

1-1-2016

An empirical study of authentication methods to secure e-learning system activities against impersonation fraud

Shauna Beaudin

Nova Southeastern University, sb1324@nova.edu

Yair Levy

Nova Southeastern University, levyy@nova.edu

James Parrish

Nova Southeastern University, jlparrish@nova.edu

Theon Danet

Florida Institute of Technology, theon.danet@dcma.mil

Follow this and additional works at: https://nsuworks.nova.edu/gscis_facarticles



Part of the [Computer Sciences Commons](#)

NSUWorks Citation

Beaudin, Shauna; Levy, Yair; Parrish, James; and Danet, Theon, "An empirical study of authentication methods to secure e-learning system activities against impersonation fraud" (2016). *CCE Faculty Articles*. 341.

https://nsuworks.nova.edu/gscis_facarticles/341

This Article is brought to you for free and open access by the College of Computing and Engineering at NSUWorks. It has been accepted for inclusion in CCE Faculty Articles by an authorized administrator of NSUWorks. For more information, please contact nsuworks@nova.edu.

An empirical study of authentication methods to secure e-learning system activities against impersonation fraud

Shauna Beaudin, Nova Southeastern University, Florida, USA, sb1324@nova.edu

Yair Levy, Nova Southeastern University, Florida, USA, levyy@nova.edu

James Parrish, Nova Southeastern University, Florida, USA, jlparrish@nova.edu

Theon Danet, Florida Institute of Technology, Florida, USA, theon.danet@dcma.mil

Abstract

The demand for e-learning systems in both academic and non-academic organizations has increased the need to improve security against impersonation fraud. Although there are a number of studies focused on securing Web-based systems from Information Systems (IS) misuse, research has recognized the importance of identifying suitable levels of authenticating strength for various activities. In e-learning systems, it is evident that due to the variation in authentication strength among controls, a 'one size fits all' solution is not suitable for securing diverse e-learning activities against impersonation fraud. The focus of this exploratory study was to investigate what levels of authentication strength users perceive to be most suitable for activities in e-learning systems against impersonation fraud and aimed to assess if the 'one size fits all' approach that is mainly used is valid when it comes to securing e-learning activities from impersonation fraud. A sample of 1,070 e-learners was analyzed using descriptive statistics and exploratory factor analysis to uncover suitable levels of authentication strength to secure e-learning activities against impersonation fraud. The findings determined that there is a specific set of e-learning activities that have high potential for impersonation and need a moderate to high level of authentication strength to reduce the threat.

Keywords: Authentication in e-learning systems, e-learning impersonation fraud, risk mitigation in e-learning, authentication in e-learning activities, suitable authentication strength in e-learning activities

Introduction

E-learning systems are becoming one of the largest growing sectors of Web-based systems (Alwi & Fan, 2010). E-learning uses a wide range of learning activities to meet learning outcomes (Levy, 2008). In addition to the prevalent use within academic institutions, e-learning systems are a strategic way for organizations from various industries to deliver training to employees in order to improve their skills or obtain certifications (Alwi & Fan, 2010; Kasraie & Kasraie, 2010). Users interact with e-learning systems through a variety of learning activities. E-learning activities can be categorized as formative or summative e-assessments (Baillie & Jortberg, 2009). Formative e-assessments are used to identify the gap between current understanding and the desired goal by providing feedback, dialogue, and non-assessed activities. Summative e-

assessments are high-stakes activities used for promotion, placement, certification, and accountability. E-learning systems must ensure that users completing e-learning activities are legitimate (Peres, Lima, & Lima, 2014).

In e-learning systems, activities are completed by users as a means to assess the success of the user's outcomes (Lam, 2004). In Levy (2008), critical value factors (CVFs) were used to identify what e-learning activities offer the most value to learners within an online learning system. Levy (2008) defined CVFs as, "the factors that educational institutions should pay attention to in order to increase the learners' perceived value, which in turn may help reduce dropout in online learner courses" (p. 1664). Levy (2008) further categorized the findings by grouping them into five CVFs: (a) Collaborative, Social, and Passive Learning Activities; (b) Formal Communication Activities; (c) Formal Learning Activities; (d) Logistic Activities; and (e) Printing Activities. Levy (2008) concluded that e-learning activities within the first three categories (a, b, & c) have the highest learners' perceived value within e-learning systems, therefore, categories (d) and (e) were not included in this study. Table 1 depicts categories (a), (b), and (c) along with the e-learning activities used within the Levy (2008) study.

