Towards a Development of a Learners' Ratified Acceptance of Multi-biometrics Intentions Model (RAMIM): Initial Empirical Results

Yair Levy
Graduate School of Computer and Information Sciences
Nova Southeastern University, USA
levyy@nova.edu

Michelle M. Ramim
H. Wayne Huizenga School of Business and Entrepreneurship
Nova Southeastern University, USA
ramim@nova.edu

Abstract

User authentication is a continuous balance between the level of invasiveness and system security. Password protection has been the most widely user authentication approach used, however, it is easily compromised. Biometrics authentication devices have been implemented as less compromised approach. This paper reports on initial results of user perceptions about their acceptance of a multi-biometrics authentication approach in the context of e-learning systems. Specifically, this paper reports on the initial empirical results on the development of a learners' Ratified Acceptance of Multi-biometrics Intentions Model (RAMIM). The model proposed look at the contributions of learners' code of conduct awareness, perceived ease-of-use, perceived usefulness, and ethical decision making to their intention to use multi-biometrics for authentication during e-learning exams. The study participants included 97 managers from service oriented organization and government agencies who attended e-learning courses. Results demonstrated high reliability for all constructs measured and indicated that perceived ease-of-use and perceived usefulness are significant contributors to learners' intention to use multi-biometrics. Conversely, code of conduct awareness appears to have little or no contribution on learners' intention to use multi-biometrics, while learners' ethical decision making appears to have marginal contribution.

Keywords: E-learning Systems, Biometrics Systems, Technology Acceptance, Online Exam Security, Secured Exam Submission.

Introduction

Security concerns associated with information systems (IS) has intensified with the growth of IS enabled networks within organizations and the growing use of organizational electronic records (Gal-Or & Ghose, 2005; Goodhue & Straub, 1991; Wang, Chaudhury, & Rao, 2008). Valid authentication of IS users is a perpetual challenge amongst organizations (Furnell, Dowland, Illingworth, & Reynolds, 2000; Siponen & Heikka, 2008). Moreover, according to Furnell et al. (2000), use of password authentication is "easily compromised" (p. 529). In the context of higher education, the explosive growth of e-learning systems has also raised concerns on the issue of valid authentication during e-learning (Ramim & Levy, 2006). According to Ramim and Levy (2007), authentication of students in e-learning systems should expand beyond the limited username/password verification upon entry to a more diverse authentication. They also noted that such approach may help reduce academic misconduct in e-learning (Ramim & Levy).

In recent years, the price of commercial biometrics authentication devices has been steadily dropping (Anderson & Choobineh, 2008). The use of security related devices has sharply increased beyond highly secured environments such as financial institutions, government agencies, and military facilities (Cavusoglu, Mishra, & Raghunathan, 2005). Nowadays, biometrics authentication devices are utilized to measure employee attendance and track employee daily activities (Yeh & Chang, 2007). However, there is a growing concern about the invasiveness of such devices, effective safeguarding of biometrics information, as well as potential misuse of information captured by biometrics devices (Lin, Chuang, & Fan, 2005). Thus, investigation of the factors that may impede the acceptance of such devices is warranted (James, Pirim, Boswell, Reithel, & Barkhi, 2006). Such investigation is future warranted in the context of e-learning systems when considering the increase issues with academic misconduct. Additionally, there is a new trend in biometrics practice to integrate more than a single biometrics method of authentication in order to increase its accuracy, transparency, and reliability beyond the initial point of entry while monitoring real-time users' activity in a non intrusive manner (Clarke & Furnell, 2005, 2007).

This research refers to the new approach as a 'multi-biometrics' authentication method. As the context of this work is in e-learning systems, this work reports on initial empirical results collected in the process to develop and validate a learners' Ratified Acceptance of Multi-biometrics Intentions Model (RAMIM). The multi-biometrics authentication approach includes two devices: fingerprint scanner and Web-cam head geometry scanner.

Theoretical Background

A vital aspect of security is authentication whereby the system verifies the user's identity as declared (Liebl, 1993). Authentication systems include two principal elements, namely identification, and, verification. During the identification stage the user declares their identity, followed by the verification stage in which the identity is validated. Consequently, authentication protocols establish the identification processes between the host and the user. Examples of authentication protocols include password authentication protocol (PAP), encryption, and Kerberos to name a few. The standardization of authentication protocols for authentication systems is critical to establishing a secured environment (Liebl, 1993; Oorschot & Thorpe, 2008).

