Evaluating the reliability of commercially available biometric devices

V. Dimopoulos, J. Fletcher, S.M.Furnell

Network Research Group, Department of Communication and Electronic Engineering
University of Plymouth, Plymouth, United Kingdom
E-mail: info@network-research-group.org
Web: www.network-research-group.org

KEYWORDS
Biometrics, authentication, security.

ABSTRACT

The need for secure and accurate authentication at the entry point of every network is becoming increasingly evident. This paper considers commercial-grade biometric technologies and investigates whether their performance is sufficient to warrant their use as replacements for current user authentication methods. For this purpose, a variety of commercial-grade biometric devices were tested and their characteristics (mainly their accuracy) were assessed. From this assessment, optical fingerprint technology proved to be generally the most reliable while other techniques (such as thermal fingerprint scanning and voice verification) demonstrated good performance characteristics; although they were subject to a number of false rejections, they still did not tolerate any impostor access the network. Keystroke analysis, face recognition and dynamic signature verification all displayed average performance characteristics, with occurrences of false rejections as well as false acceptances.

INTRODUCTION

The rapid evolution of e-commerce and of the Internet has meant that networks previously inaccessible by most people can now be accessed on-line. This has introduced a variety of new security vulnerabilities, and increased problems like hacking, identity theft, malicious impersonation and data theft [Furnell 2001]; subsequently it introduced a requirement for better network security.

First in the procedure of securing a network is strengthening the point of entry by providing secure and reliable authentication. There are three common ways to verify the identity of an individual who is attempting to access valuable company assets, sensitive data and private/personal information [Smith 2002]. The first is by verifying something that ideally only the legitimate user **knows**, for example a password or a PIN. However this sort of information is often vulnerable to becoming compromised, as it can be guessed, shared or written down. [Monrose et al 1999]. A second method of authenticating someone's identity is by making use of something that ideally only this user **has** possession of. This can be for example an electronic identity card or some other form of physical token. This method however still has the disadvantage that the token can be shared or even stolen, and non-legitimate users can gain unauthorised access to the protected resources. Finally, the third method of authenticating someone's identity is provided by biometrics. This method uses something that the user **is** to verify an identity. As their definition indicates, *biometrics is the automated use of behavioural and physiological characteristics to determine user identity* [Dye et al 2001]. A person's behavioural characteristics are the way he signs, talks or even types a sentence, whereas the shape and features of a users' face, fingerprint or eye, hand can be categorised as physiological characteristics. The concept of identifying someone by utilising these characteristics is not new; human beings have the ability to identify each other by simply looking at a face or hearing a voice, while there are reports of signatures and fingerprints being used as a means of identity verification from as early as the 14th century [Novell 2001].

The basic principles of operation are similar for all biometrics. There are essentially two stages: the first is the registration of a user with a device and the creation of an individual biometric template and, from then on, the second stage is the verification/identification of a users' claimed identity, by comparing an acquired sample against the template already held.

Using a biometric based authentication method introduces a number of advantages; in verification systems, none of the measured characteristics can be stolen, forgotten or shared, resulting in an approach that is theoretically more secure, and also more convenient, since the user does not need to remember long passwords.

However, despite these advantages biometrics have yet to become widespread in commercial everyday applications. In fact according to a CSI/FBI survey biometrics are only being used in 10% of computer systems [Power 2002]. The aim of this paper is to investigate the reasons why, in spite of all their inherent advantages, biometrics have been largely confined within the environment of labs and test facilities. This is established by evaluating the performance criteria of the different biometric techniques in order to assess whether they can reliably find applications in authentication.

BIOMETRIC ASSESSMENT CRITERIA

There are many different biometrics techniques available today. Some are commercially available and others are still at a research level. The commercially available biometric products that were obtained and evaluated for the purposes of this investigation are based on the following techniques:

- Fingerprint Verification: This is a method of authenticating a person's identity by obtaining an image of their fingerprint.
- Facial Recognition: As the name suggests this technique authenticates someone by obtaining a picture of the persons' face and comparing it against a reference profile it has stored in its database to determine if there is a match or not.
- Keystroke Analysis, is a biometric technique that analyses the way a user types words on a keyboard or keypad in order to identify characteristic rythms.
- Dynamic Signature Verification: this biometric method utilises distinctive characteristics in the way a user signs to authenticate a claimed identity.
- Speaker Verification: this technique is based on the analysis of certain unique characteristics of a person's voice that can be used to establish an identity.

