Biometric Security Systems: Finally, a Friend?

Krassie Petrova, ***Member, IEEE***

Abstract **--Information systems security has broadened its meaning and significance and has started to affect our lives and behaviours. The research literature identifies five related research domains: information systems, security policies, security technologies, security assurance, and security interfaces. This paper discusses some aspects of user acceptance of biometrical measurements for the purposes of authentication and access control and concludes that initial user rejection of the commonly implemented biometrics and fear of privacy abuse have been replaced by a de facto user acceptance. It hypothesizes that there is correlation between users' awareness of the broader consequences of a particular biometric system and the level of their acceptance of the system.**

***Index terms*—Identification of Persons, Access Control, Privacy, Security**

I. Introduction

Information systems security has broadened its meaning and significance and has started to affect our lives and behaviours. Looking at the research literature in the area, one notices that towards the mid 90's of the previous century research in information and systems security moves away form the single area of trustworthy systems with multi-layered data protection. As shown in [1], five broader and more general research domains are identified: information systems, security policies, security technologies, security assurance, and security interfaces.

The security framework suggested by Meadows includes "access control" as a technique to enforce a security policy within a system, and "authentication" as a technique to protect a system against intrusion form outside. This paper discusses some aspects of user acceptance of biometrical measurements ("biometrics") for the purposes of authentication and access control; the paper concludes that initial user rejection of the commonly implemented biometrics and fear of privacy abuse have been replaced by a de-facto user acceptance, and hypothesises that there is correlation between users' awareness of the broader consequences of a particular biometric system and the level of their acceptance of the system.

The paper is organised as follows: the next two sections discuss the basic objectives of information and system security, describe authentication as a precursor to access control, and introduce a framework for biometric authentication and access control. The next section presents a literature review on biometrics, biometric applications and technologies, and organizational implementations with a focus on user acceptance and factors affecting it. The discussion and conclusion section summarises the current view on user acceptance of biometric security systems and suggests directions for further research.

K Petrova is with the School of Information Technology, Auckland University of Technology, Private Bag 92006, Auckland 1020, New Zealand (e-mail: krassie.petrova@aut.ac.nz)

ICITA2002 ISBN: 1-86467-114-9

II. Information and System Security Objectives

Most of the literature on information and systems security discusses issues, problems and solutions along the three dimensions of data *integrity*, information *secrecy* (confidentiality), and information *availability* [2]. The objectives of providing integrity, secrecy and to some extent – availability can be met through establishing security *access control*. In turn *authentication* is as an approach towards implementing successful access control schemes [3]. Authentication is a process involving a series of steps which aims to establish the identity of the participating parties and deny or allow access to information resources controlled by these parties. The authentication process can be one- or bi-directional [4] and typically relies on several types of authentication information [5]. Authentication algorithms and procedures for human participants in an access control scheme users can be quite versatile.

Reference [6] identifies four methods to provide user authentication: i) passwords, ii) digital signature, iii) token devices and smart cards, and iv) biometric measurements. Similar classifications can be found in [4] and in [6]. As these authors suggest, biometric authentication can be implemented independently or in conjunction with other authenticating methods, and can be encrypted for preserving the integrity of the biometrical data. On the other side, security devices such as digital signatures and tokens can incorporate biometrics either as abasic content, or in the form of digital signature. Such biometric security systems can be quite complex.

In [6]-[7] a biometric system is defined as an automated method of measuring some physical characteristic or some aspect of personal behaviour, and comparing the measurement to a pre-recorded sample for the purposes of verification and identification. Most contemporary biometric security systems implement a multi-modal approach – integrating the biometric measurements of several individual human traits [8]. The use of several characteristics allows the systems to overcome some implementation difficulties (for example, the case of non-homogenous population - people with no eyes and an eye recognition system).

Biometrics as an approach to the achievement of a security objective can be dated back to ancient Egypt when people were identified through their physical measures [6]. The involvement of information technology with biometrics started in the early 60's of the last century and has continued through cycles of success ([6]; [[9]-[10]) – or failure ([11]-12]). A detailed description of the different biometrics used

in industry and in research is outside the scope of this paper, but most of them are introduced in the paragraphs below.

