Malaysian Journal of Computer Science, Vol. 17 No. 2, December 2004, pp. 90-97

HEALTH BIOMETRICS: READY TO BE A SMART INTERNET TECHNOLOGY?

Jenine Beekhuyzen and Liisa von Hellens
School of Computing and Information Technology
Griffith University, Nathan Campus, Brisbane, Australia
email: j.beekhuyzen@griffith.edu.au
l.vonhellens@griffith.edu.au

Mark Siedle and Rodney Topor
School of Computing and Information Technology
Griffith University, Nathan Qld 4111, Australia
Tel. No.: +61 7 3875 5047
Fax No.: +61 7 3875 5051
email: M.Siedle@griffith.edu.au
r.topor@griffith.edu.au

Stella Stevens
Service Industry Research Centre
Griffith University Gold Coast Campus
email: s.stevens@griffith.edu.au

ABSTRACT

Health informatics is increasingly of interest due to its potential in making our health care systems safer. The term 'health or medical informatics' refers to the "application of information technologies to optimise information management within all aspects of health care delivery" [1]. A research project has been initiated to explore the effectiveness of hospital clinicians and their professional group by developing tools to support electronic wireless access to medical literature, patient records and hospital databases. PDAs and other portable devices are considered as technologies that enable such access, but their suitability for clinicians depends on a range of organisational and technical issues including privacy and security of the systems. This paper introduces a selection of different technologies including signature recognition and a range of fingerprint scanning technologies designed for authentication and authorisation and critically evaluates their merits in accessing the health care systems.

Keywords: Health, Mobile, Biometrics, Internet, Technology

1.0 INTRODUCTION

Health care services are faced with unprecedented demands from governments and consumers to improve safety and quality. At the same time there has been a rapid growth in the volume of medical research findings and associated changes in recommended practice, and in the information available to clinicians about their own performance and that of their institution. Underpinning this situation is an increasingly litigatious ordeal and all involved have a real concern about privacy and security issues. Information has to be synthesised, acted upon and safe guarded against intrusion, but the current state of information technology infrastructure and applications does little to meet this demand.

A major opportunity exists for IT specialists and the health industry to work together to devise solutions. A marrying of health and information technologies is currently prevalent in research areas in Australia with the opening of a $150 million E-Health research centre in Brisbane, Queensland. Along these lines, a number of government and industry-funded projects also have Health high on their agenda, one of these projects being the Smart Internet Technology Cooperative Research Centre (www.smartinternet.com.au). In line with the rapid growth of information for health practitioners, this paper provides a discussion of the current literature on the security and privacy of biometrics technologies, which has enabled us to evaluate the most appropriate for adoption in a health environment. This critical review of the literature will provide the basis for technology development and it considers access to information that is internal and external to the user's work environment.

In improving point of care patient safety, this paper is set within the context of a current project, the Smart Electronic Medical Information System (SEMIS). The SEMIS project continues to build towards developing Smart Personal Assistants (SPA) for use by clinicians and their professional group within a hospital environment (in this context, the term 'clinicians' refers to doctors and the term 'their professional group' includes nurses and allied health professionals). The aim of SEMIS is to ultimately increase the effectiveness of hospital clinicians and their professional group by developing improved systems and tools to support electronic, wireless access to patient records, medical literature and hospital databases. Of great importance is the authentication process for access to

such devices, and the applicability of them to the health care environment. This discussion contributes to the design and development of such devices according to User Centred Design principles [2].

This project is motivated by the rapid growth of medical literature and the barriers to its convenient access by busy hospital clinicians and their professional group. Within Australian hospitals, there is currently difficulty in accessing fragmented and often incomplete patient records and hospital databases, and there are also documented problems with organisational issues such as problems with teamwork, user resistance and lack of management commitment to improved access to research knowledge in health care organisations.

