Defence Research and Development Canada
Recherche et développement pour la défense Canada

DEFENCE R&D DÉFENSE

Trusted User Authentication Using Biometrics

Qinghan Xiao

Defence R&D Canada - Ottawa
TECHNICAL MEMORANDUM
DRDC Ottawa TM 2002-122
November 2002

Canada

Trusted User Authentication Using Biometrics

Qinghan Xiao
Information Operations Section

Defence R&D Canada — Ottawa

Technical Memorandum

DRDC Ottawa TM 2002-122

NOVEMBER 2002

Abstract

User authentication is the process of confirming one's identity by checking one's credentials. It is a cornerstone of information security. Traditionally, users access information systems by applying something they know, such as passwords, or something they possess, such as tokens. A third method, biometrics is based on something users are, such as fingerprints. Nowadays, to protect sensitive information, these methods are deployed together to form a strong three-factor authentication.

This report presents an overview of different authentication factors, analyzes their advantages and disadvantages, and indicates the common problems facing each factor. Since there are various biometric technologies, each with its own strengths and weaknesses, this report discusses only the most popular biometric technologies in detail. The purpose of this report is to position biometrics in user authentication to enhance information security. As a result, a system architecture is presented to provide a solution for information protection in secure or sensitive environments.

Résumé

Le processus de confirmer l'identité d'un usagé par la vérification de certains de ses justificatifs d'identité est appelé l'authentification de l'usagé. L'authentification est une pierre angulaire de la sécurité de l'information. Un usagé peut habituellement accéder à un système d'information en présentant l'un ou l'autre des deux facteurs d'authentification: un facteur qu'il connaît comme un mot de passe ou un facteur qu'il possède comme un jeton de sécurité. Un troisième facteur, basé sur une caractéristique biométrique de l'usagé comme les empreintes digitales, peut être rajouté pour protéger l'information sensible ou classifiée. Lorsque qu'une méthode d'authentification d'un usager est faite à l'aide de ces trois types de facteurs, nous dirons que cette méthode en est une à trois facteurs d'authentification.

Dans ce rapport nous présentons un aperçu des différents facteurs d'authentification, analysons leurs avantages et inconvénients, et indiquons les problèmes associés à ceux-ci. Puisqu'il existe plusieurs technologies biométriques ayant chacune ses forces et ses faiblesses, nous abordons en détail seulement les technologies biométriques les plus populaires. Le but de ce rapport est de positionner l'authentification des usagers par la technologie biométrique pour accroître la sécurité de l'information. Pour ce faire, nous présentons une architecture de système utile dans des environnements où de l'information sensible ou classifiée est stockée.

This page intentionally left blank.

Executive summary

The need for heightened information security has expanded the research focus from securing the network to authenticating individual users. User authentication is the process of confirming the identity of a user with whom a system is communicating or conducting a transaction. User authentication is an essential foundation for protecting an information infrastructure. It is implemented to prevent unauthorized access to the resources of a network. User authentication is even more crucial in a classified or sensitive environment. Today, user authentication can be accomplished using one or more of three factors: knowledge, possession, and biometrics.

The most common form of user authentication is knowledge, something users know, such as a password or a PIN. It is the oldest and easiest authentication method to implement. Smith [1] and Dale [2] have shown that this approach is not secure since the passwords are particularly subject to eavesdropping. In addition, users may easily forget their passwords.

Administrators can add another level of security by requiring possession, something users have such as tokens or smart cards, also known as intelligent tokens. However, tokens are still subject to human carelessness, primarily about their password or PIN. Users may also loose them.

To enhance user's authentication, a third level of security can be added through biometric factors, something users are, such as their fingerprints or the pattern of their iris. Three-factor authentication combines password, smart card and biometrics.

Starting in 1999, the United States Department of Defense (DoD) has been implementing the Common Access Card (CAC) across the department. The CAC is a secure, multi-application smart card for physical identification, building access, and network access. Recently, DoD has selected a contractor team to investigate biometric technologies, such as voiceprint, fingerprint, iris pattern or facial contour, as an added layer of security for the CAC. Mary Dixon, director of DoD's Access Card Office, said: "We will add biometrics as one more way in which we can authenticate a person's identity" [3].

The objective of this paper is to propose a trusted user authentication to protect network resources that require higher security. We first present an overview of user authentication, the fundamentals of authentication and the essentials of authentication systems. In particular, we examine how authentication works, what the current stage of authentication is, and why we need a strong authentication. Second, we present three authentication factors and discuss their properties, security levels and weaknesses. A procedure for a three-factor authentication is also presented. Then, popular biometric technologies are reviewed and their major characteristics are compared in terms of advantages, disadvantages, usages, and costs. Next, some current biometric applications are introduced to show the applicability and effectiveness of biometric technologies. Based on the above discussions and because the major concerns of most commercial products are cost and convenience, but not high security, an example of user authentication system for protecting high security resources is proposed.

Xiao, Q. 2002. Trusted User Authentication Using Biometrics. DRDC Ottawa TM 2002-122. Defence R&D Canada — Ottawa

Sommaire

En plus de sécuriser les réseaux informatiques, le besoin de renforcer la sécurité de l'information de ces réseaux a étendu le domaine de recherche à l'étude de l'authentification des usagés de ces réseaux. Le processus qu'un système fait pour confirmer l'identité des usagés avec qui il communique ou fait des transactions est appelé l'authentification d'usagers. L'authentification des usagers est une base essentielle pour la protection de l'infrastructure de l'information. Ceci est encore plus vrai dans les environnements où l'information est sensible ou classifiée. Actuellement, l'authentification des usagers peut être faite en utilisant un ou plus des trois facteurs suivant : connaissance, possession et biometrique.

La méthode la plus commune d'authentifier un usagé est basée sur la connaissance par l'usagé d'un élément ou facteur— en général un mot de passe ou un NIP —. C'est la plus ancienne et facile méthode d'authentification. Smith [1] et Dale [2] ont montré que cette approche n'est pas sûre puisque les mots de passe font l'objet d'écoutes clandestines. De plus, les mots de passe peuvent être oubliés.

Les administrateurs peuvent ajouter un autre niveau de sécurité en requérant de l'usagé la possession d'un élément physique telle qu'une carte à puce ou un jeton de sécurité. Une carte à puce est un exemple de jeton intelligent. Cependant, les jetons sont sujets à la négligence humaine surtout lorsqu'ils sont protégés par des mots de passe. De plus, ils peuvent être perdues.

Pour améliorer l'authentification des usagers, un troisième niveau de sécurité peut être ajouté en additionnant un facteur biométrique: ce que l'usager est. Ce facteur peut être par exemple ses empreintes digitales ou la forme des ses iris. L'authentification à trois facteurs utilise un mot de passe, un jeton et un facteur biométrique.

Débutant en 1999, le United States Department of Defense (DoD) a implanté dans ses structures l'utilisation par ses usagers de la carte appelée Common Access Card (CAC). La CAC est une carte à puce multi-applications pour l'identification des usagers pour l'accès aux édifices et réseaux informatiques. Récemment, dans le but d'ajouter une couche de sécurité à la CAC, le DoD a sélectionné une équipe pour évaluer les technologies biométriques associées aux empreintes vocales et digitales, aux contours faciaux, et à l'iris. Mary Dixon, directrice du Access Card Office du DoD a dit que «Nous allons considérer les biométriques comme un moyen de plus par lequel nous pourrons authentifier l'identité des personnes » [3].

L'objectif de ce rapport est de proposer une méthode d'authentification sûre pour protéger les ressources réseaux qui requièrent un niveau de sécurité élevé. Nous présentons d'abord un aperçu sur l'authentification d'usagers en donnant les éléments fondamentaux nécessaires et les composants essentiels des systèmes d'authentification. Deuxièmement, nous présentons trois facteurs d'authentification et discutons de leurs propriétés, de leur sécurité, et de leurs faiblesses. Une procédure d'authentification utilisant ces trois facteurs est présentée. Les technologies biométriques populaires sont analysées. Leurs caractéristiques sont comparées et énumérées en termes d'avantages, de défauts, d'usage, et de coûts. Finalement, certaines applications biométriques actuelles sont introduites pour montrer l'applicabilité et l 'efficacité de la technologie biométrique. Basé sur les discussions ci-haut et puisque les principaux

objectifs des produits commerciaux de sécurité sont les coûts et la facilité d'usage et non la haute sécurité, un exemple de système d'authentification d'usagés est proposé pour ce dernier objectif.

Xiao, Q. 2002. Trusted User Authentication Using Biometrics. DRDC Ottawa TM 2002-122. R&D pour la défense Canada — Ottawa

Table of contents

List of figures

List of tables

Acknowledgements

I would like to express my thanks and appreciation to Dr. Mark McIntyre, Head of the Information Operations Section, for his encouraging words and guidance throughout the course of this report; Dr. Sahnoune Dahel, Group Leader for Information Protection and Assurance, for his comments on various aspects of this draft; Dr. Jean Savoie for his expertise on information security and technical review; Dr. Steve Zeber for his help on report format; Matthew Kellett for his careful correction and editing. Any errors, of course, are the responsibility of the author alone.