Reference [6] identifies four types of physiological characteristics suitable for automated biometrics (face, fingerprints, hand, eye) and three types of behavioural characteristics (signature, voice, and keystroke dynamics). Later eye recognition breaks into two subtypes - the retina pattern and the iris image [13]. Reference [7] includes skin pores and wrist/hand veins as usable biometrics but points out that only the retina, the iris and fingerprints can be considered truly unique biometric identificators. Reference [14] extends the list behavioural and physiological characteristics to include some rarely used biometrics (such as body-signals and scull measurements), and adds a new type: imposed physical characteristics – such as embedded microchips. All biometric measurements are taken through various types of sensors – some general (like cameras and microphones), other highly specialised (see for example, the devices used for optical fingerprinting and for capacitative fingerprinting in [15]. Measurement devices are part of the biometric system. The next section introduces a simple model of a biometric system which is used as a framework for studying of biometric authentication for access control and user acceptance of biometrics.

III. Biometric Authentication and Access Control

As shown in Fig. 1, the biometric system interacts with a user supplied biometric (or multiple biometrics) and with a reference database. References [16], [1], [12] and later [17]-[20] identify sets of requirements which a biometric system needs to comply with. These include performance (for example, speed of recognition), consistency (recognising the user identity in different circumstances y - in voice recognition, for example), dependability (providing a unique identity), and acceptability (the human participant of a biometric systems does not object either to the method of collecting a biometric sample or to the way it is being used and protected by the system).

The security objective of authentication in this model is to confirm a person's identity – as a legitimate user of the systems resource ("one among many" such users) and/or verify a person's identity ("one to one" match between the user and the database of legitimate users). These two authentication types are sometimes referred to as "identification" and "verification" ([20],[5]). More precisely, biometric identification is defined as process which allows a security system to accept or reject an assertion by the user that he or she has a particular identity. The decision to accept or reject involves a pattern recognition process and is based on the outcome of a search process across the entire database. Systems providing identification are refereed to as "one-to-many" or "recognition systems" - in contrast to "one-to-one" or "verification systems" where the database search aims to establish with a certain degree of confidence whether or not the user has the right to claim the identity represented by the biometric data. While in some cases of identification there might be no need for a biometric system to store a personal profile, verification does require such a profile [20]-[21].

One of the benefits of user authentication through an integrated biometrics-based security is the significantly improved control of the access to an organization's information resource. Will the individual user – the subject of biometric identification and verification, be willing to accepts the potential invasion to his or her privacy as the organization imposes a better control on its informational assets?

There is a potential conflict between the interests of the individual and the objectives of the organization. Based on prior research, [11] compiles an impressive list of user "fears"; among them are the fear that a biometric system will help enhance the power of the organization over the individual. Discussing the problem of user acceptance of biometrically controlled access, he notes that technological advancement has already contributed enormously to the improved accuracy of identification, leading to the reduction of the organization's administrative costs. He also observes that the public acceptance of biometric, privacy-invasive schemes "apparently" has increased. According to [11], as far as the use of biometrics conforms with the "standards of and expectations of a privacy-minded society", individuals would accept albeit unwillingly the increased power of organizations in their use of biometrics.

Discussing the same issue, [22] points out that it is not the biometric itself which is the threat to individual rights and privacy but rather the potential danger that unspecified third parties would be able to access the stored biometric data and use it for purposes not intended by the original security scheme. Applying preventive measures (such as encryption) to biometrical data can help create a safe environment where the organization and the individual share control over the use and the integrity of stored biometrics.

Shared control would empower the individual and increase the chances of a biometric security system to succeed. The maxim of information technology which Reference [6] summarizes as "No matter how good the information technology, if people do not want it, it will not work", is applicable to biometric security systems. As identified in [14] , "benefits to the user" is among the three factors which determine the success of a biometrics scheme. Can the perceived benefits of a system outweigh fears of privacy invasion and malicious use of biometric data? In what circumstances will the user forgo privacy fears and embrace biometrics as a " friend " and privacy protector? In the next sections we will summarize and discuss some literature results form the last ten years on the use and acceptance of biometrics to control access to organizational information resources.

