International Journal of Information Technology and Knowledge Management
January-June 2008, Volume 1, No. 1, pp. 155-161

BIOMETRICS FOR IDENTIFICATION AND AUTHENTICATION

Sukhdev Singh, Arun Jain & Jaipal

Abstract

In spite of numerous advantages of biometrics-based personal authentication systems over traditional security systems based on token or knowledge, they are vulnerable to attacks that can decrease their security considerably. Reliable person identification is an important problem in diverse businesses. Biometrics, identification based on distinctive personal traits, has the potential to become an irreplaceable part of any identification system. While successful in some place, the biometrics technology has not yet delivered its promise of foolproof automatic identification. For these reasons biometrics is used in crime with proud to investigation. This paper specifically addresses the use of biometrics for Identification and Authentication (ID&A). In the context of this paper "biometrics" is defined as "the automated means of recognizing a living person through the measurement of distinguishing physiological or behavioral traits". Choosing a biometric solution for a government application is often a daunting task. Faced with little reliable information about biometrics (vendors, products, and integrators), how do you go about making a sensible decision? The intent of this paper is to provide sound and practical advice for government managers trying to create a solid, biometric procurement proposal or operational requirement. The advice contained within this paper is intended to supplement, not replace, accepted project management best practices and methodologies.

Keywords: *Biometrics, Identification, verification, Authentication.*

1. Introduction

Since the beginning of civilization, identifying fellow human beings has been crucial to the fabric of human society. Consequently, person identification is an integral part of the infrastructure needed for diverse business sectors such as finance, health care, transportation, entertainment, law enforcement, security, access control, border control, government, and communication. These systems rely on the evidence of fingerprints, hand geometry, iris, retina, face, hand vein, facial thermo gram, signature, voice, etc. to either validate or determine an identity[1].

As our society[2] becomes electronically connected to form one big global community, it has become necessary to carry out reliable person identification often remotely and through automatic means. Biometrics, which refers to automatic identification of people based on their distinctive physiological (e.g., face, fingerprint, iris, retina, hand geometry) and behavioral (e.g., voice, gait) characteristics, should be

Figure 1: Establishing Identity

an essential component of any effective person identification solution because biometric identifiers cannot be shared, misplaced, and they intrinsically represent the individual's identity. The aims of this paper are:

- To identify the issues to be addressed before a biometric based ID&A system is introduced;
- To identify the implementation issues to be addressed after a biometric based ID&A system is chosen;
- To provide advice on how to specify and choose a biometric based ID&A system;
- To define some of the common terms used in biometrics;
- To provide references to other reading matter and user groups.

1.1 User Privacy Concerns

The collection[3] of biometric information may be the subject of privacy concerns among the target audience. Certain biometrics engender a greater perception of privacy invasion among the public than others. Also, what legal requirements must be satisfied governing the collection and storage of the information?

1.2 User Perception

Public perception, which may correspond to the degree of a particular device's intrusiveness, can severely impact user acceptance of certain biometrics. For example, while retinal scanning devices (ones which use infrared technology to look at the pattern of blood vessels at the back of the eye) may claim greater accuracy than other biometrics, the perceived invasiveness of the capture device has, in the past, resulted in public reluctance to routinely use this biometric.

1.3 User Difficulties

Some populations have difficulty using certain biometric capture devices. Difficulties may be encountered with the degree of alignment necessary in the feature capturing

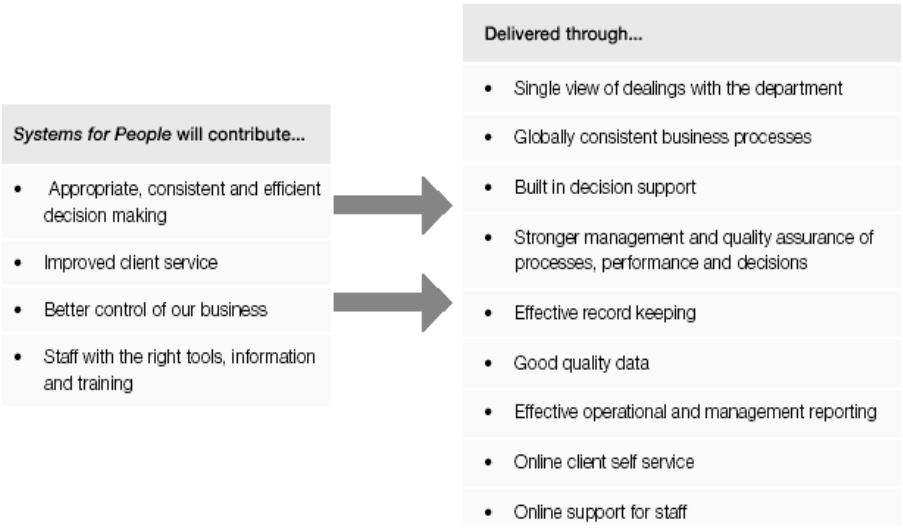

Figure 2: Benefits of System for People

process or with certain inherent characteristics of a given target population (e.g. the elderly tend to have very dry skin, which can make adequate contact with certain types of fingerprint capture devices difficult). Disabilities within your user population must be taken into account (height of the device for wheelchair users, inability to provide a sufficiently admissible biometric feature, etc.).