This page intentionally left blank.

1. Introduction

Modern information systems are composed of three primary components — authentication, authorization, and accountability. Authentication is the most fundamental of these three elements because it precedes the other two. In the information technology environment, authentication means either the process of verifying the identities of communicating equipment, or verifying the identities of the equipment's users. This report will focus on verifying the identity of a user, in other words "user authentication".

With computers now being used in every major function of society, information security is becoming increasingly important. Information systems require a method to establish the credentials that define a user's identity. Today, the majority of information systems use passwords as credentials to authenticate the user's identity. The major problem with this type of identification mechanism is that given a password can we confirm that it belongs to the person who presents it? To provide secure information operating environments, a trusted authentication system must be developed to prevent unauthorized users from gaining access to classified or sensitive data. A strong authentication can be achieved by combining different authentication factors. This is especially important when legally signing a user into a secure system and allowing access to secure or sensitive data. Some unique, unchangeable aspect of the user must be used to verify his or her identity namely a biometric.

The objective of this paper is to position biometrics in the field of information security and propose a trusted authentication solution for protecting sensitive resources. The seven sections of this paper are organized in the following manner. Some problems with authentication and how to solve them are introduced in Section 1. Section 2 presents a general overview of authentication and authentication systems. Then, different authentication factors are introduced with analyses on their security levels and weaknesses in Section 3. After reviewing popular biometric technologies, Section 4 presents a detailed comparison on the advantages, disadvantages, usages, and costs of these technologies. In order to show the applicability of biometric technologies, Section 5 is devoted to real biometric applications with emphasis on military use. Since the major concerns of most products on the market are cost and ease of use, but not high security, in Section 6, a user authentication system for protecting high security resources is proposed. Section 7 concludes the report with a suggestion about the direction for future investigation.

2. Authentication

Personal recognition is the process that associates a particular individual with an identity. It can be in the form of either authenticating a claimed identity (called one-to-one matching) or comparing a person's unclaimed identity to the entire database (called one-to-many matching). In an information community, user authentication has long been an issue. The goal in user authentication is to allow valid parties access to databases and information services from anywhere at anytime. We want to let authorized users in while keeping others out, by checking what they have submitted.

Authentication is the process of confirming the identity claimed by a user. It can be accomplished by using one or more of the validation approaches: knowledge factor (something users know), possession factor (something users have), or a biometrics factor (something users are). With the rapid evolution of information technology, the military's reliance on IT systems to carry mission-critical information is rapidly growing. As a result, the ability to achieve a highly accurate authentication is becoming more critical for protecting sensitive information.

2.1 Authentication system

An authentication system is one used to validate that the user logging on the system is the right person who claims to. There are several elements usually present in an authentication system. There is a person to be authenticated; an administrator who is responsible for the system; the distinguishing characteristics that differentiate this particular person from others; and an authentication mechanism that verifies the presence of those distinguishing characteristics. In the end, the user can be granted or denied some privileges depending on the success or failure of the authentication.

A genuine example is the password controlled login operation in most computing environments. The person to be authenticated has privileges to use the computer. The administrator assigns an identification code and a user name to that person. The distinguishing characteristic for the person is his or her secret username/password. The authentication procedure is defined as the user login process. It prompts the person for his or her user name and password, and then matches the typed-in password, in plaintext or after the application of a one-way function, to the corresponding credentials in the system's password file. The authentication mechanism allows the person to use the computer if the match succeeds. Authentication plays a very important role in computer security because, when access is granted, the user has full use of the resource.

2.2 Strong authentication

Today's authentication systems have evolved from decades of attacks, many of them were successful. Starting with password-based systems in the early days of timesharing, authentication systems have been under constant attack. For example, network sniffing can recover a user's password; a weakly protected password file allows its contents to be stolen;

interception and replay of a one-time password will block the legitimate user from successfully logging on. One of the methods to achieve a strong authentication incorporates two or three factors so that the benefits of one factor can compensate for the shortcomings of another. As well, strong authentication is a means of preventing attackers from simulating other users' identities. Only biometrics, which uses a unique physical or behavioural feature of the person being authenticated, satisfies with this requirement.

2.3 Current authentication stages

Nowadays, two widely used types of authentication are based on knowledge and/or ownership. The knowledge-based approaches use something the user knows to authenticate a claimed identity, such as a password, personal identification number (PIN), or secret answers to challenge questions. The ownership-based approaches use something the user possesses, such as an ID card, key, token, or smart card, to authenticate a claimed identity. Since these traditional methods are not based on any inherent attributes of an individual, they suffer from a number of disadvantages. For instance, passwords may be stolen or guessed by impostors or forgotten by the user; tokens may be stolen, forgotten, misplaced, or borrowed. In the field of information security, the actual person at the other end of the network link must be identified making simple user ID or token logons insufficient [4], [5]. To legally sign a user into the system and access sensitive data, some physical part of the user should be verified using biometrics to decrease certain types of impersonation attacks.

3. Authentication Factors

As we have mentioned before, there are three commonly used authentication factors: knowledge, ownership and biometrics. In this section, these factors are introduced and their advantages and disadvantages are highlighted.

3.1 Password: something you know

Knowledge factors are something that users know, such as a password or a PIN. The password authentication technique was introduced into the computing environment around 1950. It has been used worldwide as an essential identification and access control technique. Passwords are the most cost-effective security mechanism. They are usually free and built into almost all information systems. Passwords are simple and easy to use. Most users understand them so there are no barriers to implementation; however, there are numerous problems with use of password authentication. Many end users do not know what authentication refers to in the realm of computer security. They want passwords that are short and easy to remember, while security administrators want passwords that are long, hard to guess and difficult to crack.

3.1.1 Password secrecy

In order to remember a password, users often write it down. This is especially true if the user has different passwords for different systems, or if a system requires the user to change passwords frequently. No such methods exist to prevent the user from writing the password on a piece of paper and sticking it to his or her monitor. Even if the passwords are kept secret, users tend to pick obvious passwords, such as names of their partner, children, loved ones, or telephone numbers. Those passwords are relatively easy to guess. Studies indicate a 90% success rate for gaining access to password-protected systems if these and other obvious choices are used.

3.1.2 Password vulnerabilities

Very often password is transmitted from the user to the system in clear text on the communication lines. This makes it easy for an eavesdropper to observe the communication and capture the password. This avenue of attack has repeatedly proven effective in networks that have been incorrectly assumed to be safe from eavesdroppers.

Password files tend to store passwords in hashed or encrypted form, but often there is no restriction on reading the password file. This makes the password very amenable to dictionary attacks in which a dictionary of possible passwords is created and each tried in turn by a computer until it gets the right guess. Such brute-force attacks have proven very effective in finding weak passwords.

In 1985, a Dutch scientist named Wim van Eck described how one could eavesdrop on any video monitor using relatively simple techniques [6]. The signals of video tube are called van Eck radiation and, in theory, are visible from as far as 1 kilometre. An attack with the right equipment could read passwords and other secrets displayed on any nearby video screens.

3.1.3 Weakness of password

Studies by the FBI and the Congressional hearings that led to passage of the U.S. Computer Security Act of 1987 revealed that most computer crimes had resulted from the inadequacies of password authentication. Vulnerable areas include personal computers and local area networks, where passwords are broadcasted to all stations, allowing for capture and replay. New technologies threaten the password authentication as well. Hackers have been using the latest technological advances, often freely available over the Internet, to access valuable information resources from anywhere in the world. The two most advanced developments to crack passwords are L0phtcrack and Pwdump3. Both tools are effective against password encryption and are used extensively by hackers. In summary, passwords by themselves are weak in providing an adequate mechanism for authentication.

3.2 Token: something you have

As mentioned above, the disadvantage of password authentication is that it relies solely on something users know. This knowledge is entered and sometimes stored in a file that can be read or copied with ease. There is no way to detect a passive adversary that simply reads information with unrestricted access. One solution to this problem is to add protection to the control of information access. Ownership-based authentication schemes depend on something the user possesses being presented in order for authentication to succeed.

3.2.1 Token authentication

An alternative to the current security approach is token authentication. Normally a token is used in conjunction with PIN/password in case the token inadvertently falls into the wrong hands. The user provides two items: a PIN and a token, a device used to generate passwords while logging onto a network. This two-factor authentication is one step closer to providing strong assurance that the user is the authorized individual. Tokens used for authentication can be a wide variety of shapes, sizes, and forms, such as a magnetic stripe card, a smart card, or a password calculator. The essence of token-based authentication is that the user has to have this device, which requires the knowledge of a PIN to be activated, in order to log onto the system. Tokens are low cost and easy to use. Since everyone understands that to open a door, he or she has to have a correct key, users have no barriers in using tokens to access information resources. The practice of allowing users to choose their own PIN, as well as changing it whenever they like, gives users the feeling that the token is their private tool and not controlled by anyone else.