IV. User Acceptance (1992-2002)

Earlier research in the area of biometrically controlled access focuses on the properties of the emerging technologies and on specific aspects of their application [16], [12], [23]. User acceptance is seen mostly as a function of the technical variables which define a particular biometric system, and also of the way it is used to collect the sample (intrusive vs. non-intrusive).

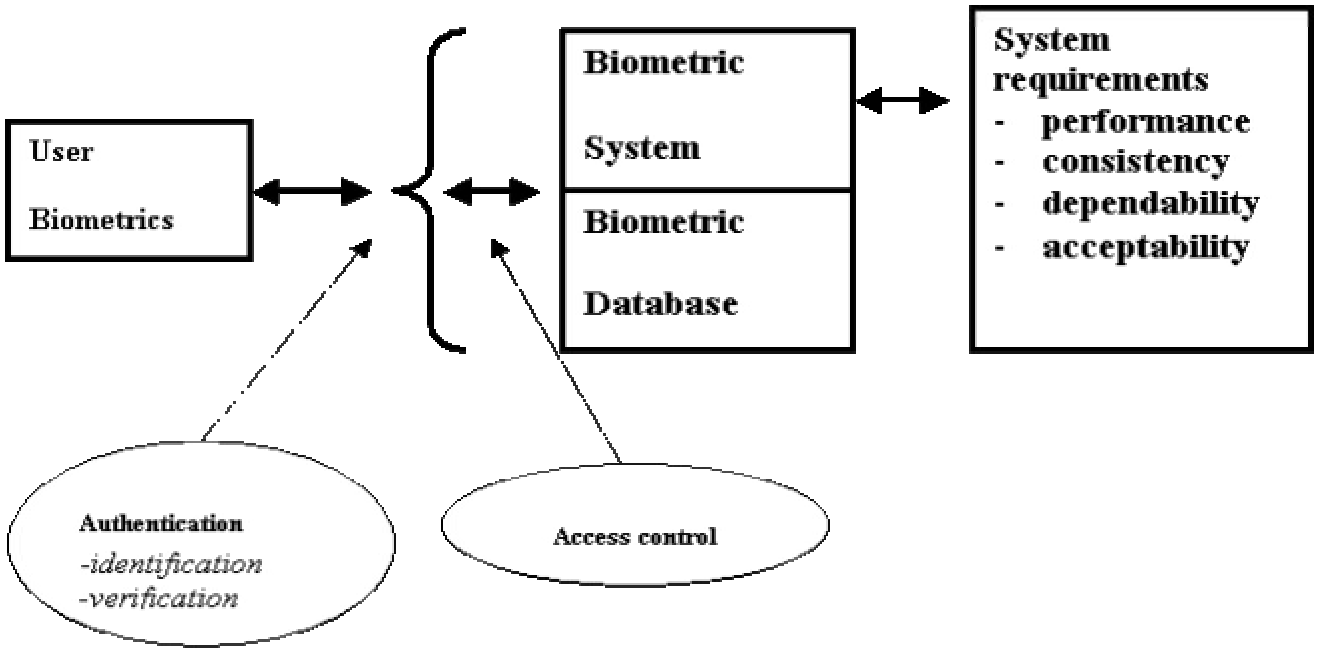

Fig.1. Authentication and access control in a biometric security system

Sherman in [16] classifies biometrics into six types (face print, fingerprint, hand geometry, keystroke dynamics, retinal patterns, signature dynamics, voiceprint). Among the organizations testing biometric systems are banks (signature dynamics, voice recognition). Sherman predicts that widespread acceptability of biometrics will not become a fact before at least 2002, and concludes that the success of future biometric systems will depend on their capacity to satisfy reduced cost expectations of users and organizations alike.

Kim in [12] adds iris pattern recognition to the list of biometrics used in the security industry. Discussing user acceptance, he identifies two factors which influence it –the level of the individual's literacy (in dynamic signature verification, for example), and the presence or absence of physical unease (in the case or retina scans). Kim concludes that user awareness and the provision of user training is crucial for the successful implantation of biometrical security devices in the existing organizational culture, along with the implementation of adequate safeguards to protect personal characteristics.