According to Furnell et al. (2000), "There are three main approaches to user authentication: something the user knows (e.g. password or personal identification number (PIN)), something the user has (e.g. a card or other token) and something the user is (e.g. a biometric characteristic)" (p. 529). Funnel et al. (2000), Oorschot and Thorpe (2008), as well as Rodwell, Furnell, and Reynolds (2007) suggested that while passwords are the most common authentication process, passwords tend to be undermined by users. Though users perceive passwords to be the preferred method, there is a need to promote additional authentication methods including physiological and behavioral biometrics. As a result, researchers recommend enhancing authentication methods by utilizing multiple means of authentication to provide for better authentication verification (Mizuno, Yamada, & Takahashi, 2005; Tsalakanidou, Malassiotis, & Strintzis, 2007).

Research efforts in the area of biometrics have been driven partly as a result of the increase of identity fraud crimes and the compromising of existing identification methodologies (James et al., 2006). Moreover, the U.S. Federal Trade Commission (2008) has reported that financial loss resulting from such crimes has been mounting and exceeding $1.2 billion annually. Business organizations and government agencies have been motivated to identify and adopt advanced identification technologies (James et al., 2006; Wang et al., 2008). While prices of biometrics solutions has been declining, ongoing research about biometrics has focused on three main themes. The three themes include: a) adoption and utility (James et al., 2006; Woodward, 1997), b) methods including biological and behavioral (Clarke & Furnell, 2007; James et al., 2006; Pusara & Brodley, 2004), and c) evaluation of beck-end technologies (Abate, Nappi, Riccio, & Sabatino, 2007; Rodwell et al., 2007).

James et al. (2006) defined biometrics a process that employees "biological features, especially with regard to the study of unique biological characteristics of humans" (p. 3). Such unique biological characteristics refer to individual humane identities such as DNA, voice, retinal and iris, fingerprints, facial images, hand prints, or other unique biological characteristics. James et al. (2006) noted that biometric is "a method of identification that has been growing in popularity" (p. 2). Moreover, Pons (2006) as well as Jain, Hong, and Pankanti (2000) noted that biometric devices are technological devices that utilize an individual's unique physical or behavioral characteristic to identify and authenticate the individual precisely. Essentially, biometric technologies operate by scanning a biological characteristic and matching it with the stored data. Sasamoto, Christin, and Hayashi (2008) as well as Pusara and Brodley (2004) referred to keystrokes dynamics and mouse clicks as examples of behavioral characteristics. Though behavioral-characteristics-based biometrics has been associated with a low error rate in lab settings, further work is needed to commercialize such methods to large scale systems.

Following prior literature about biometrics, this paper proposes a new definition for multi-biometric in which a multilateral model scheme that utilizes biological and or physiological characteristics that the end-user has. Multi-biometrics aids to authenticate and verify users in a secured environment. Additionally, multi-biometrics can enable ongoing non-intrusive verification not only at the point of entry but also throughout the logged-in session.

Researchers have studied extensively users' acceptance of technology. One heavily used model in IS research is the classical Technology Acceptance Model (TAM) that was proposed by Davis (1986, 1989). The TAM model is based on the Theory of Reasoned Action (TRA) proposed by Ajzen and Fishbein (1980). IS literature reports extensive evidence that users' perceived usefulness and ease-of-use are strong predictors of technology acceptance (Davis, 1989; Simon & Paper, 2007; Venkatesh, Morris, Davis, & Davis, 2003; Viswanath & Hillol, 2008). Moreover, there is a compelling empirical evidence in IS literature that intention to use a technology is a significant contributor to actual technology acceptance and use (Bagozzi, 2007; Gefen, Karahanna, & Straub, 2003).

The surge in use of e-learning systems in higher education has been documented by numerous studies (Eshet-Alkalai & Geri, 2007; Geri & Gefen, 2007; Levy, 2006). However, ethical issues with the use of e-learning systems have also been a growing concern for higher educational institutions as well as for researchers (Kennedy, Nowak, Raghuraman, Thomas, & Dacis, 2000; McCabe, 2003; Ramim, 2007). As a consequence of these concerns, researchers emphasized the need to conduct studies that investigate students' ethical decisions making (McCabe, 2004; Pincus, 2003; Rawwas, 2004). Additionally, organizational behavior literature provides support that employees' code of conduct awareness and their ethical decision making are potential contributing constructs to their use of IS (Cronan, Leonard, & Kreie, 2005; Kreie & Cronan, 1998). However, literature indicates that in general the existence of a code of conduct is not enough; rather, the extent of individuals' awareness of the code appeared to be a key factor (Chonko, 2003; Harris, 2002; Wotruba, Chonko, & Loe, 2001). Despite these findings, issues related to the role of code of conduct awareness and ethical decision making in e-learning remain unresolved.

