Association for Information Systems
AIS Electronic Library (AISeL)

WISP 2012 Proceedings

Pre-ICIS Workshop on Information Security and Privacy (SIGSEC)

Winter 12-14-2013

Investigating the Role of Multibiometric Authentication in Professional Certification E-exams

Garrett Smiley
Nova Southeastern University

Yair Levy Ph.D.
Nova Southeastern University, levyy@nova.edu

Nathan Clarke
Plymouth University

Eric Ackerman
Nova Southeastern University

Investigating the Role of Multibiometric Authentication in Professional Certification E-exams

Garrett Smiley
Graduate School of Computer and Information Sciences, Nova Southeastern University, Ft. Lauderdale, FL, USA

Yair Levy[1]
Graduate School of Computer and Information Sciences, Nova Southeastern University, Ft. Lauderdale, FL, USA

Nathan Clarke
Centre for Security, Communications and Network Research, Plymouth University, Plymouth, Devon, UK

Eric Ackerman
Graduate School of Computer and Information Sciences, Nova Southeastern University, Ft. Lauderdale, FL, USA

ABSTRACT

E-learning has grown to such an extent that paper-based testing is being replaced by computer-based testing also known as e-exams. Because these e-exams can be delivered outside of the traditional proctored environment, additional authentication measures must be employed in order to offer similar authentication assurance as found in proctored, Paper-Based Testing (PBT). In this study, we extended the body of knowledge in e-learning research by comparing e-exam scores and durations of three separate groups of e-exam takers using different authentication methods: Online Using Username/Password (OLUP), In-Testing Proctored Center (ITPC), and Online Proctored with Multibiometrics (OPMB). The aim was to better understand the role as well as the possible effect of continuous and dynamic multibiometric authentication

[1] Corresponding author: mailto:levyy@nova.edu; +1-954-262-2006

on professional certification e-exam scores and durations. Our results indicated that group affiliation, i.e. type of authentication methods, had no significant effect on differences among e-exam scores and durations. While there was a clear path of increased mean e-exam score as authentication method was relaxed, it was evident from the analysis that these were not statistically significant, probably due to the limited sample size. Age was found to have a significant effect on e-exam scores where younger participants were found to have higher e-exam scores and lower e-exam durations than older participants. Gender was not found to have a significant effect on e-exam scores nor durations. This study's results can help organizations better understand the role, possible effect, and potential application of continuous and dynamic multibiometric authentication as a justifiable approach when compared with the more common authentication approach of User Identifier (UID) and password, both in professional certification e-exams as well as in an online environment.

Keywords: biometrics, multibiometrics, authentication, e-exam, proctored e-exam, professional certification, e-learning, Information Technology Proficiency (ITP), Certified E-exam Developer (CED), Multibiometric Unified Layered Learning Engine Network (MULLEN)

INTRODUCTION

There still remains a great difficulty in ensuring correct identification and authentication in any Web-based system in general, both prior to and during taking an e-exam specifically (Levy & Ramim 2009; Reguzi & Marks 2008). The need for valid authentication in education can be felt in general in e-learning systems, in e-exams in particular, and especially in professional certification e-exams. Moreover, it appears that in high-stakes e-exams, such as

professional certification, a weak form of authentication brings the possibility of non-course takers who are experts in the area of the exam to take it for the course takers. An exploratory investigation on the effects of *continuous* and *dynamic* authentication on e-exam scores appeared to be highly desired (Levy & Ramim, 2009; Ramim & Levy 2007). Furthermore, given that many professional certification e-exams are scored and timed, while multibiometrics is one of the most secured authentication mechanisms available today, an exploratory investigation on the effects of continuous and dynamic multibiometric authentication on e-exam scores appeared to be warranted (Baron & Crooks 2005; Ramim & Levy 2007). Thus, the goal of our study was to compare e-exam scores and durations of three separate groups using three different authentication methods: Online Using Username/Password (OLUP), In-Testing Proctored Center (ITPC), and Online Proctored with Multibiometrics (OPMB) to better understand the role of continuous and dynamic multibiometric authentication on professional certification e-exams. The scope of our study was to examine whether or not there was an impact of the different authentication methods on e-exam score and duration due to differing levels of authentication. The relevance and significance of this study were in its novel investigation on the effects of continuous as well as dynamic multibiometrics on e-exam scores and durations as compared to the most common authentication mechanisms, the username and password combination.

LITERATURE REVIEW

Authentication

There is a pressing need for valid authentication (Jain et al. 2000). Valid authentication is needed for correct authorization (Clarke & Furnell 2007; Jain et al. 2004). A stronger and more

effective authentication mechanism can help to ensure the identities of those being authenticated (Clarke et al. 2003; Maltoni et al. 2009; Ramim & Levy 2007). In light of the problems associated with passwords, it is necessary to consider alternative methods of authentication that may reduce such problems without introducing unnecessary complexity to the end user, rendering the system difficult to use (Irakleous et al. 2002; Masys et al. 2002).

Biometrics

Of the three authentication methods, biometric-based authentication mechanisms are considered to be the most secure (Clarke & Furnell 2007; Hwang et al. 2008). Biometric identifiers use unique physiological or behavior-based identifiers, generally do not vary over time, cannot be shared, easily guessed, or stolen; thus, making biometrics difficult to abuse and less prone to attacks (Bosworth et al. 2005; Jain 2007; Ribaric & Fratric 2005; Wang et al. 2008). Several studies have been undertaken illustrating that using single factor biometrics alone for a robust, accurate, and secure authentication is insufficient (Hao et al. 2006; Joyce & Gupta 1990; Marcialis et al. 2009; Nagar et al. 2009; Park et al. 2007; Song et al. 2007; Teoh et al. 2006; Teoh, Kuan, & Lee 2008; Vielhauer & Steinmetz 2004). Furthermore, using an authentication method that relies on multiple 'who you are' authentication mechanisms is more secure than using an authentication method that relies on a single 'who you are' authentication mechanism (Ailisto et al. 2006; Bouchaffra & Amira 2008; Jain & Ross 2004).