Based on the adoption of biometrical identification by banks, Marshall & Steve [23] also include "customer acceptance" as a critical success factor to the adoption of biometrics by financial companies, and point out that customer perception of a security device as an acceptable one depends on its speed and usability (for example, it should not introduce delays at the point of sale, or should not deny access to a valid bank customer). Comparing existing biometric technologies they conclude that none of them overcomes the problem of user acceptance.

Towards the second half of the 90's the focus of research on user acceptance broadens to include issues such as privacy and possible fraudulent or otherwise malicious use of stored biometric information. For example, Monrose & Rubin [24] identify the advantages of permanent passive monitoring as a method of collecting keystroke dynamics samples, but warn that their methodology would be applicable only in environments where users have "no expectation of privacy". Another example is provided by Clarke in [18]; critically analyzing chip-based authentication schemes Clarke discusses the feasibility of a chip-card with a biometrical component and points out that for many people "biometrics are … threatening". In his paper Clarke formulates two sets of system requirements, all of which are aimed at protecting privacy and empowering the individual. Specifically related to biometrics are the requirement not to maintain a central storage of biometrics, and the requirement to include a two-way authentication process in the access control procedure (i.e. personal chips should not simply respond to the signal of a security device but should verify the device's authenticity). Clarke acknowledges the fact that implementing these and similar design requirements would present significant challenges to organizations but concludes that this would be the only way to ensure user acceptance of organizational security measures.

The importance of the first requirement is underlined by some examples found by Davis [9]: the existence of a federal centralized national database of biometric identifiers for commercial driver's licenses (USA), the digital fingerprint databases in the states of Pennsylvania and Florida (USA). Davis suggests that user acceptance will be ensured through the use of "one-to-one" chip-based matching systems that will need a centralized database. According to Davis the security industry itself will be the driving force behind the development and the adoption of biometrics standards for the protection of user privacy. In her work Davis identifies one factor which might be construed as an impediment to user acceptance: user discrimination (an example is the case of eye biometrics and blind people).

User awareness of the possibility to use legitimately collected biometric data for unspecified purposes (for example identifying the individual's race from an iris scan) as another factor which might influence user acceptance. In the literature of next period, the emphasis on speed and reliability is no longer as strong as in the early 90's as there is a choice of biometric systems and an organization can select one that suits its requirements – including improved user acceptance. One example is the tutorial on automated

biometrics-based identification and verification in [21]. The authors provide a methodology for evaluating different schemes and selecting the best, and the selection criteria variables include "user-specified system requirements".

Woodard in [7] examines the specificity of privacy concerns implicated by biometrics. According to Woodward, at the heart of privacy concerns raised by the use of biometrical security systems lies the need of the individual to exercise full control in determining how, when, why and to whom information in the form of a biometric identifier should be disclosed. Based on an extensive range of cases and on specialized research in the areas of biometric technologies, Woodard identifies three different groups of privacy threats: i) when a unique biometric identifier is provide by an user, it is 'given up" (and the process cannot be reversed); ii) biometric information can be bough and sold by third parties without the individual's knowledge or his or her consent (and there are only a few if any legal limits to such transactions); iii) biometric information obtained for authentication is in fact invasive as it might disclose a significant amount o details about an individual (for example, genetically based diseases.) Woodard discusses critically the advantages and disadvantages of biometric security systems and argues that in fact biometrics can and should protect information integrity and information privacy. He argues that the level of biometric security acceptance by individuals would increase with the increased awareness of the public at large of the possibilities to use biometrics as a privacy-enhancing technology and as a protector of the interests of the legitimate users of an organizational resource, but acknowledges the role of factors such as cultural objections (e.g. fingerprinting of welfare beneficiaries), possible religious and /or philosophical objections, and objections based on the actual physical harm and invasiveness.

Further concerns about user acceptance are raised by Tomko [17] and Schneier [25]: they point out that some biometric characteristics are not secret and can be obtained easily with malicious intent (eg a photograph or a fingerprint), or simply stolen. As a preventive measure Tomko [17] and also Clarke [18]-[19] suggest the use of trust models; according to them authenticating for eligibility rather than for identification and verification would be more acceptable to the individual. Among the five information privacy principles designed by Clarke feature: the requirement that an organization should justify publicly the purpose and use of any privacy –invasive information systems, and the requirement to provide the choice of anonymity and pseudonymity to the subject of a biometric security scheme.