There are several major criteria upon which biometric techniques and products can be judged. Primarily these are a technique's technical, operational and economic characteristics, as well as the level of support provided by the manufacturer [Polemi 1997].

The main technical characteristic of a biometric is its accuracy (i.e. the rates of false acceptances and false rejections that a device is capable of accomplishing) so that it can achieve the required security levels. The operational criteria are for it to be convenient to use (ease of use, speed of enrolment and authentication), acceptable to the public by not being invasive and independent of any influences to its performance by the environmental conditions. The economic aspect of a biometric is its purchase, licensing, installation and staff training costs. For this investigation however the devices under test were chosen to be from the lower-cost end of the market (under £150 per unit). What this selection aims to achieve is to make this assessment more realistic to the majority of companies that are relatively satisfied with the security they have achieved (with minimum costs) with passwords and do not have a huge budget to spend for increasing security.

INVESTIGATION OF BIOMETRIC TECHNOLOGIES

The experimental procedure followed in this investigation involved registering a set of users with the devices, who firstly attempted to access their legitimate accounts (so that the False Rejection Rate can be calculated) and subsequently attempted to 'fool' the devices and gain access to each others' accounts (so that the False Acceptance Rates for the techniques can be evaluated).

Fingerprint scanning (physiological)

Fingerprints are recognised to have distinctive characteristics, which has led to their use in various criminology applications throughout the world to identify individuals. There are several techniques for scanning a fingerprint to extract those features that can be used for successfully identifying an individual; namely, optical, silicon, ultra-sound, and thermal technology [IBG 2002]. For the purposes of this investigation tools based on the optical and the thermal were tested.

Among the advantages of this technique, is the fact that it is proved to be capable of reliable identification of individuals. Also, many of the fingerprint sensors are of small size and minimum power requirements, which allows them to be integrated into other hardware such as keyboards and mice. The biggest disadvantage for this technique is the requirement for the purchase of a specialised reader; this elevates the costs of deployment for finger scan.

Technical: Optical finger scan
Optical technology is the most mature and commonly used finger scan technology. It is based on the use of a scanner (essentially a camera) that records images of fingerprints held against a coated glass or a plastic platen, which are then transformed into a template by the underlying software. [Ndlangisa 2001]. For the accuracy assessment of this method seven users enrolled four fingers each and followed the experimental procedure described earlier. The results are in table 1.

Security level	False Rejection Rate	False Acceptance Rate
1 (Low)	4/105 = 3.8%	0/90 = 0%
2 (Medium)	4/105 = 3.8%	0/90 = 0%
3 (High)	5/105 = 4.7%	0/90 = 0%

Table 1: Accuracy of optical finger scan

Thermal finger scan
The second method evaluated is based on capturing a full size image of a fingerprint by sweeping the finger over a thermal CMOS sensor. This technique uses infrared to measure the minimal temperature differences between the ridges and valleys of the users' heated finger. [Smallback 2002]. Seven users registered four fingers with the device and the accuracy results for the experiment are displayed in table 2.

FRR	FAR
45/180 = 25%	0/1260 = 0%

Table 2: Thermal finger scan accuracy

Operational
As far as the operational aspect of fingerprint scanning is concerned, the optical method's ease of use, good speed of enrolment (approximately 15 seconds) and authentication (approximately 3 seconds) favoured it considerably. The thermal finger scanning method took a significant amount of time to enrol and authenticate a user because of unsuccessful scanning attempts (i.e. failure to acquire a sample). This made it slightly inconvenient to use. When tested under changing environmental conditions, i.e. various temperatures, the thermal sensor did not suffer any effect from temperature variations and the optical sensors' performance was not influenced when in a poorly lit environment. It was however degraded when under extreme light.

