prevent fooling the system, newer fingerprint identification systems also measure blood flow to the finger, so that a fake finger can’t be used. Listed and shown below are the 3 relatively inexpensive fingerprint recognition devices that were used in this study.

Microsoft Fingerprint Reader – Model 1033.

Retail Price of \$50.

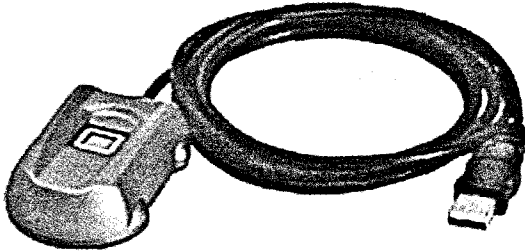
Average Attempt of 1.08 over 6 runs.



APC Biometric Fingerprint Reader– Model BioPodMP4.

Retail Price of \$50.

Average Attempt of 1.10 over 6 runs.



BioCert Fingerprint Reader – Model Hamster III.

Retail Price of \$130.

Average Attempt of 1.07 over 6 runs.



Data Collection and Results for Fingerprint Recognition Devices:

Microsoft Fingerprint Reader

From the data collected, we saw on average that there were no runs that require more than 2 scans to identify the individual. We also saw that adults 40 and up had a lower average on attempts for the device to recognize them versus that of adults 18 to 39. Observations were made that the reason this is probably

true is that the older group took more time when placing their finger upon the device. We also found out that there was not enough evidence to distinguish a difference in the attempts for males versus that of females.

APC Fingerprint Reader

From the data collected, we saw on average that there were no runs that require more than 2 scans to identify the individual. The APC device however, recognized the adults 18 to 39 better than the adults 40 and up. We also found out that this device required less attempts to recognize the males than the females.

BioCert

From the data collected, we also saw that on average there were no runs requiring more than 2 scans to identify the individual. The device manufactured by BioCert also required less attempts to recognize adults 18 to 39 versus that of the adults 40 and up. When comparing males to females, this device had the same average attempts for both sexes.

Recommendations for Fingerprint Recognition Devices:

The purpose of this study was to test and compare the reliability of the current low cost biometric fingerprint recognition devices. As we can see, the results will vary according to brand. On average alone, the BioCert reader had the best at 1.07, closely followed by the Microsoft at 1.08. The APC ended up with an average of 1.10. However, the majority of the tested preferred the Microsoft reader, then the BioCert, and finally the APC reader.

This study has shown that on average, the current low cost providers of fingerprint recognition devices that were used in this study are reliable enough in which it can recognize an individual on average of less than 2 attempts. Common problems that were noticed that caused a person not to be recognized were fingers that were wet, had substances such as dirt or food on them, or cuts would result in a rejection. Also, residue that was left from the last person that used the device sometimes caused the device not to recognize an individual.

Possible users for this type of device are large corporations that have user and password log-ons that maybe stolen. Or the same corporation could implement such devices for a time clock to help prevent time clock fraud in which another person can punch another person's employee number in. Another possible use would be credit card companies having a fingerprint scan on the magnetic strip and when it is used, instead of a signature, fingerprint verification would be needed.

Iris Recognition Devices:

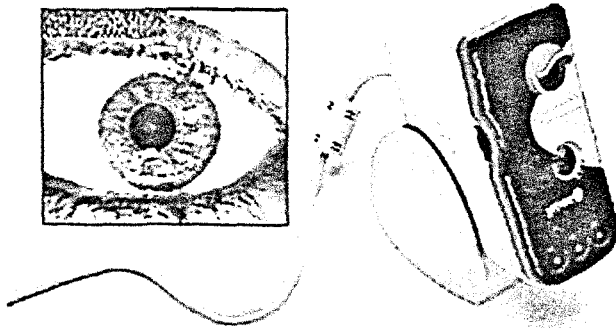
Iris recognition technology examines the unique features of the human iris, the colored portion of the eye, to create an image of the iris. This is then translated into a data template, which can later be used to identify individuals or authenticate user privileges. The iris of the eye possesses physical patterns unique to each person. Similar to fingerprints, no two irises are alike in the world. Iris recognition biometric systems can analyze over 200 points of the iris, including rings, furrows and freckles. Eyeglasses, contact lenses, and eye surgery do not change the characteristics of the iris.

This method of identification is becoming widespread, and is only second behind using fingerprints for identification due to its relative cost and accuracy. To prevent fooling the system iris recognition systems often vary the light in order to see that the pupil dilates, so that a fake eye can't be used. Due to continual advances and range of costs in biometric iris technology, not all of the devices that were originally planned to be used in this study were acquired. Shown below is the only iris recognition device used in this study because all the other iris recognition devices were too expensive.

Panasonic Authenticam – Model BMET100US.

Retail Price of \$200.

Average Attempt of 1.255 over 6 runs



Data Collection and Results for Iris Recognition Devices:

The iris recognition device in this study also was able to recognize an individual on average in 2 attempts. However, adults 40 and up did have more problems than the adults 18 to 39 when it came to the device identifying the individual. When comparing males to females, both sexes had a very similar average in attempts required for identification.