Towards the end of the period reviewed in this paper the literature on biometric authentication for access control focuses again on technological advancement (see, for example [8] and [26]-[33]), the application of specialized biometric security systems [34]-[37], emerging industry standards ([14] as well as [38]-[40]), and on systems evaluation and usability issues [6], [10], [20], [41]-[42]. The next paragraphs summarize the results of three studies which explicitly qualify user acceptance of several biometric authentication methods.

In [41] Furnell et al point out that most biometric security schemes are based on a "compromise between high security and low user acceptance - low security and high user acceptance". Their empirical study of user preferences includes eight biometrics; some of their results are shown in Table I (Part A), based on Fig. 2 in the referenced work. The first row in Part A shows the biometric method. The second row shows user acceptance of the method when implemented as a login security device, and the third row shows acceptance of the method when implemented through continuous monitoring. To be able to compare these results with other research findings, user responses (in percentages in the original work) are qualified here as 'low' if the empirical results in the source indicate positive acceptance below 40%, 'very low' for negative acceptance, and 'high' – positive acceptance above 40%. Table I (Part B) contains a data from Table 2 in [20]. The evaluation of the acceptability of a biometric security device in this work is based on the study of the perceptions of three biometric experts. And finally, Table I (Part C) contains data from Table 1 in [42]; the authors derive their findings from views expressed in security industry sources. The next section continues with a discussion of these results in the light of the literature review, and with a conclusion.

V. DISCUSSION AND CONCLUSION

Biometric security technologies have shown considerable progress in improving their performance, and are moving towards standardization and interoperability: Reference [40] formulates and justifies security requirements for biometric systems as part of a proposed biometric standard, bodies such the BioAPI Consortium and ANSI are working towards creating interoperable industry standards and security system evaluation protocols, and the security industry is booming [10], [39]. In the current climate of fear of terrorism some researchers like Jim Wayman, director of the Biometric ID Research group at San Jose State University of California (as cited in [35]) suggest that 'as more people use biometric systems, their acceptance of the technology will grow, and privacy concerns subside". He supports this suggestion stating that data collected as early as 1990 shows a very high level (90%) of acceptance among people who are current users of a biometric security system and are aware of its benefits.

The data in Table I demonstrates a similar pattern; biometric security experts and professionals are optimistic in their views on user acceptance (medium to high), and end-users (who are presumably exposed to biometric security as employees of the organizations targeted by the Furnell survey) are mostly in favour of a one-off security identification procedure. Still, the low or even negative level of acceptance of biometric monitoring procedures can be attributed to privacy concerns, as indicated earlier in the works on privacy concerns related to biometrics security.

The advancements of the technology and the increasing number of biometric security implementations have obviously allayed user fears related to intrusiveness, physical discomfort, and social status damage. A 'rosy' picture of widespread user acceptance is actively promoted by academics and industry professionals [43]; the interview with Richard Norton, executive director of IBIA – International Biometric Industry Association in [44]. Although authors such as Roger Clarke regularly voice concerns about the dangers of adopting biometric security without safeguards and checking mechanisms [45], we can conclude that end users in organizations are not too concerned with the issue.

Further research into the reasons why individuals seem to accept biometric security access control might help find correlation between user acceptance and an identified set of factors. A hypothesis to test is that user awareness of negative consequences and privacy threats and general educational background influence strongly the individual's level of acceptance of a particular biometric. User type (customer or employee) and organization type (private or government) could be incorporated as moderating variables.

Table I. Biometric Security Acceptance Levels

	Key-stroke ana-lysis	***Face reco-gnition***	***Mouse dyna-mics***	***Voice veri--fication***	***Sign-ature ana-lysis***	***Iris scan-ning***	***Hand geo-metry***	***Finger-print ana-lysis***	***Retinal scan***
A. Furnell et al	Low	High	Low	High	High	High	High	High	N/A
	Low	Low	Low	Low	Very low	Very low	Very low	Very low	N/A
B. Jain et al	N/A	High	N/A	High	High	Low	Medium	Medium	Low
C. Liu & Silver-man	N/A	Medium	N/A	High	Medium	Medium	Medium	Medium	Medium

REFERENCES

[1] C. Meadows, "An outline of a taxonomy of computer security research and development", *Proceedings of the 1992-1993 ACM SIGSAC on New Security Paradigm Workshop, pp. 33-35,* August 1993.

