Information Technology Security Report
Lead Agency Publication R2-001

Biometric Technologies: An Assessment of Practical Applications

Technical Security Branch
Technical Operations
Royal Canadian Mounted Police
Issued: June 2002

TABLE OF CONTENTS

1 Project Specifications

1.1 Project Objectives

i. To investigate the current state of the biometric device industry.
ii. To evaluate promising biometric solutions for a desktop-network interface.
iii. To recommend either implementation of a biometric solution or further investigation.

1.2 Project Members

The Biometrics Project was a joint undertaking by the Technical Security Branch and the Departmental Security Branch of the Royal Canadian Mounted Police (RCMP). These branches were represented by Heather Riou and Jennifer Mulligan respectively. Portions of the Joint Biometrics Project were contracted to Ian Summerell.

1.3 Project Activities

During the course of this Biometrics Project, the state of the biometrics marketplace was investigated extensively. A variety of information is available from vendors, distributors, resellers, academic groups, industry associations, government sources, and the Internet. Some excellent books dealing with biometrics have been recently published. Meetings were conducted with vendors, distributors and resellers. Heather Riou and Jennifer Mulligan attended an industry conference titled "Successful Application of Biometric Technologies". In-house technology evaluations were carried out to determine the suitability of certain promising biometric solutions for logical computer access from the desktop.

2 Acknowledgement

The Technical Security Branch and the Departmental Security Branch of the RCMP would like to acknowledge the Canadian Police Research Centre (CPRC) for their generous financial contribution and assistance in this biometric research project.

3 Biometrics Introduction

3.1 What is Biometrics?

Biometrics has been defined in many ways. In this report, the definition borrowed from the Police Information Technology Organization (PITO) will be used: "[Biometrics is] the automated identification or verification of a human identity through measurable physiological or behavioural traits."[1]

3.2 Uses of Biometrics

The purpose of biometrics is to use computer technology to identify or verify the identity of an individual and subsequently enable the appropriate privileges assigned to that individual. Many other uses of biometrics have been developed, and applications exist whenever an automated identification or identity verification is useful. Some established solutions include punch-clock replacement, enrolment for social benefits and surveillance for criminals. Commonly, biometric authentication is used to control access privileges; these fall into two groups: physical access and logical access.

Physical Access

A biometric system controls a lock on a door. A process that uses biometrics to establish a user's identity is used to open the lock. For example, a user places his thumb on a scanner that collects a thumbprint, and if the biometric system identifies the individual as an authorized user, the lock opens and permits entry through a door.

Logical Access

A biometric system controls the use of a computer system or computer network. A process that uses biometrics to establish a user's identity is used to permit access to the computer system or network. For example, a user places his thumb on a scanner that collects a thumbprint, and if the biometric system identifies the individual as an authorized user, the computer system or network becomes available to the user.

4 Automated Authentication Techniques

Automated authentication procedures consist of one of the following techniques or a combination of the following techniques.

4.1 Passwords

Passwords are often explained as "something the user knows", and they are the *de facto* standard for automated authentication. They are very common in computer systems and most users are very comfortable with them. Passwords have some major weaknesses in that they can be easily shared, forgotten or stolen. Often, the legitimate password user is unaware that the password is no longer secure. Most users write down passwords for future reference, and this written record is easily compromised since it is rarely afforded proper security. In fact, many users keep their computer access passwords on small notes within easy reach of the keyboard. Despite these shortcomings, it should be noted that passwords are used daily by millions of users with acceptable results. In a post-9/11 survey of government managers, 96 percent said their agency's password policies were generally effective[2].

4.2 Tokens

Tokens are often explained as "something the user has". Tokens are small, portable devices that carry information about a user. Two examples of well-established tokens from the financial industry are credit cards and bank cards, both of which carry information on a magnetic strip mounted on a plastic card. More advanced examples of tokens are smart cards and USB tokens which both have integrated computer chips that contain several kilobytes of memory and sometimes have processing capabilities. Smart cards are about the same size and shape as a standard credit card and require a special reader to interface with another computer system. USB tokens are generally about the size of a large pen cap and can interface with another computer system through a standard USB connection.

In a mechanical lock system a key opens a set of locks and the individual who has possession of the key can access any place that is secured with one of these locks. Similarly, in a token system, privileges and rights are assigned to a token and the user who has possession of the token is given all of these privileges and rights. Like passwords, tokens can be shared, lost or stolen.

4.3 Biometrics

Biometrics is often explained as "something the user is". The technology involves the measurement and computer evaluation of part of a user's body to identify the user. The most common types of biometric technologies are fingerprint scans, iris scans and face scans. The evaluation of a biometric scan is challenging because a person's body changes naturally over time, which leads to different images being captured at each biometric scan. The systems that evaluate the biometric scans must be able to accommodate these natural changes, while still reliably detecting an impostor. Compared to passwords or tokens, biometrics may provide poorer technical reliability due to the natural variability of a person's body, but may give better overall reliability since a person's physical characteristics cannot be borrowed or stolen like a password or token. Biometrics is a younger technology than passwords or tokens, and

issues like performance over time have not been fully addressed. Although biometrics cannot be shared or stolen they may be "lost" due to injury. For example, an injured finger may not be useable to authenticate to a fingerprint scanning biometric system. These problems can be minimized with proper policies, for example, requiring the enrolment of at least one finger from each hand.

5 Biometrics Industry Jargon

5.1 Template

Biometric systems generally do not directly compare visual images of a person's characteristics. Instead, the visual images are processed to make them more suitable for computerized comparison and to minimize storage size. Generally, an image cannot be recreated from the template that is developed from it. Fingerprint templates are created according to proprietary algorithms developed by each vendor, but the process is similar for all:

1) An image of the fingerprint is captured.
2) The image is processed to clearly resolve the image into ridges and valleys.
3) The ridge pattern is assessed to find irregularities in the pattern, known as minutiae. Some common examples of minutiae are known as crossovers, cores, bifurcations, ridge endings, islands and deltas.
4) The relative locations of the minutiae are measured, resulting in a pattern known as a "minutia graph" that forms the basis of the fingerprint template.

A visual example of a Fingerprint Processing Algorithm is shown in Figure 1.