Table 1. Adapted From List of the CVFs on Online Learning Activities (Levy, 2008)

Category	Item Description
Collaborative, Social, and Passive Learning Activities	<ol style="list-style-type: none">1. Participating in chat sessions (unofficial with other students)2. Sharing my assignments with the other students (via discussion forum)3. Sharing my assignments with other students (via e-mail)4. Participating in chat session (official sessions with the professor)5. Participating in live voice-chat sessions6. Reviewing chapters slides online7. Sending e-mails to other students8. Reading other students' assignments (via discussion forum)9. Listening to course audios online10. Reading e-mails from other students
Formal Communication Activities	<ol style="list-style-type: none">1. Reading e-mails from the professor2. Reviewing professor's feedback on assignments (online)3. Sending e-mails to the professor4. Reading the professor's discussion forum messages5. Reading information off the school's site6. Checking grades online7. Register for courses online8. Reading assignments' guidelines online9. Checking for course(s) updates

Table 1. Adapted From List of the CVFs on Online Learning Activities (Levy, 2008) (continued)

Category	Item Description
Formal Learning Activities	<ol style="list-style-type: none"> 1. Replying to students' discussion forum messages 2. Posting new discussion forum messages 3. Reading other student's discussion forum messages 4. Submitting course(s)' assignments online 5. Reviewing other students' personal Websites 6. Developing personal Website, profile, or blog 7. Replying to professor's discussion forum messages

Categories (a) and (b) have been traditionally classified as formative assessments. Sadler (1989) described the purpose of formative assessments as a way to identify the gap between current understanding and the desired goal by providing feedback, dialogue, and non-assessed activities that can be developed into learning. Category (c) has been traditionally classified as summative assessments. Rovai (2000) described summative assessments as high-stakes assessments used for promotion, placement, certification, and accountability in learning environments. As depicted in Table 2, e-learning in an organizational context has grouped learning activities into similar categories' such as instructional, collaborative, practice, and assessment (Fry, 2001).

Table 2. Learning Management System Activities (Fry, 2001)

Categories	Learning Activities
Instructional	<ul style="list-style-type: none"> Deliver concepts Demonstrations Workshop content Reference articles Web links
Collaborative	<ul style="list-style-type: none"> Expert led chats Mentoring Peer-to-peer chat Discussions Mentored exercises Group meetings
Practice	<ul style="list-style-type: none"> Exercises Projects Lab work Simulations

Table 2. Learning Management System Activities (Fry, 2001) (continued)

Categories	Learning Activities
Assessment	Performance testing Proficiency testing Certification testing Customized assessments

In addition to Levy (2008)’s list of valuable learning activities, studies have identified exams, quizzes, and course projects as critical summative assessments (Bailie & Jortberg, 2009). Bailie and Jortberg (2009) compiled a list of 10 broad categories of e-learning assessments from 3,200 responses sorted by frequency of use depicted in Table 3.

Table 3. Types of Assessment on Online Learning (Bailie & Jortberg, 2009)

Responses	Frequency	Percent
Homework assignments	655	20%
Online tests and/or quizzes	606	19%
Bulletin-board postings	547	17%
Projects/papers	494	15%
Participation in chat room	313	10%
Proctored tests and/or quizzes	234	7%
Team projects	149	5%
Reflective journal	92	3%
Student portfolio	79	2%
Other	31	1%

E-assessments have been defined by the Joint Information Systems Committee (JISC) (2006) as, “the end-to-end electronic assessment processes where [Information & Communications Technology] ICT is used for the presentation of assessment activity and the recording of responses” (p. 43). Bailie and Jortberg (2009) stated that “proving identity in every situation that a student performs is not realistic, practical or cost effective” (p. 199). For the purpose of this study, items from Tables 1, 2, and 3 adapted from prior studies that meet the JISC (2006) definition of e-assessments that are either formative or summative, known collectively as e-learning activities, were included in the initial survey instrument.