According to Ramim and Levy (2007), there is very little research conducted about the incorporation of biometrics into educational settings, let alone into the authentication process of students in e-learning environments. Thus, this study propose to investigate the learners' perceptions about their acceptance of 'multi-biometrics' authentication method including two devices: fingerprint scanner and Web-cam head geometry scanner. This study attempted to develop and validate a learners' Ratified Acceptance of Multi-biometrics Intentions Model (RAMIM). The model is based on the contribution of the constructs of perceived usefulness, ease-of-use, code of conduct awareness, and ethical decision making to learner's perceived intention to use multi-biometrics specifically during online exam taking.

Methodology

This study used validated measures from prior literature. The items to measure the constructs of perceived ease-of-use, perceived usefulness, and intention to use were adopted from Gefen et al. (2003) as well as James et al. (2006). Additionally, the items to measure code of conduct awareness and ethical decision making were adopted from Ramim (2007). All items used 5-point Likert-type scale.

Population and Sample

The sample included 97 managers from service oriented organization and government agencies in USA who attended e-learning Masters of Business Administration (MBA) and Masters of Public Administration (MPA) courses.

Propositions

Proposition 1: Learners' code of conduct awareness will have a significant positive contribution to their intention to use multi-biometrics for authentication during e-learning exams.

Proposition 2: Learners' perceived ease-of-use will have a significant positive contribution to their intention to use multi-biometrics for authentication during e-learning exams.

Proposition 3: Learners' perceived usefulness will have a significant positive contribution to their intention to use multi-biometrics for authentication during e-learning exams.

Proposition 4: Learners' ethical decision making will have a significant positive contribution to their intention to use multi-biometrics for authentication during e-learning exams.

Figure 1 depicts the conceptual map for the learners' Ratified Acceptance of Multi-biometrics Intentions Model (RAMIM).

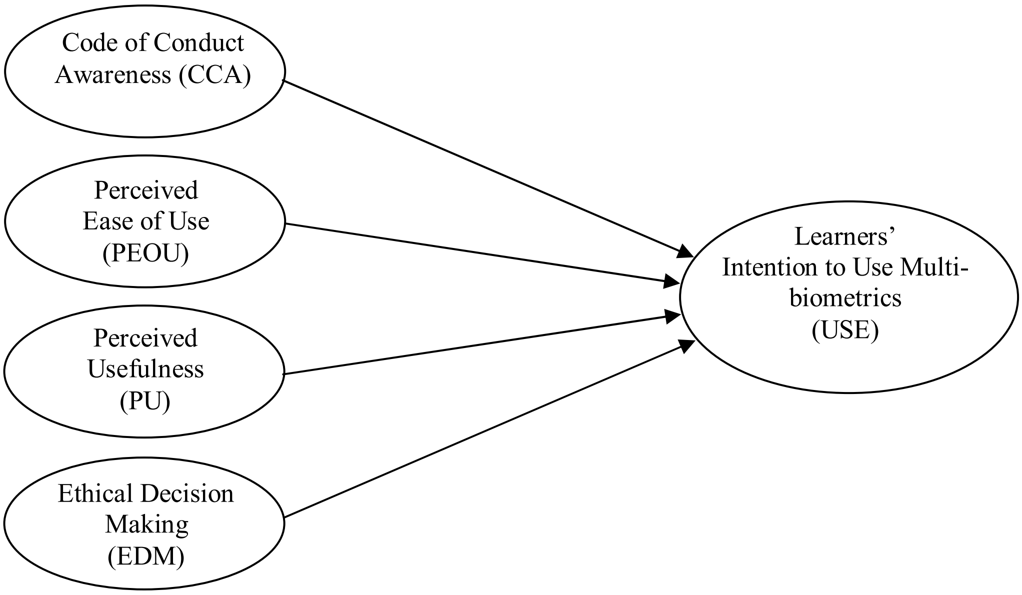
Code of Conduct Awareness (CCA)
Perceived Ease of Use (PEOU)
Perceived Usefulness (PU)
Ethical Decision Making (EDM)
Learners' Intention to Use Multi-biometrics (USE)

Figure 1. Conceptual Map for the Ratified Acceptance of Multi-biometrics Intentions Model (RAMIM)

Results

Descriptive Statistics

Table 1 depicts the demographics of the initial sample collected. The sample includes about 40% females and 60% males. Additionally, the initial sample includes a bi-polar distribution on ages with about 60% between the ages of 19 to 34, and about 30% between the ages of 40 to 54. Majority of the learners have experience with e-learning courses and more than half of the learners are working full time.