Recommendations for Iris Recognition Devices:

The purpose of this study was to test the reliability of the current low cost biometric iris recognition devices. As we saw in this test, iris recognition was not as reliable as fingerprint recognition. Also, this device was the least favorite among all the biometric devices that were used in the study. The Panasonic

Authenticam was often much slower in recognizing the individual and not as easy to use as described by most surveyed. While we had an average of less than 2 attempts for recognition, there is still plenty of room for development of a cost effective iris recognition device. Faster recognition and ease of use are among the top two.

Although eyeglasses and contact lenses do not change the characteristics of the iris, we did notice that they did affect the results. Eyeglasses tended to cause glare when the device tried to read the iris and sometimes were required to be taken off to get a good read on the iris. Currently, I would not recommend the use of a low cost iris recognition device as many people find them bothersome and are not very likely to accept them at their current state.

Other Biometric Devices Not Used In Study:

Retinal scanning systems look at the pattern of blood vessels at the back of the eye. Retina scans use a light to shine on the retina, and require that the person place their eye close to the scanner, remain still, and focus on a specified location. Biometric retina recognition systems are among the most accurate of all biometric technologies and as such are used at military installations and other high-risk facilities. It is also quite expensive due to the hardware needed. Retica systems is currently is the only full-eye biometric technology company.

Biometric facial recognition measures and analyzes the physical attributes of a person's face. Characteristics measured include the overall structure and shape of the face, and distances between the eyes, nose, mouth, and jaw edges. Face recognition systems can accurately verify the identity of a person standing two feet away in less than five seconds.

Biometric hand geometry recognition measures and analyzes the physical attributes of a person's hand. Characteristics measured include the overall size and shape of the hand, including the lengths of the fingers and joints, and characteristics of the skin such as creases and ridges.

Hand recognition systems are fairly common, however they are expensive due to the proprietary hardware and not that accurate compared to other technologies.

Speech recognition is another biometric technology that distinguishes an individual. The device is not the most accurate as a person's voice can change as different symptoms such as sickness or allergies appear. Speech recognition technology has been in development for a while, as right now it is commonly used to dictate text into the computer or to give commands to the computer (such as opening application programs, pulling down menus, or saving work). While the accuracy of speech recognition has improved over the past few years some users still experience problems with accuracy either because of the way they speak or the nature of their voice.

Emerging Biometric Technologies:

Newer biometric technologies using diverse physiological and behavioral characteristics are in various stages of development. The biometric devices describe in this area are currently being developed and may emerge over the next 2 to 4 years, while others are many years from implementation currently only available commercially. There are a few that are available, but very limited and only to those who are willing to put the capital into further developing and research these devices. Each biometric method's performance, as with all biometric devices, can vary widely, depending on how it is used and its environment in which it is used.

One emerging biometric technology is facial thermography which detects heat patterns created by the branching of blood vessels and emitted from the skin. The patterns, known as thermograms, create a very unique image. Even identical twins have different thermograms. Developed in the mid-1990s, thermography works much like facial recognition, except that an infrared camera is used to capture the images. Currently the efforts into furthering this technology are on pause due to the high cost.

Researchers are investigating a biometric technology that can distinguish and measure body odor. This technology would use an odor-sensing instrument, an electronic "nose", to capture odor that is emitted through the skin's pores all over the body, which in return would make up a person's smell. However, distinguishing one individual's odor versus that of another may one day be a realistic, using this technology is currently very complex due to different variables that may take place such as the use of deodorants or perfumes. Different diets and medications can also influence the body odor emitted from a person and makes the development of this technology slow.

A popular route in today's market is combining multiple biometric measures into one device to ensure validity when taking a reading. Retica Systems, the only full-eye biometric technology company, is currently developing a handheld device that will compare both the retinal and iris to ensure that the individual being scanned is who they say they are.

Another technology currently in development is a vein scanning biometric technology that can automatically identify a person from the patterns of the blood vessels in the back of the hand. The technology uses near-infrared light to detect vein vessel patterns. Vein patterns are distinctive between twins and even between a person's left and right hand. Developed before birth, they are highly stable and robust, changing throughout one's life only in overall size. The technology is not intrusive, and works even if the hand is not clean.

The key distinction for biometric devices is a unique trait that can be measure. The exact composition of all the skin elements is distinctive to each person and makes it a prime

candidate for being a biometric measure. Skin has layers that differ in thickness and pigmentation differences that make each individual's measure unique. Skin pattern recognition technology measures the characteristic spectrum of an individual's skin. Current skin pattern recognition technologies use a light sensor to illuminate a small patch of skin with a near-infrared light. The light is then analyzed by a spectroscope and then a distinct optical pattern can be formed.

Privacy Issues:

With any new security measure, the issues of personal privacy and invasion arise. This is especially the case when it comes to biometric devices and their uses for identification. People fear that their biometric readings will link them to their personal data or allow them to be tracked, in a "Big Brother" type situation. A common question that appears when the topic of biometrics comes up in reference to privacy is if the government or some other group or person could get a hold of their personal information if they had access to the biometric system. The common misconception is that the readings that are taken during the enrollment phase do not actually hold any personal information, but it is the relationship between the image and the database that holds and relates the personal information. More common identification methods such as driver's license reveal much more information than a biometric measure, and are much easier to steal or counterfeit.