The issue of patient safety is ubiquitous in the health care industry globally. Within Australia, about 50,000 people annually are left permanently disabled and 18,000 people die each year alone due to medical error. These mistakes cost the nation more than $5 billion annually [3]. Major health care systems throughout the world are attempting to solve these costly and dangerous problems with enterprise information technology solutions [4], but limitations still exist. Recent improvements in information technologies have made research findings, data, and other public health information more widely accessible to professional audiences, policy makers and the general public. However, to effectively utilise the vast array of data and program information however, practitioners need an understanding of the types of databases available, knowledge of their contents, and the ability to effectively access relevant information through some sort of technology device [5].

Evidence-based practice is said to integrate the best evidence from research with clinical expertise, patient preferences, and existing resources into clinical decision making about the health care of individuals [6, 7]. Recent research within a hospital environment suggests that there is a push to implement evidence-based medicine, patient safety and quality initiatives and performance approaches [8]. However, the largest threat that clinicians (for example) might face is that using their own systems render them vulnerable to a lack of knowledge about overall trends at the macro level within their specialties, which can only come from some form of centralised data collection. This could be achieved through government, colleges or professional institutions [9]. It suggested that even small improvements in the current medical situation could lead to significant benefits [8].

2.0 METHODOLOGY AND THE SEMIS PROJECT

The context of this study is the health care environment, and the particular problem that this paper attempts to address is the security of mobile devices thus leading to the privacy of personal and confidential information. Special attention is being given to authentication, primarily because of the advantages currently found by the joint academic/industry project utilising biometrics, known as SEMIS. Within SEMIS, biometrics is being researched in conjunction with Personal Digital Assistants (PDAs) to allow clinicians and their professional group to improve patient safety by increasing speed and access to medical information and patient records, while providing the enhanced security that today's technological endeavours demand. Through the use of biometrics and mobile devices, it is hoped that issues such as accountability, productivity, access to information, privacy, trust and security, as well as a host of other issues, will be vastly improved within the medical sector.

Within the hospital environment, user studies have been and will continue to be conducted to help identify areas where Smart Internet Technologies may be constrained, or have particular opportunity, due to likely responses of potential users. Examples of key areas being explored include boundaries of acceptable natural language interaction, trust, security, privacy, universal/inclusive design, cross-cultural variations, organisational characteristics, and particular activity applications requirements.

The use of User Centred Design principles, utilising personas and scenarios will help to identify successful technologies by giving a deeper understanding of how a user (eg clinicians and their professional group) will interact with a particular technology (eg mobile device such as a PDA and software to enable access to research knowledge) in a specific organisational context (eg specific task in hospital surgery carried out by clinicians). The development process of the biometric systems and products for the health care environment discussed in this paper includes: formulating the design concept of the products, participating actively in the detailed product design providing an evaluation framework to assess the usability/usefulness of the artefact/products (action research/co-design), and performing the usability testing (iterative design) [10]. The approach to development in this project includes the application of User Centred Design methodologies which has been tested within a number of contexts and is discussed further in [11, 12].

Initial stages of the user studies involve identifying user requirements and comparing them to discussions in the current literature. This will also include an analysis of possible technology solutions in relation to particular user groups eg. Surgeons have limited access with their hands when dealing with a patient, whereas an anaesthetist generally has more flexibility of access to a device when with a patient. Culture is widely cited in the information systems literature as a possible barrier to technology adoption. The early stages of the project will also explore the cultural environments of the case sites and how they will possibly influence the introduction of new technology and practices.

3.0 HEALTH BIOMETRICS : TECHNOLOGY

Security in health care is defined as the measures taken by clinicians and their professional group to protect the privacy, integrity, and accessibility of information and systems [13]. Privacy in health care is defined as the obligation of clinicians and their professional group not to disclose information and the extent to which patients, clinicians and their professional group can control the circulation of information [14-16].

Biometrics is the process of measuring unique human physical characteristics, such as the face, fingerprints, retinal/iris composition and voice patterns, as a basis for later identifying the same individual [17, 18]. Currently, information security in organisations is largely limited to knowledge and possession factors such as usernames and passwords, personal identification numbers (PINs), keys, photo badges and so on; none of which truly bind access to a unique individual because they can all be obtained through various means [19]. As such, organisations need to be looking towards newer technologies such as biometrics to thoroughly protect their information assets, especially when the information is of vital importance to both the organisation and its customers.