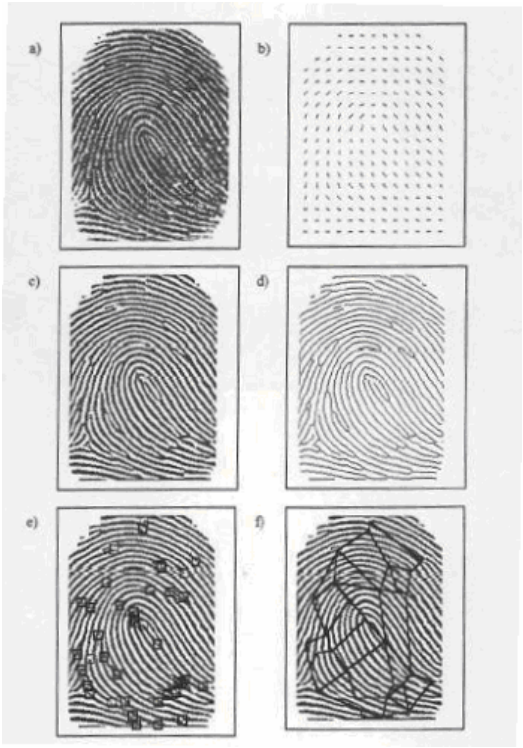

Figure 1. Sequence of Fingerprint Processing Steps

Figure 1. Sequence of Fingerprint Processing Steps: a) original, b) orientation, c) bi-narized, d) thinned, e) minutiae, f) minutia graph

[Reprinted with permission from "Biometrics: Personal Identification in Networked Society" by Jain, Bolle, Pankanti]

5.2 Enrolment Template

This is the template that is produced when a new user is enrolled in the system. This enrolment template is stored and used as the authentic version for subsequent comparisons. The enrolment template should be of a high quality since it is used as a standard. Because it forms the standard of automated biometric authentication, it is critical that the correct enrolment template is collected from a new user at enrolment time. If the template of an impostor is enrolled, the biometric system will continue to allow the impostor access until the identity is suspended. Because of this, user enrolment is a critical time for maintaining the security of a biometric access system, and definite positive identification of a new user must be established before the new user can be allowed to create an enrolment template.

5.3 Authentication Template

An authentication template is created each time a user attempts to authenticate with a biometric device. Unlike enrolment templates, authentication templates are not permanently stored. In the authentication process, the user's biometric characteristics are scanned to produce an image, and then the image is processed to produce an authentication template. The authentication template is compared against the enrolment template to determine if it is an adequately close match to permit identification or verification.

5.4 Identification

Identification is the use of a biometric to completely identify an individual. Identification systems are often known as "1:N" systems since a match is made by comparing one authentication template (1) against a large number of enrolled templates (N). In an identification biometric system, a sample of the user's biometric characteristic is taken (e.g. a fingerprint scan) and an authentication template is created from it and compared against a library of enrolment templates. If a match is found between the user's authentication template and an enrolment template, the user is awarded the privileges (e.g. social assistance) associated with the identity linked to the enrolment template. If a match is not found, the user is assessed to be invalid and privileges are not awarded.

Identification systems are implemented in situations where users must not be enrolled more than once. Before each enrolment, the user's biometric template must be compared against all templates in the library to ensure that the user is not already enrolled. For example, a recipient of social services may attempt to register under several names to receive multiple payments, but an identification system would check the user's biometric template against the entire enrolled library and would not allow multiple enrolments. Identification systems require large amounts of input information to check against large libraries and they are relatively slow. Identification can take several minutes, hours or days, depending on the size of the enrolled template library and the degree of required accuracy. The enrolment procedure for an identification biometric system must be closely supervised to prevent the submission of bad scans. Enrolment templates for identification must contain a lot of information in order to reliably match a particular authentication template against a very large number (perhaps tens of millions) of stored enrolment templates. In a fingerprint-based identification biometric system, the enrolment template usually consists of several fingerprints. Large-scale identification is beyond the reasonable abilities of the biometric solutions discussed in this report.

5.5 Verification

Verification is the use of a biometric to confirm an identity that has been claimed by an individual. Verification systems are often known as "1:1" systems since a match is made by comparing one authentication template against one enrolment template. Verification is technically much easier than

identification. In a verification biometric system, users first identify themselves in some fashion to the system. The identification method need not be highly secure, and often consists of a password, user name or a token. This allows the verification system to locate the enrolment template of the user. The user is then subjected to a biometric test (e.g. a fingerprint scan) and the resulting authentication template is compared against the enrolment template. If the two templates are assessed to match, the user is awarded the privileges (e.g. access to a network) associated with the identity linked with the enrolment template. If the two templates are not assessed to match the user is denied the privileges. Verification is a suitable method of user authentication in situations where the user is cooperative and wants the system to work. Generally, verification authentication is suitable for logical access problems and physical access problems. Compared to an automated identification solution, automated verification requires less storage space, processing power and time to return a decision. Verification solutions can also be implemented without a central enrolment template library. Since the system needs access only to the particular user's enrolment template, and not all users' enrolment templates, the solution can be implemented without storing all the templates together.

6 How Biometric Access Systems Work

A considerably wide variety of technologies can be described as biometric access systems, and they all work along the same principles. Their purpose is to deny access to a target (usually a room or a computer network) for individuals who have not been specifically authorized access, while permitting easy access to individuals who have the proper permissions. Their operating procedures are as follows.

6.1 Enrolment

A biometric access system must have access to a record of the biometric characteristic that will be used for access. This record is created during an initial enrolment routine when the user's biometric characteristic is sampled and the enrolment template is created and stored. It is critical that the user's true identity and true set of privileges be established when the user is enrolled, since all subsequent automated testing of this identity and these privileges will simply reference the enrolment information.

6.2 Enrolment Template Storage

The enrolment template must be stored so that it is available for future comparisons. The way it is stored can vary depending on the architecture of the biometric system. An identification system must search all enrolment templates therefore they must all be stored in a central directory. A verification system only needs access to the enrolment template of the claimed identity, therefore the enrolment templates may be stored in a central directory or they may be stored on a transportable medium assigned to the user, namely, a token.

