https://doi.org/10.48009/2_iis_2011_116-122

BIOMETRICS IN NETWORKING: BALANCING IMPLEMENTATION WITH THE RIGHT TO PRIVACY

Kevin Lee Elder, Georgia Southern University, kelder@georgiasouthern.edu
Jaime Rodriguez, US Air Force

ABSTRACT

Have you ever forgotten your ATM PIN number? Or have you forgotten your password at work? How about the dozens of other passwords you need to check accounts on-line? In the not too distant future, we will be able to put away our card readers, discard all those credit cards and forget our passwords because biometrics, the identification and authentication of the real 'you' is here and it is here to stay. Since it will play an increasing role in the systems we use every day, we as IS educators need to include it more in our curriculums. If you search the IS 2010 Model Curriculum for IS programs you will only find Biometrics listed once, in an elective course [14]. *This paper will serve as a primer on biometrics to get IS educators thinking about how they can include it in their curriculum.*

Keywords: Biometrics, Networks, Privacy, Ethics, IS Curriculum

INTRODUCTION

Does Bob have authorized access to this network? Is Alice entitled access to this web site or sensitive information? The answer to these questions requires a combination of authorization and identification. Proper user identification is essential for reliable access control [6]. Traditional authentication systems are based on something a user has (a token such as an access card) or something a user knows (like a PIN or password). The problem with these authentication systems is that they do not actually identify the user as being who he claims [6]. For instance, an access card can be lost or a password can be posted on the monitor or under the keyboard. The individual that acquires the token or password can use it to gain access to the system or network. An existing alternative is to require something that the user "is". A third type of security authentication, biometrics, identifies the user for whom he claims to be. Unlike the previously mentioned methods, a biometrics is the most secure and convenient authentication tool since it cannot be borrowed, lost, forgotten, or stolen [3]. Along the benefits associated with the technology comes the cost of a loss of privacy. First, this paper defines what biometrics are, their applications, and describes various biometric systems and compares characteristics of several biometric systems. Next, this paper investigates balancing the implementation of biometrics in networks with right to privacy.

BACKGROUND

Since 9/11 there has been more interest to use biometrics to secure authentication in a networked society [9]. Biometrics are gaining increased attention as organizations are searching for more secure methods of network access, e-commerce, and other security applications [3]. Biometrics are "automated methods of authentication based on measurable human physiological or behavioral characteristics" [6]. Biometrics comes from the Greek words bios (life) and metrikos (measure) [8]. Unlike traditional authentication systems that rely on what you know or what you have, biometrics relies on who you are or what you do [8]. In order to recognize or authenticate a user's identity, biometrics measure the user's unique human physiological or behavioral characteristics [3]. Some common physical characteristics include fingerprints; hand or palm geometry; and retina, iris, or facial characteristics. Common behavioral characteristics include signature, voice, keystroke pattern, and gait. Technologies for voice and signature are the most developed in the behavioral class of biometrics [3]. Prabhakar suggests any physiological or behavioral characteristic can serve as a biometric characteristic as long as it meets these requirements [8]:

- Universality. Each individual should have the same characteristic.
- Distinctiveness. Any two individuals should be different in terms of characteristics.

- Permanence. The characteristic should be sufficiently in-variant over a period of time.
- Collectibility. The characteristic should be quantitatively measurable.

Biometrics are used for two main purposes: identity verification and recognition. These two uses will be further defined in the following section. In the past, the primary application of biometrics is for physical security in providing access to restricted locations [3]. Biometrics allows unmanned access control and are very useful for high volume access control [3]. In the past, biometric-base network and computer access was cost prohibited, and analyst saw virtual access as the application that will move biometrics for network and computer access from the "Sci-Fi" realm to real system components [3]. Prabhakar categorizes biometric applications into three main groups [8]:

- Commercial applications. These include computer network logins, electronic data security, e-commerce, internet access, ATMs, credit cards, physical access control, cellular phones, PDAs, medical records management, and distance learning.
- Government applications. These include national ID cards, correctional facilities, driver's licenses, social security, border control, passport control, and welfare-disbursement.
- Forensic applications. These include corpse identification, criminal investigation, terrorist identification, parenthood determination, and missing children.