3.2.2 Token security

There are numerous products in the market which use token-based authentication for both computer and non-computer applications. One important property is that tokens take away much of the burden of memorization. A token can reliably store a much more complicated password than most people can memorize. For example, a six-character password using all uppercase letters has a total possible combination of 26^6 = 308,915,776, while an eight-character password using the same character set has a total possible combination of 26^8 = 208,827,064,576.

Following table shows a comparison of potential combinations for six-character-length and eight-character-length passwords.

Table 1. Possibilities for 6-character and 8-character passwords

	6-CHARACTER-LENGTH PASSWORD	8-CHARACTER-LENGTH PASSWORD
Alpha	308,915,776	208,827,064,576
Upper/lowercase alpha	19,770,609,664	53,459,728,531,456
Numeric	1,000,000	100,000,000
Upper/lowercase alpha + numeric	56,800,235,584	218,340,105,584,896
Extended	1,073,741,824	1,099,511,627,776
Upper/lowercase alpha + numeric + extended	689,869,781,056	6,095,689,385,410,816

Token-based authentications improve security, lower costs and minimize unauthorized access to services. The benefit of two-factor authentication is that even if the token falls into someone else's hands, a PIN number is still required to activate it.

3.2.3 Smart card

The smart card, also referred to as an intelligent token, is the size of a credit card, but is embedded with memory chip and a microprocessor that can be programmed to perform tasks and store information. There are different types of smart cards including: memory cards, processor cards, Java cards, and more recently USB tokens. Memory cards are designed to store and protect information on the card. They do not have sophisticated processing power and do not manage files dynamically. Processor cards use the on-board microprocessor and RAM to allow for data processing, which offers multiple functions such as encryption, local data processing and complex interactive calculation. A Java card is a smart card that is able to execute Java byte code, similar to the way Java-enabled browsers can. One advantage of Java

card is that Java is a popular programming language with a lot of developers worldwide. According to Rainbow Technologies [7], USB tokens are "technologically identical to Smart Cards, with the exception of their form factor and interface". The chief advantage of a USB token offers over a smart card is that there is no need for a card reader, so the cost can be reduced. First introduced over two decades ago in France, smart cards have been used extensively in Europe, South America, and Asia. Recently smart cards have started to take off in North America with the American Express, MasterCard and CIBC Visa Card initiatives. Most recently, the DOD has been committing to issue 4.3 million cards over the next year for physical and on-line access control. Because they can provide not only memory capacity but also computational capability, smart cards are often adopted in applications that require strong protection and authentication. Smart cards have three main advantages over magnetic-stripe cards. First, they can carry 10 or even 100 times more information and hold it much more robustly. Second, the smart card can execute complex tasks in conjunction with a terminal (card reader) so that authentication can be performed by checking the PIN against the information on the card itself. Therefore, the password is not sent over an easily-tapped communication line for verification. Finally, since the data on a smart card can be encrypted, it cannot easily be read, transferred, or altered.

3.2.4 Weakness of tokens

Tokens and smart cards share certain security strengths and weaknesses. Everyone has personal experiences with keys: losing them, finding them, locking them in the car, and so on. Much of this can be found with authentication tokens. It is quite easy for a user to lend a token to someone else, or for the token to be lost or stolen. Users who carelessly choose poor PINs or keep their PINs in wallets or desks raise another problem. In such circumstances, risks are similar to those of passwords because the authenticating system is unable to determine that the user accessing the system is not really the person that he or she claims to be.

The smart card seems to be a superior tool for enhancing authentication, but some esoteric ways to attack smart cards exist. For example, by raising or dropping the supplied voltage of the microprocessor, researchers have learned how to steal a smart card's supposedly secret key. At Cavendish laboratory in Cambridge, a technique is being developed for reverse engineering the circuit chips. The layout and function of the chip can then be identified [8].

3.3 Biometrics: something you are

The problem of lending or losing tokens can be solved by using "tokens" that are impossible to lose and counterpart. A straightforward solution is to use some unique physical attribute of a person for user authentication, such as biometrics. The word biometrics is a combination of the Greek words *bio* and *metric*, which when combined, means "life measurement." Biometric technology refers to any technique that uses measurable physiological or behavioural characteristics to reliably distinguish one person from another. Common physiological biometrics includes fingerprints, hand geometry, retina, iris, and facial images, while common behavioural biometrics includes signature, voice recordings (also has a physiological component) and keystroke rhythms. Any one of these biometric measurements is sufficient to positively identify an authorized person from among hundreds of others (with some techniques, from among thousands or millions).

3.3.1 Biometric authentication

Practically all biometric authentication systems work in the same manner. The first process is called enrolment in which each new user is registered into a database using a specified method. Information about a certain characteristic of the person is captured. This information is usually passed through an algorithm that turns the information into a template that the database stores. Note that it is the template that is kept in the system, not the original biometric measurement as many people suspect. Compared with the original measurement of the biometrics, the template is a very small amount of information; it is no more than a collection of numbers with no meaning except to the biometric system that produced them. When a person needs to be authenticated, the system will take the appropriate measurement, translate this information into a template using the same algorithm that the original templates were computed with, and then compare the new template with the database to discover if it is a match, and hence, an authentication.

3.3.2 Biometrics security

Very often users need to remember various passwords to deal with different application and systems. To ensure password security, users are required to change the passwords regularly. Surveys show a large percentage of help desk support calls relate to forgotten passwords. "We're also trying to promote biometrics within our own organization, which would cut 50% of our help desk costs because there will be no more lost passwords," says David Mintie, project director at the Connecticut Department of Social Services [9]. The way to eliminate forgetting and disclosure of passwords is to use an authentication system that is able to authenticate users from direct measurement of unique human characteristics. Since it represents a unique physiological or behavioural characteristic of each individual, biometric measurement can be used to prevent theft or fraud. Unlike passwords and PINs, biometric signatures such as fingerprints cannot be forgotten, stolen or shared. Although two fingerprint patterns may be similar, no two fingerprints have been found to contain identical individual characteristics.

There are three advantages of biometrics over passwords, PINs and tokens.

- Biometric authentication requires the user to be present at the point of authentication.
- Biometric authentication eliminates the need to remember a password or PIN.
- Passwords and PINs may be forgotten and tokens may be forged, stolen or lost, but the individual’s biometrics is hard to lose, cannot be forgotten, and cannot be forged without the user’s cooperation.

Recent academic and media studies reveal that biometric technologies are susceptible to attack in which fake fingerprints, static facial images, and static iris images can be used successfully as biometric samples [10]. A company, called SecuGen Corporation, announced new technology to detect methods used to defeat fingerprint recognition systems in May 2002. SecuGen claims that it's advanced optical fingerprint sensor and algorithms have long been able to reject latent fingerprints left on the sensor surface as an invalid input. This new

technology will be available as an option in the SecuGen(R) line of biometric peripherals beginning in September 2002 [11].

3.3.3 Biometrics accuracy

The three terms that are commonly used to relate accuracy in the biometrics field are: false accept rate (FAR), false reject rate (FRR) and equal error rate (EER). FAR is the probability that an unauthorized individual is authenticated at a certain acceptance threshold, while FRR is the probability that an authorized individual is inappropriately rejected at a certain acceptance threshold. A false acceptance allows an unauthorized user to access high security resources. A false rejection denies an authorized user the ability to use the resources. Hypothetical distributions of FAR and FRR probabilities depend on the acceptance threshold *t*, which is used to set a desired security. The error curves in Figure 1 show that changing the threshold to decrease FAR(*t*) increases the other type of error rate FRR(*t*). Therefore if the threshold setting is increased to make the access harder for impostors, some authorized people may find it harder to gain access.

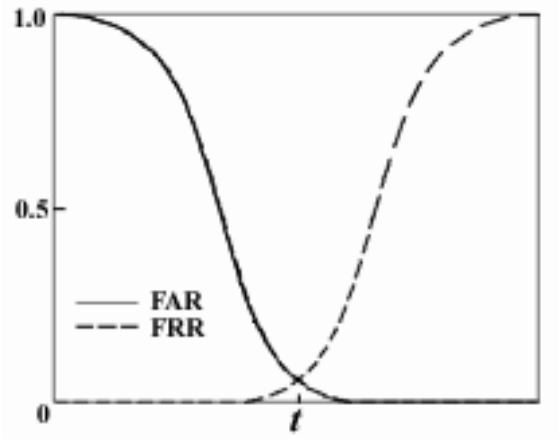

Figure 1. *Error Rates as A Function of Acceptance Threshold*

The equal error rate is the point where the FAR and FRR curves cross and may represent a more realistic measure of accuracy than either FAR or FRR taken alone. These measures are expressed in percentage, with an equal error rate of somewhere around 0.1% being a typical figure. ERR is often used as a figure of merit for a biometrics system. Sometimes it is better to set the threshold higher or lower than the EER. For example, to verify a bank safety box user, it may be better to favour rejecting a legitimate customer rather than accepting an illegitimate one. In that case, the threshold may be adjusted to have a high FRR and a low FAR.