6.3 Access Attempt

After enrolment, a user has access privileges to a protected resource. On each access attempt, the enrolled user submits to the gathering of a biometric sample (e.g. a fingerprint scan). This sample is processed to produce an authentication template. In a verification system, the user provides identification such as a username, a password or some other verifiable tag that is used to locate the enrolment template associated with the identity. In an identification system, the authentication template itself is used to search the directory of all enrolment templates.

6.4 Awarding Privileges

The authentication template is compared to the enrolment template to determine if they are "close enough" to be considered a match. Note that the authentication template will never be identical to the enrolment template since every biometric sample that is gathered will be slightly different, so the template

that is created from it have a slight difference. A computer algorithm that looks for similarities between the templates decides whether the templates are "close enough" to be a match. Usually, the system administrator can use a security setting to control the number of template similarities required for a match.

If the templates fail to match access privileges are not awarded. Often, a record of the failed access attempt is kept in a log that can be reviewed by the system administrator. Failing to match templates does not necessarily indicate a malicious intrusion attempt. Often it simply means that the biometric sample that was taken to create the authentication template was of poor quality.

Access privileges are awarded if the templates match. The nature of these privileges varies with the design of the system. For a physical access system, the awarded privilege is usually an electric signal to unlock a door. For a logical access system, the awarded privilege is usually the release of a stored, encrypted password to gain access to an application.

6.5 Biometric as a Replacement for Logical Access Passwords

The distinction between password release and password replacement is important for anyone developing policy or specifications for biometric access systems. There is a common perception that using a biometric system replaces passwords - and from the user's perspective it does. Technically, using a biometric usually does not replace a password but it facilitates the use of passwords and improves the security of using passwords. In most cases, when a biometric system grants a logical access privilege, a stored and encrypted password is released and used in place of a user-entered password. Security is increased because the stored, encrypted password can be longer and more complex than would be practical for a user-entered password, and because it is stored in encrypted form instead of being stored as text as many users do. Some systems actually create the password and change it every time it is used without any additional user involvement. The practice of password release instead of true password replacement is necessary to make biometric access systems compatible with the wide range of applications that have been designed to use passwords.

In all cases, the authentication template cannot technically be used directly as a "key" since each new authentication template will be somewhat different from the enrolment template on file, due to variations in collection of the image and natural variations in the user's physical body. The system must always compare the authentication template and the enrolment template to determine if they are close enough to be considered a match. The condition of finding a match is equivalent to having a key.

7 State of the Biometric Industry

As of the spring of 2002, biometric solutions have not made the leap to broad usage. Current early adopters tend to be government agencies, the military and very large companies. The research behind biometrics is fairly well established, but the practical implementation of solutions has not yet found firm direction from the marketplace. The set of vendors is fairly fragmented and consists mostly of small companies specializing in biometric solutions for particular problems. Very recently there have been some significant mergers, acquisitions and agreements among biometric vendors and these surely indicate the direction of the industry towards larger, more stable companies with a wider range of products. For example, the following are recent mergers:

- Identix (Nasdaq: IDNX) and Visionics (Nasdaq: VSNX) announced a merger on February 22, 2002. Identix is arguably the leading vendor of fingerprint-based biometric systems and Visionics is a leader in face-recognition and fingerprint biometrics.

- Ankari, a leading Canadian company specializing in fingerprint biometrics, was acquired by ActivCard (Nasdaq: ACTI), a leading provider of smart cards and digital identity provisioning products, as announced on November 14, 2001.

8 Standards for Biometric Devices

The proliferation of biometric devices and solutions has been hampered somewhat by the lack of universal standards. Manufactures of biometric devices and middleware typically develop their own proprietary designs and there is little or no interoperability among them. Some middleware developers make efforts to support a range of third-party hardware devices while others support only their own hardware devices. Progress has been made in the development of standards for biometric devices, but there are two competing standards and each has a strong foothold. Currently it is not clear which direction the biometric industry will take. One of the reasons that end-users are leery of committing to a particular biometric solution is the concern that it may become obsolete and unsupported if the biometric industry moves in another direction.

8.1 BioAPI

A standard for biometric device interoperability known as "BioAPI Specification, version 1.1", was approved and published as an American National Standard, designated as ANSI/INCITS 358 in March 2002. Biometric devices that are designed to the BioAPI specification will work with any Microsoft Windows operating system (except Windows CE), and future devices will be supported in Unix, Linux, Mac OS, and Java-based systems[3]. Having a recognized standard will likely encourage manufacturers to develop products that are compliant with the standard, and this will eventually lead to interoperability within the industry. As of May, 2002, there are eight manufacturers that claim to offer products compliant with the BioAPI standard[4].

8.2 BAPI

Microsoft was an early supporter of the BioAPI initiative, but withdrew before the specification was finished. Microsoft intends to incorporate support for biometric devices directly into future versions of their Windows operating system. They have acquired I/O software's BAPI (Biometric Application Program Interface) technology and SecureSuite biometric data management software for this purpose. It should be noted that BAPI is different from the BioAPI specification. Microsoft has indicated that it would be feasible to map functions between BioAPI and BAPI, effectively supporting BioAPI-compliant devices through a BAPI interface. Because of Microsoft's very strong presence in the desktop operating system and software market, many industry observers feel that BAPI may eventually become the *de facto* standard for biometric device interoperability, despite BioAPI's official designation. In April of 2002, there were fourteen manufacturers developing products for the BAPI standard.

9 Currently Available Commercial Biometric Technologies

9.1 Fingerprint Scan

Fingerprint scanning is currently the most popular biometric technology, representing about 85% of the current systems, and this percentage is projected to increase in the coming years. It is the most mature, most highly developed and most tested type of biometric technology.