A risk to e-learning systems is when users deliberately reveal their authentication details to allow another user to impersonate them (Apampa, Wills, & Argles, 2010). Impersonation is considered the intentional collaboration between users with the intent to commit a fraudulent behavior by the misrepresentation of identity potentially undermining the value of the system (Apampa et al., 2010; Gathuri, Luvanda, & Kamundi, 2014).

As a countermeasure to impersonation fraud, authentication is a critical preventative control used in e-learning systems in order to determine the user’s identity (Helkala & Snekenes, 2009). Authentication controls have three common factors that challenge what: a user knows (a password), a user has (a token), or a user is (a biometric) (Furnell, 2007). Although, a number of differing solutions have been proposed to address this prevailing issue by using authentication controls with a wide variation of strength, there is a lack of consistency in what level of authentication strength is suitable (Jalal & Zeb, 2008; Penteado & Marana, 2009). Authentication strength is measured by the combinations of the number and the type of authentication factors used to identify a remote system user (O’Gorman, 2003). Single-factor authentication is a

username/password or personal identification number (PIN), a token, or a single biometric. Passwords can be easily distributed so this authentication method is often considered inadequate to protect critical e-learning activities from impersonation fraud (Apampa et al., 2010). Biometrics is defined as the identification of an individual based upon the uniqueness of physiological and behavioral characteristics, which is a stronger authentication than simply using passwords (Gao, 2012). Biometric authentication may only deter impersonation because an imposter can take over the activity once the biometric is matched (Apampa et al., 2010; Levy & Ramim, 2007; Song, Lee, & Nam, 2013). Due to the ease of use and high user acceptance, single-factor authentication such as username/password, a token, or a biometric is most commonly used to authenticate users within e-learning systems (Jalal & Zeb, 2008).

To improve authentication strength, two single-factor authentications can be combined into a two-factor authentication (Gao, 2012; Marnell & Levy, 2014). A two-factor authentication approach is the use of live-proctor authentication along with username/password or biometric authentication. Live-proctor authentication is the observation of remote e-learners via a Webcam and a live proctor over the Internet, irrespective of the location (Kitahara, Westfall, & Mankelwicz, 2011; Hylton, Levy, & Dringus, 2016). Multi-factor authentication, combining three factors, creates a very strong authentication and improves reliability against impersonation fraud (O’Gorman, 2003; Ross, 2007; Ross, Nandakumar, & Jain, 2006). The problem this study addressed is that identity and authentication controls do not reliably secure the diverse activities in Web-based systems against user impersonation fraud (Apampa et al., 2010; Prince, Fulton, & Garsombke, 2009). Therefore, the research questions this study focused on are organized into 4 sets shown in Tables 4, 5, 6, and 7.

Table 4. Research Questions on High Potential for Threats of Impersonation

Set 1	High Potential for Threats of Impersonation for E-learning Activities
RQ1a:	What e-learning activities are perceived by users to have a high potential for threats of impersonation?
RQ1b:	What e-learning activities users perceived that their peers will identify to have a high potential for threats of impersonation?
RQ1c:	How do the e-learning activities perceived by users to have a high potential for impersonation differ than what is perceived by users that their peers will identify?

Table 5. Research Questions on Suitable Level of Authentication Strength

Set 2 Suitable Level of Authentication Strength for Assessed E-Learning Activities

-
- RQ2a: What levels of authentication strength are perceived by users to be most suitable against the threats of impersonation for these assessed e-learning activities?
-
- RQ2b: What levels of authentication strength are perceived by users that their peers will identify to be most suitable against the threats of impersonation for these assessed e-learning activities?
-
- RQ2c: How do the levels of authentication strength perceived by users to be most suitable against the threats of impersonation for these assessed e-learning activities differ than what is perceived by users that their peers will identify?
-

Table 6. Research Questions on Significant Components for Assessed E-Learning Activities

