Towards a Model of Factors Affecting Resistance to Using Multi-Method Authentication Systems in Higher-Education Environments

Joseph W. Marnell[1], Yair Levy[2]
[1]Information Systems
Wayland Baptist University-Lubbock
801 N. Quaker Avenue, Lubbock, Texas 79416, USA
[2]Graduate School of Computer and Information Sciences
Nova Southeastern University
3301 College Avenue
Fort Lauderdale-Davie, Florida 33314-7796, USA
marnellj@wbu.edu

ABSTRACT: *Over the course of history, different means of object as well as person identification and verification have evolved for user authentication. In recent years, a new concern has emerged regarding the accuracy of authentication and of protection of personal identifying information (PII), because previous information systems (IS) misuses have resulted in significant financial loss. Such losses have escalated more noticeably because of identity-theft incidents due to breaches of PII within multiple public-access environments, such as institutions of higher-education. Although the use of various biometric and radio frequency identification (RFID) technologies is expanding, resistance to using these technologies remains an issue. As such, in this research-in-progress paper, we outline a predictive study to assess the contribution of campus student's perceptions of the importance of protecting their PII, noted as Perceived Value of Organizational Protection of PII (PVOP), authentication complexity (AC), and invasion of privacy (IOP) on their resistance to using multi-method authentication systems (RMS) in higher-education environments. In this work-in-progress study, we seek to better understand the theoretical foundations for the effect of student's perceptions on their resistance to using multi-method authentication systems (RMS) in higher-education environments and uncover key constructs that may significantly contribute to such resistance. A quasi-experiment is proposed including clearly identified procedures and data analyses.*

Keywords: Authentication on-campus, Student's Resistance to Biometrics, Identity Theft, Biometric Measures on-campus, IT Complexity on-campus

Received: 2 December 2013, Revised 3 January 2014, Accepted 7 January 2014

1. Introduction

Recent research suggested that electronic-commerce (e-commerce) transactions are not the primary source of identity theft (Collins, 2003; Newman, 2004). However, Shareef and Kamur (2012) proposed that identity theft plays a substantial role in purchase resistance for consumers of e-commerce. Increasing demands to prevent identity theftare advocated in recent literature, newspapers, and government policies. According to Shareef and Kamur (2012), "*current research addresses the issues of identity theft; source, type, and preventative measuring tools*" (p. 30). Additional studies indicated that inadequate user authentication (UA) methods are a contributing factor for identity theft(Fichtman, 2001). A national survey conducted by

the Federal Trade Commission (FTC) (2008) revealed that 4.7% of American adults experienced identity theft that involved the loss of personal identifying information (PII), while such numbers appear to grow rapidly every year. Industry responses to combat the aspects of identity theft are focused on the verifiable identification of individuals through the development of acceptable multi-method authentication systems (Bellah, 2001). While current research has shown significant advances in biometric recognition, users continue to resist using biometric technology to enhance password security including in institutionsof higher-education (Levy & Ramim, 2009). This resistance is attributed to concerns related to protecting their PII, invasion of privacy (IOP), and authentication complexity (AC).

It appears that a need exists to better understand the problem with identity theft escalation as a result of users sharing, reusing, and losing passwords, as well as the mishandling of PII during e-commerce transactions also in the context of institutions of higher-education (Furnell, Dowland, Illingworth, & Reynolds, 2000). This has resulted in significant losses from illegal authentication and theft of PII. Efforts to combat the weaknesses in current methods of username/password entries have influenced the development of biometric forms of identification (Altinkemer & Wang, 2011). However, single-authentication biometrics still exhibit misreads and susceptibility to spoofing vulnerability, so organizations have turned to testing multi-method authentication systems for user authentication (Gunson, Marshall, Morton, & Jack, 2010). Increased monetary losses occurring due to privacy attacks during e-commerce activities within organizations have swayed individuals' perceptions of the importance of protecting PII (PVOP), lessened their use of Internet purchasing, and could influence their resistance to new authentication methods (Dowling & Staelin, 1995; Mayer, Davis, & Schoorman, 1995). Presently, many of the charges for tuition, books, dormitories, meal plans, trips, and other activities both on-campus as well as off-campus are conducted over the Internet or via kiosks throughout their campus. As a result of these increasing demands, institutions of higher-education are implementing chip-based student IDs that can incorporate the student biometric characteristics. However, little is known about the various factors affecting resistance to using multi-method authentication systems in higher-education environments. As such, this work-in-progress research is aimed at proposing a model tovalidate empirically the contribution of the constructs of PVOP, IOP, and AC on individual's resistance to using multi-method authentication systems (RMS) in higher-education environments.