Multibiometrics

The overall validity of an authentication process can greatly be improved by using multibiometric mechanisms (Ailisto et al. 2006; Bouchaffra & Amira 2008; Jain 2007; Jain et al.

2005; Ross, Jain, & Reisman 2003). Fusion associated with multibiometric authentication can greatly reduce error rates, False Rejection Rate (FRR), and False Acceptance Rate (FAR) (Maurer & Baker 2008; Nandakumar et al. 2008; Ribaric & Fratric 2005). As with single factor biometrics, some of the most serious obstacles to widespread multibiometric adoption are directly tied to user acceptance and interaction. Several studies suggested that people are hesitant to adopt multibiometrics due to such issues as comfort levels, pleasantness, perceived usefulness, and ethical decision making (Hernández et al. 2007; Levy & Ramim 2009; Levy et al. 2011). Yet, multibiometrics can significantly decrease error rate, driving the chances of an incorrect identification to a negligible percentage (Ailisto et al. 2006; Jain 2007; Walton 2005). Thus, it can be concluded that multibiometric authentication is the strongest and most defensible authentication solution available nowadays (Clarke et al. 2003). As it is relatively new to e-learning, there is still a strong need for better understanding of multibiometric implementations in educational settings (Levy et al. 2011). Specifically, Levy and Ramim (2009) stated that, "[f]uture studies may attempt to examine the use of multibiometrics in e-learning exams in an experimental setting and compare results with a control group" (p. 391), thus, supporting the need for our study.

E-Learning

E-learning systems and e-exams have significantly increased in the past decade, with organizations moving away from more historically common testing delivery methodologies such as PBT (Bunz 2005; Prince et al. 2009; Wallace & Clariana 2005). In contrast to traditional brick and mortar teaching methods, e-learning systems provide opportunities previously not available to students, such as automatic e-exam grading, ease of access, ease of use, flexible class time, e-

exam scheduling, lack of geographical constraints, and tailored instruction (Furnell et al. 1998; Irving 2006; Patterson 2006; Sanchez-Franco 2010; Tan 2009). Information Technology Proficiency (ITP) has been found to be an effective indicator of the intention to use technology and to use it effectively; an example being an e-exam candidate proficient with Information Technology (IT) taking an e-exam delivered via an e-learning system potentially resulting in an affected e-exam score (Ball & Levy 2008; Ballou & Huguenard 2008; Barker & Brooks 2005; Sanchez-Franco 2010; Thompson et al. 2006). Controls such as age, gender, and experience are often measured variables in exam score studies (Anstine & Skidmore 2005; Ballou & Huguenard 2008; Chyung 2007; de Winter & Wieringa 2008; Gratton-Lavoie & Stanley 2009; Howard 2005; Ihme et al. 2009). Academic dishonesty is one of the strongest arguments for a more secure solution with e-learning systems (Haney & Clarke 2007; Harmon & Lambrinos 2008; McCabe 2009; Nathanson et al. 2006; Rudd & Stoll 2004; Woodward et al. 2007). In light of the problems associated with knowledge-based authentication mechanisms and the long standing need for security within academia for e-learning, it is necessary to consider alternative mechanisms of authentication (Kambourakis et al. 2007; Rezgui & Marks 2008). The viability for the future of e-learning partially rests on meeting the challenge of accurate assessments (González-Tablas et al. 2008; Sandoe & Milliron 2000; Weippl 2007). Effectively authenticating students is crucial to preventing academic dishonesty of online assessments, particularly in e-exams (Haney & Clarke 2007; Harmon & Lambrinos 2008).

Professional Certification

The past decade has seen much growth for certified professionals in diverse industries (Coleman et al. 2009; Kavanagh 2006; Langley 2006). Many professional certifications are

acquired through exams, using a traditional PBT format, an e-exam format, or both (Kavanagh 2006; Leak & Spruill 2008; Shellenbarger 2008). Professional certification e-exams are considered high-stakes e-exams, where the chances of misconduct increase, especially in an online setting. Inaccurate authentication of the individual taking e-exams could support granting certification to those who should not have passed the e-exams or denying those who deserved to pass (Haney & Clarke 2007; Weippl 2007). Not only do professional certification e-exams have the well-established risks associated with standard exam formats and the additional risks associated with e-learning systems, but they also have the heightened risks of misconduct due to their high-stakes status. Thus, valid authentication is crucial for professional certification e-exams.

METHODOLOGY

The methodology used in this study was quasi-experiment using post-test only, non-equivalent groups, while group assignment was non-random due to participant accessibility. The study used three groups: ITPC, OPMB, and OLUP. The sample was all professionally certified members of a private organization. All organization members were included in the study's official sampling frame as they were participating in a professional certification e-exam.

Independent, Dependent, and Control Variables

The Independent Variable (IV) used in this study (the authentication method) is a combination of the most commonly used exam location (testing center), the most common online authentication approach (username & password), and the multibiometric approach. Measurement

of the IV was based on group assignment; this variable was nominal (categorical) in nature. The IV approach and justification are found in Table 1.