Table 1. Descriptive Statistics and Demographics of Learners (N=97)

Item	Frequency	Percentage (%)
Gender		
Male	59	60.8%
Female	38	39.2%
Age		
18 or under	1	1.0%
19-24	17	17.5%
25-29	25	25.8%
30-34	17	17.5%
35-39	5	5.2%
40-44	16	16.5%
45-54	14	14.4%
55-59	1	1.0%
60 or older	1	1.0%

Number of previous e-learning courses taken		
None, this was my first	10	10.3%
1	8	8.2%
2	11	11.3%
3	3	3.1%
4	7	7.2%
5 to 9	22	22.7%
10 or more	36	37.1%
Weekly hours for work/job		
No, I'm not working	16	16.5%
Less than 20	4	4.1%
20 to 29	10	10.3%
30 to 39	5	5.2%
40 to 49	45	46.4%
50 to 59	13	13.4%
60 or more	4	4.1%

Validity and Reliability

The overall validity of the instrument was twofold including the use of existing validated measures and a small group of five subject matter experts who reviewed the instrument. The reliability of the measures was investigated using Cronbach's Alpha. According to Mertler and Vannatta (2001), measures with Cronbach's Alpha of over .70 are considered reliable. The initial results indicate a Cronbach's Alpha of 0.848, 0.916, 0.922, 0.946, and 0.892 for usefulness, ease-of-use, code of conduct awareness, ethical decision making, and intention to use respectively (see Table 2).

Table 2. Summary of Construct Reliability Analysis using Cronbach's Alpha (N= 97)

Construct	No. of Items	Cronbach's Alpha
Code of Conduct Awareness (CCA)	4	0.922
Perceived Ease of Use (PEOU)	6	0.916
Perceived Usefulness (PU)	6	0.848
Ethical Decision Making (EDM)	21	0.946
Intention to Use (USE)	8	0.892

Ordinal Logistic Regression Analysis

The long term goal of this research is to employ structural equations modeling (SEM). However, the current initial sample size collected doesn't confirm to the use of SEM. As such, the current study used Ordinal Logistic Regression (OLR). Results of the initial data indicate that the overall OLR model fit is significant at -2 Log Likelihood=207.59, χ^2(df=4)=53.326, p<0.0001 (See Table 3). Table 4 depicts the results of the OLR analysis. These initial results indicate that code of conduct awareness appears to have little or no contribution on learners' intention to use multi-biometrics. Therefore, *Proposition 1* appears not to be supported. Additionally, ease-of-use and usefulness are significant. Thus, these results indicate that *Proposition 2* and *Proposition 3* are indeed supported at a significance level of p=0.021 and p

<0.001 correspondingly. Moreover, learners' ethical decision making appears to have marginal contribution with a significance level of p=0.071, thus, suggesting that *Proposition 4* is warranted additional investigation on a larger sample.

Table 3. Overall Ordinal Logistic Regression Model Fit (N= 97)

Model	-2 Log Likelihood	Chi-Square	df	Sig.
Intercept Only	260.915			
Final	207.589	53.326	4	0.000*

* p < 0.0001

Table 4. Ordinal Logistic Regression Parameter Estimates Results (N= 97)

	Estimate	Std. Error	Wald	df	Sig.		95% Confidence Interval	
							Lower Bound	Upper Bound
EDM	0.785	0.434	3.271	1	0.071		-0.066	1.636
PU	1.242	0.256	23.536	1	0.000	*	0.740	1.744
CC	0.201	0.254	0.628	1	0.428		-0.297	0.700
PEOU	0.700	0.303	5.348	1	0.021	**	0.107	1.293

* p < 0.001
** p < 0.05

Conclusions and Discussion

This work is an initial step in an investigation on the factors that may hinder learners to use multi-biometrics authentication during e-exams. The essence of this work is to better understand what factors may help increase the acceptance of multi-biometrics authentication approach when learners take e-exams. Although this work will seek additional data to better validate the initial model and results, these initial findings are substantial for higher educational institutions. First, higher educational institutions must fully understand the centrality of their learners' perceived usefulness and ease-of-use related to multi-biometrics authentication when implementing such technology in order to increase its acceptance. Second, it appears that ethical decision making may have some contribution to learners' acceptance of multi-biometrics authentication; however, such contribution might be limited or mediated by another construct. Third, it appears that contrary to other organizational behavior literature that indicated the centrality of employees' code of conduct awareness in security related issues, in the case of their acceptance of multi-biometrics authentication it may not have any direct contribution. This study highlights the need to incorporate multi-biometrics approach as no single biometrics device appears to be wholly appropriate to fit successfully a wide range of authentication needs of e-learning systems.