3.3.4 Weakness of Biometrics

System reliability is critical to the success of a biometric authentication system. Unlike passwords and tokens, biometric matching cannot be 100% accurate. Instead, a biometric

authentication mechanism can only calculate the confidence level of a match to decide whether the user is who he or she claims to be. The confidence level can be adjusted based on the security level of the system. The higher the confidence level, the more secure the system, but the less convenient for the user.

A challenge for biometric authentication is user acceptance. Many users may object to the recording of personal biometric data on the basis of privacy. This is the key to a successful implementation because if the authentication method creates too many constraints, then it will be rejected.

3.4 Three factor authentication

As mentioned above, each authentication method has its own advantages and weaknesses. Passwords are difficult to control, easy to replicate, easy to guess or easy to illegally obtain. Tokens can be duplicated, lost, or stolen. Biometrics is quite expensive, it cannot be 100% accurate and may be inconvenient to the user. There is really no one best factor to authenticate users. Nevertheless, the weakness of one authentication method can be compensated for by combining other methods to form a more complicated authentication scheme. By combining different factors, authentication can be significantly strengthened.

A user gains three-factor authentication by combining a password, a token, and biometrics. If the user loses the token, the token is inoperable without the biometrics. A forged biometric is weeded out with use of the password. The following is a procedure outline of three-factor authentication. First, the user has to insert a smart card into a card reader. The smart card contains a PIN and user's biometrics template. Then, the user is asked to enter the PIN to unlock the biometrics template. Next, a specific biometric characteristic of the user has to be captured. The captured biometric information must then be converted into a template that will be compared with the template saved on the smart card. If the matching passes a confident level, the authentication is successful and finally the user can log on.

In this procedure, a higher level of security has been achieved. Even if the smart card is stolen and the PIN is uncovered, the system is still protected by biometrics. As with combining authentication factors, there are different biometric measurements to choose from, which can vary based on security levels, user friendliness and application environment.

4. Overview of Biometric Technology

When designing a user authentication system, different biometric approaches with varying levels of security must be analyzed. There are often trade-offs among biometric technologies. The question, "which is the best biometric method?" cannot easily be answered since it really depends on the application and security level involved. All methods differ in cost, convenience, security, and user acceptance. The most common biometric technologies will be introduced in the following sections. They are hand geometry, fingerprint authentication, face recognition, retinal scan, iris pattern, voice print, and signature verification.

4.1 Hand geometry

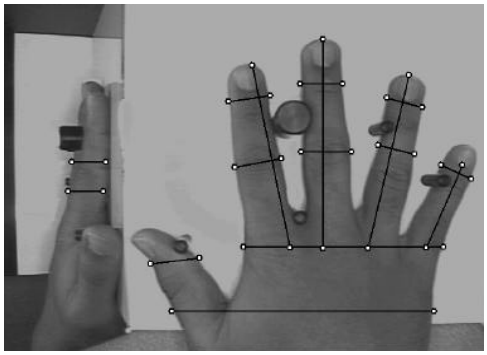

Figure 2. *Hand Geometry [13]*

Hand geometry is one of the oldest biometric technologies. In the 1960's, the first modern biometric device called the Identimat was installed at the Shearson Hamill investment bank on Wall Street [12]. As the name suggests, hand geometry involves analyzing and measuring the shape of the hand, that is, measuring the length, width, and height of a user's hand and creating a 3-D image. Infrared lights and a digital camera are used to capture hand data.

Hand geometry readers offer a reasonable level of accuracy and are relatively easy to use. The most popular usages of hand geometry include time and attendance recording, and access control. Since a typical hand geometry file requires only 9 bytes of biometrics data, it could produce many duplicates if used against a large population. Hand geometry readers are big and heavy, which limits their use in many applications.

4.2 Fingerprint authentication

Figure 3. *Fingerprint*

Fingerprints have been used for civilian identification for years because of their invariability and uniqueness. They are the most understood and extensively studied biometric measurement. A fingerprint is the pattern of ridges and furrows found on the surface of a fingertip. Most fingerprint readers will take a fingerprint image and detect interruption points of the normal flow of the ridges.

These key points are called minutiae, which are the characteristics or features used to identify the fingerprint. In automatic fingerprint recognition, the minutiae are regarded as either ridge endings or bifurcations [14] - [17]. The relative location of minutiae and the ridge count

between minutiae form the fingerprint template ranging in size from around 100 to over 1000 bytes. The reader then stores this fingerprint template, but not a fingerprint image as many people thought to be.

A greater variety of fingerprint readers are available than any other biometric equipment. They are used in different applications such as: access control, ATM transactions, computer logon, network authentication. On June 21, 2002, Federal Computer Week reported that "the Defense Department recently selected a contractor team lead by KPMG Consulting Inc. to test and evaluate biometric technologies as an added layer of security for its department wide smart card, the Common Access Card (CAC)"[18]. One problem with fingerprint technology is that a build-up of skin oils and dirt on some sensor plates can cause false rejection. Another problem is user acceptance, because fingerprints have been associated with criminal investigations and police work for ages.

4.3 Facial recognition

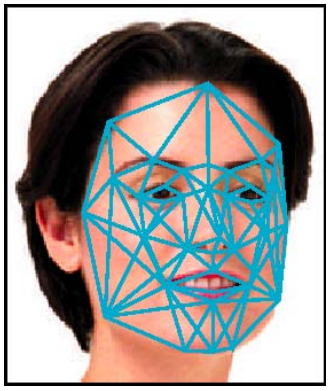

Figure 4. *Facial Image [19]*

Facial images are probably the most natural biometric measurement used by humans to make a personal identification. A typical facial recognition system captures images with a CCTV camera and processes the images using a PC, similar to a video imaging system. Facial recognition is a non-intrusive technique and people generally do not have any problem in accepting it as an authentication tool.

There are four facial recognition technologies: feature analysis, eigenface, neural network mapping, and automatic face processing. Local feature analysis is a technology that extracts dozens of features from different regions of the face and uses them as building blocks. The types of blocks and their arrangement are used to identify the face. Eigenface technology analyzes two-dimensional greyscale images to generate a space of the face with dimensions that account for face variability. A face is represented by a vector in that space [20], [21]. The neural network mapping method uses an algorithm to determine the similarity between the unique global features of a live facial image and a stored image, by learning as much about the facial images as possible. Automatic face processing tries to use individual features such as the eyes, the end of the nose and the corners of the mouth to capture and identify facial images. Most of the facial recognition technologies are designed to compensate for glasses, hats, and beards.

The template stored within a database requires approximately 1K of memory per facial template, compared with between 150K and 300K for a facial image. Facial recognition has been used in different applications. It may play a very important role in the areas such as border control and airport security in the near future. It is pointed out that "the problems of lighting and pose variation and the similarity of faces make this biometric less reliable than fingerprints" [22].

4.4 Retinal scan

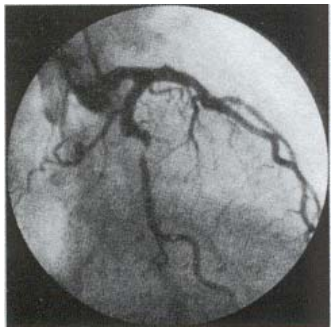

Figure 5. *Retinal Image [24]*

Retinal scanning is an old eye-related biometric measurement, which has been commercially available since 1985. The pattern formed by the layer of blood vessels on the back wall of the eye is stable and unique [23]. The image of retina can be acquired by projecting a low power infrared light against the back of the retina at close range (within 1-2 inches). A retinal scan will extract up to 192 data points. The sizes of veins, location of vein bifurcations and capillary endings form a unique set of minutiae so that the matching is similar to a fingerprint.

The template stored within a database requires approximately 100 bytes of memory per retinal image. Retinal scanning is very accurate and is currently perceived to be the most secure biometric technique. Retinal scan systems have been widely used to verify the identity of criminals when they are about to be released from prison. Retinal scanning is expensive and has a user acceptance problem because the user's eye has to be in close contact with the reading device.