Facial recognition (physiological)
Another method of biometric authentication is by measuring and comparing unique features that exist in peoples' faces such as the distances between the eyes, the nose and the mouth. Several methods have been developed to scan a face, the most common being eigenfaces, feature analysis, neural networks and automatic face processing [facial-scan.com 2002]. For the purposes of this assessment, a product that uses a neural network technique was selected and tested.

Advantages of this technique are its ability to integrate with existing imaging equipment (e.g. webcams) and its ability to obtain the required images transparently i.e. without disrupting the user. As a disadvantage, however, its performance can be degraded by poor background lighting, as well as by the users' positioning against the camera.

Technical
Neural network systems use algorithms to determine the similarity between an 'on the spot' image of a user's face with the one that was stored during registration. Neural network systems are capable of learning and adjusting themselves over time according to which features they judge to be more effective for matching [Nanavati and Thieme 2002]. The product tested determines the degree of similarity between the acquired and stored images on a scale from 1 to 10. The security administrator can then set the threshold, essentially the minimum degree of similarity that would still allow a user access to the system, according to the requirements of an application. Table 3 illustrates the accuracy of this similarity rating. Essentially, if the strictness threshold is set at 5 (which is the manufacturers default setting), then the FRR for this method is 46% while the calculated FAR for this technique at the same security setting reaches 3%.

User	Attempt 1	Attempt 2	Attempt 3	Attempt 4	Attempt 5	Attempt 6	Attempt 7	Attempt 8	Attempt 9	Attempt 10
A	3.82	5.67	5.21	4.17	7.86	6.21	7.12	5.65	4.69	4.89
B	5.96	7.43	5.32	2.35	5.61	5.23	3.34	6.16	2.72	4.63
C	7.52	6.31	8.14	4.23	3.24	3.51	4.84	2.56	6.51	5.42
D	5.83	5.39	7.25	4.59	3.32	5.38	7.31	3.46	5.92	5.83
F	3,76	4.69	6.28	4.62	4.83	5.93	2.89	8.12	4.35	4.17

Table 3: Degree of match between acquired and stored sample as evaluated by the facial scan device

Operational

When evaluating the operational aspects of this technique, it demonstrated a good ease of use characteristic, an average speed of enrolment (approximately a minute) and good speed of authentication (around 15 seconds) although there was some negative feedback by those subjected to the test on the functionality of its interface with the user. When tested with the users wearing glasses or growing facial hair the technology appeared to be unaffected and displayed fairly similar results. Varying background lighting however did have an effect in increasing the devices' False Rejection Rate. This device was also fooled by a photograph and granted access to the impostor almost 50% of the attempts.

Keystroke analysis (behavioural)

This technique is based on the concept that every user types characters on a keyboard or keypad in a distinctive way. Consequently it verifies a claimed identity by analysing the users' typing patterns. There are several data acquisition techniques, and different typing metrics, upon which keystroke analysis can be based. Specifically it can be static at login, periodic dynamic, continuous dynamic, keyword specific and application specific [Dowland et al 2002]. The device under testing in this investigation is based on the static at login approach (which means that the technique is applied when users enter their username and password, and the system looks not only at what they typed, but how they typed it). The advantages offered by this technique are firstly the combination of the knowledge of secret information (password) with a biometric to increase the security levels, and secondly that there is no need for the purchase of any additional costly hardware. A disadvantage is that it does not improve user convenience since the user still has to remember this secret information, and also that authentication occurs as a one-off judgement (unlike the case of the continuous dynamic technique for example).

Technical

The keystroke analysis product under test offers the option for the administrator to set the security level (from 1 to 10) that is most appropriate for a specification. In theory, setting the security level higher should reduce the false acceptance rates but simultaneously increase the false rejection rates. The recommended minimum password length to be used for optimal results is eight characters. To assess the false rejection characteristic for this technique, seven users were enrolled and they all attempted to access the system ten times on each security setting and for various password lengths as illustrated in the table below:

Password length / Security setting	4	5	6	7	8	9	10
1	0%	0%	0%	10%	0%	0%	10%
2	0%	0%	10%	10%	0%	10%	10%
3	0%	0%	20%	20%	0%	0%	0%
4	0%	10%	20%	20%	10%	0%	10%
5	10%	30%	30%	30%	30%	40%	30%
6	10%	30%	20%	30%	40%	20%	40%
7	30%	40%	30%	30%	40%	50%	40%
8	40%	50%	50%	50%	40%	70%	40%
9	50%	70%	60%	80%	50%	70%	50%
10	70%	90%	70%	70%	70%	90%	80%

Table 4: Keystroke analysis FRR

The calculated results for the False Acceptance Rates of the keystroke analysis technique are displayed in table 5. From these last two tables it can be gathered that when operating at the default security level 5, the average False Rejection Rate for this device is 28.5% while the False Acceptance Rate is 14.7%.

Password length / Security setting	4	5	6	7	8	9	10
1	93%	80%	80%	86%	83%	72%	60%
2	91%	53%	68%	51%	78%	53%	51%
3	83%	23%	51%	35%	58%	33%	18%
4	71%	11%	25%	20%	25%	15%	8%
5	66%	5%	6%	5%	15%	3%	3%
6	48%	0%	2%	0%	6%	0%	2%
7	23%	0%	0%	0%	3%	0%	0%
8	11%	0%	0%	0%	0%	0%	0%
9	5%	0%	0%	0%	0%	0%	0%
10	5%	0%	0%	0%	0%	0%	0%

Table 5: Keystroke analysis FAR

Operational

From the operational point of view, this technique is characterised by low speed of enrolment, which can be from 3 to 5 minutes, as it requires the user to re-type the username and password several times so that the device can 'learn' the users' typing patterns. The speed of authentication is exclusively dependant on the users' typing speed and length of username and password. This technique's performance does not suffer during environmental changes due to its software-only nature but factors such as fatigue and injury could affect the user's performance.

Dynamic signature recognition (behavioural)

This type of technology is based on authentication through the analysis of distinctive characteristics in someone's' writing, and particularly the way a user produces a signature [The biometrics institute 2002]. It is one of the most widely acceptable biometrics since the majority of users are already accustomed to using their signature to authorise transactions and to verify their identity.

The examination of a user's signature is achieved either by the statistical analysis of characteristics such as the duration, pressure and acceleration of the signing or by a sequential method where the signature is uniformly divided and each piece is examined individually.

The products based on this technique can be either pen based (the mechanism that captures the information is a specialised pen) or tablet based (a writing tablet with a special surface that collects the data). This technology can find applications for accessing personal computers, PDA and for authorising transactions over the Internet [CIC 2002]. While the advantages of this technique can be considered to be its low price and availability for direct purchase and download over the Internet, disadvantages are that users can find it inconvenient to sign accurately on a pad and that false rejection rates increase with inconsistent signatures.

Technical

For this investigation a tablet was used as the acquisition mechanism for a verification program that analyses both the sequential stroke patterns and the timing elements of a signature. The accuracy results for the false acceptance characteristics came after enrolling eight users and three additional "simple" signatures and attempting to forge the legitimate signatures twenty times and are illustrated in table 6. The average rate of false rejections according to these results is 2.5%, and the average percentage of false acceptances is 2.5% as well.

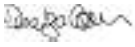
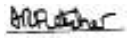
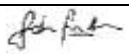
Signature samples	User A Posing as	FAR	User H Posing as	FAR	User D Posing as	FAR	User G Posing as	FAR
A 	-	-	A	20%	A	0%	A	20%
B 	B	5%	B	0%	B	0%	B	5%
C 	C	0%	C	0%	C	0%	C	5%
D 	D	0%	D	0%	-	-	D	0%
E 	E	5%	E	0%	E	0%	E	10%
F 	F	0%	F	5%	F	0%	F	0%
G 	G	0%	G	0%	G	0%		-
H 	H	0%	-	-	H	0%	H	5%
	Simple 1	45%	Simple 1	100%	Simple 1	15%	Simple 1	80%
	Simple 2	85%	Simple 2	90%	Simple 2	35%	Simple 2	60%
	Simple 3	90%	Simple 3	90%	Simple 3	45%	Simple 3	50%

Table 6: False acceptance assessment for signature verification

To observe the false rejection characteristics of this technique six registered users attempted verification twenty times. The results are exhibited in table 7 below.