Set 3 Significant Components for Assessed E-learning Activities

-
- RQ3a: What are the significant components of the levels of authentication strength perceived by users to be most suitable against the threats of impersonation for these assessed e-learning activities?
-
- RQ3b: What are the significant components of the levels of authentication strength perceived by users that their peers will identify to be most suitable against the threats of impersonation for these assessed e-learning activities?
-
- RQ3c: What are the differences between the significant components of the levels of authentication strength perceived by users to be most suitable against the threats of impersonation for these assessed e-learning activities versus than what is perceived by users that their peers will identify?
-

Table 7. Research Questions on Demographic Variables

Set 4 Significant Differences of Demographic Variables

-
- RQ4a: Are there significant differences of perception of high potential for threats of impersonation based on gender?
-
- RQ4b: Are there significant differences of perception of high potential for threats of impersonation based on age?
-
- RQ4c: Are there significant differences of perception of high potential for threats of impersonation based on e-learning experience?
-

Methodology

In this exploratory study, an initial Web-based survey instrument was developed to measure users' perceptions about suitable authentication methods. This study also built upon the work of Levy (2006b) that identified the top 10 most valuable activities in e-learning systems, and the work of Levy (2008) that developed CVFs for activities in e-learning systems. This research study used summative and formative learning activities within these categories to identify the activities that users perceived to have a high potential for impersonation fraud. Following the initial development of a survey instrument (Phase 1), the Delphi methodology was used to gather

feedback from an expert panel to adjust the instrument to improve validity (Phase 2). Table 8 lists the 18 e-learning activities to be assessed in this study.

Table 8. Assessed E-Learning Activities

E-Learning Activities

1. Develop a personal Website, profile, or blog
2. Participate in text-chat sessions with the professor
3. Participate in text-chat sessions with other students
4. Participate in live voice-chat sessions with the professor
5. Participate in live voice-chat sessions with other students
6. Post a new discussion forum message with the professor
7. Post a new discussion forum message with other students
8. Reply to discussion forum messages with the professor
9. Reply to discussion forum messages with other students
10. Send e-mails to the professor
11. Send e-mails to other students
12. Share assignments with other students (via discussion forum)
13. Share assignments with the other students (via e-mail)
14. Submit assignments online
15. Submit exams online
16. Submit quizzes online
17. Submit ungraded practice quizzes online
18. Submit projects online

The survey contained three sections (Section A, B, & C). To answer RQ1a, RQ1b, and RQ1c, Section A asked respondents to rate the following for the e-learning activities listed in Table 8:

- I think this e-learning activity has a high potential for impersonation fraud by users, and
- I think my peers will identify that this e-learning activity to have a high potential for impersonation by users.

Section A used a 7-point Likert scale ranging between the positive and negative extremes (1) ‘Strongly Agree’, (2) ‘Agree’, (3) ‘Somewhat Agree’, (4) ‘Neither Agree or Disagree’, (5) ‘Somewhat Disagree’, (6) ‘Disagree’, to (7) ‘Strongly Disagree’.

To answer RQ2a, RQ2b, and RQ2c, Section B asked respondents to rate the following for the e-learning activities listed in Table 8:

- I think the selected Authentication Strength is suitable for the e-learning activity to reduce impersonation fraud, and
- I think my peers will identify the selected Authentication Strength as suitable for the e-learning activity to reduce impersonation fraud.

Section B used a 7-point Likert scale ranging between weak and strong authentication extremes (1) ‘Extremely Low Strength’, (2) ‘Very Low Strength’, (3) ‘Low Strength’, (4) ‘Moderate Strength’, (5) ‘High Strength’, (6) ‘Very High Strength’, to (7) ‘Extremely High Strength’. The purpose of using relative authentication strength terms such as ‘low or ‘high’ strength was “to identify combinations that complement strengths and reduce weaknesses against different attacks” (O’Gorman, 2003, p. 4). Results from Section A and Section B were used to assess RQ3a, RQ3b, and RQ3c.

Figures 1 and 2 depict how RQ1a and RQ1b as well as RQ2a and RQ2b assessed e-learning activities for high potential for impersonation and suitable authentication strength.