References

Abate, A. F., Nappi, M., Riccio, D., & Sabatino, G. (2007). 2d and 3d face recognition: A survey. *Pattern Recognition Letters, 28*(14), 1885-1906.

Ajzen, I., & Fishbein, M. (1980). *Understanding attitudes and predicting social behaviors*. Engelwood Cliffs, NJ: Prentice Hall.

Anderson, E. E., & Choobineh, J. (2008). Enterprise information security strategies. *Computers & Security, 27*(1-2), 22-29.

Bagozzi, R. P. (2007). The legacy of the technology acceptance model and a proposal for a paradigm shift. *Journal of the Association for Information Systems, 8*(4), 243-256.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2005). The value of intrusion detection systems in information technology security architecture. *Information Systems Research, 16*(1), 28–46.

Chonko, L. B., Wotruba, T. R., & Loe, T. W. (2003). Ethics code familiarity and usefulness: Views on idealist and relativist managers. *Journal of Business Ethics, 42*(3), 237-252.

Clarke, N. L., & Furnell, S. M. (2005). Authentication of users on mobile telephones - a survey of attitudes and practices. *Computers & Security, 24*(7), 519-527.

Clarke, N. L., & Furnell, S. M. (2007). Advanced user authentication for mobile devices. *Computers & Security, 26*(2), 109-119.

Cronan, T. P., Leonard, L. N. K., & Kreie, J. (2005). An empirical validation of perceived importance and behavior intention in IT ethics. *Journal of Business Ethics, 56*(3), 231-240.

Davis, F. D. (1986). Technology acceptance model for empirically testing new end-user information systems: Theory and results. Massachusetts Institute of Technology. (UMI No. AAT 0374529), MA, USA.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319-339.

Eshet-Alkalai, Y., & Geri, N. (2007). Does the medium affect the message? The influence of text representation format on critical thinking. *Human Systems Management, 26*(4), 269-279.

FTC. (2008). *Consumer freud and identity theft complaint data January – December 2007*. Retrieved September 14, 2008. from http://www.ftc.gov/opa/2008/02/fraud.pdf.

Furnell, S. M., Dowland, P. S., Illingworth, H. M., & Reynolds, P. L. (2000). Authentication and supervision: A survey of user attitudes. *Computers & Security, 19*(6), 529-539.

Gal-Or, E., & Ghose, A. (2005). The economic incentives for sharing security information. *Information Systems Research, 16*(2), 186–208.

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and tam in online shopping: An integrated model. *MIS Quarterly, 27*(1), 51-90.

Geri, N., & Gefen, D. (2007). Is there a value paradox of e-learning in MBA programs? *Issues in Informing Science and Information Technology, 4*, 163-174.

Goodhue, D. L., & Straub, D. W. (1991). Security concerns of system users : A study of perceptions of the adequacy of security. *Information & Management, 20*(1), 13-27.

Harris, J., Cummings, M., & Fogliasso, C. . (2002). Ethical codes and their effect on conduct. *Journal of Consortium for Computing Sciences in Colleges, 18*(1), 259-269.

Jain, A., Hong, L., & Pankanti, S. (2000). Biometric identification. *Communications of the ACM, 43*(2), 91–98.

James, T., Pirim, T., Boswell, K., Reithel, B., & Barkhi, R. (2006). Determining the intention to use biometric devices: An application and extension of the technology acceptance model. *Journal of Organizational and End User Computing, 18*(3), 1-25.

Kennedy, K., Nowak, S., Raghuraman, R., Thomas, J., & Dacis, S. (2000). Academic dishonesty and distance learning: Student and faculty views. *College Student Journal, 34*(2), 309-315.

Kreie, J., & Cronan, T. P. (1998). How men and women view ethics. *Association for Computing Machinery. Communications of the ACM, 41*(9), 70-78.

Levy, Y. (2006). *Assessing the value of e-learning systems*. Hershey, PA: Information Science Publishing.