In the case of the current health project, the 'customers' are in fact patients disclosing private information that could very easily affect their wellbeing if modified in a malicious manner. Imagine what could happen if something as simple as a blood type was modified? The consequences could easily result in death. And herein lies the problem…trust. Hospitals have always stood for life, and in an age where our society places so much emphasis on computers to increase productivity, we need to maintain that reputation by protecting information in the most effective way possible. This paper discusses and attempts to bring to light the use and applicability of proven biometric technologies to safeguard our delicate information within the specific environment of health care.

The argument against biometrics currently is this; although biometrics can obtain unique human information such as the fingerprint, the risk of repudiation is lowered, but not removed altogether [19]. The social implications for biometrics are vastly different from any kind of security used currently in society, such as passwords and PINs, solely because of the risk of theft. If an individual's biometric data is compromised in any malicious manner, that individual has no way to create new biometric information for protection, unlike passwords, which can be changed easily if stolen or lost [20]. One could call it identity theft. However, unlike identity theft, a user will no longer have the advantage of being assigned a new name, address and drivers license as a way to start a new life. A better term would be indefinite identity theft, as identities could literally be taken over, with whoever possessing the stolen biometric information having the means to use it in certain hospitals and be accepted by security as the stolen identity. Careful thought will be required regarding the consequences of any privacy policies made in conjunction with any project should biometrics be implemented as part of the health care solution.

4.0 HEALTH BIOMETRICS: SECURITY AND PRIVACY CONCERNS

Portable Digital Assistants (PDAs) are a productive way for clinicians and their professional group to access medical, drug and other information [21, 22]. Industry observers state that, "the early success of PDAs in health care is largely because the hardware and software truly match the needs of physicians" [21, 22].

Rosenthal [23] notes that traditionally, nurses were reluctant to incorporate electronic devices into their clinical routines, possibly because of the "touch versus tech" education preparation when the advantages of computers were still largely unknown and disputable. The statistics put forward by Rosenthal [23] indicate that in 2001, approximately 1% of Registered Nurses in the United States used PDAs. This low figure could be attributed to the minimal nursing specific software available for PDAs. It is expected that increased nursing specific software will soon be available due to an increased demand for PDAs in the medical community throughout Australia. Rosenthal [23] also makes note of the uptake of PDAs by clinicians in the United States and the increase trend that is expected, with figures for 2002 of 18% for clinician PDA usage and an expected figure of 33% by 2007.

Biometric implementations have already commenced on portable computing devices, such as laptops and pocket PCs. An example of such infrastructural security can be seen in the new iPAQ Pocket PC h5400 series by Hewlett-Packard [17]. Research by Poulter [24] shows the staggering statistics from respondent companies where laptop PCs are lost, stolen and damaged. Biometrics then, when used for private access control, such as laptop security, has enormous potential to reduce theft rates of such devices, which is a major concern of clinicians who access hospital databases using PDAs. Over time, surely motivation to steal a laptop or PDA would diminish if the devices were rendered useless by a biometric scanner to everyone except the owner.

For all biometric scanning technologies, any technology limitations will affect the security of the biometric device. As such, Pierce [17] notes that the data should be encrypted immediately inside the scanner before being transmitted to a database for matching. Also, the database in which biometric templates are kept and any data channels will also require relevant security to prevent network and database hacking, regardless of the operating system's supposed network protection [25].

Taking these issues into consideration, a number of specific biometric scanning technology options are available. Fingerprint scanning provides a biometric means to authenticate access to a mobile device. Although there are various fingerprint scanners available, they are all related in some way to the three main scanners available: Silicon-based, Optical-based, and Ultrasound-based scanners [19]. Optical-based scanners are discussed minimally due to their lack of applicability to this project.