Fingerprint Scan Strengths	Fingerprint Scan Weaknesses
• Mature, proven technology • Capable of high accuracy • Deployable in a range of environments • Ergonomic, easy-to-use devices • Ability to enrol multiple fingerprints to increase accuracy and reliability	• Unable to enrol a small percentage of users • Performance can deteriorate over time • Psychological association with criminal investigation

Figure 2. Strengths and weaknesses of fingerprint scanning biometrics[5]

Fingerprint scanning systems consist of a fingerprint scanner and the software that controls the system. The fingerprint scanners fall into two main categories: optical scanners and chip-based capacitive scanners. Optical scanners consist of a small digital camera that takes a picture of a fingerprint that is pressed against a glass surface. Chip-based capacitive scanners consist of a flat silicon chip that measures the relative capacitance of the areas of a finger that pressed against it. This matrix of relative capacitances forms an image of the fingerprint based on the degree of contact the fingerprint ridges have with the silicon chip surface. Optical scanners tend to provide a larger and better quality fingerprint image but they are usually larger than capacitive scanners. Chip-based scanners generally have a small surface reading area and show a smaller portion of a fingerprint. Chip-based scanning is a newer technology that is popular with manufacturers because of decreased cost and a better-perceived resistance to spoofing. Limited spoofing tests performed for this report, however, showed a chip-based scanner to be more susceptible to spoofing than two tested optical scanners.

Reports of successful fingerprint-spoofing techniques have been presented in conferences and on the Internet. Some testing done to confirm these techniques has revealed some susceptibility to spoofing. This testing is described elsewhere in this report. In light of these techniques, fingerprint biometrics cannot be considered adequately secure unless they are combined with another automated authentication method such as a password or a token.

9.2 Automated Fingerprint Identification Systems (AFIS)

Automated fingerprint identification systems (AFISs) fall outside the area of interest of this report. AFIS is mentioned only to highlight that the fingerprint scanning technologies discussed elsewhere in this report are not the same as those used for criminal proceedings.

AFIS technology is used by law-enforcement agencies to perform large-scale identification of a fingerprint against a database of registered fingerprint images (not fingerprint templates). The result is usually a small list of potential matches that must be individually checked by a fingerprint-matching expert. The results are often used for criminal investigations, for background checks, and for registration for public services (welfare) in some jurisdictions.

9.3 Facial Scan

Facial scanning biometric systems are interesting because they can be used at a distance without the subject's cooperation. Currently, there are initiatives to use facial scanning systems in airports to detect terrorists before they can board an airplane. Facial scanning technology is also advancing for the management of criminal mug shots. The software works by identifying points on a subject's face such as the corners of the eyes, tip of the nose, cheek bones, etc. The relative locations of these points and the distances between them are used to create a template of the subject's face that can be compared against templates that have already been enrolled. The technology is generally not as accurate as other biometric technologies, but the developers claim that common disguises like hats, facial hair, or eyeglasses cannot

fool it. The technology requires proper lighting of the subjects and works best when a full frontal image of the subject's face is submitted for analysis.

Facial Scan Strengths	Facial Scan Weaknesses
• Can leverage existing image acquisition equipment • Can search against static images, like driver's licence photographs • Only commercially-available biometric technique that can operate without the subject's cooperation	• Changes in the image acquisition environment (mostly lighting and camera angle) can affect matching accuracy • Changes in physiological appearance can fool the system • Strong privacy concerns because of it's non-cooperative enrolment and identification capabilities

Figure 3. Strengths and weaknesses of facial scanning biometrics[6]

Recent testing in real U.S. airports has shown successful target identification rates of about 50% and fairly high false identification rates. Security advocates declare that this is a success, and that this means that half of the terrorists who would have otherwise evaded security would be detected. Privacy advocates declare this a terrible failure and that it presents an unacceptable privacy intrusion given that almost half of the suspected terrorists would still evade security. The developers of the technology claim that the success rate can be improved substantially, perhaps to 80% or 90%, with optimum lighting and camera placement. A subject that is identified by the facial scanning system would receive extra attention from the airport's security personnel but would not automatically be arrested or detained.

9.4 Iris Scan

Iris scanning is considered to be the most accurate of biometric technologies. The iris is the coloured part of the eye that surrounds the black pupil. Careful inspection shows that it contains many detailed structures. These structures develop early in life and are believed to be unique to each individual, even with identical twins. The structures in the iris are said to remain constant until death. The iris is sufficiently detailed that it can be used for full identification of a user, unlike fingerprints and other biometric technologies that are best used for verification. The iris is not subject to wear, unlike fingerprints. It is reported that the appearance of the iris can change in extreme cases of diabetes due to increased vascularization and adhesions between the cornea and the iris. In this unusual situation, the image of the iris would change and an old enrolment template would no longer be usable. Iris-based biometric solutions are available for network access and physical access.

Iris scanning technology is not as user-friendly as fingerprint-scanning technology. The user must present the eye for scanning by locating the head in a very precise location and staring into a camera with a wide-open eye for several seconds. This presents considerable difficulty for some users. Some users cannot enrol in the system because of the physical procedure and the associated discomfort. However, the procedure is not too demanding for a user with a reasonable level of health and mobility.

Iris Scan Strengths	Iris Scan Weaknesses
• Potential for very high accuracy • Can be used for identification and verification • Iris structures are stable over a person's lifetime	• Acquisition of image requires some training and practice • Acquisition of image involves some user discomfort. This is enough to prevent the enrolment of some individuals

	• Higher false rejections than other technologies

Figure 4. Strengths and weaknesses of iris scanning biometrics[7]

9.5 Voice Scan

In voice scanning technologies, a user speaks a certain phrase that is analysed for identifying characteristics such as pitch, gain, frequency and others, which may or may not be detectable to human ears. These characteristics are compiled into a template that is used for verification. Voice scan templates tend to be quite large at 2000 to 10,000 bytes, compared to a typical fingerprint template at 250 to 1000 bytes. Template size is not significant in a network-based directory but a large template presents storage problems on a typical token.

Voice scan biometric technology is often used for automated password reset. In such a situation, a user who forgot his/her password would call an automated help desk, verify identity with a voice sample, and be assigned a new password. In this roundabout way, voice scanning is competitive with the password-replacement software packages that often rely on the use of fingerprint or other biometric technologies.