4.5 Iris scan

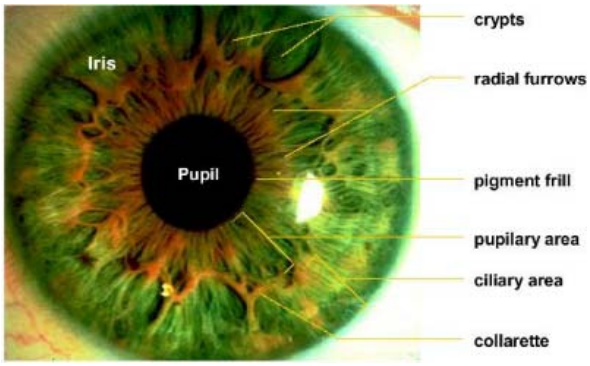

Figure 6. *Iris Image [22]*

The iris is the coloured ring of the eye surrounding the pupil. Iris scanning, while relatively new, is undoubtedly the least intrusive of the eye-related biometric measurement. It utilizes a CCD camera to capture iris image from approximately 10-20 inches away. To represent an iris pattern, a series of concentric circular zones are established, and the textural information along the circumference of each zone is extracted. Since the furrows, crypts and other structures of the iris do not change significantly through life and even irises of identical twins are different, iris scanning has the potential to achieve higher than average template matching performance [23].

The template stored within a database requires 512 bytes of memory per iris image. The real benefit of iris recognition is in the false reject rate. Fingerprint scanners have a 3 percent false-rejection rate, whereas iris-scanning systems boast rates at the 0 percent level. Because the image can be captured from several inches away, iris scan is considered much less intrusive than a retinal scan. There are few vendors to supply iris scanners, but all of them use the same algorithm licensed from IriScan Inc., which holds the worldwide patent for iris recognition technology. Since the iris is quite small, hard to find in an image, and requires precise focus, it is difficult to get a good image of the iris, especially for registration.

4.6 Voice recognition

Voice recognition is viewed by users as one of the most natural forms of biometric technology because it is not intrusive and requires no physical contact with a system reader. The voice characteristics of human speech are determined by speech pattern, which is unique for each individual [23]. These speech patterns are formed by a combination of both behavioural and physiological factors. Voice recognition systems are either text-dependent or text-independent, depending on whether specific worlds must be spoken in a fixed order or not.

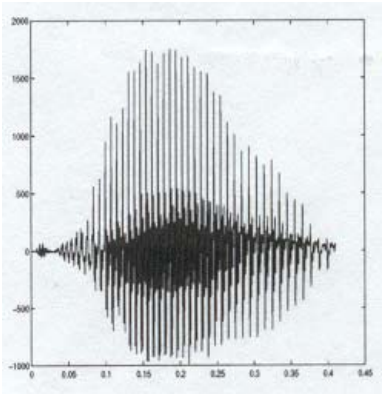

Figure 7. *Voice Print [24]*

A voice template needs 2K to 10K of memory storage varied from different applications. Generally, people are willing to accept voice-based biometric systems. However, poor quality and ambient noise, as well as the emotional and physical state of the speaker can affect the accuracy of voice recognition.

4.7 Signature verification

People have used signature for centuries to authenticate paper documents. Signature verification systems usually include a special pen and tablets. The verification can be accomplished by analyzing characteristics such as position, speed, velocity, and pressure of pen strokes [25]. Two approaches utilized in this field are static and dynamic signature verification. The static approach only analyzes the geometric features (shape) of a signature, while the dynamic approach analyzes both static and dynamic features such as speed, velocity etc. Each person has a unique style of signature and no two signatures of a person are the same. Despite the variations in an individual's signature, there have been relatively few successful signature-based applications to date in comparison with other biometric methodologies.

Figure 8. *Signature Verification [24]*

4.8 Comparison of biometric technologies

As reviewed above, every biometric technique has its own advantages and disadvantages. For example, some techniques can provide high accuracy, but may be expensive or difficult to use; some techniques require no effort to be accepted by users, but may be unable to provide enough level of security. Table 2 presents a comparison of these biometric techniques with their usage, advantages, disadvantages and cost.

Table 2. Advantages, disadvantages, usage and cost of common biometric techniques				
TECHNIQUE	ADVANTAGES	DISADVANTAGES	USAGE	COST
Hand Geometry	• Better suited for environments where dirt & nicks on the hands could cause problems with a finger scan • Minimal storage requirements • Intuitive operation	• More expensive • Less accurate than fingerprint recognition • Slow • Large system, difficult to integrate • Difficult to use for left-handers • False rejection could occur for very small or very large hands	• Time and attendance • Access control	$1,200 – $2,150
Fingerprint Scanning	• Better security than face recognition • Can accommodate cuts, etc. • Less expensive • Small • Easy to adapt to many purposes • Widely accepted	• Each finger only has 50 discriminators • False rejection could occur if oil is left from a previous user • 5% of the population cannot give a fingerprint	• Law enforcement • Corporate database	$50 – $1,200
Facial Recognition	• Video camera equipment is inexpensive and is becoming a standard in computer monitors • Unobtrusive/Passive • Allows for audits from stored face images	• Awkward lighting in the image can affect authentication • Subject to spoofing attempts	• General	$200 – $3,000
Retina Scanning	• Very accurate	• Uncomfortable for the user • User concern over infra-red or laser scanning of retina • Retina can change over a person's life • 15% of the population cannot have their retain scanned	• Prison	$5,000
Iris	• The iris remains unchanged throughout a person's life • The left and right irises are different and each iris has 170 discriminators • Very accurate • The iris's image can be captures from a distance • Reduced fraud: modification of the iris could result in the loss of vision	• More expensive • Subject to user motion • Large template • 15% of the population cannot have their iris scanned	• Access control • ATM • Airport	$200 – $3,000
Voice Print	• Less expensive • Can be used remotely (over telephone lines or a sound card) • PCs already have the necessary hardware	• Not accurate • More susceptible to rejections • Does not work in noisy environments • Can be fooled with a tape recorded voice	• Remote banking • Remote database access	$10 – $1,200
Signature Verification	• Less expensive	• Not accurate • More susceptible to rejections • More susceptible to forgery	• Industrial	$120 – $1,000
Summarized from ADVANCED IMAGE and Labcal's proposal				

From the table above, it can be seen that there is no "best" biometric technique; each has its advantages and disadvantages. The choice of biometric techniques really depends on the

authentication environments. For instance, voice recognition is perhaps the cheapest to implement, but it also is potentially the least secure. The main attraction for voice recognition is telephone applications where most of the necessary hardware is already in place, but it is not a good candidate for secure user authentication. Of all the biometric technologies, retinal scanning has been proven the most accurate biometric measurement. However, it is unacceptable to many users because it requires the user to look directly into an infrared light. Iris scanning is accurate and medium in cost compared to the other biometric technologies. The problem that bothers the users is the long-term effects of having their eyes photographed repeatedly. The risk of macular degeneration exists, and until now, there have been no studies conducted to proclaim the process safe. Although signature identification is attractive to some vendors, it is not a mature technique and is less secure and accurate than other biometric techniques at the moment.

Hand, face, and fingerprint authentication techniques are all accurate enough for most user authentication purposes. Hand geometric has been applied for physical access and attendance checking, but the requirement of bulky reader hardware makes it unsuitable for computer and network user authentication. Although facial recognition technology has been improved drastically during the past few years, the requirement of relatively even and consistent lighting conditions is still a problem. Thus, it cannot be a strong candidate for secure user authentication. This leaves fingerprint identification as the most established, reliable, and acceptable biometric technique for secure user authentication. Moreover, live fingerprint authentication has the potential to become the most pervasive biometric technique because fingerprint readers are relatively small, inexpensive, effective, and easy to embed in PC peripherals.

5. Biometrics Applications

There are many biometric applications in areas such as the military, government, business, and information security. This section will introduce some real applications.

5.1 Financial transactions

In the point-of-sale area, Bank United is the first bank in the United States to introduce Iris Recognition Automated Teller Machine (ATM). The ATM was developed by Diebold — one of the world's largest ATM manufacturers — using iris recognition products supplied by Sensar, Inc. The Iris Recognition ATMs have been placed at three Bank United branches — one in Houston, one in Dallas and one in Fort Worth — all located inside Kroger supermarket stores. Thousands of consumers are able to withdraw cash from their accounts at the ATM just by looking at it. At the ATM, the customer's iris can be captured even through glasses, contact lenses, and most sunglasses. Sensar uses, under license, the iris recognition process developed and owned exclusively by IriScan.

Bank United believes the technology is the key to the bank of the future. Robert Van Naarden, Vice President of Sales, Marketing and Customer Service for Sensar, said: "We currently have 12 pilot tests in 9 countries, including the U.S., where customers have used iris recognition to withdraw cash at ATMs and teller stations. Soon, you'll even be able to use your iris to securely buy products over the Internet. Clearly, iris recognition is becoming the global standard in personal electronic identification."

5.2 Airport security

With the ever-increasing concern for airline safety after the terrible events of September 11, governments and aviation officials are planning to use biometric recognition systems to scan passengers and airport terminals for suspected terrorists.