4.1 Silicon-Based Scanners

The fingerprint is one of many prime candidates for biometrics, with other possibilities including the eye, the entire hand, the face, the voice and also signature recognition [26, 27]. According to studies by Hewlett-Packard [17], fingerprints are the most reliable biometric feature for human identification. This information corresponds with Calderon and Subbaiah [28] who state that "*fingerprints are the most widely used biometric for automated authentication in business information systems, and more than 80 percent of all vendors of biometric devices specialise in fingerprint technology*". However, Cambier [26] directly contradicts the claims by Hewlett Packard by stating that "*iris recognition is widely acknowledged within the biometric industry as the most reliable and accurate technology available*". Both Morrissey [29] and Short [30] back up this research by saying that retinal scanning is considered to be the most secure. However, the previous authors' opinions disregard how easily retinal scanners can be fooled through the use of contact lenses, just as certain fingerprint scanners can be fooled by artificial skin patterns. With all these options available to the biometric security industry, why are over 80 percent of biometric vendors focussing on the fingerprint and not the eye?

Several possible reasons exist. Fingerprint scanning technology currently appears to have far more potential for reducing the fraudulent use of biometric scanners, with current research focussing on integrating a form of human flesh identification into fingerprint scanning devices. This recent evidence shows that with this invention "*it is not possible to obtain access authorisation with fake fingers or cut-off fingers*" because of the human checking aspect of the scanner [18]. Possibly the most obvious reason fingerprint scanning is mainstream in the biometric industry is because of its usability prospects, which is especially applicable to the health care environment because of clinician and their professional group's need for mobility, as well as 'ease of use' when either consulting patients or accessing medical research 'on the run'.

Because of the potential silicon-based chips have for integration into mobile phones and other portable devices, companies are making the chips even smaller to reduce the cost of production [31]. Automatically, this compromises the security of the device. The entire fingerprint pattern is considered to be unique, not a small part of it. Also, smallness is definitely not in the best interests of clinicians and their professional group where silicon-based scanners are concerned, because although this may increase attractiveness upon first impression, this reduces the operability the user has in entering their fingerprint, hence decreasing its attractiveness prior to use, especially in medical emergency situations [19, 31].

Silicon-based scanners measure an individual's ridge and valley-depth patterns through the use of small electric charges, hence producing a high quality image with suitability for all individuals with fingers [19]. The accuracy of these devices is dependent on the fingerprint not changing since the individual's enrolment into the system [19]. Any calloused, dry or oily skin of an individual being scanned may have a direct effect on the fault tolerance of the device. Also, if the device itself has any residue on its surface, error rates may increase. Silicon-based scanners were found to be easily fooled by fake fingers made of gelatin by a Japanese researcher, Tsutomu Matsumoto, thus

the security of silicon-based scanners leaves much to be desired [32].

These scanners are quick to capture the fingerprint image, with recorded time behaviour of one tenth of a second. However, Babyak [33] states that they can be easily damaged by electrostatic discharges from human contact. If any electrostatic discharge were to damage or modify the image that was received by the system for pattern matching, either upon enrolment into the system or during later authentication, the security of the device may be compromised. If such technology was to undergo usage by a large social population, damage would surely be imminent and clinician's dependence on such systems would not be well received.

The fragile nature of silicon leaves the durability of the device with problems. However, Costlow [34] notes the advancements by Lucent Technologies where they developed coatings 100 times stronger than glass for silicon chips; a positive for durability to satisfy potential volume demands of clinicians and their professional group.

4.2 Ultrasound-Based and Optical-Based Scanner Analysis for Signature Recognition

In the words of Pierce [17], "*ultrasound systems can succeed where optical systems may not*". Ultrasound-based scanners are the newest of the biotechnologies and are not affected by skin problems, such as calloused skin, dryness, oily skin or dirt [35, 36]. Ultrasound-based scanners transmit auditory emissions to generate a 3-dimensional image of the fingerprint and its ridges and valleys by measuring the time and distance the emissions travel before hitting certain parts of the skin. They are also capable of penetrating grime on both the finger and the scanner surface and see past the challenges of skin pigmentation and oil on a finger, thus adding to its reliability and accuracy [19, 36]. In other words, they eliminate surface contamination variables whilst still gaining a high quality scan, which is a significant fault tolerance advantage over its predecessors.