[2] W. Stallings, *Network Security Essentials: Applications and Standards*, pp. 9-15, Upper Saddle River, NJ: Prentice Hall, 2000, pp. 9-15.

[3] D. Gillman. *Computer Security*, Chichester, WE: John Wiley & Sons, 1999, pp. 205-208.

[4] R. Sandhu, and P. Samarati, "Authentication, access control and audit", *ACM Computing Surveys*, Vol. 28 , pp. 241-243, Jan. 1996.

[5] E. E. Schultz, R. W. Proctor,M. C. Lien, and G. Salvendy, "Usability and security: an appraisal of usability issues in information security methods", *Computers & Security* Vol. 20, pp. 620-635, July 2001.

[6] B. Miller, "Vital signs of identity", *IEEE SPECTRUM*, pp. 22-30, Febr. 1994.

[7] J. D. Woodward, "Biometrics: privacy's foe or privacy's friend?", *Proceedings of the IEEE* , Vol. 85, pp. 1480-1997, Sept. 1997.

[8] F. L. Podio, "Personal authentication through biometric technologies", *Proceedings of the IEEE 4th International Workshop on Networked Appliances*, pp. 57-66, 2001.

[9] A. Davis, "The body as a password", *Wired*, Vol. 5, 1997, http://www.wired.com/wired/archive/5.07/biometrics.html (3 May 2002).

[10] P. J. Phillips, A. Martin, C. L. Wilson, and M. Przybocki, "An introduction to evaluating biometric systems", *IEEE Computer*, pp. 56-63, Febr. 2000.

[11] S. Davies, "Touching big brother: how biometric technology will fuse Flesh and machine", *Information Technology and People"* Vol. 7, Apr. 1994, www.privacy.org./pi/reports/biometric.html (1 May 2002).

[12] H.-J. Kim, "Biometrics, is it a viable proposition for identity authentication and access control?" ,*Computers & Security* Vol. 14, pp. 205-214, 1995.

[13] D. Sims, "Biometric recognition: our hands, eyes, and faces give us away", *IEEE Computer Graphics and Applications, pp. 14-15,* Sept., 1994.

[14] R. Clarke, "Biometrics and privacy", 2001, www.anu.edu.au/people/Roger. Clarke/DV/Biometrics.html (3 May 2002).

[15] G. Lawton, "Biometrics: a new era in security", *IEEE Computer*, pp. 16-18, Aug. 1998.

[16] R. Sherman, R. "biometrics futures", *Computers & Security* Vol. 11, pp. 128-133, Febr. 1992.

[17] G. Tomko, "Biometrics as privacy-enhancing technology: friend or foe of privacy?", *Proceedings of the Laws & Business 9th Privacy Commissioners'/Data Protection Authorities Workshop*, 1998, www.dss.state.ct.us/digital/tomko.htm (4 May 2002).

[18] R. Clarke, "Chip-based ID: promise and peril", *International Conference on Privacy* (Sept.), Montreal, 1997. www.anu.edu.au/people/Roger.Clarke/DV/IDCards97.html (4 May 2002)

[19] R. Clarke, " Internet privacy concerns confirm the case for intervention", *Communication of the ACM*, Vol. 42, pp. 60-67, Febr. 1998.

[20] A. Jain, L. Hong, and S. Pankanti, "Biometric identification", *Communications of the ACM* , Vol. 43, pp. 91-98, 2000.

[21] W. Shen, M. Surette, and R. Khanna, "Evaluation of biometrics-based identification and verification systems", *Proceedings of the IEEE*, Vol. 85, pp. 1464-1477, 1997.

[22] A. Cavoukian, "Privacy and biometrics", *Information Technology and People*, Vol. 7, 1994, www.pco.org.hk/english/infocentre/files/cakoukian-paper.dov (30 April 2002).