One good example is the Ben Gurion International Airport in Tel Aviv, Israel, one of the world's busiest air terminals. A hand geometry system, which includes 21 automatic inspection kiosks throughout the airport, is being used to identify travellers. The passengers at Ben Gurion now go through the airport's automatic inspection kiosks. During enrolment, the system captures biographic information and hand geometry data. When they arrive or depart, passengers use an ID card for initial identification, and the system verifies their identity with the hand geometry template. The system then prints a receipt to allow travellers to proceed.

Instead of using hand geometry, many airports have adopted the facial recognition techniques to enhance security. For example, Logan International Airport in Boston, Oakland International Airport in Oakland, California, and Fresno Yosemite International Airport in California installed facial recognition systems to check passengers and identify suspected criminals or terrorists whose information is already stored in a database.

In the new era of air travel, biometrics combined with smart cards are the key to making travel not only more secure, but also more convenient. In addition to an extremely high level of passenger security, this technological combination moves ticketless travel into a realm of cost savings and efficiencies that the airlines have never seen before [26]. However, the biometric technologies have to be improved before widespread implementation. There have been several complainants that biometrics misidentifies some innocent people as criminals and lets other suspected or convicted criminals slip through security checks.

5.3 Internet/information security

Using biometrics for information security has become popular as we search for more secure, more convenient and cost-effective security means. Biometric security systems solve the problem of forgotten, expired, or stolen passwords that can compromise security and increase overall network administration costs.

NASA will begin testing the Internet as a means for sending and authenticating the biometric measurement information of NASA officials who access secure network servers from remote locations. NASA's Goddard Space Flight Center in Maryland wants its technicians and scientists to be "biometrically authenticated from the road or home," said David Teitelman, president and chief executive officer of eTrue Inc., the company setting up the system.

Anyone attempting to hack into a NASA system will have his or her own biometric characteristics logged and recorded, according to Teitelman, whose company is supplying the hardware and software to build the biometrics database and will maintain the data on its servers.

What adopting biometric security does not do is strengthen the network as a whole. It improves desktop — and a certain amount of network — security. Although the true back-end security will not be altered with the adoption of biometrics, the problem of weak passwords account for a frightening number of network security exploits.

5.4 Access control

Access control appears to be one of the biggest early successes for biometrics. Hospitals use fingerprint identification for patient tracking and for access to secure areas. Disney uses hand geometry machines to verify yearly pass access. MasterCard uses fingerprint scanning to allow access into its headquarters building.

The United States Department of Defense is currently procuring biometric technology for use throughout the entire department. It is planning the Smart Access Common ID Program, which will replace the current ID cards and will eventually be used by 4.3 million U.S. military personnel. As such, fingerprint authentication will be part of this new generation of military ID badges. It adds a high level of security to the smart card and is useful for all IT security and physical access needs at the military bases.

The smart card has been designed with Java-enabled software for logon to networks, physical access, or other special applications required by the Army, Navy, or Airforce unit. The

fingerprint template has been stored in an encrypted form on the smart card that helps the users gain both security and personal integrity.

5.5 Military security

The U.S. Army is moving forward with its biometrics initiative. It is exploring whether commercial security products and services are the answers to DoD biometrics needs or not. The Army's Communications and Electronic Command Acquisition Center, Fort Huachuca, Ariz., has detailed the department's needs for biometrics hardware, software, and services. The products would secure information activities within the United States and operational zones such as Bosnia and South Korea.

All products must comply with the Biometrics Application Programming Interface standard overseen by the BioAPI Consortium. The products must also comply with the National Security Telecommunications and Information Systems Security Committee's acquisition policy that calls for DoD to give preference to products evaluated under the international Common Criteria Evaluation and Validation Scheme.

Although various biometrics authentication products exist, they are not yet good enough to work under combat conditions. Jonathan and Mathew [27] pointed out "the movement of biometrics into the mainstream is being fuelled not solely by companies' desire to improve security per se, but by the recognition that biometrics can reduce user frustration". The DoD has established its Biometrics Management Office (BMO) to ensure the availability of biometrics technologies within the Department. In addition, the DoD has set up its first biometric testing laboratory, the Biometrics Fusion Center, which will scientifically test, evaluate, and formulate recommendations for hundreds of commercial biometrics products. The goal at that Center is to determine if any of the near 600 products on the market are good enough for widespread use by Defense Department personnel for gaining access to computer networks or facilities.

6. Biometric Design Considerations

As mentioned above, there is a variety of biometric technologies, and each has its own strengths and weaknesses. One technology may be better suited than another in certain types of applications. For example, it would be a good idea using voice recognition to sign on a telephone banking customer, but a bad choice utilizing voice biometrics in a noisy environment. Indeed, there is no single best biometric technology. An application-based comparison is presented in Table 3, which compares the level of security, ease of use, accuracy, user acceptance, and environmental impact. When designing a biometric user authentication system, at least certain factors, such as security level required, accuracy, cost and user acceptance have to be considered.

Table 3. Application-based comparison

CHARACTERISTIC	HAND	FINGER	FACE	RETINA	IRIS	VOICE	SIGNATURE
Security level	Medium	High	Medium	Excellent	High/Exc	Low	Low
Unique Identifiers	96	30 - 90	~ 128	~ 192	266 - 400	6 frequencies	~ 10 variables
Template Size (bytes)	9	100 – 1000	84 – 1300	96	512	2,000-10,000	…
Accuracy (relative)	High	High	High	Excellent	High/Exc	Medium	Medium
Ease of Use	High	High	Medium	Low	Medium	High/Exc	High/Exc
Ease of Enrolment	High	Medium	Medium	Low	Low/Med	High	High/Exc
Ease of Integration	High	High	High	High	High	High/Exc	Excellent
Speed (relative)	Excellent	High	Medium	High	High	High	High
Cost	Medium/Hi	Low/Med	Medium	High	Med/Hi	Low	Low/Med
Environmental Affects	None	Temperature, Moisture, Dirt	Lighting, Position	None	None	Noise, Acoustics	None
Physical Contact	Bulky	Clean surface	None	Light source	None	None	None
Human Factor Limitations	Missing fingers, Too small or too big hand	Worn fingertips	Beards, Skin tone, Cosmetics	None	Blind	Emotional state	Emotional state
Mature Technology	Yes	Yes	Yes	Yes	Yes	No	No
User acceptance	Medium/Hi	Medium	Medium/Hi	Low/Med	Medium	High	Medium/High
Long-term stability	Medium/Hi	High	Medium	High	High	Medium	Medium
Summarized from Biometrics Market Intelligence							

6.1 Level of security

When implementing a biometric authentication system, the selection of biometric technology must be based on the level of security required. For example, a device connecting with a classified database should have an extremely high level of security — even at virtually high cost — and users of the system should be willing to tolerate some inconvenience. However, a device protecting a regular network requires a high level of user convenience, and a certain level of security could be traded for a lower cost.

It is an organization's responsibility to decide the right level of security required for the specific application: low, moderate, or high. This decision will greatly influence which biometrics are most appropriate. Generally, physiological biometric traits are stable and therefore offer a higher level of security than behavioural biometric traits.

6.2 Accuracy

Every biometric system has a certain percentage of errors, either in the form of a false rejection or a false acceptance. As mentioned in 2.3.3, biometric accuracy can be evaluated by: false accept rate (FAR), false reject rate (FRR) and equal error rate (ERR). Most people consider it important to keep the "bad guys" out, so a low FAR is preferred. Consequently, this leads to a high FRR making it harder for the "good guys" to get in, when frequent rejections might be unacceptable. Fortunately, FAR and FRR can be adjusted to compensate while giving an acceptable level of system accuracy and user convenience. Because FAR and FRR are interdependent, we must be careful to understand exactly how vendors arrive at quoted values of FAR and FRR.

6.3 Cost

The cost is always an important issue when implementing a new technology. While examining the cost of a biometric application, people often focus on just the cost of the capture hardware (sensor) and matching software (algorithm). However, the actual cost of implementing any of biometric technology goes far beyond these basic elements [28]. It is associated with installation, integration, administration, user education, data collection, and system maintenance.

Biometric capture hardware cost: comparing the prices of different sensors and evaluating the costs of different biometric technologies.

Processing power cost: including the computer systems, software, database, and possibly smart card.

Integration cost: integrating a biometric with existing or new applications.

Installation cost: mounting devices, connecting networks, and varying hardware and operating system configurations.

Research and testing cost: requiring special laboratories, trained personnel, and specialized equipment.

Training cost: designing and running a training program that will not only teach users using the biometric, but also answer their questions on privacy and general operations.

Maintenance cost: including technical support, help desk and system upgrades.

It is essential to build a solid business case for a biometric application that considers the real cost of the system rather than concentrating on one or two areas.