Optical-based scanners can be thought of as an advanced version of a common photocopier/scanner. In that respect, these scanners obviously have problems when trying to read fingerprints that have changed or been damaged in any way, because they read the outer-most layer of the skin. Hence, any resulting damage to the outer-layer of the skin results in this technology failing. For these reasons, optical-based scanners have not been examined in this paper in respect to privacy and security, as they are not a valid medical-based biometric solution. Ultrasound–based scanners however have great potential to bypass these problems by essentially seeing through this outer-layer to the underlying fingerprint of the individual, with current ultrasound scanners even detecting prints through latex gloves for environmental workers [25, 37]. As one can imagine, this prospect is especially useful for clinicians and their professional group.

5.0 CONCLUSION

Piotrowski [38] suggests that any solution must have the direct engagement of clinicians and their professional group from the very beginning. It was further suggested that in order to achieve 'success', a number of steps must be followed. A solution must a) be practical; b) be easily accessible; c) Improve clinician workflow, and d) support decision-making. An example of these steps taking place has been shown at Rush-Copley in the US where their solution included "*remote access for clinicians to view and update a patient's medical record from their office, home or anywhere in the world*" [38].

The relevance of biometric approaches to the health care context is critical if the move to mobile devices is to be inevitably made. Mobile devices can facilitate the linking of information technologies with medical information in order to increase the accuracy of decisions and the productivity of clinicians and their professional group. Until recently, the most reliable sources of medical information available to this user group for best practices were the medical textbook, in which the latest medical information was published. However, this 'latest' information was no longer the most recent because of the publishing cycle of paper-based literature [39].

The only technological option available has been for clinicians to run a computer search on the National Library of Medicine's MEDLINE database, which has been deemed by some health care professionals as "*time consuming and seldom feasible during a patient visit*" [39]. The SEMIS project is striving for IT-enabled evidence-based medicine, which, if planned and implemented with careful consideration, can help to not only centralise the latest best practices, but also sort through extensive amounts of medical data to assist in patient care. There is perhaps no greater need for fast access to current and accurate information than by medical practitioners. The potential of mobile technologies in this context has been left largely unexplored to date.

6.0 REFERENCES

[1] D. R. Masys, *Medical Informatics: Glimpses of the Promised Land.* Academic Medicine, 1989. 64 (January): pp. 13-14.

[2] K. Vredenburg, S. Isensee, and C. Righi, *User-Centered Design: An Integrated Approach*. 2002, New Jersey: Prentice Hall.

[3] P. Brown, C. McArthur, L. Newby, R. Lay-Yee, P. Davis, and R. Briant, "Cost of Medical Injury in New Zealand: A Retrospective Cohort Study". *Journal of Health Services Research and Policy*, 2002. 7 (Suppl 1: S1:): pp. 29-34.

[4] Cerner, *Cerner Corporation: Health Care Information Technology Systems*. Cerner Corporation. http://www.cerner.com, 18 March 2004.

[5] C. Ross, E. Brownson, A. Baker, T. L. Leet, and K. N. Gillespie, eds. *Evidence-Based Public Health*. Vol. October, New York, Oxford University Press, 2002.

[6] D. L. Sackett, W. M. Rosenberg, J. M. Gray, R. B. Haynes, and W. S. Richardson, "Evidence-Based Medicine: What It Is and What It Isn't". *British Medical Journal,* 1996(321): pp. 71-2.

[7] A. DiCenso, N. Cullum, and D. Ciliska, "Implementing Evidence-Based Nursing: Some Misconceptions". *Evidence-Based Nursing,* 1998(1): pp. 38-40.