2. Theoretical Background

2.1 Perceived Value of Organizational Protection of Personal Identifying Information

According to Dowling and Staelin (1994) as well as Mayer et al. (1995), the PVOP of PII is demonstrated by the elevated concerns of IOP resulting from financial losses occurring from identity theft. These losses are increasing due to individuals exhibiting unsafe password behaviors such as reusing and sharing passwords, as well as the lack of awareness of the costs associated with PII theft (Eisenstein, 2008; Furnell, 2008; Kumar, Mohan, & Holowczak, 2008; Levy, 2008). Users are unaware that illegal access to PII enables unauthorized access to use, copy, release, destroy, deny, or gain access to create imposter accounts (Furnell, 2008; Obrien, 2002; Rezgui & Marks, 2008; Shaw et al., 2008).

According to Eisenstein (2008), PII loss stems from a variety of causes, resulting in significant financial loss. These occurrences include merchant failures to protect client data under their personal control, stolen mail, computer data breaches; illegally reproduced pay sites such as PayPal©, viruses, and phishing scams (Furnell, 2008; Kumar, 2008; Shaw et al., 2008). Furnell (2008) identified users as a) those informed of areas of identity theft risk and are doing something to protect themselves, as opposed to b) those who remain indifferent to the seriousness of the loss of PII.

2.2 Invasion of Privacy

According to Karyda and Gritzalis (2009), privacy can generally be defined as "t*he individual's ability to control the terms by which their [sic] personal information is collected and used*" (p. 195). Thus, the prevention of IOP could represent protection or freedom from interference by others (Gritzalis, 2004). The concept of acknowledging an individual's right to privacy includes the factors of necessity, finality, transparency, and proportionality (Karyda & Gritzalis, 2009).

Furthermore, privacy crusader Alan Westin defined privacy as "*the claim of individuals, groups, or institutions to determine for themselves, when, where, how, and to what extent information about themselves is communicated to others*" (Hough, 2009, p.7). However, Westin's contemporary, David Flaherty, separated privacy further into four sections. His four sections are comprised of:

Solitude: The perfect and unblemished state of privacy whereby you can easily restrict access to yourself from others by

withdrawing your presence.

Intimacy: This is a by membership only and groups protect their members.

Anonymity: This is a form of being "*off the grid*" in that you are able to protect yourself from ongoing public recognition or involvement.

Reserve: This is the measure of trust that one places in others not to disclose specific information about oneself, such as what, where, when, and how (Hough, 2009).

2.3 Authentication Complexity

Furnell et al. (2004) reported on a study of alternative authentication methods. Their study identified infrastructures as trying to cope with the increasing number of password-protected systems. Adding to the growing burden are Websites, resulting in the ever-increasing occurrences of reuse and sharing of password-sensitive authentications. Regardless, security personnel still prefer password and personal identification number (PIN) usage as trade-offs, as the number of imposters and false alarm rates are still high. Thus, the responsibility of memorizing, not sharing, multitudes of passwords, and not sharing any with others is not easy, due to their inconvenience. Such issue can result in significant security breaches of PII and in identity theft. Sasse et al. (2001) conducted a study that indicated that with PINs being more difficult for customers to remember than passwords, individuals are resorting back to using date of birth or writing information on paper.

Furthermore, Furnell et al. (2004) identified UA methods that provide lowered identity theft occurrences as single-factor authentications, based on something that the user knows (e.g. passwords or PIN), possesses (smart card, token, or RFID device), or is (e.g. a biometric characteristics like fingerprints, eye retina, face, voice, etc.). Multi-factor authentication can be based on any two of these methods combined (Levy & Ramim, 2009; O'Gorman, 2003). Furthermore, Murdoch, Drimer, Anderson, and Bond (2010) conducted a study that showed that strengths in multi-factor authentication systems indicated a remarkable decline in fraud following a compulsory usage requirement after implementation. This decline is significant in that other online banking fraud rose by 55% during the same time period (Gunson et al., 2010). As a result of increased fraud leading to identity theft, two-factor authentication use is increasing in the UK within outside vendor use. However, the fraud rate with single-factor authentication, within known banking entities, remains unaffected (Gunson et al., 2010).