6.4 User acceptance

To make the system successful, it is important to consider the user resistance, such as fear of technology, invasion of privacy, etc. Privacy advocates worry about the potential for mislaid biometric information and the danger of user profiles being assembled and sold. Putting privacy concerns aside, the cooperation of the user can have an impact on performance. The attitude of the users towards the intended biometrics can make or break the implementation of a biometric system. The acquisition method for capturing biometric samples will also influence user acceptance. For example, many users feel uncomfortable with retinal scan because it requires them to place their eyes a few inches from an infrared beam. Generally, less intrusive biometric systems requiring less user effort have greater user acceptance.

An education program can help users accept authentication by biometrics. Users should be provided with information and training on the biometric technology and privacy policy, so they have a chance to become familiar with biometrics before the system is implemented.

6.5 Threats

Even if biometric authentication technologies are much safer than the other authentication technologies, threats still exist. There are some common threats against biometric authentication technologies. The threat agents may be either unauthorized users (impostors) or authorized users.

An impostor may make a zero-effort forgery attempt to impersonate an authorized user. The chance of such an attack being successful is measured by the FAR of the device. For instance, the attack may be successful if the system has a high FAR, or the impostor has a close biometric template with an authorized user.

An impostor may be able to reproduce the biometric characteristics by making artificial handprints or fingerprint, changing his or her voice, forging a signature, etc. This threat represents an attack, which is related to the biometrics capture device. The impostor may practice mimicry of the biometric characteristics to generate an accepted biometric sample.

The threats posed from inside by authorized users include users attempting to exceed their authentication level and administrators misusing their authority. “While the threat agent and attack type varies for different threats, the motivation is generally the same — to gain illegal entry to the portal controlled by the biometric system, and in turn the assets contained there in or to deny entry to legitimate users” [29].

There has yet to be a physical or cyber security system that any security specialist would say is foolproof, or hacker-proof, biometric systems are no exception. Regardless, using biometrics can provide an additional level of security and help significantly reduce overall risk to the current authentication systems.

6.6 System solution

Based on the previous analysis and discussion, this section presents a system infrastructure for three-factor authentication in order to provide a secure IT environment with cryptographic strategies. Since the biometric characteristics are represented by templates, and the templates are sent to and from computer networks, designing a system infrastructure is only half the battle. It is also necessary to consider where the biometric templates should be stored and what impact template security will have on the network.

6.6.1 Storage of biometric data

After a biometric system is selected for authentication solution, the next step is to figure out how and where to store the biometric templates. This is both a security and protection issue. There are four levels of storage: Clear, Encrypted, Hidden-Clear, and Hidden-Encrypted. In the past, most of the vendors saved templates in the clear so that the attacker could easily uncover the content of templates simply by getting the template files. This also allowed attackers to easily inject unauthorized templates that enabled them to gain access to the protected network, system, or application. In order to secure the templates, cryptographic technology, such as Public Key Infrastructure (PKI), can be adopted. Biometric templates can be digitally signed and stored as encrypted files. In that way, the integrity and authenticity of biometric information can be maintained. To make it even more difficult to attack biometric templates, a hidden folder can be created making it and its contents invisible. For all practical purposes, the folder does not exist and other users of the system will not even know it is there.

Generally, there are three places for storage: templates can be saved on a biometric reader, saved on a token, or stored in a centralized database. Storing the template locally decreases processing time, but the user is tied to that specific reader. This can be inconvenient for many users who have to access the network from machine to machine. Using tokens gives the user portability, but if the token is lost or stolen, the user must re-enrol, which can be a costly, time-consuming process. A centralized database is easy to deploy and offers complete mobility, but will add a substantial amount of traffic to the network.

6.6.2 Secure communication

The information being sent through the network is convenient for users and cyberthieves alike. A problem exists if biometrics can be spoofed by hackers. Because the biometric templates will be transmitted over a network, attacks could involve the interception of biometrics data and replay the data to access a security system or network later on. How this can be done depends on how the biometrics data is transmitted on the network. Encryption of any user data moving over the network is a standard solution to this problem.

Encryption provides a way to incorporate biometrics into the modern world of network computing. A basic strategy for cryptographically protecting biometric data is demonstrated as follows. The biometric device collects data and cryptographically protects the data. The device resides within a physically protected environment and uses a base secret to protect the data before and during transmission through the network. The receiver uses its own copy of the base secret to decrypt and verify the biometric data. For example, PKI can provide cryptography-based security services to network applications and services.

6.6.3 System architecture

Based on the above, a system architecture for trusted authentication, in high security applications, is proposed as follows. In order to protect highly sensitive information, three-factor authentication has to be adopted because it supplements two-factor authentication [1], [2]. The password is the basis of this solution (Section 3.1). The smart card is selected to represent the possession factor because it is superior to the other kinds of tokens (Section 3.2.3). According to the comparison of biometric technologies (Section 4.8), the most suitable biometrics technology for three-factor authentication is fingerprint identification.

Because authorized users cannot change their biometrics, not only the authentication system, but also the data transmitting must be carefully designed so as not to expose biometric data to unsecured environments.

Figure 8 shows the architecture of proposed three-factor authentication system. Its logon procedures are explained as follows:

1. Insert a smart card into a card reader. The smart card contains cryptographic keys and the user's fingerprint template.

2. Enter user PIN to unlock the fingerprint template stored in the smart card.

3. Place finger on the authentication device to generate a live-scan fingerprint.

4. The device compares the live fingerprint with the fingerprint template.

5. If the data matches, the smart card fingerprint data is converted into a number and combined with the smart card secret PIN, then used as a symmetric cryptographic key to decrypt the private key.

6. A nonce (random number) is passed from the server to the smart card.

7. The private key on the smart card is used to encrypt the nonce and pass it back to the server.

8. The server uses a certified public key to decrypt the encrypted message from the card.

9. If the same nonce that was originally passed to the card is revealed, then a connection is set up.

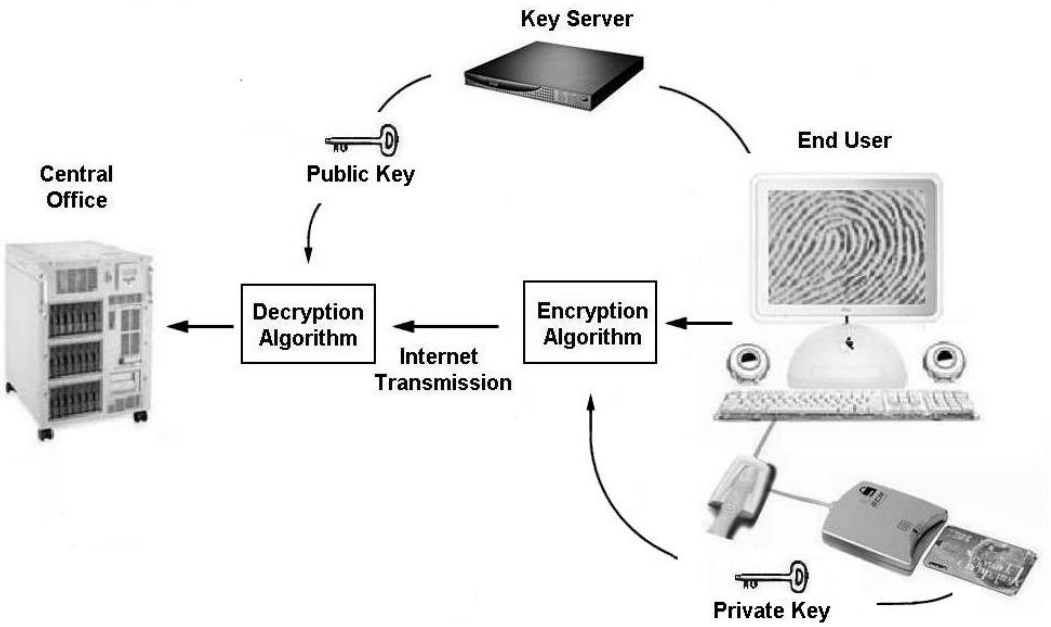

Figure 9. *Trusted Authentication system*

Not only does the above process authenticate the person presenting the card as the same person to whom the cryptographic keys belong, but also it preserves the privacy of user's biometric information.

7. Conclusions

This report addresses the importance of user authentication in modern society. With the progress of telecommunication and network technology, the technology of user authentication must be improved to secure sensitive information. The common problems and weaknesses of the current user authentication approaches are discussed in this report in order to indicate the necessity of new authentication solutions.

With more and more organizations interested in three-factor authentication, the technology will get more accurate and less expensive. For example, vendors are already offering keyboards, mice, and laptops with inexpensive biometrics readers. Some common applications are introduced in this report to demonstrate the applicability and potential of biometrics.

In a security sensitive environment, three-factor authentication might be adopted even if it would cost more money and require personal effort. Every time a factor is added, the security can be increased dramatically. In this report, different biometric technologies used to enhance authentication have been evaluated to be able to find the most suitable authentication solution. Note that in a military application, the right choice must be based on heightened security. It is the most important concern of this report.