[8] S. Stevens, I. Scott, L. von Hellens, and G. Iselin, "Closing the Loop: the Role of Clinical Leaders in Integrating Research and Practice. *Australian Health Review*, 2004. 27(1): pp. 56-64.

[9] I. A. Scott, "Time for a Collective Approach from Medical Specialists to Clinical Governance". *Internal Medical Journal,* 2002. 32: pp. 499-501.

[10] J. Burke, M. Castro, S. Singh, and T. P., *SITCRC User Needs Project * Phase 1 Overview.* 2002, User Needs Project, User Environment Program, SITCRC: Melbourne, Australia.

[11] J. Beekhuyzen, L. von Hellens, M. Morley, and S. H. Nielsen. Searching for a Methodology for Smart Internet Technology Development, in *11th International Conference on Information Systems Development*. 2003. Melbourne, Australia.

[12] G. Astbrink, and J. Beekhuyzen. *Synergies of Universal Design and User-Centred Design*. in *Proceedings of the International Conference on Human Computer Interaction (HCI)*. 2003. Crete, Greece.

[13] K. Frantz, *How Much Security Is Enough When It Comes to HIPAA?* Journal of Health Care Compliance, 2003. 5(4): pp. 47, 2pgs.

[14] E. F. Stone, and D. L. Stone, *Privacy In Organizations: Theoretical Issues, Research Findings, and Protection Mechanisms.* Research in Personnel and Human Resources Management, 1990. 8: pp. 349-411.

[15] D. Zweig, and J. Webster, *Where Is The Line Between Benign and Invasive? An Examination of Psychological Barriers to the Acceptance of Awareness Monitoring Systems.* Journal of Organisational Behaviour, 2002. 23(5): pp. 605.

[16] Maradiegue, A., *The Health Insurance Portability and Accountability Act and Adolescents.* Pediatric Nursing, 2002. 28(4): pp. 417, 4pgs.

[17] Hewlett_Packard, *[WHITE PAPER] Biometric Security with the iPAQ Pocket PC h5400 Series*. 2003, Smart Handheld Group. pp. 1-10.

[18] S. Chartrand, *Verifying People's Identities By Using Their Hands, Eyes or Voices*, in *New York Times*. 2003: New York. p. C.2.

[19] G. Calderon, and V. Subbaiah, *Automated Fingerprint Identification Systems: What Internal Auditors Need to Know.* Internal Auditing, 2003. 18(3): p. 15.

[20] S. Harris, *Biometrics Need a Measure of Security.* Government Executive, 2003. 35(9): p. 70.

[21] B. Kelly, *PDAs: Handy Reference Tools.* Health Data Management, 2001. 9(11): p. 24, 3pgs.

[22] R. Miller, *Mobile Content Goes to the Doctor.* EContent, 2003. 26(8/9): p. 52, 4pgs.

[23] K. Rosenthal, *"Touch" vs. "Tech": Valuing Nursing-Specific PDA Software.* Nursing Management, 2003. 34(7): p. 58.

[24] C. Poulter, *Information Security and Company Executives*, in *National Business Bulletin: Australia's Leading Management Magazine*. 2003. pp. 30-32.

[25] D. Willis, *Let Your Fingers Do the Logging in.* Network Computing, 1998. 9(10): p. 122, 4pgs.

[26] J. L. Cambier, *For Accurate Biometric Identification, The Eyes Have It*, in *HP Chronicle*. 1999: Austin. p. 1, 2pgs.

[27] E. Weise, *Body MayBe KeyTo A Foolproof ID:[FINAL Edition]*, in *USA Today*. 1998: Arlington. p. 04.D.

[28] J. Borzo, *Technology (A Special Report); The To-Do Life: Safeguard Confidential Personal Information.* Wall Street Journal, 2003: p. R.9.

[29] J. Morrissey, *Eyeing A New Solution.* Modern Healthcare, 2002. 32(47): p. 28, 1pg.

[30] B. Short, *Getting the 411 on Biometrics.* Security, 2002. 39(7): p. 48, 2pgs.