User	Successful Attempts (out of 20)	FRR
A	20	0%
B	20	0%
C	20	0%
D	19	5%
E	20	0%
F	19	5%

Table 7: FRR for signature scan.

Operational
The ease of use of dynamic signature technique is good. Moreover it has a good speed of enrolment (typically 30 seconds) and authentication (around 10 seconds). Unfortunately, the performance of this biometric is effected to a great extend by all the elements that prevent a user from signing properly, for example hand injuries and tense emotional states as well as the positioning of the signing pad.

Speaker Verification (Behavioural)
Another biometric authentication technique based on a behavioural characteristic is speaker verification. Since humans can distinguish each other by their voices, this suggests voice has distinctive characteristics. This is the concept behind voice recognition authentication techniques. Voice verification biometric products are essentially software that use a standard microphone (or telephone for certain applications) as the medium to obtain samples through. Among the distinctive features utilised by the various speaker verification products to authenticate users are the fundamental frequency and pitch of a voice, the short time spectrum of speech, and the formant frequencies [Nanavati and Thieme 2002].

Among the advantages of using voice as a means of authenticating individuals is the nature of the hardware necessary for acquiring the voice samples. The potential to use existing microphones and telephone devices makes it suitable for a large variety of applications including, for example, its integration in call centres. This technique also has the potential of operating without the users being aware. A disadvantage is that the sample acquisition and the identity verification processes can be disrupted by environmental effects such as the background noise. Two different speaker verification products were obtained and tested for the purposes of this investigation both using proprietary algorithms to generate and compare templates (voiceprints).

Technical: Speaker verification product A
The first speaker verification device that was tested, offers the administrative option to set the desired levels of FAR over FRR. A series of tests was performed on every security level available by enrolling six users, who then attempted authentication ten times on each setting. Table 8 bellow contains the calculated false acceptance rates for this product.

Selected FRR Level	FRR Achieved
0.28	1.6%
0.4	3.3%
0.55	3.3%
0.73	0%
0.93	5%
1.19	0%
1.51	0%
1.84	6.6%
2.24	5%
2.76	3.3%
3.43	3.3%

Table 8: comparison between set and measured FRR

When investigating its rate of false acceptances, this product proved to be rather accurate since there were no occurrences of such an event apart from when it was run on the lowest security levels, where the device would grant access to literally everyone.

Speaker verification product B
With six enrolled users attempting access to their legitimate accounts ten times each, the calculated False Rejection Rate for this product is illustrated in table 9.

User	Number of attempts	FRR
A	10	20%
B	10	0%
C	10	20%
D	10	20%
E	10	10%
F	10	0%
Total	60	11.6%

Table 9: FRR for speaker product B

When assessing the devices False Acceptance characteristic, in 450 attempts to fool the product by having 6 users attempting to gain access to each other's accounts there were zero occurrences of a false acceptance.

Operational

Evaluating the operational attributes for the speaker verification biometric technique, it was found to have good ease of use. The speed of the enrolment is generally low (about 4 minutes) since the process of the user having to repeat a phrase several times so as to train the device is time-consuming. However the authentication process only lasts a few seconds. Regarding the environmental effects upon the operation of the device, it was found to be unaffected by small variations of the background noise levels but, as mentioned earlier, performance is degraded critically under extreme noise conditions.