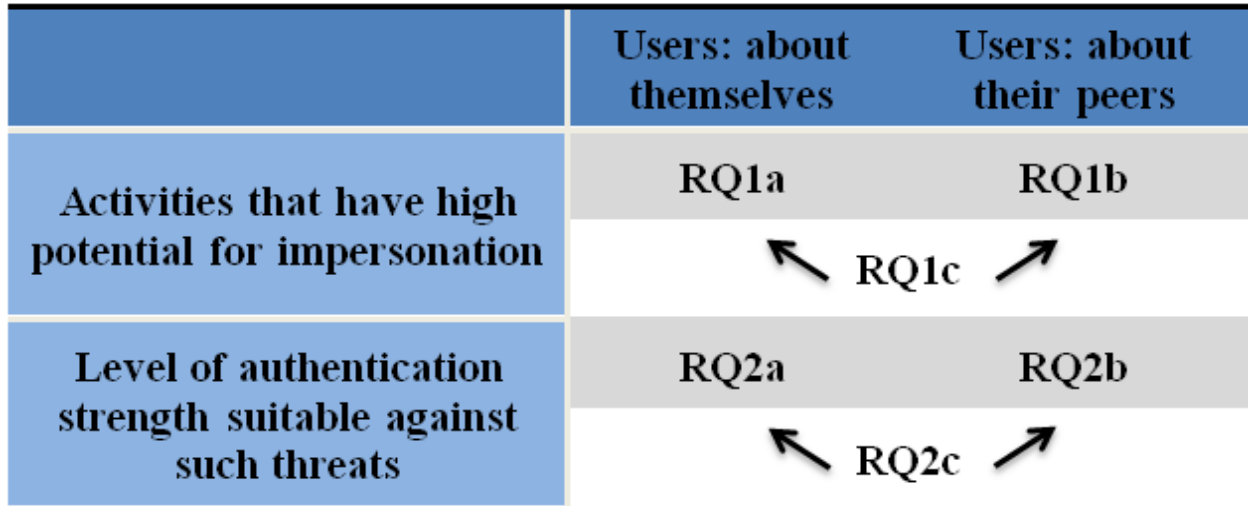


Figure 1. Process of Assessment for E-Learning Activities and Suitable Authentication Strength

<u>RQ1a & RQ1b</u>		
What e-learning activities have perceived high potential for impersonation?		
<ol style="list-style-type: none"> 1. Develop a personal Website, profile, or blog 2. Participate in text-chat sessions with the professor 3. Participate in text-chat sessions with other students 4. Participate in live voice-chat sessions with the professor 5. Etc... 		
↓		
<u>RQ2a & RQ2b</u>		
What level of authentication strength is most suitable?		
<u>Single-Factor</u>	<u>Two-Factor</u>	<u>Three-Factor</u>
Extremely Low Strength (Password)	Moderate Strength (Password & Biometric)	Extremely High Strength
Very Low Strength (Token)	High Strength (Password & Live-Proctor)	(Password, Biometric, & Live-Proctor)
Low Strength (Biometric)	Very High Strength (Biometric & Live-Proctor)	

Figure 2. Research Factorial Design for Assessment of E-learning Activities and Suitable Authentication Strength (RQ1s & RQ2s)

The same e-learning activities that were assessed for high potential of impersonation were used in RQ2a and RQ2b, respectively. RQ2a and RQ2b identified what levels of authentication strength to be most suitable for assessed e-learning activities. Section C collected demographic data on gender, age, and e-learning experience, while it was used to assess for RQ4a, RQ4b, and RQ4c. The finalized survey instrument was used to collect quantitative data for analyses (Phase 3). The link to the Web-based survey was sent to all e-learners at a single university within the northeastern United States (US). A pre-analysis data screening was conducted to detect abnormalities with the data collected, which resulted in 1,070 cases for final analysis.