Voice Scan Strengths	Voice Scan Weaknesses
• Can leverage the vast telephony infrastructure • Layers well with speech recognition and oral passwords • Lacks the negative perceptions of some other biometric technologies	• Conceptually susceptible to replay attacks • Low-quality capture devices and ambient noise often limit accuracy • Template sizes are typically very large compared to other biometric technologies

Figure 5. Strengths and weaknesses of voice scanning biometrics[8]

9.6 Hand Scan

Hand scanning biometric technology uses the bottom and side silhouettes of a user's hand to verify identity. The fingertips are excluded in the scan to avoid problems with changing fingernail lengths. The large, wall-mounted scanners include a numeric pad for entering a user ID number. The scanners are fairly large, occupying about 20 cm by 30 cm of wall space, and they protrude about 20 cm from the wall. Hand scanning currently has thousands of successful deployments for physical access and "time and attendance" applications. The technology is not marketed for logical access. The matching quality of hand scanning is not particularly accurate, but is sufficient for low-security identity verification. Verification is very quick, taking about one second. Enrolment is also very quick, taking about five seconds. Hand scanning is notable for its extremely small template sizes of 9 bytes, which explains the lack of high accuracy. Individuals with arthritis may not be able to orient their hands properly, and individuals with very small hands may not be able to trigger the sensor. The price is fairly high at about $1,500 USD per unit.

Hand Scan Strengths	Hand Scan Weaknesses
• Well established, reliable technology • Generally perceived as non-intrusive • Fast verification and enrolment	• Limited accuracy • Large form factor may limit applications • May be difficult to use for individuals with arthritis or very small hands

Figure 6. Strengths and weaknesses of hand scanning biometrics[9]

9.7 Retina Scan

Retina scanning biometric technology uses the vascular structures on the retina for identification and verification. The retina is the back surface of the eye that detects light that has entered through the pupil. Note that retina scanning is different from iris scanning, which uses the characteristics of the coloured portion located on the front surface of the eye. Retina scanning offers exceptionally high security and resistance to spoofing, and is sometimes used for very high security physical access. The process of obtaining a retina scan, however, is fairly intrusive. It requires the user to position the head in a guiding device and stare into a camera while an infrared light is shone into the eye to dilate the blood vessels on the retina. Acquisition of a retina image takes four to five seconds, and a full enrolment procedure can take more than a minute. Many users cannot enrol at all, even after several minutes. Some medical conditions, like cataracts, can prevent the use of a retina scan. Retina scanning biometric devices are not currently commercially available although they are in use in some government organizations.

Retina Scan Strengths	Retina Scan Weaknesses
• Highly accurate • Very difficult to spoof	• Quite difficult to use • Not commercially available

Figure 7. Strengths and weaknesses of retina scanning biometrics[10]

9.8 Signature Scan

Signature scanning biometric technology is an extension of a very old identification technique. For centuries, a person's signature has been accepted as a means of identification and verification. Assessing a user's signature with computers can improve on this system by detecting details that are not available to human inspectors. In a traditional signature identification system, the user writes a signature on paper and a human inspector detects only the shape of the end product of a signature. In a signature scanning biometric, the user writes a signature on a pressure sensitive pad. An attached computer detects the pen speed, pressure applied, direction of strokes, total size of signature, and the ratio of pen-up time to pen-down time. These characteristics are processed to create a template of the signature that can be used in comparisons for identification or identity verification. New users are generally receptive to signature scanning biometrics because it seems so similar to the usual signature identification system. A weakness of the signature scan system is that it requires a fairly consistent signature behaviour, which individuals may not always use for their regular signatures.

Signature Scan Strengths	Signature Scan Weaknesses
• More resistant to impostors than regular signatures • Generally perceived as non-intrusive • Users can change signatures for different uses	• Inconsistent signatures increase the error rates • Users are not accustomed to signing on computer tablets

Figure 8. Strengths and weaknesses of signature scanning biometrics[11]

9.9 Keystroke Scan

Keystroke scanning biometric technology uses an individual's typing habits for identity verification. This technology is fairly young and not very well developed, but it appears promising for low-cost, non-intrusive logical access applications. Biometric data acquisition is performed through the standard keyboard as the user types. Typing habits such as time between keystrokes and length of time of key holding are monitored as individual characteristics. Generally, the technology is paired with password authentication, and an enrolled user must enter the correct password with the correct keystroke properties

to gain access to a system. Enrolment in a keystroke scan system involves typing in the password many times, preferably over the course of several days, to provide a good sample of the user's typing style. Users with strong touch-typing skills tend to have similar keystroke characteristics, so a keystroke scanning biometric technology may not differentiate well among this set of users.

Keystroke Scan Strengths	Keystroke Scan Weaknesses
• Leverages existing hardware • Leverages a password authentication process • A password can be changed as necessary • Perceived as non-intrusive	• Young technology • Adds only security, not convenience • Retains many of the flaws of password-based authentication

Figure 9. Strengths and weaknesses of keystroke scanning biometrics[12]

9.10 Gait Recognition

Gait recognition biometric technology uses a subject's posture and walking characteristics to aid in identification. This technology is still in the research phase, but it has interesting characteristics. Like face scanning, gait recognition has the ability to recognize a subject at a distance without the subject's cooperation or knowledge. It has applications in surveillance and may be more resistant to disguises than face scanning. Considerable work remains before gait recognition will be a viable commercial technology.

Gait Recognition Strengths	Gait Recognition Weaknesses
• Alternative to facial scanning • Can operate without a subject's cooperation	• Not well developed or commercially available • Behavioural changes in gait can fool system • Strong privacy concerns because of it's non-cooperative enrolment and identification capabilities

Figure 10. Strengths and weaknesses of gait recognition biometrics[13]

10 Influential Organizations in the Biometrics Industry

10.1 Biometric Consortium

The Biometric Consortium serves as the U.S. government's focal point for research, development, test, evaluation and application of biometric-based personal identification/verification technology.

10.2 Biometrics Management Office (BMO)

The Biometrics Management Office (BMO) in the U.S. Department of Defense will lead, consolidate, and coordinate the development, the adoption and the institutionalization of biometric technologies to enhance joint service interoperability and operational effectiveness.

10.3 The U.K. Biometrics Working Group (BWG)

The U.K. Biometrics Working Group (BWG) co-ordinates the Office of the e-Envoy (OeE) Biometrics Programme, the goal of which is to enable the use of biometric authentication technology to support the e-government aims and to facilitate the adoption of biometrics in support of wider government business.

10.4 National Institute of Standards and Technology (NIST)

As part of the U.S. Commerce Department's Technology Administration, the National Institute of Standards and Technology (NIST) develops and promotes measurements, standards and technology to enhance productivity, facilitate trade and improve the quality of life.