2.4 Mixed-Method Authentication Systems

With increasing demands being placed on the financial service industries, enhanced means of protecting PII through added security measures is being investigated (Hiltgen et al., 2006). According to Weir et al. (2009), mixed methods of identification are referred to as multi-method, or two-factor, authentication, versus single-factor, and are being tested as well as implemented in varying degrees. Two-factor authentication is comprised of multiple objects such as card readers or tokens represented by '*what you have*', in addition to a multitude of other types of identification. These other authentications refer to passwords/PINs or biometric devices identified as '*personal characteristics*.' Some of these recognized biometric traits are voiceprints, facial features, fingerprints, and gait. Additionally, radio frequency identification is increasingly being used in financial transactions through mobile devices.

According to Coventry, De Angeli, and Johnson (2003), gaining secure access to sensitive areas through possession of held objects, knowledge, or physical characteristics has accelerated significantly through a multitude of consumer devices, services, vehicles, and banking interfaces. However, this expansion of methods to gain authentication has resulted in a battle of supremacy between usability, memorability of passwords, securing of PII, and a consideration of multi-method authentication systems (Adams & Chang, 1993; Adams & Sasse, 1999; Levy & Ramim, 2009; Yan, Blackwell, Anderson, & Grant, 2001). According to De Angeli, Coutts, Coventry, Johnson, Cameron, and Fischer (2002) as well as Dhamija and Perrig (2000), the continual upgrading of mixed methods of password usage impacts the complexity levels of authentication methods. This impact comprises replacing PINs with forms of biometric identification that includes photos and fingerprints (De Angeli, Coutts, Coventry, Johnson, Cameron, & Fischer, 2002; Dhamija, & Perrig, 2000).

2.5 Resistance to using Multi-method authentication systems

Resistance to using multi-method authentication systems (RMS) is defined as the reluctance to accept alternative methods of user verification due to perceived security, complexity, and privacy concerns (Bellah, 2001; Van Hoose, 2008). According to Huixian and Liaojun (2009), the challenge of providing "*privacy protection of biometric data has become a common concern of the public*" (p. 295). Therefore, IOP is recognized as a significant influence over the degree of acceptance of biometric-

based authentication. Biometric technologies come with an array of problems that are both technical as well as behavioral (Pons & Polak, 2008). These difficulties include data degradation and variances in data recorded. However, resistance to usingis "*based on attitudes and behaviors related to user acceptance, trust, habits, etc*". (p. 115). As a result of inconsistent attitudes regarding the concerns over privacy, storage, protection, and the potential loss of PII, the measuring of user resistance is a challenging task. This can be attributed to users exhibiting fear, hesitancy, and discomfort over demands to change from current forms of authentication (Pons & Polak, 2008).

3. Research Problem and Study Goals

This research problem that we seek to address is identity-theft incidents due to breaches of personal identifying information (PII) (Venkatesh, Morris, Davis, & Davis, 2003; Zviran & Erlich, 2006). Such PII breaches are significant threats to invasion of privacy (IOP) during e-commerce activities by users in public-access environments, including higher-education (Venkatesh et al., 2003; Zviran & Erlich, 2006). Kim, Jeong, Kim, and So (2011) identified PII as financial card numbers, usernames, passwords, medical records, driver's licenses, and Social Security numbers (Kim et al., 2011). These PII represent targets of online theft during e-commerce activities. Doolin, Dillon, Thompson, and Corner (2005) defined e-commerce as information networks that enable data flow for business, capital, and logistical support. Existing methods to protect PII during e-commerce activities are based on three types of authentication: username/password, tokens/smart cards, and biometrics (Levy & Ramim, 2009; Millett & Holden, 2003). According to Venkatesh et al. (2003), resistance to accepting emerging technology is based on the difference between an individual's nonadoption and his or her acceptance levels. Thus, resistance on the part of individuals may be the cause of significant failures in the implementation of multi-method authentication systems(Robey, Ross, & Boudreau, 2002).

We attempt to achieve six research goals. The first three specific goals are to investigate empirically the contribution of PVOP, IOP, and AC to RMS, respectively, in higher-education environments. The fourth specific goal is to investigate empirically the contribution of the interaction of the three independent variables, PVOP, IOP, and AC on students RMS in higher-education environments. The fifth specific goal is to investigate empirically whether any significant differences of PVOP, IOP, AC, and RMS exist based on student's ages (AGE), gender (GEN), person's prior experience with identity theft (EXP), and person's acquaintance experience with identity theft (EXA).

The main research question (RQ) that this study will address is: What is the contribution of PVOP, IOP, AC, and interaction on student's resistance to using multi-method authentication systems in higher-education environments?