The ordinal Likert scale data is described as categorical. However, Carifio and Perla (2007) as well as Norman (2010) argued that assigning an equal distance between ordinal categories creates a quantitative representation of the responses that is more interval than ordinal. Thus, response means and standard deviations can be analyzed as interval quantitative data. The practical use of parametric statistical analysis such as paired sample t-test on ordinal data is demonstrated in a significant number of studies where the assigned distance between each Likert value is identical and, therefore, can be analyzed as interval quantitative data (Norman, 2010). Since the value of each item represents likeliness of the perception and given the direction of the responses from *Strongly Agree* to *Strongly Disagree*, Velleman and Wilkinson (1993) stated that Likert scale data does not necessarily underperform in analyses intended for continuous data with respects to reliability analysis such as Cronbach's Alpha. Given these methodological limitations acknowledged, the parametric statistical analyses were performed for this study.

To answer RQ1a and RQ1b the useful cases were analyzed using descriptive statistics to calculate the means and standard deviations for e-learning activities. The means were sorted from lowest to highest perceived potential for threat of impersonation. The results were separated into two groups: (a) agree – all e-learning activities that have a mean of < 3.0 ; and (b) disagree – all e-learning activities that have a mean of ≥ 3.0 .

Figure 3 depicts the two groups, which shows a clear distinction between the e-learning activities with a perceived high potential for impersonation as opposed to those that do not. The left pie graph identifies four e-learning activities (22%) for RQ1a that had a mean of < 3.0 indicating they have a high potential for impersonation. They were: 'Submit quizzes online', 'Submit exams online', 'Submit assignments online', and 'Submit projects online', which are considered high-stakes summative e-assessments. The remaining 14 e-learning activities (78%) for RQ1a had a mean of ≥ 3.0 indicating they do not have a high potential for impersonation.

The right pie graph identifies five e-learning activities (28%) for RQ1b that had a mean of < 3.0 were the same four from RQ1a but also included 'Participate in text-chat sessions with the professor', which is a formative e-assessment. The remaining 13 e-learning activities (72%) for RQ1b had a mean of ≥ 3.0 indicating they do not have a high potential for impersonation.

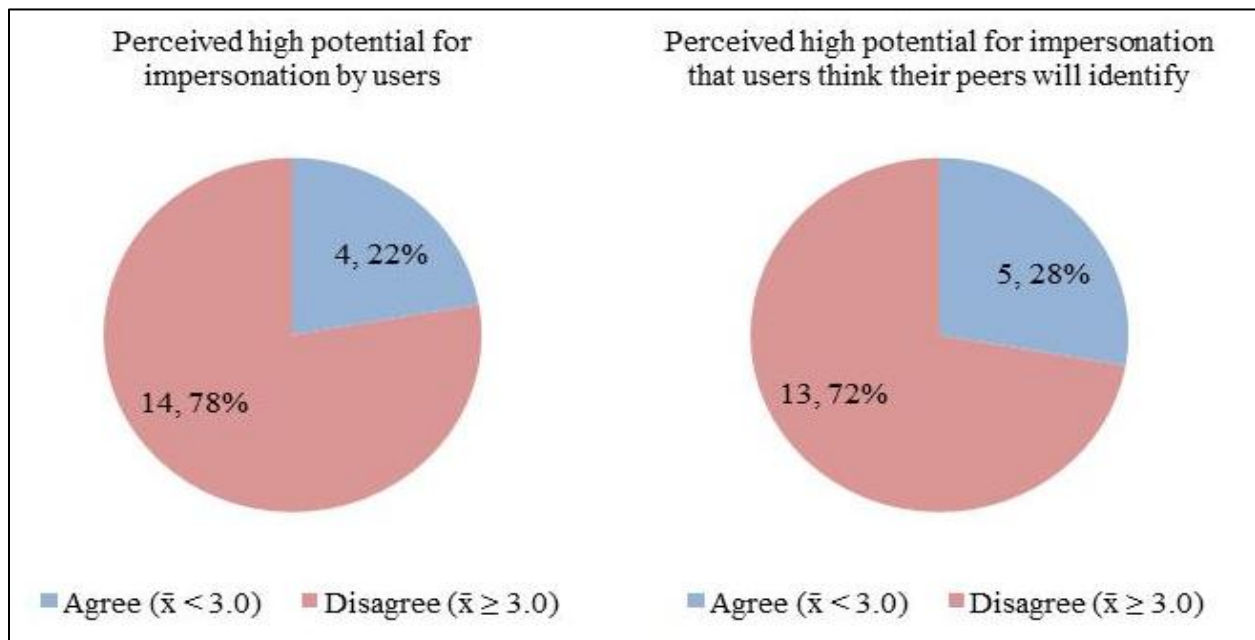


Figure 3. Grouped Means for RQ1a and RQ1b (N=1,070)