11 Reasons to use Biometrics

11.1 Improved Security

The addition of a biometric system to an existing security procedure will always improve overall security, especially when it replaces a complex password authentication system. However, most biometric technologies, including fingerprint scans and iris scans, can be spoofed with enough time and effort. Because of this, the use of biometrics alone does not offer a complete security solution. But when a biometric is used in addition to other security layers, it can offer considerable security improvements over competing authentication methods. For example, a fingerprint scanning biometric device used to control physical access to a building probably wouldn't offer adequate security if the building is isolated, not monitored, and an impostor had lots of time to work on fooling the system. But a fingerprint scanning biometric system, layered with a token authentication system and located in a place where an impostor would raise suspicion with strange repetitive behaviour, would offer a very high level of security.

11.2 User Convenience

User convenience is probably the most compelling reason to use a biometric authentication for physical or logical access. When passwords are used and password rollover is enforced, users are required to memorize a new password at every rollover. This can quickly become overwhelming for the users who will almost invariably choose the easiest possible passwords and keep them written in a convenient location, which is a security hazard. A biometric system is much easier for a user to maintain, since there is no need for multiple passwords or password rollovers from the user's perspective.

11.3 Lower Costs

Biometric solutions can be costly to implement, but they usually pay for themselves within a short period of time because of lower administration costs compared to password-based authentication. Biometric vendors claim a return on investment within 12 to 18 months when a biometric system is used in place of passwords for system access. Costs associated with forgotten passwords is estimated to be $200 to $400 per workstation per year for a large organization[14]. Within the RCMP, the Informatics Central Help Desk received 281 calls for password resets during the 20 working day period from April 1, 2002 to April 24, 2002[15].

12 Limitations of Biometrics

12.1 Security Versus Other Benefits

Commercially-available biometrics solutions are designed to be fast, convenient, reliable and cost-effective alternatives to password authentication. The security that these biometrics solutions provide is generally considered to be greater than passwords, but ultra-high security is not the objective because it could only come at the expense of these other goals. Improving the security of a biometric system requires a lower False Acceptance Rate (FAR), but this requires a higher False Rejection Rate (FRR), meaning less convenience and reliability. More complex templates and more rigorous matching algorithms could be used but this makes the system slower and more expensive. Biometrics is best considered as a tool that can be used to facilitate identity verification, but it isn't the answer for all access problems. Layering a biometrics solution with other security measures and identity verification techniques provides the best available security for automated authentication.

There is still no replacement for human judgment to handle unforeseen circumstances and conditions.

12.2 Individuals' Abilities to Use Biometrics

Not all individuals can successfully use a particular biometrics system. Approximately 2% of people cannot successfully use a fingerprint scanning biometrics system for a variety of reasons. Some people have very dry fingers that will not register properly on a fingerprint scanner, but most of these people can improve their success rates by rubbing the fingerprint on the opposite palm or breathing on the fingerprint to add moisture. Some people have fingerprints that are constantly worn smooth from doing rough work with their hands and their fingerprints simply will not register. In other biometric technologies, such as iris scanning or hand scanning, a small subset of users will not be able to use the biometric technique due to some physical limitation. When designing an authentication policy, it is important to recognize that not all the users will be able to use biometrics and will require an alternative authentication technique. Usually, these individuals will use a password in place of a biometric.

12.3 Importance of Positive Identification at Enrolment Time

Any identity verification simply evaluates offered proof that an individual has rights to a previously established identity. This places a considerable security requirement on the process used to originally establish the identity.

> "A biometric does nothing more than re-establish the connection between the person and the established identity. If the established identity is weak, so are all subsequent verifications."[16]

When using a biometric system, it is imperative that a new user's identity is correctly established when the biometric template is enrolled. If an impostor enrols with a legitimate user's identity, the impostor will be granted all of the privileges associated with the legitimate identity. After enrolment, the biometric system will have no way to detect if a user is legitimate – the system assumes legitimacy when the individual is enrolled. An enrolled impostor will have access to the system until he is discovered by other means. It is, therefore, critical that proper user identification be performed before biometric enrolment is performed.

12.4 Biometrics Spoofing Reports

Biometric spoofing means fooling a biometric system into identifying an impostor as a legitimate enrolled user. In the spring of 2002, reports of spoofing techniques for defeating biometrics were made available.

An academic report titled "Impact of Artificial 'Gummy' Fingers on Fingerprint Systems" by Tsutomu Matsumoto et al. of the Yokohama National University in Japan describes techniques to create a gelatin-based copy of a user's fingerprint that will fool a wide range of available fingerprint scanners. The gelatin copy is most easily made with the cooperation of the legitimate user, but a more complex technique is also described to create a copy from only a latent fingerprint. These techniques were reported to be very effective in defeating several types of fingerprint-based biometric systems.

"c't", a German technology magazine, released a detailed report on the Internet explaining techniques to defeat a range of biometric devices. The report entitled "Body Check: Biometric Access Protection Devices and their Programs Put to the Test" was written by Lisa Thalheim, Jan Krissler and Peter-Michael Ziegler. The authors were able to defeat a number of fingerprint biometric systems using a combination of techniques including breathing a "fog" onto a fingerprint left on a scanner, placing a plastic bag filled with water over a fingerprint left on a scanner, and making fake fingers of silicon using a

candle-wax mold. A facial scanning system was fooled using a short video of an enrolled user's head. The authors were also able to defeat an iris scanning biometric system with a printed image of an enrolled iris. The pupil part of the printed image was cut out to provide a hole for the tester to look through as the image was brought into the proper position for scanning.

12.5 Biometrics Spoofing Experiments

During the research performed for this report, some attempts were made to replicate the results claimed by some of these spoofing reports. These tests were performed in a way that favoured the spoofing attempts in order to maximize the probability of a successful spoof. The testing conditions are not fully representative of an actual biometrics authentication system. Nonetheless, results of the tests indicate what may be possible to achieve with a spoofing attempt on an actual biometric apparatus, if the impostor were allowed enough time.

This fingerprint spoofing experiment was not intended to be an exhaustive test of the susceptibilities of fingerprint-based biometric systems. The intention was to test whether the weaknesses claimed in these reports were true.