Further discussion on these types of applications is left for another section of this paper. The next section defines and describes various biometric systems.

Biometric Systems

A biometric system is basically "a pattern recognition system that recognizes a person based on a feature vector derived from a specific physiological or behavioral characteristic that the person possesses" [8]. Biometric systems can operate in two modes, verification or identification, depending on the application context [8]. In identity verification, or one-to-one matching, the system compares the user's biometric data to the records in the system's database when a user claims to be enrolled in the system [6]. For example, Bob attempts to gain access into a system operating in this mode. He claims an identity and presents his login name, PIN, or smart card. The system checks Bob's record and performs a one-to one comparison to determine if it really is Bob. The system answers the question: Is this Bob? Identity verification is generally used to perform positive identification, where the goal is to prevent several people from using the same identity [8].

During identification, also called recognition, search, or one-to-many matching, the system compares the user's biometric data to all the records in the system's database to find a match since the user's identity is unknown [6]. For example, Alice is scanned by a system operating in this mode. The system performs a one-to-many comparison of the records in the system's database to determine her identity. The system may even fail if she was never enrolled into the system. The system answers the question: Who is this person? Identification or recognition is generally used to perform negative recognition, where the goal is to prevent a single person from using multiple identities [8]. Now that the modes of operation for biometric systems have been further defined and described, the next several sections describe various biometric systems in detail.

Fingerprints

The use of fingerprints is the oldest biometric-based method for identification and predates the invention of computer technology [9]. Fingerprint devices have the greatest variety and availability of all the biometric devices [3]. Despite the criminal stigma that accompanies it, as the cost of the device and processing drops, fingerprint recognition is gaining wider acceptance for user verification [3]. A fingerprint examines the patterns found on a fingertip. There are several approaches to fingerprint verification. Some mirror the traditional police method of matching details, others use pattern-matching devices, and others are a bit more distinct, using moiré fringe patterns and ultrasonics [3]. One advantage to some fingerprint verification devices is the ability to detect when a live finger is presented [3]. Fingerprint verification is a possible solution for situations where the system operates in a controlled environment and users can get sufficient explanation and training [3]. Due to low cost, size, and ease of integration, fingerprint authentication devices dominate the workstation access application area [3].

Facial Recognition

Facial recognition depends solely on the analysis of facial characteristics. The casino industry has utilized this biometric application to populate a facial database of scam artists for rapid detection by security personnel [3]. Since additional peripheral hardware is required for facial recognition, there is only a small market for network authentication. Dallas--Fort Worth and Palm Beach International Airports use facial recognition systems to check passengers against an FBI watch list [13].

Hand Geometry Recognition

Hand geometry involves the analysis and measurement of the shape of the user's hand. This biometric is easy to use and offers a descent balance of performance characteristics [3]. Hand geometry is a first choice for many biometric projects due to ease of integration and ease of use. The ability to adjust performance and configuration allows for a high degree of accuracy if required and allows usage for a wide range of applications [3]. A couple applications of this biometric include access to Scott AFB via the light rail system and the Immigration and Naturalization Service Passenger Accelerated Service System, a hand geometry based system (installed in major airports in the US and border crossings in Texas) had over 65,000 volunteers enrolled [17].

Iris Recognition

When it comes to biometrics involving the eyes, the iris recognition is considered more user friendly and less intrusive when compared to retinal scans. The previous use of a retina-based biometric involved the analysis of the layer of blood vessels located at the rear of the eyeball. Although an established technique and quite accurate, retinal scanning required users to look into a device emitting a light source and focus on a given point. Users wearing eye glasses or concerned with close contact with the scanning device do not warmly accept this form of biometric due to inconvenience and hygiene concerns.