As discussed, one of the challenges for using biometrics authentication is user acceptance. This is the key to a successful security implementation because until now most of the applications required user cooperation. Eventually, users will find it much easier to use a biometric reader than to try to remember which password goes with which system. With biometric authentication, they can replace the passwords with a biometric measurement and have one-scan access to all of their authorized resources.

8. References

1. Smith, R. E. (2001). Authentication: from passwords to public keys. Addison-Wesley Longman, Incorporated, p 549.

2. Dale, R. Biometric security. (Online) *Dr. Dobb's Journal*. http://www.biometricgroup.com/a_press/Dr.Dobbs_Journal_Nov2001.htm (Nov. 2001).

3. Jones, J. DOD to pair biometrics and smart cards. (Online) *Federal Computer Week.* http://www.fcw.com/supplements/homeland/2002/sup2/hom-bio1-06-24-02.asp (June 2002).

4. Andress, M. Authentication. (Online) TechTarget Network. http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci784350,00.html (Dec. 2001).

5. Saito, W. (Oct. 2000). Biometrics — understanding the architecture, API's, encryption and authentication security for integration into existing systems & applications. (Online) *Proceedings of the 23th National Information Systems Security Conference.* Baltimore, MD. http://csrc.nist.gov/nissc/2000/proceedings/papers/305slide.pdf

6. van Eck, W. (1985). Electromagnetic radiation from video display units: an eavesdropping risk? Leidschendam, The Netherlands: PTT Dr. Neher Laboratories.

7. About USB smart tokens and smart cards. (Online) Rainbow Technologies. http://www.rainbow.com/ikey/index.html (Dec. 2001).

8. Anderson, R. and Kuhn, M. (1996). Tamper resistance - a cautionary note. Computer Laboratory, Cambridge University, and Department of Computer Sciences, Purdue University.

9. Radcliff, D. Busted! (Online) *Computer World.* http://www.idg.net/english/crd_biometrics_194585.html (Dec. 1998).

10. Thalheim, L., Krissler, J., and Ziegler, P. Body check. (Online) *C'T Magazine*, 11, 114. URL: http://www.heise.de/ct/english/02/11/114/ (May 2002).

11. New technology solution detects even the "gummy finger". (Online) SecuGen Biometric Solutions. http://www.secugen.com/company/doc/02detection.htm (May 2002).

12. Davis, A. The body as password. (Online) *Wired Magazine.* http://www.wired.com/wired/5.07/biometrics_pr.html (July 1997).

13. Jain, A. K., Rose, A., and Pankanti, S. (Mar. 1999). A prototype hand geometry-based verification system. In *Proceedings of Audio- and Video-Based Personal Identification (AVBPA-99),* 166-171. Washington D.C.

14. Pernus, F., Kovacic, S., and Gyergyek, L. (Dec. 1980). Minutiae based fingerprint recognition. In *Proceedings of the 5th Int. Conf. Pattern Recognition*, 1380-1382. Miami, Florida.

15. Kawashima, M. and Kiji, K. (1984). Personal identification by fingerprint or palm-print. *Information Processing*, 25, 599-605.

16. Xiao, Q. and Bian, Z. (Oct. 1986). An approach to fingerprint identification by using the attributes of feature lines of fingerprint. In *Proceedings of the 8th Int. Conf. Pattern Recognition*, 663-665. Paris.

17. Xiao, Q. and Raffat, H. (1990). Combining statistical and structural information for fingerprint image processing, classification and identification. In R. Plamondon and H. Cheng, (Ed.), *Pattern recognition: architectures, algorithms and applications*, pp. 335-354. Singapore: Worlds Scientific Publishing Co. Pte. Ltd.

18. Caterinicchia, D. Team to test CAC biometrics. (Online) *Federal Computer Week.* http://www.fcw.com/fcw/articles/2002/0617/web-cac-06-21-02.asp (June 2002).

19. Face recognition systems. (Online) Omron Technology. http://www.society.omron.com/faceid/tech/index.html.

20. Kirby, M. and Sirovich, L. (1990). Application of the Karhunen-Loève procedure for the characterization of human faces. *IEEE Trans. Pattern Anal. Mach. Intell.*, 12, 831-835.

21. Hill, R. B. (1978). Apparatus and method for identifying individuals through their retinal vasculature patterns. US Patent No. 4109237.

22. Dawson, B. (2001). Biometrics measures physical traits. *Vision Systems Design*, 3, 25-30.

23. Daugman, J. G. (1993) High confidence visual recognition of persons by a test of statistical independence. *IEEE Trans. Pattern Anal. and Mach. Intell*., 15, 1148-1161.

24. Jain, A. K., Hong, L., and Pankanti, S. Biometrics: promising frontiers for emerging identification market. (Online) Connecticut Department of Social Services. http://www.cse.msu.edu/cgi-user/web/tech/document?ID=436 (Feb. 2000).

25. Nalwa, V. (1997). Automatic on-line signature verification. *Proc. IEEE*, 85 (2), 213-239.

26. A sense of place. (Online) Tourism Industry Association of Nova Scotia. http://www.tians.org/advocacy/airport.html.

27. Gossels, J. G. and Martin, M. Should you care about biometrics? (Online) System Experts. http://www.systemexperts.com/tutors/biometrics.pdf (2001).

28. **Polemi, D**. Review and evaluation of biometric techniques for identification and authentication - final report. (Online) *INFOSEC*. http://www.cordis.lu/infosec/src/stud5fr.htm (May 1999).

29. Biometric system protection profile for medium robustness environments. (Online) U. S. Department of Defense Biometrics Office. http://www.iatf.net/protection_profiles/biometrics.cfm (Mar. 2002).

DOCUMENT CONTROL DATA

(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)

1. ORIGINATOR (the name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g. Establishment sponsoring a contractor's report, or tasking agency, are entered in section 8.)

Defence R&D Canada - Ottawa
Ottawa, ON K1A 0Z4

2. SECURITY CLASSIFICATION (overall security classification of the document, including special warning terms if applicable)

UNCLASSIFIED

3. TITLE (the complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S,C or U) in parentheses after the title.)

Trusted User Authentication Using Biometrics (U)

4. AUTHORS (Last name, first name, middle initial)

Xiao, Qinghan

5. DATE OF PUBLICATION (month and year of publication of document)	6a. NO. OF PAGES (total containing information. Include Annexes, Appendices, etc.)	6b. NO. OF REFS (total cited in document)
NOVEMBER 2002	41	29

7. DESCRIPTIVE NOTES (the category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Technical Memorandum

8. SPONSORING ACTIVITY (the name of the department project office or laboratory sponsoring the research and development. Include the address.)

Information Operations Section
DRDC - Ottawa

9a. PROJECT OR GRANT NO. (if appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant)	9b. CONTRACT NO. (if appropriate, the applicable number under which the document was written)
15bf27	

10a. ORIGINATOR'S DOCUMENT NUMBER (the official document number by which the document is identified by the originating activity. This number must be unique to this document.)	10b. OTHER DOCUMENT NOS. (Any other numbers which may be assigned this document either by the originator or by the sponsor)
DRDC - Ottawa TM 2002-122	

11. DOCUMENT AVAILABILITY (any limitations on further dissemination of the document, other than those imposed by security classification)

(X) Unlimited distribution
( ) Distribution limited to defence departments and defence contractors; further distribution only as approved
( ) Distribution limited to defence departments and Canadian defence contractors; further distribution only as approved
( ) Distribution limited to government departments and agencies; further distribution only as approved
( ) Distribution limited to defence departments; further distribution only as approved
( ) Other (please specify):

12. DOCUMENT ANNOUNCEMENT (any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in 11) is possible, a wider announcement audience may be selected.)

13. ABSTRACT (a brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual).

User authentication is the process of confirming one's identity by checking one's credentials. It is a cornerstone of information security. Traditionally, users access information systems by applying something they know, such as passwords, or something they possess, such as tokens. A third method, biometrics is based on something users are, such as fingerprints. Nowadays, to protect sensitive information, these methods are deployed together to form a strong three-factor authentication.

This report presents an overview of different authentication factors, analyzes their advantages and disadvantages, and indicates the common problems facing each factor. Since there are various biometric technologies, each with its own strengths and weaknesses, this report discusses only the most popular biometric technologies in detail. The purpose of this report is to position biometrics in user authentication to enhance information security. As a result, a system architecture is presented to provide a solution for information protection in secure or sensitive environments.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus. e.g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus-identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

User Authentication, Biometrics, Information Security, Access Control, Security and Privacy

Defence R&D Canada

Canada's leader in defence
and national security R&D

R & D pour la défense Canada

Chef de file au Canada en R & D
pour la défense et la sécurité nationale

www.drdc-rddc.gc.ca