The spoofing tests were done with Software A (software manufacturer's name withheld) because this package had a "test mode" that facilitated multiple authentication attempts. In test mode, the software continuously attempted to read a fingerprint from an attached fingerprint scanner. A small window showed the image that was being sensed by the fingerprint scanner - this provided useful feedback to the tester. If a finger was sensed on the scanner, the software activated its matching algorithm to see if the fingerprint matched any enrolled fingerprints for the specified user. Whether the match passed or failed, the software continuously loops to detect another finger to scan. This allows a tester to continuously attempt to authenticate while making small adjustments in fingerprint presentation technique. When the software is running in normal mode, a user or tester can only present a fingerprint at a particular time, and a failed match results in the display of an error window that must be cleared before attempting another authentication.

In the test, an enrolled fingerprint was lubricated slightly with Vaseline Intensive Care skin lotion so that it would leave a clear fingerprint on the glass. The fingerprint was placed on the clean scanning surface and a successful authentication was achieved. This fingerprint presentation also left a clearly visible fingerprint on the scanning surface. Attempts were made to exploit this greasy fingerprint to achieve successful authentication without presentation of another enrolled finger.

Two spoofing techniques were attempted. In the first technique, the tester breathed a fog onto the scanning surface while watching the detected fingerprint image on the computer monitor for visual feedback. The level of humidity applied to the scanning surface was controlled by the rate and location of breathing and by using hands cupped over the scanning surface. The level of background lighting was controlled by the hands cupped over the scanning surface while the tests were performed in an office with normal fluorescent lighting. In the second technique, a clear, colourless, thin-walled plastic bag was filled with water to test the water bag method. For both techniques, the amount of spoofing effort was measured in time and not in the number of attempts because of the continuously cycling nature of Software A's test mode. Three devices were chosen to represent the range of available fingerprint scanning devices. Device A was an optical scanner with a plain glass surface on the scanner. Device B was a chip-based capacitive scanner. Device C was an optical scanner similar to Device A, except that it had a clear rubber coating on the scanner surface which is said to significantly improve the quality of the fingerprint scans.

The success of the spoofing tests were measured with two results: the rate of fingerprints sensed and the rate of fully successful authentications. A sensed fingerprint was noted whenever the software attempted

to match a spoofed fingerprint image against an enrolled template. A fully successful authentication was noted whenever the software assessed a sensed spoofed fingerprint to be a valid match of an enrolment template. The results of testing with these three devices are detailed in Figure 11.

Scanning Device	Scanning Device Type	Attempted Spoofing Method	Approximate Testing Time	Instances (approx) of Fingerprints Sensed	Successful Authentications
Device A	Optical, plain glass	Breathed fog	10 minutes	2 instances	None
		Water bag	5 minutes	None	None
Device B	Capacitive	Breathed fog	15 minutes	3 to 4 times per minute	1 instance
		Water bag	5 minutes	None	None
Device C	Optical with rubberized coating	Breathed fog	10 minutes	1 instance	None
		Water bag	5 minutes	None	None

Figure 11. Results of fingerprint spoofing tests

For all three scanning devices, the "water bag" spoofing method did not work at all. The test software's visual feedback of the "water bag" method showed no fingerprint image at all.

The "breathed fog" spoofing technique was more successful. Visual feedback showed an image of the fingerprint for all tested scanners, with the quality of the image varying with the breathing technique. It was not difficult to create a clear image - after some practice. Despite the image clarity, the software usually did not sense the presence of a fingerprint. Both optical scanners Device A and C were not as susceptible to false fingerprint detection, which is likely the reason no successful authentications were made with the optical scanners during the spoofing tests. The capacitive scanner Device B was found to be surprisingly susceptible to the "breathed fog" spoofing technique, and the software detected a fingerprint about three to four times a minute.
After 15 minutes of testing, the software had been spoofed into granting one false authentication. It is notable that visual feedback showed clear fingerprint images for all three scanners, but Device B was much more susceptible to the spoofing attempts. The reason for this is unknown.

Clearly it is possible to spoof a fingerprint-based biometric system, but it should be remembered that an operational system would be more difficult to defeat than this test environment. In an operational system, the software's fingerprint detection would not be on a constant loop, a clear greasy fingerprint likely would not be left on the scanning device, and the prolonged breathing technique would likely attract attention from anyone in the area. However the "gummy finger" technique described in the *Biometric Spoofing Reports* section above might produce better results for an infiltrating impostor because it is claimed to be more accurate, more discrete and doesn't require a greasy fingerprint to have been left on the scanner.

13 Privacy Concerns

In the general population, there are many groups with serious concerns about privacy and the use of biometrics. Mostly the concerns relate to technologies that can assess an individual without the individual's consent, such as face scanning biometrics systems. Some people are simply uncomfortable with any system that can identify them accurately, even if they have nothing in particular to conceal. Many people distrust the idea of using biometrics because it facilitates the collection of information about an individual for any purpose.

In the United States, the American Civil Liberties Union (ACLU) has taken a strong stand against using face scanning in airports and other locations, stating that the technology does not work and that it represents a threat to the liberty of Americans.[17]

Some Christian groups object to biometrics in general on the grounds that it is similar to the prophesized "mark of the Beast" from the book of Revelations in the Bible. According to the prophecy, all individuals will require a mark on the hand or the forehead in order to buy or sell merchandise, and the mark is somehow related to "the Beast" which represents Satan. Some Christians feel that using a fingerprint for identity verification, perhaps one day for economic transactions, is similar to having a mark on the hand. Similarly, using an eye-scanning biometric technology is felt to be similar to having a mark on the forehead.

The legal issues of requiring the use of biometrics have not been well explored in Canadian law, but citizens' rights to privacy are well entrenched in Canadian society. The House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities commented eloquently on the Canadian perspective on privacy:

> Canadians view privacy as far more than the right to be left alone, or to control who knows what about us. It is an essential part of the consensus that enables us not only to define what we do in our own space, but also to determine how we interact with others -- either with trust, openness and a sense of freedom, or with distrust, fear and a sense of insecurity.[18]

Most advocates of biometric technologies recognize the concerns of certain individuals about privacy and other issues surrounding biometrics. Generally, it is recommended users be permitted to opt out of a biometrics implementation if desired, and to make use of another authentication method. It is assumed that the convenience and security values of a biometrics-based solution will persuade most users to opt to participate in the biometrics implementation.