Iris recognition focuses of the analysis of the features of the colored ring of tissue surrounding the pupil. Iris scanning is less intrusive than retinal scanning since it requires no close contact between the user and the scanning device. This biometric even works with eye glasses in place and is one of the few that works well in identification mode. The iris is unique to each individual, even in identical twins [10]. This uniqueness characteristic makes an iris scan a good candidate for high security requirements. Moreover, in the measurement of template-matching performance iris recognition has the potential for higher than average performance [3]. In a field trial pilot program (which ran for 6 months with over a thousand users) at the Nationwide Building Society, Swindon, England, survey results yielded the following: 91% prefer iris scanning to a PIN or signature, 94% would recommend iris scanning to friends or family, and 94% were comfortable or very comfortable with the technology [7].

Voice Recognition

Voice recognition is hampers by ambient noise during verification. Capturing this biometric appears to be more complicated and results in users perceiving that this biometric is less user friendly. A couple of applications of this biometric include: tele-banking and the Automated Permit Port (used after hours in small ports along the border of Canada), which uses voice verification to confirm identities of individuals crossing the border [17].

Signature Based Recognition

Signature based recognition involves the analysis of the way an individual signs his name. The final shape of the signature is only part of the way a person signs his name. Other features such as speed, velocity, and pressure are just as important as the final shape of the signature [3]. Signature verification shares an existing process that the other biometrics do not. Signatures are the accepted practice of the transaction-related identity verification process.

Most users can see a direct connection with extending this biometric to the verification process. The devices for signature verification are accurate and fit well into applications that accept signatures as a common identifier. Signature recognition rates high on ease of use and acceptability as a biometric. Signature recognition was selected over the iris scan for Nationwide Building Society. The selection of signature pads results in a project encompassing the UK's largest biometrics installation for public use [1].

COMPARISON OF BIOMETRIC SYSTEMS

In the preceding sections, various biometric systems were described. There is no single biometric that will cover all application contexts. In this section, a qualitative comparison of the various biometric systems covered will be presented.

For a practical biometric system, the issues of performance, acceptability, and circumvention must be considered [8]. Performance is measured by the speed, accuracy, and resources required of the system. Acceptability refers to acceptance by the intended population and the requirement that the system would be harmless to the user. Circumvention is addressed by a sufficient ability to thwart various fraudulent methods and attacks.

Table 1 displays the comparison of various biometric technologies as of the article release date of 2001. The table illustrates that no single biometric is an optimal solution in all categories. The retinal scan has the only low rating for ease of use for all biometrics listed. An item to note is that both the iris and retinal scan rate very high for accuracy as all other biometrics rate high for this characteristic. Looking at Table 1, it appears that the iris scan is the biometric to select for high security applications.