1.4 Ease of Use

The acquisition method for the user's biometric feature, problems with the user authentication process, and/or speed of a product can greatly influence user acceptance. Less intrusive, procedurally quick biometric systems are more likely to be successful.

2. RELATED WORK

Numerous media reports over the past couple of years have highlighted recent U.S. and Canadian efforts to strengthen border security[4]. These efforts have involved the implementation of numerous new initiatives under an overarching bi-lateral agreement known as the Smart Border declaration[5], central to the Smart Border agreement is the use of biometric identifiers. The implementation timetable for these programs was considerably accelerated in the days following the September 11, 2001 terrorist attacks. Various biometric systems have been in use by different agencies across the world for several years now. The largest system coupled to a database is the FBI's Automatic Fingerprint Identification System (AFIS) which has been operating for over 30 years[7]. While automated, AFIS is not similar to systems proposed for border control in that

matches are generally confirmed by manual human inspection. Systems for border control would ideally operate with minimal human inspection. That being said, a number of small automated systems are in operation. Among others, the U.S. Defense Department has used biometric fingerprint identification for access to military bases in South Korea[8] and, since 2002, the U.S. Immigration and Naturalization Service (INS) has been using a hand geometry system on a very limited basis to reduce inspection times for trusted travelers at seven U.S. and two Canadian airports[9]. As well, Canada is running programs such as CANPASS (Canadian Passenger Accelerated Service System) at a number of airports and other points-of entry (POE). Many European Union members also have biometric authentication and identification systems operational at various POE.

3. TECHNICAL ISSUES FOR IDENTIFICATION & AUTHENTICATION

The biometric feature selected as the identifier for your users must be an accurate, relatively unalterable, distinguishing, physical or behavioral characteristic that can be captured, recognized, and authenticated over an indefinite (but certainly not infinite, due to the inevitable changes that occur through ageing, illness, or injury) period of time.

Furthermore, the method of capturing the biometric identifying feature should be unobtrusive to the user. The method selected must be socially acceptable and must not endanger the health, safety, or welfare of any user. The system has to be simple to use. Use of the system must be easily understood by the employees administering the system and must be simple to explain to the users. Departments should contemplate the following product considerations when selecting a biometric:

3.1 Template Storage

The size of each template (i.e. the information recorded representing a user's biometric features) may be a factor when selecting a particular biometric product for your application. In choosing a biometric solution, you need to consider the template size and whether multiple templates per user will be required. Several different templates may be needed from each user (e.g. multiple fingers, eyes, face plus voice, etc.) to achieve necessary levels of System accuracy/security and to account for the accidental unavailability of a user's biometric feature.

The amount of storage needed for these multiple templates may influence the viability of card storage and/or your computer processing capabilities. For example, if you choose to provide your users with a smartcard as a means of storing their biometric templates, many (but not all) biometric systems offer templates small enough to reside on a smartcard. You must be aware of the current, maximum capacity for the storage of

your users' templates on whatever medium you choose (smartcards, magnetic stripe cards, various barcode technologies: 1D, 2D, and 3D; computer memory, etc.), as well as its processing power/capabilities and compatibility with the hardware involved. Security and protection of the template data is also an issue (does the level of risk or the need to protect privacy in your application warrant the encryption of templates and/or the transmission of data?). How will your solution provide for this?