Survey and Data Results:

Listed in this section is a summary of the issues that were asked in the survey. The total numbered surveyed was 82 subjects. Subjects can be classified in these sets:

1. 53 subjects were between the ages of 18 and 39
2. 29 subjects were ages 40 and up.

1. 55 subjects were male.
2. 27 subjects were female.

1. 21 subjects were female and between the ages of 18 and 39.
2. 6 subjects were female and ages 40 and up.
3. 32 subjects were male and between the ages of 18 and 39.
4. 23 subjects were male and ages 40 and up.

The questionnaire revealed that most people prefer fingerprint readers over that of iris scanners and that although 60% of the people surveyed had heard of biometrics, only 21% of those surveyed had ever used a biometric device. The public does not feel that these devices provide complete security, but does provide a reliable means for identification.

When the issue of identity theft was asked in the survey, 67% of the women 40 and up and 61% of the men 40 and up felt that their identity was not secure. In comparison, 42% of the women 18 to 39 and 36% of the men 18 to 39 felt that their identity was not secure.

We also found that 53% of the women 18 to 39 and 45% of the men 18 to 39 view that the security of biometrics were secure. In comparison, 50% of the women 40 and up and 52% of the men 40 and up felt that biometric devices were secure.

When asked how likely they were to accept biometrics in day to day life, 57% of females 18 to 39 and 30% of the males 18 to 39 we willing to accept the usage of biometric devices. However, only 30% of females ages 40 and up and 48% of males 40 and up are willing to accept the usage of biometric devices into daily life.

Conclusion:

Though currently not widely accepted as a reliable and secure method of identification, biometric devices have made great advances in both reliability and price. This study provides very valuable insights into using inexpensive biometric devices for identity authentication and how the public view these devices. This research concludes that the fingerprint devices are preferred over the iris recognition device and the fingerprint devices were more reliable than the iris scanner that was used in this study. We can also see that people are also favorable to the idea of using biometric devices to verify their identity when making credit card purchases. The majority of the people surveyed were also likely to accept biometric usage into daily life. Using the data collected from the device testing, we ran a statistical analysis through SAS and found that Time and Device are statistically significant but the interaction between the two is not.

Hypothesis 1: Was confirmed without statistical analysis. The average number of times required to identify a person averaged less than 1.5 for all devices—which rounds to 1. Thus, it can be concluded that the biometric devices accurately identify people on average on the first attempt. Hypothesis 2: Using SAS 9.1 and an alpha of .05, we discovered that time was significant factor. Hypothesis 3: Using SAS 9.1 and an alpha of .05, there is a significant difference between the devices and age. Further, the interaction of gender and device was also significant.

The possibilities for biometrics being implemented into society are limitless and only a few issues were addressed in this study. One of the main issues that will always come up when it comes to personal identification will be privacy, and the general public will fear that their information will be obtainable by all. This study that determined the public does not feel that these devices provide complete security, but does provide a reliable means for identification. Although biometrics does not completely solve the problems of identity theft, fraud, and security, it is a good step in trying to deter those problems.

References:

- Jain, R. Bolle, and S. Pankanti, Eds., *Biometrics: Personal Identification in Networked Society*. Norwell, MA: Kluwer, 1999.
- Lawton, George. "Biometrics: A New Era in Security." *Computer* August 1998: 16-18.
- Lawton, George (1998, August). Biometrics: A new era in security. *Computer*, 31(8), 16-18. Retrieved February 1, 2006, from Research Library database.
- Souter, Colin. "Biometric System Performance and Security" 18 Oct. 2005 <http://www.bioscrypt.com/assets/bio_paper.pdf>
- Wayman J.L., Ed., "National Biometric Test Center Collected Works", August 2000. 18 Oct. 2005 <<http://www.engr.sjsu.edu/biometrics/nbtccw.pdf>>

Faculty comments:

Dr. David Douglas said of his student's work,

Brian Tran conducted research on the science of biometrics for identification and security purposes. His research provides examples of business costs of incorrect identity and security. Certainly, security has been a focal issue over the past few years.

After a broad background study on the field of biometrics, Brian focused on the availability of inexpensive biometric devices. Advances in technology have spawned a number of inexpensive devices. Two questions surface regarding these devices—are they reliable enough for general usage and will people be willing to use them?

Brian designed a repeated measures experiment, with corresponding hypotheses, to answer the first question. This experiment used three fingerprint readers and one iris reader—all inexpensive devices. Age and gender were also factors in the experiment. His well designed experiment provides a basis for evaluation of the devices in terms of accurate identification for security purposes. This part of the research is important because not only were the inexpensive devices found to be accurate but the design provides a basis for further research with additional factors such as race and with other devices as they appear in the marketplace.

Further, Brian developed a questionnaire to capture the subjects' acceptance of such devices for security reasons. This information is valuable in two ways—used a gauge of whether the devices will be acceptable at this point in time and as a reference point to determine if attitudes change over time.