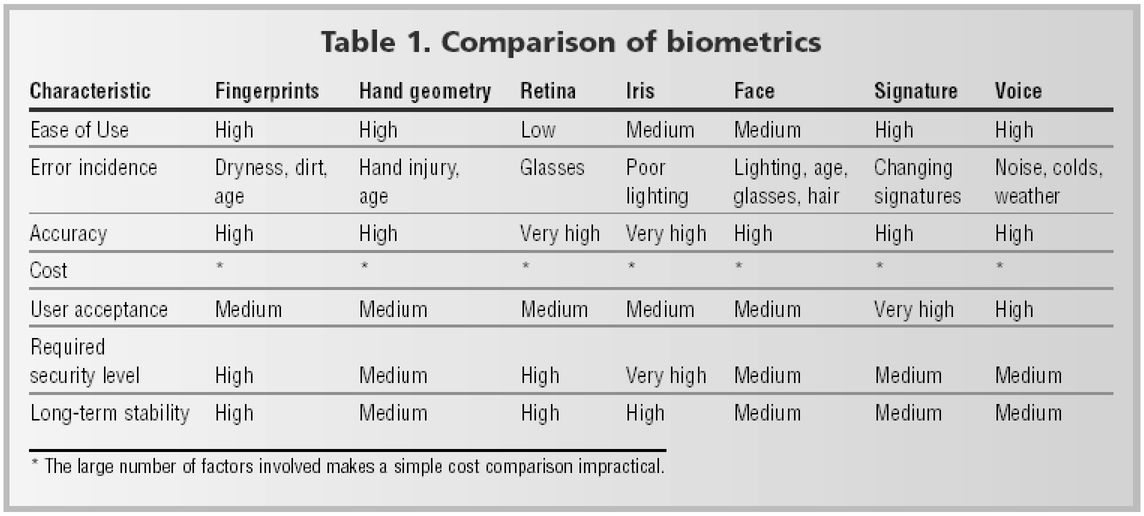


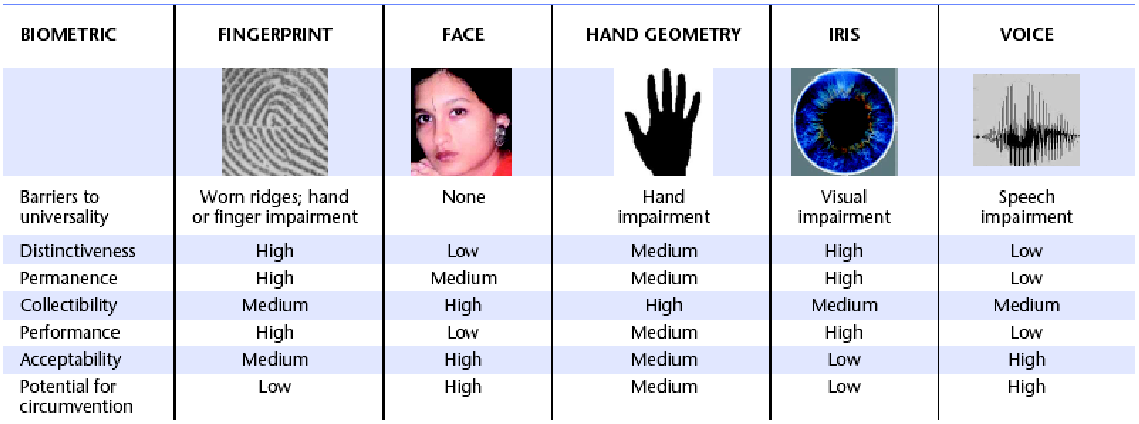
Table 1. Comparison of biometrics

Characteristic	Fingerprints	Hand geometry	Retina	Iris	Face	Signature	Voice
Ease of Use	High	High	Low	Medium	Medium	High	High
Error incidence	Dryness, dirt, age	Hand injury, age	Glasses	Poor lighting	Lighting, age, glasses, hair	Changing signatures	Noise, colds, weather
Accuracy	High	High	Very high	Very high	High	High	High
Cost	*	*	*	*	*	*	*
User acceptance	Medium	Medium	Medium	Medium	Medium	Very high	High
Required security level	High	Medium	High	Very high	Medium	Medium	Medium
Long-term stability	High	Medium	High	High	Medium	Medium	Medium

* The large number of factors involved makes a simple cost comparison impractical.

Table 2 displays the comparison of various biometric technologies as of the article release date of 2003. Similarly, to the previous table, this table illustrates that no single biometric is an optimal solution in all categories. The iris scan has the only low rating for acceptability. An item to note is that both the iris and fingerprint scan rate very similar to this particular author and would be selected for high security applications. Looking at Table 2, it appears hand geometry provides a mid-level biometric that would be selected for high volume applications.

Table 2



BIOMETRIC	FINGERPRINT	FACE	HAND GEOMETRY	IRIS	VOICE
Barriers to universality	Worn ridges; hand or finger impairment	None	Hand impairment	Visual impairment	Speech impairment
Distinctiveness	High	Low	Medium	High	Low
Permanence	High	Medium	Medium	High	Low
Collectibility	Medium	High	High	Medium	Medium
Performance	High	Low	Medium	High	Low
Acceptability	Medium	High	Medium	Low	High
Potential for circumvention	Low	High	Medium	Low	High

Balancing Privacy with Implementation

This section presents the issue of balancing the benefits of biometric technology with the cost of citizens losing a right to privacy. Prabhakar describes three classifications of biometric applications: commercial, government, and forensic [8]. Two types of commercial applications that have an impact on the right to privacy include e-commerce and medical records management. Developing commercial applications of biometrics raises new concerns over a right to privacy. Securing transactions involved in e-commerce and medical records management will provide an added level of security and authentication. The challenge occurs in developing the policies and establishing the legal framework needed to ensure individuals' rights to privacy. Industry will have to establish the acceptable practices for using biometrics and securing the biometric data for financial transactions and other commercial applications.