Table 1. IV Categorical Breakdown

Group	Authentication Approach	Justification
ITPC	Username and Password w/ 2 Forms of ID (Proctored)	uses the most common authentication approach as it is the control group
OLUP	Username and Password (Non-proctored)	uses the most common online approach (e.g., Blackboard & WebCT)
OPMB	Multibiometric – Finger and Face Recognition (Proctored)	uses the treatment, as it is the experimental group

E-exam score and duration were used as Dependent Variables (DVs) in our study. Measurement of these DVs included score, which was a percentage of correct responses on the certification e-exam (%) and duration (mm:ss); these variables were interval in nature and were collected by the MULLEN system. Age, gender, and ITP were used as control variables.

Reliability and Validity

Cronbach's Alpha was used in order to address reliability for the e-exam and ITP survey instrument. Table 2 shows the results:

Table 2. Instrument Reliability

Instrument	Number of Remaining Items	Alpha
Certification E-Exam	18	0.730
ITP Survey	8	0.805

In addressing external validity, the study attempted to replicate as much as possible the most common professional certification e-exam setting(s). Instrument validity was addressed for the certification e-exam, as it was based on the organization's item writing standards, which are

based on industry standards and exam development best practices. Instrument validity for ITP Part I (IT Ability) was addressed in that it was based upon Ball and Levy (2008)'s ITP Instrument, which had a reliability score of 0.859 and it represented five accepted areas for an IS professional (Caputo 2010; Gowan & Reichgelt 2010). Instrument validity for ITP Part II (IT Professional Development) was addressed in that it was based on Yoon (2008)'s ITP instrument, which indicated factor loadings > 0.671, with each factor section having Cronbach's Alpha > 0.785 and where the corrected item-total correlation was both positive and significant ($p \leq 0.01$). Internal validity for our study was addressed by using similar groups, providing a similar testing experience, and using appropriate covariates.

RESULTS

General Screening of the Dataset

In our study, we obtained a total of 81 participants over the three groups: with 27 participants in the ITPC group, 26 in the OPMB group, and 28 in the OLUP group. Even though the sample size was relatively small for this quasi-experiment, it was sufficient and justifiable for the inference testing that was used in the main analysis, as the sample size for each group exceeded the required sample size for Analysis of Variance (ANOVA) (greater than 12 in each group) and Analysis of Covariance (ANCOVA) (greater than five in each group). Table 1 provides the descriptive statistics of the study participants.

Instruments were delivered online so as to minimize errors. Responses were restricted through the use of multiple choice and Likert items. Human error was mitigated through automated data collection and storage. No missing data and no values outside of the

possible ranges were confirmed through visual checks. Using frequency distributions and descriptive statistics, the means and standard deviations for each variable were found to be within expectation. In looking for outliers, we used Mahalanobis Distance (MD). Three extreme values were identified in regards to e-exam score and removed prior to the main analysis. Prior to full data analysis, the ANOVA and ANCOVA assumptions were assessed and met including normal distribution, equal population variance, covariate independence, and linearity.

Table 3. Descriptive Statistics of the Study Participants

Gender	***Frequency***	***Percent***
Male	59	72.8%
Female	22	27.2%
Total	81	100.0%

Age	***Frequency***	***Percent***
26 - 35	37	45.7%
36 - 45	24	29.6%
46 - 55	8	9.9%
56 - 65	12	14.8%
Total	81	100.0%

ITP Score	***Frequency***	***Percent***
41 - 50	4	4.9%
51 - 60	19	23.5%
61 - 70	25	30.9%
71 - 80	19	23.5%
81 - 90	14	17.3%
Total	81	100.0%

E-exam Score	***Frequency***	***Percent***
11 - 20	3	3.7%
21 - 30	0	0%
31 - 40	2	2.5%
41 - 50	2	2.5%
51 - 60	8	9.9%
61 - 70	21	25.9%
71 - 80	27	33.3%
81 - 90	13	16.0%
91 - 100	5	6.2%
Total	81	100.0%

E-exam Duration	***Frequency***	***Percent***
851 - 910	5	6.2%
911 - 970	8	9.9%
971 - 1030	14	17.3%
1031 - 1090	9	11.1%
1091 - 1150	18	22.2%
1151 - 1210	14	17.3%
1211 - 1270	6	7.4%
1271 - 1330	3	3.7%
1331 - 1390	3	3.7%
1451 - 1511	1	1.2%
Total	81	100.0%

Data Analysis and Results

Our first hypothesis (H1) stated that there is no significant difference on certification e-exam scores across the three authentication methods (OLUP, ITPC, & OPMB). The null was not rejected for H1, as there was not a significant difference between the means of the three groups. However, there was a clear trend in the means of the three groups, where the ITPC group had the lowest mean, followed by the OPMB group, and then the OLUP group. The authentication groups did not have a significant effect on e-exam scores at the $p < 0.05$ level, $F(2, 75) = 0.503$, $p = 0.607$. Hypothesis H1a stated that there is no significant difference on certification e-exam scores across the three authentication methods (OLUP, ITPC, & OPMB) when controlling for age. The null was not rejected for H1a, as the ANCOVA was found to have no statistically significant main effects, $F(2, 74) = 0.052$, $p = 0.949$. When the effect of a person's age was removed (or accounted for), group affiliation still did not produce a significant difference. Hypothesis H1b stated that there is no significant difference on certification e-exam scores across the three authentication methods (OLUP, ITPC, & OPMB) when controlling for gender. For H1b, all effects were statistically non-significant at the 0.05 significance level. The main effect of authentication groups yielded an F ratio of $F(2, 72) = 0.358$, $p = 0.700$, indicating that there was no significant difference on e-exam scores among the three authentication groups. The main effect of gender yielded an F ratio of $F(1, 72) = 2.349$, $p = 0.130$, indicating that there was no significant difference on e-exam scores between male and female participants. The interaction effect was also non-significant, $F(2, 72) = 0.020$, $p = 0.980$. While there was a clear path of increased mean for e-exam score as the authentication method was relaxed, it is evident from the analysis that these were not statistically significant, and maybe due to the sample size. Figure 1

illustrates the results by depicting the means plot for the three groups, which shows that while there was not a significant difference between the means in each group; it is obvious that the ITPC group had the lowest mean, followed by the OPMB group, and then the OLUP group.