In addressing the main RQ, this proposed study will seek to assess three specific directional propositions and six hypotheses (noted in null form):

P1: Perceptions of the importance of protecting PII (PVOP) will have a statistically significant *negative* influence on Student's resistance to using a multi-method authentication system (RMS) in higher-education environments.

P2: Invasion of privacy (IOP) will have a statistically significant *positive* influence on student's resistance to using a multi-method authentication system (RMS) in higher-education environments.

P3: Authentication Complexity (AC) will have a statistically significant *positive* influence on student's resistance to using a multi-method authentication system (RMS) in higher-education environments.

H4: There will be no significant interaction effect of *PVOP*, *IOP*, and *AC* on student's resistance to using a multi-method authentication system (*RMS*) in higher-education environments.

H5a: *PVOP*, *IOP*, *AC*, and *RMS* will have no statistically significant difference based on age (*AGE*).

H5b: *PVOP*, *IOP*, *AC*, and *RMS* will have no statistically significant difference based on gender (*GEN*).

H5c: *PVOP*, *IOP*, *AC*, and *RMS* will have no statistically significant difference based on person's prior experience with identity theft (*EXP*).

H5d: *PVOP*, *IOP*, *AC*, and *RMS* will have no statistically significant difference based on person's acquaintance experience with identity theft (*EXA*).

H6: There will be no statistically significant differences on *PVOP*, *IOP*, *AC*, and *RMS* based on students who used a multi-method authentication system in higher-education environments and those who haven't.