DISCUSSION

Even though behavioural biometrics did not prove to be as accurate as one of the established physiological techniques (fingerprint), the nature of the features extracted by the behavioural biometrics makes the authentication process more acceptable and less invasive. However the process of enrolment for the behavioural methods is generally more time consuming and complicated, since the devices need training, they can sometimes be perceived as not being user friendly [Silverman 2001]. Behavioural biometric techniques are also cheaper to deploy in terms of the price of the hardware required. Nevertheless, since what most companies would look for in an ideal authentication method would probably be accuracy for a reduced cost, the most accurate techniques are the physiological techniques that also require expensive hardware. During the assessment of the techniques, finger scan displayed high levels of accuracy, especially when using the optical method. Even the thermal scan that had many occurrences of false rejections still did not allow any impostors in. Thus, even if it increased the inconvenience for the user, it still did not put any valuable assets at risk. The keystroke analysis method displayed minimum FAR only above security level 6 with over 6 letter passwords while the FRR at the same security level remained as low as 20% which could be tolerable in the sense that legitimate users might get asked to re-login once in every five attempts, but many people are used to this anyway as a result of mistyping their passwords. Moreover, this technique has the advantage that it combines secret information with the biometric to increase security in the case that a user's password is compromised. Thus it can tolerate a certain number of false acceptances since it is very likely that only the legitimate user will have the knowledge of the password. As the results from this technique demonstrate, when the device's 'strictness' threshold is set to 5, the legitimate user is being rejected approximately 46% of the time. This is a very high average. It is likely that more sophisticated products would provide very different results but as was explained earlier, this investigation is based on the low price, commercially available products. Signature verification was tested to have lower FRR than most of the techniques, but its false acceptance characteristic would probably make it an unacceptable solution for many applications. When the technique was tested with very simple signatures, it was established that people with very basic signatures would find that impostors could easily forge them. Finally, for the voice verification biometric technique, there were no occurrences of any false acceptances, and a small but noticeable percentage of false rejections. Nevertheless, the drawbacks of this technique that make it less favourable from some of the others is the long period it takes for a user to train the program and the fact that both the products tested were significantly more expensive than any other of the biometrics obtained for the purposes of this investigation. Table 10 summarises the results of the assessment.

Product	Lowest **FRR**	Average **FRR**	Highest **FRR**	Lowest **FAR**	Average **FAR**	Highest **FAR**
Optical fingerprint	3.8%	4.1%	4.7%	0%	0%	0%
Thermal Fingerprint	25%	25%	25%	0%	0%	0%
Keystroke analysis	2.8%	28.5%	40%	3%	14.7%	66%
Dynamic Signature	0%	2.5%	5%	0%	2.5%	20%
Voice verification	1.6%	5%	3.3%	0%	0%	0%
Voice verification	11%	11%	11%	0%	0%	0%
Face recognition	30%	46%	70%	0%	3%	10%

Table 10: Summary of the assessment results at the default security level for each device

Technique	FAR	FRR
Face Recognition	0.25%	25%
Fingerprint scan (chip)	0.025%	10%
Fingerprint scan (chip) (Same reader as previous but with different software)	0.003%	6.5%
Fingerprint scan 2 (optical)	0.15%	22%
Speaker Verification	0.012%	12%
Signature Verification	0.4%	0.7%
Keystroke Analysis (Bleha et al)	2.8%	8.1%
Keystroke Analysis (Joyce and Gupta)	0.25%	16.67%

Table 11: Accuracy results reported in other research papers

The results of this investigation suggest that biometrics are not as accurate as they have been reported in previous research papers that evaluated the same techniques. [Mansfield et al 2001] performed an assessment of some of the major biometric techniques, namely face, fingerprint and voice scan. According to the results from their experiments, which were held under 'normal office conditions' with participants from both genders and all age groups, the measured performance of these techniques with the decision threshold set at the default (optimal) level indicated fingerprint to be more reliable both in terms of false acceptances as well as false rejections. More analytically the results are shown in table 11. According to the results of a similar report published by the Biometrics Consortium [biometrics.org 1995], when tested, signature verification technologies achieve accuracy rates of 0.7% false rejection rate and 0.4% false acceptance rate, while in an actual implementation the measured rates of false rejections were 0.1%. Finally, several papers. [e.g. Bleha et al 1990, Joyce and Gupta 1990] report keystroke analysis as being able to achieve the error rates that are displayed in table 11 as well. There are many reasons behind this dissimilarity of the results, the main being that this investigation assessed the accuracy of the commercially available products that are available for the enterprises that are not willing to invest a large amount of money to upgrade their existing authentication system. Secondly, this assessment was not performed under the ideal lab testing and operating conditions but under conditions that were varied in order to test the relative stability of the devices operation. Moreover the users that assisted with the evaluation of the products did not have any experience with such technologies and concepts, but were chosen to be ordinary PC and network users, as would be the case with any real-life implementation of such a technique.