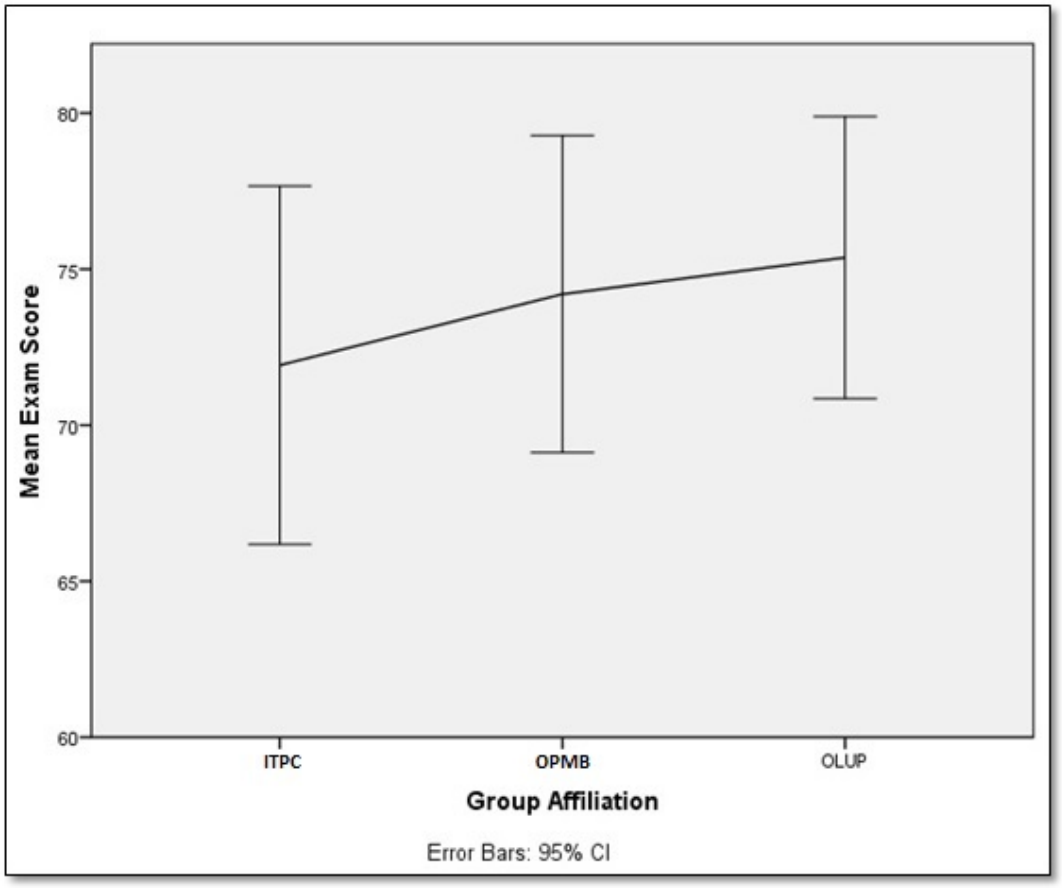

Figure 1. Means Exam Scores vs. Group Affiliation (i.e. strength of authentication)

Hypothesis H1c stated that there is no significant difference on certification e-exam scores across the three authentication methods (OLUP, ITPC, & OPMB) when controlling for ITP. The null was not rejected, as the ANCOVA was found to have no statistically significant main effects, $F(2, 74) = 0.683$, $p = 0.508$. When the effect of a person's ITP was removed (or accounted for), group affiliation still did not produce a significant difference. Hypothesis H2

stated that there is no significant difference on certification e-exam duration across the three authentication methods (OLUP, ITPC, & OPMB). The null was not rejected, as there was not a significant difference between the means in each group; however, it should be noted that the OPMB group had the largest e-exam duration mean among the three groups. The authentication groups did not have a significant effect on e-exam durations at the $p < 0.05$ level, $F(2, 75) = 0.448$, $p = 0.640$. The p-value was 0.640 which was greater than the Alpha level set at 0.05. Hypothesis H2a stated that there is no significant difference on certification e-exam duration across the three authentication methods (OLUP, ITPC, & OPMB) when controlling for age. The null was not rejected, as the ANCOVA was found to have no statistically significant main effects, $F(2, 74) = 0.648$, $p = 0.526$. When the effect of a person's age was removed (or accounted for), group affiliation still did not produce a significant difference (p=0.526). Hypothesis H2b stated that there is no significant difference on certification e-exam duration across the three authentication methods (OLUP, ITPC, & OPMB) when controlling for gender. The null was not rejected, as the main effect of authentication groups yielded an F ratio of $F(2, 72) = 0.111$, $p = 0.895$, indicating that there was no significant difference on e-exam durations among the three authentication groups. The main effect of gender yielded an F ratio of $F(1, 72) = 1.131$, $p = 0.291$, indicating that there was no significant difference on e-exam durations between male and female participants. The interaction effect was also non-significant, $p = 0.454$. Hypothesis H2c stated that there is no significant difference on certification e-exam duration across the three authentication methods (OLUP, ITPC, & OPMB) when controlling for ITP. The null was not rejected, as the ANCOVA was found to have no statistically significant main effects, $F(2, 74) = 0.655$, $p = 0.522$. When the effect of a person's ITP was removed (or

accounted for), group affiliation still did not produce a significant difference (p=0.522). Table 2 provides a summary of the main analysis findings.