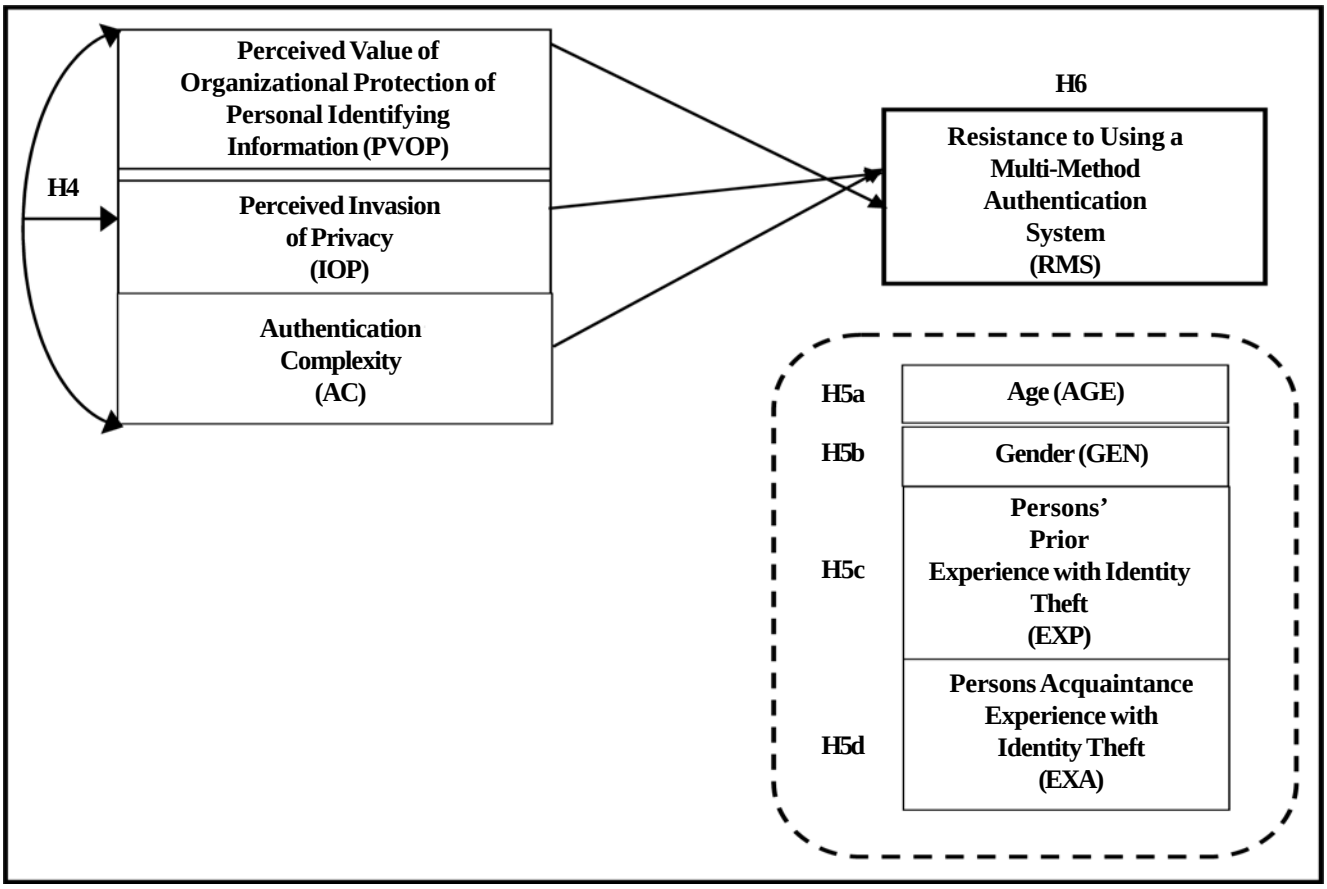

Figure 1. Proposed Conceptual Map for Predicting RMS in higher-education environments

Figure 1 presents the proposed conceptual map for predicting RMS in higher-education environments.

4. Experimental Research and Methodology

To investigate the effects of introducing multibiometrics for user authentication, a lab experiment will be implemented. Three groups consisting of two experimental and one control will be used (Levy & Ellis, 2011). As indicated above, organizations, both public and private, require secure authentication to their systems to ensure protection of data and certainty as to prevention of privacy intrusion. This research seeks to uncover whether multibiometrics can be accepted as a means of authentication by users without added complexity. Control Group A will consist of approximately 50 participants. Experimental Group B will consist of approximately 50 participants. Control Group C will consist of 50 participants. The experimental study participants will consist of students from a local private university that has various degrees for differing academic levels. All participants in the three groups will be randomly assigned. The experiment is planned over the timeframe of a full term consisting of 11 weeks.To measure the effects of resistance to using multibiometrics for user authentication, a system will be set up whereby all three groups will asked to log in to the system using a different method for each group. Once logged in, the users will be asked to answer a Web-based survey. The system will track the number of logon attempts for each group. The survey will also ask the participants questions to measure each of the constructs (PVOP, IOP, AC, & RMS), and questions to collect some demographics information needed for the analysis (AGE, GEN, EXP, & EXA).

Following the experimental data collection, a pre-analysis data screening process will be conducted to be certain that the accuracy of data collected doesn't improperly influence validity results (Levy, 2006; Mertler & Vannatta, 2010; Tabachnich & Fidell, 1996). Following that, the data will be analyzed using Partial Least Square (PLS) and a multivariate analysis of variance (MANOVA) to address the hypotheses proposed. Moreover, descriptive analysis will be done to provide some statistics about the participants.

5. Conclusions

This work-in-progress study is anticipated to provide greater understanding and contribution to the field of Information Security in the context of higher-education in two significant ways. First, it will investigate the biometric and RFID technologies that affect resistance (RMS) in higher-education environments during e-commerce activities that have been developed to respond to the increasing number of occurrences of identity theft either on-campus or off-campus. Second, it will investigate the primary constructs of PVOP, IOP, and AC contributing to student's RMS, while controlled for age (AGE), gender (GEN), identity theft experience (EXP), and the experience of acquaintance (EXA) in higher-education environments. Thus, the results of this study are anticipated to help in providing recommendations for both the research and use of multibiometrics systems in public access environments. It is the main objective and hope of this study to be able to determine which of the constructs has a significant contribution on RMS.

References

[1] Adams, A., Chang, S. Y. (1993). An investigation of keypad interface security. *Information & Management,* 24 (1) 53-59.

[2] Adams, A., Sasse, M. (1999). Users are not the enemy. *Communications of the ACM,* 42 (12) 41-46.

[3] Al-Harbi, A., Osborn, S. (2011). Mixing privacy with role-based access control. *Proceedings of the Fourth International Conference on Computer Science and Software Engineering*. ACM: New York, NY. 1-7.

[4] Altinkemer, K., Wang, T. (2011). Cost and benefit analysis of authentication systems. *Decision Support Systems*, 51 (3) 394-404.

[5] Attaran, M. (2006).The coming age of RFID revolution. *Journal of International Technology and Information Management,* 15 (4) 77-88.

[6] Barton, B., Byciuk, S., Harris, C., Schumack, D., Webster, K. (2005). The emerging cyber risks of biometrics. *Risk Management,* 52 (10) 26-31.