Liebl, A. (1993). Authentication in distributed systems: A bibliography. *ACM Operating Systems Review, 27*(4), 31-41.

Lin, C.-L., Chuang, T. C., & Fan, K.-C. (2005). Palmprint verification using hierarchical decomposition. *Pattern Recognition, 38*(12), 2639-2652.

McCabe, D. L. (2003, Sep 10). Caught copying: Electronic plagiarism is a new addition to the IT lexicon. *Businessline,* 1-3.

McCabe, D. L., & Pavela, G. . (2004). Ten updated principles of integrity. *Change, 36*(3), 10-17.

Mertler, C. A., & Vannatta, R. A. (2001). Advanced and multivariate statistical methods: Practical application and interpretation. Los Angeles, CA: Pyrczak Publishing.

Mizuno, S., Yamada, K., & Takahashi, K. (2005). *Authentication using multiple communication channels.* Paper presented at the 2005 workshop on Digital identity management, Fairfax, Virginia, USA.

Oorschot, P. C., & Thorpe, J. (2008). On predictive models and user-drawn graphical passwords. *ACM Transactions on Information and System Security, 10*(4), 17-33.

Pincus, H. S., & Schmelkin, L. P. (2003). Faculty perceptions of academic dishonesty: A multidimensional scaling analysis. *Journal of Higher Education, 74*(2), 196-209.

Pons, A. P. (2006). Biometric marketing: Targeting the online consumer. *Communications of the ACM, 49*(8), 60-66.

Pusara, M., & Brodley, C. E. (2004). *User re-authentication via mouse movements.* Paper presented at the 2004 ACM workshop on Visualization and data mining, Washington, DC, USA.

Ramim, M. M. (2007). An examination of factors associated with students' ethical decision making in post-secondary e-learning programs. *Dissertation Abstracts International, 68*(12), 1-123. (UMI No. AAT 3290937).

Ramim, M. M., & Levy, Y. (2006). Securing e-learning systems: A case of insider cyber attacks and novice IT management in a small university. *Journal of Cases on Information Technology, 8*(4), 24-35.

Ramim, M. M., & Levy, Y. (2007). *Towards a framework of biometrics exam authentication in e-learning environments.* Paper presented at the Information Resources Management Association International Conference (IRMA) 2007, Vancouver, Canada.

Rawwas, M. Y. A., Al-Khatib, J. A., & Vitell, S. J. (2004). Academic dishonesty: A cross-cultural comparison of U.S. And Chinese marketing students. *Journal of Marketing Education, 26*(1), 89-100.

Rodwell, P. M., Furnell, S. M., & Reynolds, P. L. (2007). A non-intrusive biometric authentication mechanism utilising physiological characteristics of the human head. *Computers and Security, 26*(7), 468-478.

Sasamoto, H., Christin, N., & Hayashi, E. (2008). *Undercover: Authentication usable in front of prying eyes.* Paper presented at the 26 annual ACM SIGCHI conference on Human factors in computing systems, Pittsburgh, PA.

Simon, S. J., & Paper, D. (2007). User acceptance of voice recognition technology: An empirical extension of the technology acceptance model. *Journal of Organizational and End User Computing, 19*(1), 24-50.

Siponen, M., & Heikka, J. (2008). Do secure information system design methods provide adequate modeling support? *Information and Software Technology, 50*(9-10), 1035-1053.

Tsalakanidou, F., Malassiotis, S., & Strintzis, M. G. (2007). A 3d face and hand biometric system for robust user-friendly authentication. *Pattern Recognition Letters, 28*(16), 2238-2249.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly, 27*(3), 425-478.

Viswanath, V., & Hillol, B. (2008). Technology acceptance model 3 and a research agenda on interventions. *Decision Sciences, 39*(2), 273.

Wang, J., Chaudhury, A., & Rao, H. R. (2008). A value-at-risk approach to information security investment. *Information Systems Research, 19*(1), 106-120.

Woodward, J. (1997). *Biometrics: Privacy's foe or privacy's friend?* Paper presented at the IEEE, Arlington, VA, USA.

Wotruba, T. R., Chonko, L. B., & Loe, T. W. (2001). The impact of ethics code familiarity on manager behavior. *Journal of Business Ethics, 33*(1), 59-69.

Yeh, Q.-J., & Chang, A. J.-T. (2007). Threats and countermeasures for information system security: A cross-industry study. *Information & Management, 44*(5), 480-491.