Table 4. Main Analysis Findings Summary

Hypothesis	Findings
H1	The p-value (0.607) was greater than the 0.05 significance level. • Thus, there was no significant difference between e-exam scores among the three authentication groups: ITPC, OPMB, and OLUP, $F(2, 75) = 0.503$, $p = 0.607$. This was corroborated with the means plot with error bars for mean e-exam score versus group affiliation. While the p-value was not significant, the graph nicely illustrated that the mean score for the ITPC group was the lowest, followed by the OPMB group, and then the OLUP group.
H1a	According to the ANCOVA analysis: • Group affiliation had no significant effect on differences among e-exam scores, after accounting for age, $F(2, 74) = 0.052$, $p = 0.949$. • Age was found to have a significant effect on e-exam scores, $F(1, 74) = 23.666$, $p < 0.01$ • The interaction effect was not significant, $F(2, 72) = 0.290$, $p = 0.749$.
H1b	According to the factorial ANOVA analysis: • Group affiliation had no significant effect on differences among e-exam scores, after accounting for gender, $F(2, 72) = 0.358$, $p = 0.700$. • Gender also did not have a significant effect on e-exam scores, $F(1, 72) = 2.349$, $p = 0.130$. • Additionally, the interaction effect between group affiliation and gender had no significant effect on e-exam scores, $F(2, 72) = 0.020$, $p = 0.980$. These results were corroborated by the means plot with error bars of mean e-exam score versus group affiliation for each gender plotted on the same graph. These results were also corroborated by the grouped bar graph of mean e-exam score versus group affiliation by gender. While there was a clear path of increased mean e-exam score as authentication method was relaxed, it was evident from the analysis that these were not significant differences. While the p-value was not significant, the graph nicely illustrated that the mean for the ITPC group was the lowest, followed by the OLUP group, and then the OPMB group.
H1c	According to the ANCOVA analysis: • Group affiliation had no significant effect on differences among e-exam scores, after accounting for ITP, $F(2, 74) = 0.683$, $p = 0.508$. • ITP was found to have a significant effect on e-exam scores, $F(1, 74) = 32.423$, $p < 0.01$. • The interaction effect was not significant, $F(2, 72) = 0.120$, $p = 0.887$.
H2	The p-value (0.640) was greater than the 0.05 significance level. • Thus, there was no significant difference between e-exam durations among the three authentication groups: ITPC, OPMB, and OLUP, $F(2, 75) = 0.448$, $p = 0.640$. This was corroborated with the means plot with error bars for mean e-exam duration

	versus group affiliation.
H2a	According to the ANCOVA analysis: • Group affiliation had no significant effect on differences among e-exam durations, after accounting for age, $F(2, 74) = 0.648$, $p = 0.526$. • Age was not found to have a significant effect on e-exam durations, $F(1, 74) = 3.123$, $p = 0.081$. • The interaction effect was not significant, $F(2, 72) = 0.161$, $p = 0.851$.
H2b	According to the factorial ANOVA analysis: • Group affiliation had no significant effect on differences among e-exam durations, after accounting for gender, $F(2, 72) = 0.111$, $p = 0.895$. • Gender also did not have a significant effect on e-exam durations, $F(1, 72) = 1.131$, $p = 0.291$. • Additionally, the interaction effect between group affiliation and gender had no significant effect on e-exam duration, $F(2, 72) = 0.798$, $p = 0.454$. These results were corroborated by the means plot with error bars of mean e-exam duration versus group affiliation for each gender plotted on the same graph. These results were also corroborated by the grouped bar graph of mean e-exam duration versus group affiliation by gender. While there were some observed differences between the groups, it was evident from the analysis that these were not significant differences.
H2c	According to the ANCOVA analysis: • Group affiliation had no significant effect on differences among e-exam durations, after accounting for ITP, $F(2, 74) = 0.655$, $p = 0.522$. • ITP was found to have a significant effect on e-exam durations, $F(1, 74) = 14.382$, $p < 0.01$. • The interaction effect was not significant, $F(2, 72) = 1.158$, $p = 0.320$.

CONCLUSIONS AND DISCUSSIONS

The main goal of our research study was to compare e-exam scores and durations of three separate groups of e-exam takers using different authentication methods: OLUP, ITPC, and OPMB to better understand the role of multibiometric authentication on professional certification e-exam scores. The study was intended to generalize to all potential e-exam takers of professional certificates. A normally distributed sample was used for our study, which appeared to be representative of the overall population. The response rate for this quasi-experiment was 90%.

Age was found to have a significant effect on e-exam scores where younger participants were found to have higher e-exam scores and lower e-exam durations than older participants.

Even though group affiliation (i.e. authentication level) had no significant effect on differences among e-exam scores and durations, the mean scores for these variables were found to be the lowest for the ITPC group, followed by the OPMB group, and then the OLUP group. This corroborated with the results of Ihme et al. (2009) who revealed mean score differences, but these differences were explained due to age and education variance. They also were not caused by the different test settings: online and laboratory; no structural differences between the achievement scores of both samples were found. Our findings also corroborated those in another study of an online introductory economics course, where Gratton-Lavoie and Stanley (2009) found that age had a positive effect on student's performance in the course.

Gender was not found to have a significant effect on e-exam scores nor durations. Even though group affiliation had no significant effect on differences among e-exam scores, the mean scores were found to be the lowest for the ITPC group, followed by the OPMB group, and then the OLUP group. While there was a clear path of increased mean e-exam score as the authentication method was relaxed and some observed differences between the groups, it was evident from the analysis that these were not statistically significant. It might be that the low sample size obtained given our complex quasi-experiment has caused such results and additional validations are needed. Naturally, ITP was found to have a significant effect on e-exam scores and durations where greater scores with the ITP instrument indicated greater e-exam scores and lower e-exam durations.