[31] R. Spiegel, *We Know Who You Are.* Design News, 2003. 58(4): p. 109.

[32] Conry-Murray, A., *Lesson 168: Biometrics.* Network Magazine, 2002. 17(7): p. 28, 2pgs.

[33] R. J. Babyak, *The Right Touch.* Appliance Manufacturer, 1998. 46(3): p. 60, 2pgs.

[34] T. Costlow, *Fingerprint ID Points of Sales.* Electronic Engineering Times, 1997(959): p. 49, 2pgs.

[35] A. Zipern, *Before Opening Up, A Laptop Looks for Matching Prints*, in *New York Times*. 2001: New York. p. G.3.

[36] B. Fonseca, *Future Secure.* InfoWorld, 2003. 25(2): p. 1, 5pgs.

[37] F. Pierce, *Biometric Identification.* Health Management Technology, 2003. 24(5): p. 38, 2pgs.

[38] J. Piotrowski, *Looking At the Big Picture.* Modern Healthcare, 2003. 33(47): p. S8.

[39] B. Briggs, *Working Together: I.T. and Evidence- Based Medicine.* Health Data Management, 2004. 12(1): p. 24.

BIOGRAPHY

Jenine Beekhuyzen is a Senior Research Assistant and Lecturer in the School of Computing and Information Technology at Griffith University, and is the Director of Research Services for ThoughtWare Australia. After completing a Diploma of Business (TAFE Qld) and an IT Honours degree (Griffith University) on Enterprise Resource Planning Systems and Organisational Culture in 2001, she continues to be involved in a number of research projects including the WinIT (women in IT) project and a Cooperative Research Centre (CRC) project on Smart Internet Technology. She serves as a reviewer for a number of information systems academic journals and conferences. She is currently the President of the School of Computing and IT Alumni Association and Editor of their e-zine. In addition to her role at Griffith University, she works as an consultant for a small IT organisation, ThoughtWare, with a focus on knowledge management solutions.

Mark Siedle is the Director of his own Australian web development company, ihoard Pty Ltd, and works as a Research Assistant for Griffith University in Australia. Mark endeavours to find the answers to security threats relating to the use of technology in modern-day society. Culture and gender issues relating to technology acceptance are the focus of Mark's research efforts at present, while PHP web development gives Mark the constant challenges to keep his motivation high.

Liisa von Hellens is an Associate Professor in the School of Computing and Information Technology at Griffith University. She has over thirty years experience in the IT industry, including working as a programmer and systems developer, as well as university level education experience in Australia, Finland and UK. Her doctorate at Templeton College, Oxford University, was about packaged software provision and use, and her subsequent research, publications and consulting activities have covered information systems development and use in organizations, strategic quality management of software development, the management of IT human resources and the associated skills supply. Several refereed articles have been published on these topics and she has supervised several research higher degree students to a successful completion. She is also actively involved in reviewing papers for information systems journals as well as serving as a member of the program committee and an associate editor for information systems conferences.

Professor Rodney Topor is a computer scientist who has made significant contributions to the theory of program verification, logic programming, database systems, data mining and parallel query evaluation. He has worked at Monash University, the University of Melbourne and Griffith University. His current interests include XML data management, functional programming and health informatics.

Dr Stella Stevens' area of expertise is health services research and teaching. She is a Senior Lecturer at Griffith University, Australia and team leader in the Service Industry Research Centre at Griffith. Currently she is researching the use of hand held devices to assist clinicians manage data, evaluating the use of the balanced scorecard in managing performance in hospitals, and examining health promotion interventions to assist emergency care workers manage stress. Her research expertise is in qualitative methods and research involving elites. She obtained her PhD at Liverpool University in the UK, and is active in several professional organisations.

ACKNOWLEDGEMENTS

This paper draws on some of the findings of a recent project conducted by the second author on the privacy and security issues of biometric technology. The first author carried out the writing of the paper in consultation with the other three authors, who provided an information management, health services and computer science perspective respectively. The authors would like to acknowledge the support of the Smart Internet Technology CRC.