Several types of government applications that have an impact on the right to privacy include welfare-disbursement, correctional facilities, driver's licenses, and the DoD Common Access Card (CAC). The government uses biometric data for identification and verification purposes related to disbursement social welfare programs. The Lone Star card program is an example used in Texas [4]. Other applications for biometrics include authenticating the identity of prison inmates upon initial booking at correctional facilities [16]. Generally each state has a department of motor vehicles which issues a state drivers license. Most states require a fingerprint and a picture of the individual (facial pattern) prior to issuing a license. The common application the DoD members are familiar with deals with the CAC. The registration process for the CAC requires DoD employees to provide fingerprints and a facial pattern (picture). These collected biometrics are recorded and stored in some DoD data warehouse structure. Securing this information becomes paramount since it becomes the source information for authenticating an individual's identity. People expect a "reasonable use" of information gathered for an application. They expect the information collected for required business to be used for that application and not to be sold or disclosed to other organizations. The same expectation extends to an individual's biometric data. What prevents the DoD from sharing biometric data with other federal organizations? Incompatibility of the technologies used can be overcome. Finding a technical solution is the easy, but having the right business processes in place requires thought and the foundation of a legal structure.

The final application, forensics, involves actions taken to combat terrorist activities through the identification of known terrorists. In the post-9/11 environment, our focus has been on the prevention of further acts of terrorism against the citizens of the United States. The question becomes: How much individual freedom are we willing to surrender in order to achieve a level of comfort in the quest of identifying known terrorists? In testimony given to the subcommittee on government reform, John Woodward stated:

The clandestine capture of a person's face increases these fears [of establishing databases that track every civilian's move] because surveillance cameras can surreptitiously track individuals without their knowledge or permission. Moreover, the information from tracking can be combined with other personal data, acquired by other means, such as credit card or other consumer purchasing records, to provide even more insight into an individual's private life. [18].

The currently federated implementation of identification accepted through the use of driver's license could evolve into a quasi-national ID program. The United Nations has moved to incorporating biometric information into passports issued by individual nations [12]. If this nation does not quickly address the issue of using biometrics and the right to privacy, then perhaps other more global forces will have a hand in influencing future laws and policies.

SUMMARY

This paper defined what biometrics are, their applications, and described various biometric systems and compared characteristics of several biometric systems. Next, the paper investigated using biometrics in networks while balancing the right to privacy. One idea that was not prevalent in all the various articles (since the articles focus on one technology at a time) is the idea of a hierarchy of biometric technologies to provide better security [3]. Also along this line, would be coupling the biometric to a traditional authentication system [11]. For example, a smart card could be the token holder for a fingerprint biometric. This would allow for something you have, something you know, and something you are.

One issue that must be addressed is the need for a widely accepted technology standard that is adopted by the standards community. Efforts have taken place to accelerate an accepted international standard for biometrics to make them prevalent worldwide [5]. Another important issue is the development of the laws governing the legal use of biometrics with regard to the right of privacy. With a technology standard and the legal structure in place, the producers of biometric devices could work to integrate the unconnected systems that currently exist and provide a capability some would welcome and others would dread.

CONCLUSIONS

Biometrics are not going away. There are advantages and disadvantages to all forms, but the trend to use biometrics is on the rise. Many organizations will not stop at one biometric device. In the future, multiple authentications will be used. As technology develops, the use of these devices will become easier and less intrusive [2]. The Department of Defense has now organized an office called the Biometrics Management Office which is the focal point for all DoD biometric requirements.