IMPLICATIONS TO PRACTICE AND FUTURE RESEARCH

The first implication to practice is a better understanding of the role as well as the possible effect of continuous and dynamic multibiometric authentication on professional

certification e-exam scores and durations. Using multibiometric authentication in an online environment is a justifiable approach when compared with the more common authentication approach of username and password. The second implication to practice is that issues such as cost, perception, and interoperability need to be taken into account when developing a multibiometric adoption strategy. The approach used in our study provides a model for a cost-effective solution, which took into account ease of use as well as interoperability with existing technology. The third implication to practice is that a multi-layered approach should be considered in order to effectively engage end users with differing abilities and capabilities when utilizing multibiometrics. Since our study found that younger participants had higher e-exam scores as well as lower e-exam durations as compared to older participants, older participants may benefit from additional multibiometrics awareness and training. This approach may also be warranted due to the fact that participants with greater ITP also had higher e-exam scores. Additional studies in investigating other multibiometric authentication technologies in other IS contexts appear to be warranted. This study should be replicated in other contexts, with other populations using other combinations of multibiometric mechanisms for the purpose of authentication, using different types of authentications with or without proctoring, while emphasis should be made on larger sample size.

REFERENCES

Ailisto, H., Vildjiounaite, E., Lindholm, M., Makela, S., and Peltola, J. 2006. "Soft Biometrics-Combining Body Weight and Fat Measurements with Fingerprint Biometrics," *Pattern Recognition Letters* (27:5), pp. 325–334.

Anstine, J., and Skidmore, M. 2005. "A Small Sample Study of Traditional and Online Courses with Sample Selection Adjustment," *Journal of Economic Education* (36:2), pp. 107-127.

Ball, D. M., and Levy, Y. 2008. "Emerging Educational Technology: Assessing the Factors that Influence Instructors' Acceptance in Information Systems and Other Classrooms," *Journal of Information Systems Education,* (19:4), pp. 431-443.

Ballou, D. J., and Huguenard, B. R. 2008. "The Impact of Students' Perceived Computer Experience on Behavior and Performance in an Introductory Information Systems Course," *Journal of Information Systems Education* (19:1), pp. 87-97.

Barker, B., and Brooks, D. 2005. "An Evaluation of Short-Term Distributed Online Learning Events," *International Journal on ELearning* (4:2), pp. 209-229.

Baron, J., and Crooks, S. M. 2005. "Academic Integrity in Web Based Distance Education," *TechTrends* (49:2), pp. 40-45.

Bosworth, K., Lee, M. G., Jaweed, S., and Wright, T. 2005. "Entities, Identities, Identifiers and Credentials — What Does it All Mean?," *BT Technology Journal* (23:4), pp. 25-36.

Bouchaffra, D., and Amira, A. 2008. "Structural Hidden Markov Models for Biometrics: Fusion of Face and Fingerprint," *Pattern Recognition* (41:3), pp. 852-867.

Bunz, U. 2005. "Using Scantron Versus an Audience Response System for Survey Research: Does Methodology Matter when Measuring Computer-Mediated Communication Competence?," *Computers in Human Behavior* (21:2), pp. 343–359.

Caputo, D. 2010. "Gender Differences in Assessing Essential Business Information Systems Technology Skills," *International Journal of Management and Information Systems* (14:2), pp. 31-38.

Chen, H., Chen, T., Lee, W., and Chang, C. 2008. "Security Enhancement for a Three-Party Encrypted Key Exchange Protocol against Undetectable On-line Password Guessing Attacks," *Computer Standards & Interfaces* (30:1-2), pp. 95-99.

Chyung, S. Y. 2007. "Age and Gender Differences in Online Behavior, Self-efficacy, and Academic Performance," *The Quarterly Review of Distance Education* (8:3), pp. 213–222.

Clarke, N. L., and Furnell, S. M. 2007. "Advanced User Authentication for Mobile Devices," *Computers & Security* (26:2), pp. 109-119.

Clarke, N. L., and Furnell, S. M. 2007. "Authenticating Mobile Phone Users Using Keystroke Analysis," *International Journal of Information Security* (6:1), pp. 1-14.

Clarke, N. L., Furnell, S. M., Lines, B. M., and Reynolds, P. L. 2003. "Keystroke Dynamics on a Mobile Handset: A Feasibility Study," *Information Management & Computer Security* (11:4), pp. 161-166.

Coleman, E. A., Coon, S. K., Lockhart, K., Kennedy, R. L., Montgomery, R., Copeland, N., McNatt, P., Savell, S., and Stewart, C. 2009. "Effect of Certification in Oncology Nursing on Nursing-Sensitive Outcomes," *Clinical Journal of Oncology Nursing* (13:2), pp. 165-172.

de Winter, J. C., and Wieringa, P. A. 2008. "Gender Differences in Driver's License Theory Test Scores in the Netherlands," *Journal of Safety Research* (39:4), pp. 413-416.

Furnell, S. M., Onions, P. D., Bleimann, U., Gojny, U., Knahl, M., Roder, H. F., and Sanders, P. W. 1998. "A Security Framework for Online Distance Learning and Training," *Internet Research* (8:3), pp. 236-242.

Furnell, S. M., Papadopoulos, I., and Dowland, P. 2004. "A Long-Term Trial of Alternative User Authentication Technologies," *Information Management & Computer Security* (12:2), pp. 178 - 190.