[23] I. M. Marshall and J. Steve, "One in the eye of plastic card fraud", *International Journal of Retail & Management*, Vol. 23, pp. 3-15, Apr. 1995.

[24] F. Monrose, and A. Rubin, "Authentication with keystroke dynamics", *Proceedings of the 4th ACM Conference on Computer and Communications Security*", pp. 48-55Apr. 1997.

[25] B. Schneier, "The uses and abuses of biometrics", *Communications of the ACM*, Vol. 42, pp. 136-137, Aug. 1999.

[26] J. Markowitz, "Voice biometrics", *Communications of the ACM, Vol.*43, pp. 66-73, 2000.

[27] M. Negin, T. A. Chmielewski Jr, M. Salganicoff, T. Camus, U. M. C. von Seelen, P. L. Venetianer, and G. G. Zhang, G. G. "An iris biometric systems for public and personal use", *IEEE Computer* pp. 70-75, Febr. 2000.

[28] M. Peyravian, S. Matyas, A. Roginsky, and N. Zunic, N. " Multi-party biometric-based authentication", *Computers & Security*, Vol. 19, pp. 369-374, Apr. 2000.

[29] R. Sanchez-Reillo, "Smart card information and operations using biometrics", *IEEE Aerospace and Electronics Systems Magazine*, Vol. 16, pp. 3-6, Apr. 2001.

[30] D. Banisar, "A Review of new surveillance technologies", *Privacy Journal* , Vol. 28, pp. 5-9, Jan. 2001.

[31] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing Security and Privacy in Biometrics-based authentication systems, *IBM Systems Journal*, , Vol. 40, pp. 614-634, March, 2001.

[32] J. Daugman,. "High confidence recognition of persons by iris patterns", *Security Technology: Proceedings of the 35th IEEE International Carnahan Conference*, pp. 245-263, 2001.

[33] L. Biel, O. Petterson, L. Philipson, and P. Wide, P. "ECG analysis: a new approach IN human identification", *IEEE Transactions on Instrumentation and Measurement* , Vol. 50, pp. 808-812, March, 2001.

[34] R. Sukthankar, and R. Stockton, "Argus: the digital doorman", *IEEE Intelligent Systems* , Vol. 16, pp. 14-19, Feb. 2001.

[35] D. Balaban, "The privacy debate rages on", *Card Technology*, Vol. 6, pp. 32-43,, 2001.

[36] R. Lazarick, R. "Applications of technology in airport systems control", *Security Technology: Proceedings of the IEEE 35th International Carnahan Conference*, pp. 85-95, 2001.

[37] S. Bills, "Citibank, others giving biometrics the eye", *American Banker* , Vol. 167, pp. 13-16, March 2002.
[38] W. Winter, and L. Huber, "Part 6: Biometric identification: limits and possibilities", *Biopharm* , pp. 40-43, Nov. 2000.
[39] C. J. Tilton,. "An emerging biometric API industry standard", *IEEE Computer* , pp. 130-132, Febr. 2000.
[40] S. M.Matyas, and J. Stapleton, "A biometric standard for information management and security", *Computers & Security*, Vol. 19, pp. 428-441, May 2000.
[41] S. M. Furnell, P.S. Dowland, H. M. Illingworth, and P. L. Reynolds, "Authentication and supervision: a survey of user attitudes", *Computers & Security*, Vol. 19, pp. 529-539, May, 2000.
[42] S. Liu, and M. Silverman, "A practical guide to biometric security technology", *IEEE Computer Society*, 2000. www.computer.org/itpro/homepage/Jan_Feb/secuirty3/htm (7 May 2002).
[43] E. Etzioni, "Biometrics are coming! Biometrics are coming!", 1999. http://speakout.com/activism/opinions/3808-1.html (6 May 2002).
[44] T. Dunstone, T. "Interview with Richard E. Norton of the IBIA", *Biometrics Institute*, 2000, www.biomet.org/001029_ibia_interview.htm (5 May 2002).
[45] R. Clarke, R. "Person location and person tracking: technologies, risks and policy implications", *Information Technology and People* , Vol. 14, pp. 206-231, Febr. 2001.