Since biometrics will play an increasing role in the systems we use every day, we as IS educators need to include it more in our curriculums. These topics when presented and combined together as they are in this paper, could be incorporated into many of our courses, from Foundations of IS, Enterprise Architecture, IT Infrastructure, System Analysis and Design, IS Strategy, and more. Biometrics should not only be relegated to an elective course in strategy. Rather, it should be included as a security and ethics topic throughout our curriculums. It is our hope that this paper has helped IS educators in thinking about how they can include it in their curriculum.

REFERENCES

1. "E-Signatures Win Over Iris Scans," IEE Review, 49, 1:14 (January 2003).
2. Harazin Robert J., BIOMETRICS: ADVANTAGES AND APPLICATIONS. Security Technology & Design, September 2002.
3. Liu, Simon and Mark Silverman. "A Practical Guide to Biometric Security Technology," IEEE IT Pro, 3, 1:27-32 (January/February 2001).
4. Lone Star Image System Overview. Texas Department of Human Services. Accessed on March 1, 2004. Available at http://www.dhs.state.tx.us/providers/LoneStar/LSIS/
5. McMillan, Kate. "Technology Standard Pros Aid Homeland Security," IEEE Computer, 35, 5:104-105 (May 2002).
6. Matyas, Vaclav and Zdenek Riha. "Toward Reliable User Authentication Through Biometrics," IEEE Security & Privacy, 1, 3:45-49 (May/June 2003).

7. Negin, Michael, et.al. "An Iris Biometric System for Public and Personal Use," IEEE Computer, 33, 2:69-75 (February 2000).
8. Prabhakar, Salil, Sharath Pankanti, and Anil K. Jain. "Biometric Recognition: Security and Privacy Concerns," IEEE Security & Privacy, 1, 2:33-42 (March/April 2003).
9. Rahman, Mahfuzur and Prabir Bhattacharya. "Remote Access and Networked Appliance Control Using Biometrics Features," IEEE Transactions on Consumer Electronics, 49, 2:348-353 (May 2003).
10. Sanchez-Avila, C. and Raul Sanchez-Reilo. "Multiscale Analysis for Iris Biometrics," Proceedings of the 36th Annual 2002 International Carnahan Conference on Security Technology. 35-38 New York: IEEE Press, 2002.
11. Sanchez-Reilo, Raul. "Smart Card Information and Operations Using Biometrics," IEEE AES Systems Magazine, 6, 4:3-6 (April 2001).
12. Sinha, Vandana. "UN Group Decides Passports Will Include Facial Biometrics," Government Computer News (June 2003). Available at http://www.gcn.com/vol1_no1/daily-updates/22309-1.html
13. Titsworth, Tammie. "More Than Face Value: Airports and Multimedia Security," IEEE Multimedia, 9, 2:10-13 (April/June 2002).
14. Topi, Heiki, Joseph S. Valacich, Ryan T. Wright, Kate M. Kaiser, J.F. Nunamaker, Jr., Janice C. Sipior, and G.J. de Vreede. "IS 2010 Curriculum Guidelines for Undergraduate Degree Programs in Information Systems." Available at www.acm.org/education/.../IS%202010%20ACM%20final.pdf
15. Treasury Directive 87-05, Electronic Commerce Initiatives. Department of the Treasury. Accessed on March 1, 2004. Available at http://www.ustreas.gov/regs/td87-05.htm
16. Walsh, Trudy. "Florida Sheriff Adds Biometrics to Bookings," Government Computer News (December 2003). Available at http://www.gcn.com/vol1_no1/biometrics/24505-1.html
17. Wayman, James L. "Federal Biometric Technology Legislation," IEEE Computer, 33, 2:76-80 (February 2000).
18. Woodward, John D. Jr. "Privacy VS. Security: Electronic Surveillance in the Nation's Capital," Accessed on 1 March 2004. Available at http://www.dcwatch.com/issues/privacy09.htm