González-Tablas, A. I., Orfila, A., Ramos, B., and Ribagorda, A. 2008. "EVAWEB V2: Enhancing a Web-Based Assessment System Focused on Non-Repudiation Use and Teaching," *International Journal of Web - Based Learning and Teaching Technologies* (3:1), pp. 21-32.

Gowan, A., and Reichgelt, H. 2010. "Emergence of the Information Technology Discipline," *Computer* (43:7), pp. 79-81.

Gratton-Lavoie, C., and Stanley, D. 2009. "Teaching and Learning Principles of Microeconomics Online: An Empirical Assessment," *Journal of Economic Education,* (40:1), pp. 3-25.

Haney, W. M., and Clarke, M. J. 2007. *Psychology of Academic Cheating* (1st ed.). Burlington, MA: Elsevier Academic Press.

Hao, F., Anderson, R., and Daugman, J. 2006. "Combining Crypto with Biometrics Effectively," *IEEE Transactions on Computers* (5:9), pp. 1081-1088.

Harmon, O. R., and Lambrinos, J. 2008. "Are Online Exams an Invitation to Cheat?," *Journal of Economic Education* (39:2), pp. 116-125.

Hernández, A., López, B., Díaz, D., Fernández, R., Hernández, L., and Caminero, J. 2007. "A "Person" in the Interface: Effects on User Perceptions of Multibiometrics," *Proceedings of the Workshop on Embodied Language Processing (EmbodiedNLP '07)/Association for Computational Linguistics,* Stroudsburg, PA, USA, pp. 33-40.

Howard, J. R. 2005. "An Exam of Student Learning in Introductory Sociology at a Commuter Campus," *Teaching Sociology* (33:2), pp. 195-205.

Hwang, S., Cho, S., and Park, S. 2008. "Keystroke Dynamics-Based Authentication for Mobile Devices," *Computers & Security* (28:1-2), pp. 85-93.

Ihme, J. M., Lemke, F., Lieder, K., Martin, F., Müller, J. C., and Schmidt, S. 2009. "Comparison of Ability Tests Administered Online and in the Laboratory," *Behavior Research Methods* (41:4), pp. 1183-1189.

Irakleous, I., Furnell, S. M., Dowland, P. S., and Papadaki, M. 2002. "An Experimental Comparison of Secret-Based User Authentication Technologies," *Information Management & Computer Security* (10:3), pp. 100-108.

Irving, K. E. 2006. "The Impact of Educational Technology on Student Achievement: Assessment of and for Learning," *Science Educator* (15:1), pp. 13-20.

Jain, A. K. 2007. "Biometric Recognition: Q&A," *Nature* (449), pp. 38-40.

Jain, A. K., and Ross, A. 2004. "Multibiometric Systems," *Communications of the ACM* (47:1), pp. 34-40.

Jain, A. K., Hong, L., and Pankanti, S. 2000. "Biometric Identification," *Communications of the ACM* (43:2), pp. 91-98.

Jain, A. K., Pankanti, S., Prabhakar, S., Hong, L., and Ross, A. 2004. "Biometrics: A Grand Challenge," *Proceedings of the 17th International Conference on Pattern Recognition (ICPR'04),* Cambridge, United Kingdom, pp. 935-942.

Jain, A., Nandakumar, K., and Ross, A. 2005. "Score Normalization in Multimodal Biometric Systems," *Pattern Recognition* (38:12), pp. 2270-2285.

Joyce, R., and Gupta, G. 1990. "Identity Authentication Based on Keystroke Latencies," *Communications of the ACM* (33:2), pp. 168-176.

Kambourakis, G., Kontoni, D. N., Rouskas, A., and Gritzalis, S. 2007. "A PKI Approach for Deploying Modern Secure Distributed E-learning and M-learning Environments," *Computers & Education* (48:1), pp. 1-16.

Kavanagh, J. 2006. "Study Can Unlock Door to IT Security Riches," *Computer Weekly,* May, p. 40.

Langley, N. 2006. "Certification is Key to Cash in on Growth in IT Security," *Computer Weekly,* October, p. 50.

Leak, A., and Spruill, A. 2008. "Oncology Certification: What is in it for You?," *Clinical Journal of Oncology Nursing* (12:5), pp. 703-706.

Levy, Y., and Ramim, M. 2009. "Initial Development of a Learners' Ratified Acceptance of Multibiometrics Intentions Model (RAMIM)," *Interdisciplinary Journal of E-Learning and Learning Objects* (5), pp. 379-397.

Levy, Y., Ramim, M. M., Furnell, S. M., and Clarke, N. L. 2011. "Comparing Intentions to Use University-Provided vs. Vendor-Provided Multibiometric Authentication in Online Exams," *Campus-Wide Information Systems* (28:2), pp. 102-113.

Maltoni, D., Maio, D., Jain, A. K., and Prabhakar, S. 2009. *Handbook of Fingerprint Recognition* (2nd ed.). New York, New York: Springer Publishing Company, Incorporated.

Marcialis, G. L., Roli, F., and Didaci, L. 2009. "Personal Identity Verification by Serial Fusion of Fingerprint and Face Matchers," *Pattern Recognition* (42:11), pp. 2807-2817.

Marcialis, G. L., Roli, F., and Muntoni, D. 2009. "Group-Specific Face Verification Using Soft Biometrics," *Journal of Visual Languages and Computing* (20:2), pp. 101–109.

Masys, D., Baker, D., Butros, A., and Cowles, K. E. 2002. "Giving Patients Access to Their Medical Records via the Internet: the PCASSO Experience," *Journal of the American Medical Informatics Association* (9:2), pp. 181-191.

Maurer, D. E., and Baker, J. P. 2008. "Fusing Multimodal Biometrics with Quality Estimates via a Bayesian Belief Network," *Pattern Recognition* (41:3), pp. 821-832.