[7] Bellah, J. (2001). Training: Identity theft. *Law and Order,* 49 (10) 222-226.

[8] Bhattacharyya, S., JHA, S., Tharakunnel, K., Westland, J. (2011). Data mining for credit card fraud: A comparative study. *Decision Support Systems*, 50 (3) 602-613.

[9] Bolton, R., Hand, D. (2002). Statistical fraud detection: A review. *Journal of Statistics*, 17 (3) 235-255.

[10] Clarke, N. L., Furnell, S. M. (2005). Authentication of users on mobile telephones–A survey of attitudes and practices. *Computers and Security,* 24 (7) 519-529.

[11] Clodfelter, C. (2010). Biometric technology in retailing: Will consumers accept fingerprint authentication? *Journal of Retailing and Consumer Services*, 17 (3) 181-188.

[12] Collins, J. M. (2003). Business identity theft: The latest twist. *Journal of Forensic Accounting*, 1, p. 303-306.

[13] Coventry, L., De Angeli, A., Johnson, G. (2003). Usability and biometric verification at the ATM interface. *ACM*, 5, 153-160.

[14] De Angeli, A., Coutts, M., Coventry, L., Johnson, G. I., Cameron, D., Fischer, M. (2002). VIP: a visual approach to user authentication. *In*: Proceedings of the Working Conference on Advanced Visual Interfaces AVI, ACM Press, p. 316-323.

[15] DeLone, W., McLean, E. (2003).The DeLone and McLean model of information systems success: A ten-year update. *Journal of Management Information Systems*, 19 (4) 9-30.

[16] Dhamija, R., Perrig, A. (2000). A user study using images for authentication. *In*: Proceedings of 9th USENIX Security *Symposium*, 9, p. 4-4.

[17] Doolin, B., Dillon, S., Thompson, F., Corner, J. (2005). Perceived risk, the Internet shopping experience and online purchasing behavior: A New Zealand perspective. *Journal of Global Information Management,* 13 (2) 66-88.

[18] Dowling, G. R., Staelin, R. (1994). A model of perceived risk and intended risk-handling activity. *Journal of Consumer Research,* 21, p. 119-134.

[18] Eisenstein, E. (2008). Identity theft: An exploratory study with implications for marketers. *Journal of Business Research*, 61 (11) 1160-1172.

[19] Fichtman, P. (2001). Preventing credit card fraud and identity theft: A primer for online merchants. *Information Systems Security*, 10 (5) 1-8.

[20] FTC (1998). Privacy online: a report to congress, *Federal Trade Commission*, available at: www.ftc.gov/reports/privacy3/priv-23a.pdf (accessed 13 August 2008).

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

[22] Furnell, S., Papadopoulos, I., Dowland, P. (2004). A long-term trial of alternative user authentication technologies. *Information Management and Computer Security*, 12 (2) 178-190.

[23] Gottschalk, P. (2010). Categories of financial crime. *Journal of Financial Crime*, 17 (4) 441-458.

[24] Gritzalis, S. (2004). Enhancing Web privacy and anonymity in the digital era. *Information Management and Computer Security*, 12 (3) 255-288.

[25] Gunson, N., Marshall, D., Morton, H., & Jack, M. (2010). User perceptions of security and usability of single-factor and two-factor authentication in automated *telephone banking. Computers and Security*, 30 (4) 208-220.

[26] Higgins, G., Hughes, T., Ricketts, M., Wolfe, S. (2008). Identity theft complaints: Exploring the state-level correlates. *Journal of Financial Crime*, 15 (3) 295-307.

[27] Hiltgen, A., Kramp, T., Weigold, T. (2006). Secure Internet banking authentication. *IEEE Security and Privacy*, 4 (2) 21-90.

[28] Hinde, S. (2005). Identity theft and fraud. *Computer Fraud and Security*, 6, p. 18-20.

[29] Hough, M. G. (2009). Keeping it to ourselves: Technology, privacy, and the loss of reserve. *Technology in Society*, 31 (1) 406-413.

[30] Huxian, L., Liaojun, P. (2009). A novel biometric-based authentication scheme with privacy protection. *Information Assurance and Security*, 2, 295-298.

[31] Identity Theft Resource Center. (2012). 2012 Identity Fraud Report: Social Media and Mobile Forming the New Fraud Frontier. Retrieved February 26, from http://www.idtheftcenter.org/artman2/uploads/1/ITRC_Breach_Stats_Report_2011-20120207.pdf.