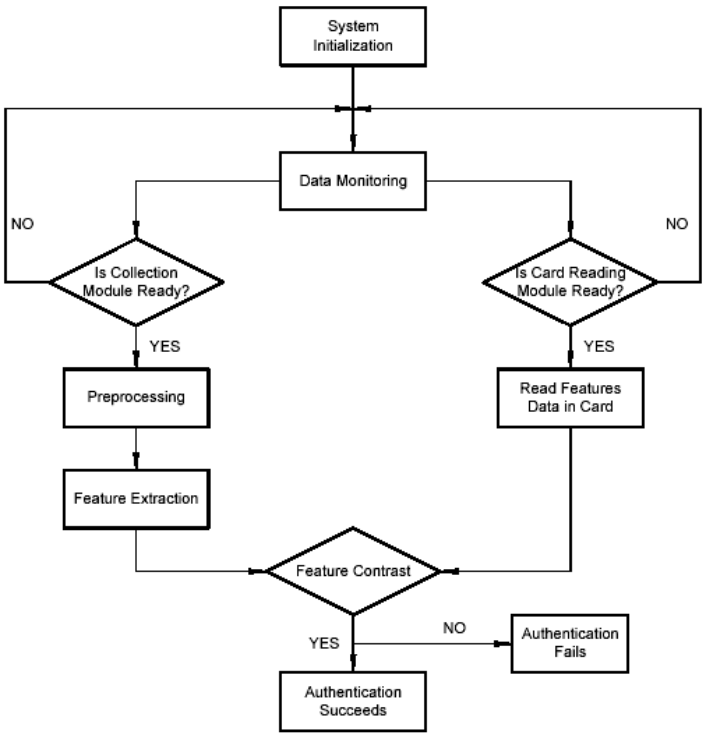

Figure 3: Authentication of Card Module by System

3.2 User Population

It is important to consider the number of users who may be prevented from using a particular biometric type (due to disability, cultural considerations, health conditions, etc.). If a large part of your user population might be precluded from using a particular biometric type, then it would be wise to choose a biometric that is more appropriate for the vast majority of your users. You cannot expect to find a single biometric that will be accessible for all of your users, all of the time. For example, user populations that contain large numbers of people that work hard with their hands (who may have more difficulty using a fingerprint device due to worn or dirty fingers) may want to choose something more suitable, such as facial recognition. Cultures with an aversion to touching public surfaces would prefer to use biometric solutions that are 'hands free'.

Are there any items of clothing or accessories (safety masks, gloves), worn by the majority of your user population, that would make a particular biometric inappropriate for use in your application? On the other hand, certain biometrics may prove to be advantageous to users having difficulty utilizing traditional access control measures (e.g. workers who are carrying things would appreciate using a voice system to gain access to a secured room, rather than having to manipulate a combination lock). It really pays to know your user population.

3.3 Computer Resources

The complexity of the algorithms used in matching the users to their enrolled templates may vary from product to product. Therefore the amount of computer processing power required will differ. In applications that do not require massive throughput and do not have enormous user populations, you are more likely to consider biometrics that perform reasonably well, using a workstation with a moderately priced processor, than those that require more expensive platforms.

3.4 Maintenance

All biometric devices will require some form of maintenance. The frequency and intrusiveness of periodic adjustments (possibly due to factors in the operating environment such as lighting, background noise, dirt/grime, weather, etc.) must be taken into consideration in order to ensure correct acquisition of the biometric data.

CONCLUSION

This paper has examined only a fraction of the controversies and possibilities surrounding the biometric border security system being implemented by the U.S. and Canada. There are serious issues that need to be addressed rationally and thoughtfully by citizens, government, and academics that are beyond the limited scope of this paper. Perhaps one of the most important issues is the potential economic impacts of such programs. It has been postulated that effects on travel and tourism could be heavy. In fact, Statistics Canada has already cited border security delays as a real factor hampering cross-border trade. Other issues touched on but not deeply explored in this paper include privacy rights, misidentification issues, control of database information and database security. Until such a time that these issues and technological challenges are overcome, biometrics, while useful for many applications, will not be an effective antiterrorist tool.

REFERENCE

[1] Jain A. K., Ross A., and Prabhakar, S., (2004), An Introduction to Biometric Recognition. *IEEE Trans. on Circuits and Systems for Video Technology*, **14**, 4-20.

[2] *http://www.biometricgroup.com/index.html*

[3] *www.cesg.gov.uk/technology/biometrics*

[4] For example: "Bio-security Still a Fantasy: Airport Screening Won't Work." The Toronto Star, 24 January 2004. *www.thestar.com*, Paul Knox, The Globe and Mail. Toronto. 7 February 2004. p. A10., "U.S. Passport Plan Draws Fire," The Globe and Mail: Toronto. 6 October 2005, p. A16., and "Prime Minister Inaugurates New Border Facilities in Beauce Region," *http://www.newswire.ca/en/releases/archive/October2005/14/c1180.html*

[5] The Complete Smart Border Declaration is Available at: *http://www.dfait-maeci.gc.ca/antiterrorism/actionplan-en.asp*. Status Updates are Available at: *http://www.dfaitmaeci.gc.ca/world/site/includes/print.asp?lang=en&print=1&*

[6] For a Proper Grasp of the Program See Nancy Kingsbury, (2002), Technology Assessment: Using Biometrics for Border Security. United States General Accounting Office (USGAO), Report #GAO-03-174, November 2002. *http://www.gao.gov/new.items/d03174.pdf*. For the Attendant Risks Brought About by the Scale of the Program: Randolph C. Hite, Homeland Security: Risks Facing Key Border and Transportation Security Program Need to Be Addressed. Washington D.C.: U.S. General Accounting Office, Report GAO-04- 569T. *http://www.gao.gov/new.items/d04569t.pdf*

[7] Jain A. K., *et al.*, (2005), "Biometrics: A Grand Challenge," Proceedings of International Conference on Pattern Recognition, Cambridge, U.K., August 2004. *http://biometrics.cse.msu.edu/biometricsgrandchallenge.pdf*, 2. Accessed.

[8] Walker, and Richard, (2003), "Security: Biometrics Gains a Foothold." *http://www.gcn.com/cgibin/udt/im.display* (Post-Newsweek Media Inc.)

[9] Kingsbury, (2003), 4.

Sukhdev Singh[1] & Arun Jain[2]
Deptt. of I. T, H. C. T. M, Kaithal, Haryana, INDIA
E-mails: Sukhdev_kuk@rediffmail.com[1]: *erarunjain@rediffmail.com*[2]

Jaipal
University Institute of Instrumentation Engineering, K. U. Kurukshetra
E-mail: sarohajp@yahoo.com