CONCLUSION

This study used a very small group of test subjects (users), which should have helped to control error rates, nonetheless significant error rates were still observed for some of the methods. An emerging area of biometrics that could produce products with significantly improved accuracy and reliability is multiple biometrics. The combination, for example, of fingerprint and face scan can boost security levels radically, while a combination of face and voice scan would improve accuracy while maintaining low invasiveness levels, since they can both operate without the knowledge of the user.

The results from this evaluation of the commercially available biometric products clearly do not represent the entire range of products available in the industry. They should however be considered by any security administrator looking to implement biometric authentication since they are results from the evaluation of the commercially available products. This assessment established that the majority of the low cost commercially available biometrics are not suitable for those applications that require high accuracy levels such as government or military use. They can however provide increased convenience and additional security in other cases.

REFERENCES

Bleha S., Slivinsky C., Hussien B., (1990) 'Computer-access security systems using keystroke dynamics', Transactions on pattern analysis and machine intelligence Vol 12, No 12, 1990.

Communication Intelligence Corporation (2002), 'Enterprise solutions, implemented applications' www.cic.com

Dowland P.S. Furnell S.M, Papadaki, M. (2002) 'Keystroke analysis as a method of advanced user authentication and response' Proceedings of IFIP/SEC 2002 17th International Conference on Information Security, Cairo, Egypt, 7-9 May.

Dye B. Gerttula J. Kerner J. O'Hara B. (2001), 'An introduction to biometrics' 20 November 2001 http://www.stanford.edu/~bjohara/introduction.htm

Furnell S. (2001) 'Cybercrime: Vandalizing the Information Society', Addison-Wesley Publishing Company.

International Biometric Group (2002), 'Optical – Silicon – Ultrasound' http://www.ibgweb.com/reports/public/reports/ finger-scan_optsilult.html

Joyce R., Gupta G., (1990) 'Identity authentication based on keystroke latencies', Communications of the ACM, Volume 33, February 1990.

Liu S., Silverman M., (2001) 'A Practical Guide to Biometric Security Technology' IEEE Computer society, January 2001 http://www.computer.org/itpro/homepage/jan_feb01/security3.htm

Monrose F., Reiter M., Wetzel S (1999), 'Password hardening Based on Keystroke Dynamics' Proceedings of the 6th ACM computer and communication Security conference.

Nanavati S., Thieme M.,Nanavati R. (2002) 'Biometrics, Identity Verification in a Networked World' John Wiley & sons Inc.

Ndlangisa N (2001). 'Biometric Authentication using fingerprints and evaluating fingerprint readers', November 2001, www.cs.ru.ac.za/research/g9610159/Documents/Writeup-Final.pdf

Novell (2001), 'Overview of biometrics' 1 July 2001, http://developer.novell.com/research/appnotes/2001/july/01/a0107013.htm

Power R. (2002), 'Computer Security Issues and Trends', CSI/FBI Computer Crime and Security Survey, Volume 8 No 1, Spring 2002, https://wow.mfi.com/csi/order/publications.html

Polemi D. (1997) "Biometric Techniques: review and evaluation of biometric techniques for identification and authentication, including an appraisal of the areas where they are most applicable", April 1997, http://www.cordis.lu/infosec/src/stud5fr.htm

Smallback, R. C. Jr., (2002) 'Security Access using biometric fingerprint Technology' 28 May 2002, http://www.biometritech.com/features/

Smith R. E. (2001), Authentication from Passwords to Public Keys, Addison-Wesley Publishing Company.

The biometric consortium (1995), 'Electronic Benefits Transfer: Use of Biometrics to Deter Fraud in the Nationwide EBT Program', 29 September 1995 http://www.biometrics.org/REPORTS/OSI-95-20.html

The Biometrics Institute (2002), 'Signature Recognition', http://www.biomet.org/signature.html

The Facial Scan Homepage (2002), 'Primary Facial-Scan' www.facial-scan.com.