[32] Jain, A. K., Ross, A. (2004). Multibiometric systems. *Communications of the ACM*\, 47 (1) 34-40. Javelin Strategy and Research (2012). Survey: ID theft on the rise again, card victims jump by 2 million annually. Retrieved February 26, 2012, from https://www.javelinstrategy.com/news/1314/92/Identity-Fraud-Rose-13-Percent-in-2011/d,pressRoomDetail.

[33] Jerman-Blaziè, B., Klobucar, T. (2005). Privacy provision in e-learning standardized systems: Status and improvements. *Computer Standards and Interfaces*, 27 (6) 561-578.

[34] Jones, M. (1991). Privacy: A significant marketing issue for the 1990s. *Journal of Public Policy andMarketing*, 10, 133-148.

[35] Karyda, M., Gritzalis, S., Park, J., Kokolakis, S. (2009). Privacy and fair information practices in ubiquitous environments: Research challenges and future directions. *Internet Research*, 19 (2)194-208.

[36] Kim, W., Jeong, O., Kim, C., So, J. (2011). The dark side of the Internet: Attacks, costs and responses. *Information Systems*, 36 (3) 675-705.

[36]Klaus, T., Wingreen, S., Blanton, E. J. (2010). Resistant groups in enterprise system implementations: A Q-methodology examination. *Journal of Informational Technology*, 25, p. 91-106.

[37] Kumar, N., Mohan, K., Holowczak, R. (2008). Locking the door but leaving the computer vulnerable: Factors inhibiting home users' adoption of software firewalls. *Decision Support Systems*, 46, p. 254-264.

[38] Lai, F., Li, D., Hsieh, C. (2012). Fighting identity theft: The coping perspective. *Decision Support Systems*, 52 (2) 353-363.

[39] Laudon, K., Laudon, J. (2010). *Management Information Systems: Managing the Digital Firm* (11th ed.). London: Pearson Education.

[40] Levy, Y. Ellis, T. (2011). A guide for novice researchers on experimental and quasi-experimental studies in information systems research. *Interdisciplinary Journal of information, knowledge, and management,* 6, p. 151-161.

[41] Levy, Y., Ramim, M. M. (2009). Initial development of a learners' ratified acceptance of multibiometrics intentions model (RAMIM). *Interdisciplinary Journal of E-Learning and Learning Objects*, 1 (5) 379-397.

[42] Mayer, R., Davis, J., Schoorman, D. (1995). An integrative model of organizational trust. *Academic of Management Review,* 20 (3) 709-734.

[43] Mertler, C., Vanatta, R. (2001). *Advanced and Multivariate Statistical Methods: Practical Application and Interpretation*. Los Angeles: Pyrczak.

[44] Millett, L., Holden, S. (2003). Authentication and its privacy effects. *IEEE Internet Computing*, 7 (6) 54-58.

[45] Murdoch, S. J., Drimer, S., Anderson, R., Bond, M. (2010). Chip and PIN is broken. 2010 IEEE Symposium on Security and Privacy (SP), 433-446.

[46] Newman, G. R. (2004). Identity theft, problem-oriented guides for police (problem-specific guides series, No. 25), Washington, DC: U.S. Department of Justice.

[47] Nosko, A., Wood, E., Molema, S. (2010). All about me: Disclosure in online social networking profiles: The case of Facebook. *Computers in Human Behavior,* 26 (3) 406-418.

[48] O'Brien, J. (2002). *Management Information Systems: Managing Information Technology in the e-Business Enterprise*. Boston: McGraw Hill.

[49] O'Gorman, L. (2003). Comparing passwords, tokens and biometrics for authentication. *In*: Proceedings of the IEEE, 91 (12).

[50] Pearce, M., Zeadally, S., Hunt, R. (2010). Assessing and improving authentication confidence management. *Information Management and Computer Security*, 18 (2) 124-139.

[51] Penny, K. I. (1996). Appropriate critical values when testing for a single multivariate outlier by using the Mahalanobis distance. *Journal of the Royal Statistical Society. Series C (Applied Statistics),* 45 (1) 73-81.

[52] Pons, A. P., Polak, P. (2008). Understanding user perspectives on biometric technology, *Communications of the ACM,* 51 (9) 115–118.

[53] Rezgui, Y., Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computers & Security,* 27 (7-8) 241-253.

[54] Robey, D., Ross, J., Boudreau, M. (2002). Learning to implement enterprise systems: An exploratory study of the dialectics of change. *Journal of Management Information Systems*, 19, p. 17-46.