McCabe, D. L. 2009. "Academic Dishonesty in Nursing Schools: an Empirical Investigation," *The Journal of Nursing Education* (48:11), pp. 614-623.

Nagar, A., Nandakumar, K., and Jain, A. K. 2010. "A Hybrid Biometric Cryptosystem for Securing Fingerprint Minutiae Templates," *Pattern Recognition Letters* (31:8), pp. 733-741.

Nandakumar, K., Chen, Y., Dass, S. C., and Jain, A. 2008. "Likelihood Ratio-Based Biometric Score Fusion," *IEEE Transactions on Pattern Analysis and Machine Intelligence* (30:2), pp. 342-347.

Nathanson, C., Paulhus, D. L., and Williams, K. M. 2006. "Predictors of a Behavioral Measure of Scholastic Cheating: Personality and Competence but not Demographics," *Contemporary Educational Psychology* (31:1), pp. 97-122.

Park, U., Jain, A. K., and Ross, A. 2007. "Face Recognition in Video: Adaptive Fusion of Multiple Matchers," *Proceedings of CVPR'2007,* Minneapolis, MN, pp. 1-8.

Patterson, D. A. 2006. "A Large-Scale, Asynchronous, Web-Based MSW Comprehensive Exam Administration," *Journal of Social Work Education* (42:3), pp. 655-668.

Prince, D., Fulton, R., and Garsombke, T. 2009. "Comparisons of Proctored Versus Non-Proctored Testing Strategies in Graduate Distance Education Curriculum," *Journal of College Teaching and Learning* (6:7), pp. 51-62.

Ramim, M., and Levy, Y. 2007. "Towards a Framework of Biometrics Exam Authentication in E-learning Environments," *Proceeding of the Information Resources Management Association International Conference (IRMA) 2007*, Vancouver, Canada, pp. 539-543.

Rezgui, Y., and Marks, A. 2008. "Information Security Awareness in Higher Education: An Exploratory Study," *Computers & Security* (27:7-8), pp. 241-253.

Ribaric, S., & Fratric, I. 2005. "A Biometric Identification System Based on Eigenpalm and Eigenfinger Features," *IEEE Transactions on Pattern Analysis and Machine Intelligence* (27:11), pp. 1698-1709.

Ross, A., Jain, A., and Reisman, J. 2003. "A Hybrid Fingerprint Matcher," *Pattern Recognition* (36:7), pp. 1661–1673.

Rudd, A., and Stoll, S. 2004. "Measuring Students' Character in Secondary Education: The Development of the Principled Thinking Inventory," *Journal of Research in Character Education* (2:2), pp. 151-164.

Sanchez-Franco, M. J. 2010. "WebCT - the Quasimoderating Effect of Perceived Affective Quality on an Extending Technology Acceptance Model," *Computers and Education* (54:1), pp. 37-46.

Sandoe, K., and Milliron, V. 2000. "E-cheating: Identifying Academic Dishonesty in an On-line Testing Environment," *Proceedings of the 11th Annual International Information Management Association (IIMA) Conference 2000*, Seattle, Washington.

Shellenbarger, T. 2008. "Preparing for Certification in Nursing Education," *Nursing Education Perspectives* (29:6), pp. 330-332.

Song, O. T., Jin, A. T., and Connie, T. 2007. "Personalized Biometric Key Using Fingerprint Biometrics," *Information Management & Computer Security* (15:4), pp. 313-328.

Tan, C. L. 2009. "Assessment via WebCT quizzes: Offline Grading Process with Customized Feedback," *Decision Sciences Journal of Innovative Education* (7:1), pp. 321-326.

Teoh, A. B., Goh, A., and Ngo, D. C. 2006. "Random Multispace Quantization as an Analytic Mechanism for Biohashing of Biometric and Random Identity Inputs," *IEEE Transactions on Pattern Analysis and Machine Intelligence* (28:12), pp. 1892-1901.

Teoh, A. B., Kuan, Y. W., and Lee, S. 2008. "Cancellable Biometrics and Annotations on BioHash," *Pattern Recognition* (41:6), pp. 2034-2044.

Thompson, R., Compeau, D., and Higgins, C. 2006. "Intentions to Use Information Technologies: An Integrative Model," *Journal of Organizational and End User Computing* (18:3), pp. 25-47.

Vielhauer, C., and Steinmetz, R. 2004. "Handwriting: Feature Correlation Analysis for Biometric Hashes," *EURASIP Journal on Applied Signal Processing* (2004:4), pp. 542-558.

Wallace, P., and Clariana, R. B. 2005. "Gender Differences in Computer-Administered Versus Paper-Based Tests," *International Journal of Instructional Media* (32:2), pp. 171-179.

Walton, R. 2005. "Combining Biometric Measurements for Security Applications," *Computer Fraud & Security* (2005:4), pp. 7-13.

Wang, L., Leedham, G., and Cho, D. S. 2008. "Minutiae Feature Analysis for Infrared Hand Vein Pattern Biometrics," *Pattern Recognition* (41:3), pp. 920-929.

Weippl, E. R. 2007. "Dependability in E-assessment," *International Journal on ELearning* (6:2), pp. 293-303.

Woodward, B., Davis, D. C., and Hodis, F. A. 2007. "The Relationship Between Ethical Decision Making and Ethical Reasoning in Information Technology Students," *Journal of Information Systems Education* (18:2), pp. 193-202.

Yoon, C. Y. 2008. "An Evaluation System for End-User Computing Capability in a Computing Business Environment," *IEICE Transactions on Information and Systems* (E91-D:11), pp. 2607-2615.