14 Best Practice for Automated Authentication

No authentication method is perfect, including biometrics. Tokens and passwords have their own strengths and weaknesses. To obtain an acceptable range of benefits offered by the different authentication methods, a combination of techniques can be combined to form a layered or multifactor authentication policy. An example of multifactor authentication is the common financial system of combining a bank card (token) with a PIN (password). Neither the bank card nor PIN alone can offer adequate security for the application, but the combination of the two has been used for more than two decades to provide identification for personal banking.

Passwords are difficult and expensive to maintain properly and can be shared or stolen, biometrics can be spoofed, and tokens can be borrowed or stolen. None of these authentication methods alone can provide high levels of security, convenience and low cost at the same time. However, combining a biometric and a token reduces the dangers of spoofing and token theft inherent in either lone system, while greatly reducing maintenance compared to passwords. This combination of biometric and token is perfect for most relatively high security applications. Other levels of security can be accommodated with different combinations of the three authentication techniques. For instance, a low-security application may require just a biometric or just a token. A very high security application may require the combination of a biometric, a token and a password. An extremely high security application may require both a fingerprint and iris-scanning biometric authentications in addition to a token and password. By layering the

authentication techniques, a flexible and responsive authentication policy can be developed for an organization.

When token-based authentication and biometric authentication are combined, it is possible to hold the enrolled biometric template on the token. This means that the user's biometric templates are never stored in a directory on the network. This architecture may alleviate some of the privacy concerns that exist due to the storage of personal information. In this architecture, the user is always in possession of the enrolled template because it is located only on the token, which the user carries.

When developing an authentication policy, it is important to consider that not all users will be able to reliably use a particular biometric, so an alternative authentication method will need to be used for these individuals. Usually, passwords are used in place of a biometric authentication in these cases.

15 Evaluation Criteria for Biometrics

The biometric project group developed the following basic criteria for the evaluation of biometric solutions.

15.1 Operational

- The device should be convenient to use. (i.e. the time required to perform enrolment, authentication and verification should be minimal).
- A device is user friendly if it is easy to use, convenient, satisfies the user's needs, and conforms to contemporary social standards.
- The long-term precision of a biometric solution is critical to a successful deployment. Re-enrolment should not be required. Stability of correct user authentication should be tested over a period of weeks or months.

15.2 Technical

- The time required to measure the human characteristics in order to create the template and the storing time of the templates should be acceptable.
- The time to authenticate (response time) as measured from the time the user wants to access the protected system to the time the user gains use of the system. Long authentication times can distract and annoy users.
- The device should not be too big or cumbersome.
- The device should be simple to use, fast and precise.
- The device should be able to perform well within reasonably harsh environmental conditions (e.g. light, noise, heat, moisture, smoke and dust).
- The device should be flexible in adjusting threshold settings depending on the security level of the application.
- The solution should have the capacity to scale up to accommodate future expected requirements without a major redesign. It should accommodate tens of thousands of users while maintaining acceptable performance in terms of security, administration and response time.
- Is there a backdoor to bypass the biometric system if necessary? This could be a user password or a capability for Administrator access without biometric authentication. This is useful for disaster recovery operations (e.g. an injured finger can't be used for fingerprint scan). Note that the implementation of a backdoor should be carefully considered when developing the security policy and it may not be suitable for all applications.
- Multiple fingers enrolled for each user provides redundancy in case a given finger becomes unusable. A common policy is to enrol a finger from each hand.

- If a user can re-enrol without help or special privileges, the template database can be kept current with small physical changes in the user base without significant administrator involvement. However, this introduces the risk of an authorized but malicious user enrolling unauthorized users with a legitimate identity.

15.3 Financial

- Cost is very important. Take into account the equipment cost, installation and training costs.

15.4 Company Profile

- How long has the company been in the biometrics business? How many employees do they have? How quickly have they grown? Do they offer a wide range of products or do they specialize in biometrics? How often do they release new software versions?
- How much market share does the company and product control? Are there any success stories?
- What is the product and company primary target market? How much experience does the company have with this target market and with other market segments?
- What organizations has the company partnered with? What third-party scanners does a software package support? What software packages does a scanner work with? How much third-party software integration work has been done?
- What is the company's stated plan for the future? Will the product continue to be produced? Will the company reinvest in biometrics or pursue other objectives?

Notes

[1] Police Information Technology Organization (PITO) UK Department of Trade and Industry (DTI) Report, "Biometrics in Law Enforcement", http://www.afb.org.uk/downloads/pito_report_1-36.pdf , accessed May 15 2002.

[2] "Agencies batten down the access hatches", April 1, 2002, http://www.gcn.com/21_7/departments/18262-1.html, accessed May 9, 2002.

[3] "Agencies don't buy biometrics yet", Dipka Bhambhani, April 1, 2002, http://www.gcn.com/21_7/news/18299-1.html, accessed May 9, 2002.

[4] http://www.bioapi.org/BioAPI_products/products.htm, accessed May 15 2002.

[5] S. Nanavati, M. Thieme, R. Nanavati, "Biometrics: Identity Verification in a Networked World", John Wiley & Sons, 2002. p. 45.

[6] Nanavati et al., Ibid., p. 63.
[7] Nanavati et al., Ibid., p. 77.

[8] Nanavati et al., Ibid., p. 87,88.

[9] Nanavati et al., Ibid., p. 99,100.

[10] Nanavati et al., Ibid., p .107.

[11] Nanavati et al., Ibid., p. 123, 124.

[12] Nanavati et al., Ibid., p. 133, 134.

[13] Nanavati et al., Ibid., p. 113.

[14] Marlene Orton, "Facing up to a secure, new world", The Ottawa Citizen, March 5, 2002

[15]Informatics Central Help Desk, personal correspondence on May 10, 2002.

[16] David Heath, Biometrics LISTSERV correspondence, May 7, 2002, heathd@BIGPOND.NET.AU

[17] "ACLU Blasts Plan to use Flawed Facial Recognition System at Statue of Liberty and other NY Landmarks", http://www.aclu.org/news/2002/n052402a.html, accessed June 8, 2002.

[18] "Priv*acy: Where do we draw the line?", Report of the House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities*, Ottawa: Public Works and Government Services Canada, April 1997, p. 6