[55] Ross, A., Nandakumar, K., Jain, A. K. (2006). *Handbook of Multibiometrics*. London, UK: Springer.

[56] Roussos, G., Moussouri, T. (2004). Consumer perceptions of privacy, security, and trust in ubiquitous commerce. *Personal Ubiquitous Computing,* 8 (6) 416-429.

[57] Sekaran, U. (2003). *Research Methods for Business – A Skill-Building Approach.* Hoboken, NJ: John Wiley & Sons.

[58] Shadish, W., Cook, T., Campbell, D. (2002). *Experimental and quasi-experimental designs for generalized causal inference.* Boston: Houghton Mifflin Company.

[59] Shareef, M. A., Kumar, Vinod (2012). Prevent/Control Identity Theft: Impact on Trust and Consumers' Purchase Intention in B2C EC. *Information Resources Management Journal (IRMJ),* 25 (3) 30-60.

[60] Shaw, R. S., Chen, C. C. Harris, A. L., Huang, H. J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education,* 52, p. 92-100.

[61] Tabachnick, B., Fidell, L. (2001). *Using Multivariate Analysis.* New York, NY: Harper Collins College Publishers.

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

[63] Van Hoose, S. J. (2008). *Attitudes Toward Biometric Authentication/Identification for Use in Student Assessment in Online Courses in Higher Education.* (Doctoral Dissertation). Retrieved from ProQuest Dissertations and Theses. (Accession Order No. [103008]).

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

[65] Wang, P., Petrison, L. (1993). Direct marketing activities and personal privacy: A consumer survey. *Journal of Direct Marketing*, 7 (1) 7-19.

[66] Weir, C., Douglas, G., Carruthers, M., Jack, M. (2011). User perceptions of security, convenience and usability for ebanking authentication tokens. *Computers & Security*, 28 (1) 47-62.

[67] Wendels, T., Mählmann, T., Versen, T. (2009). Determinants of banks risk exposure to new account fraud–Evidence from Germany. *Journal of Banking and Finance*, 33 (2) 347-357.

[68] Westin A. (1967). Privacy and freedom. New York: Atheneum.

[69] Yan, J., Blackwell, A., Anderson, R., Grant, A. (2001). The memorability and security of passwords –Some empirical results. *Technical Report No.* 500 2001, *computer Laboratory University of Cambridge*, http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/tr500.pdf

[70] Zviran, M., Erlich, Z. (2006). Identification and authentication: Technology and implementation issues. *Communications of the Association for Information Systems*, 17 (4) 90-105.

Author Biographies

Joseph Marnell has been an MIS adjunct instructor and the Information Systems and Facilities Maintenance Administrator at Wayland Baptist University, Lubbock, Texas for 14 years. He has earned two associate degrees and a Bachelor's degree in Business Administration and Computer Information Systems from Eastern New Mexico University, Portales, New Mexico. He has an MBA with MIS concentration and pursuing his PhD in Information Systems at Nova Southeastern University. He holds numerous industry certifications, including A+, Network+, RFID+, Fiber Optic Certified, NSA Security Assurance, Microsoft Certified, Auto-ID Biometric Certified. He also serves as board member for several different agencies.

Yair Levy a Professor at the Graduate School of Computer and Information Sciences at Nova Southeastern University and the director of the Center for e-Learning Security Research (CeLSR). During the mid to late 1990's, he assisted NASA to develop e-learning systems. He earned his Bachelor's degree in Aerospace Engineering from the Technion (Israel Institute of Technology). He received his MBA with MIS concentration and Ph.D. in Management Information Systems from Florida International University. His current research interests include security issues with e-learning systems, cyber-security skills, and cognitive value of information systems. Dr. Levy is the author of '*Assessing the Value of e-Learning systems*' (2006). His research publications appear in numerous peer-reviewed journals and conference proceedings. Also, Dr. Levy has been serving as a member of conference proceedings committee for numerous scholarly conferences. Moreover, Dr. Levy has been serving as a referee research reviewer for hundreds of national and international meetings on IS, scientific outlets. He is a frequent invited keynote speaker at national and international meetings on IS, Information Security, and online learning topics. Dr. Levy's teaching interests in the masters' level include MIS, system analysis and design, information systems security, e-commerce, and Web development. His teaching interests in the doctoral level include Information Systems Development (ISD) and Advanced Multivariate Research Methods and Statistics. To find out more about Dr. Levy, please visit his site: http:scis.nova.edu/~levyy/