These results indicate that e-learners do perceive a higher risk of impersonation for e-learning activities that are primarily categorized as summative or as high-risks e-assessment. In order to better secure the e-learning system, e-learning providers would be interested in these results to know which e-learning activities users are more likely to allow for deliberate impersonation. To answer RQ1c, the means and standard deviations results for each group were compared using a paired sample t-test to determine if there were significant differences between the two groups as it relates to perceived threat of impersonation for selected e-learning activities. The results of the paired sample t-test indicated that 12 out of 18 activities had means that were significantly different between the groups and are presented in Table 9.

Table 9. Paired Sample T-test Between Groups to Address RQ1a & RQ1b (N=1,070)

Item	RQ1a		RQ1b		Paired Means		
	Mean	SD	Mean	SD	t	Sig.	*
1	5.06	1.270	5.06	1.384	.052	.9584	
2	3.15	1.182	2.96	1.253	13.727	.0000	***
3	3.23	1.152	3.18	1.174	1.427	.1539	
4	5.25	1.350	5.20	1.402	5.097	.0000	***
5	5.20	1.361	5.17	1.376	3.459	.0006	***
6	3.43	1.145	3.18	1.293	7.240	.0000	***
7	3.43	1.160	3.42	1.183	.466	.6413	
8	3.27	1.283	3.01	1.351	7.190	.0000	***
9	3.43	1.213	3.41	1.223	1.765	.0779	
10	5.36	1.612	5.30	1.636	5.537	.0000	***
11	5.35	1.608	5.33	1.624	1.964	.0498	*
12	5.13	1.665	5.10	1.671	2.813	.0050	**
13	5.13	1.667	5.10	1.665	4.028	.0001	***
14	2.36	0.907	2.33	0.905	4.065	.0001	***
15	2.34	0.927	2.32	0.924	3.732	.0002	***
16	2.33	0.948	2.33	0.925	0.000	1.0000	
17	5.99	1.041	5.86	0.999	11.959	.0000	***
18	2.40	0.817	2.40	0.823	0.277	.7817	

*** p < 0.001, ** p < 0.01, * p < 0.05

In each instance the RQ1b mean response for the threat of impersonation was higher than the RQ1a response mean. Although there were significant differences in the means for more than half the e-learning activities being measured, the four activities identified in RQ1a and RQ1b with the highest perceived threat of impersonation were not significant.

To answer RQ2a and RQ2b the useful cases were analyzed by using descriptive statistics to calculate the means and standard deviations for levels of authentication strength perceived by users to be the most suitable against the threat of impersonation for assessed e-learning activities. The means were sorted from highest to lowest level of authentication strength. The results were separated into three groups: (a) High Strength including Live-proctor with a mean ≥ 5.0 ; (b) Low-Moderate Strength including Biometric with a mean ≥ 2.5 and < 5.0 ; (c) Very Low Strength with a mean < 2.5 . Responses for RQ2a and RQ2b resulted in the same grouping results for the e-learning activities. The two e-learning activities (11%) that had a mean of ≥ 5.0 were: ‘Submit exams online’ and ‘Submit quizzes online’. The second group had three e-learning activities (17%) that had a mean ≥ 2.5 and < 5.0 , which included ‘Submit projects online’, ‘Submit assignments online’, and ‘Participate in text-chat sessions with the professor’. The remaining 13 e-learning activities (72%) had a mean of < 2.5 . Figure 4 depicts the three groups, which show a clear distinction between the levels of authentication strength suitable for assessed e-learning activities.

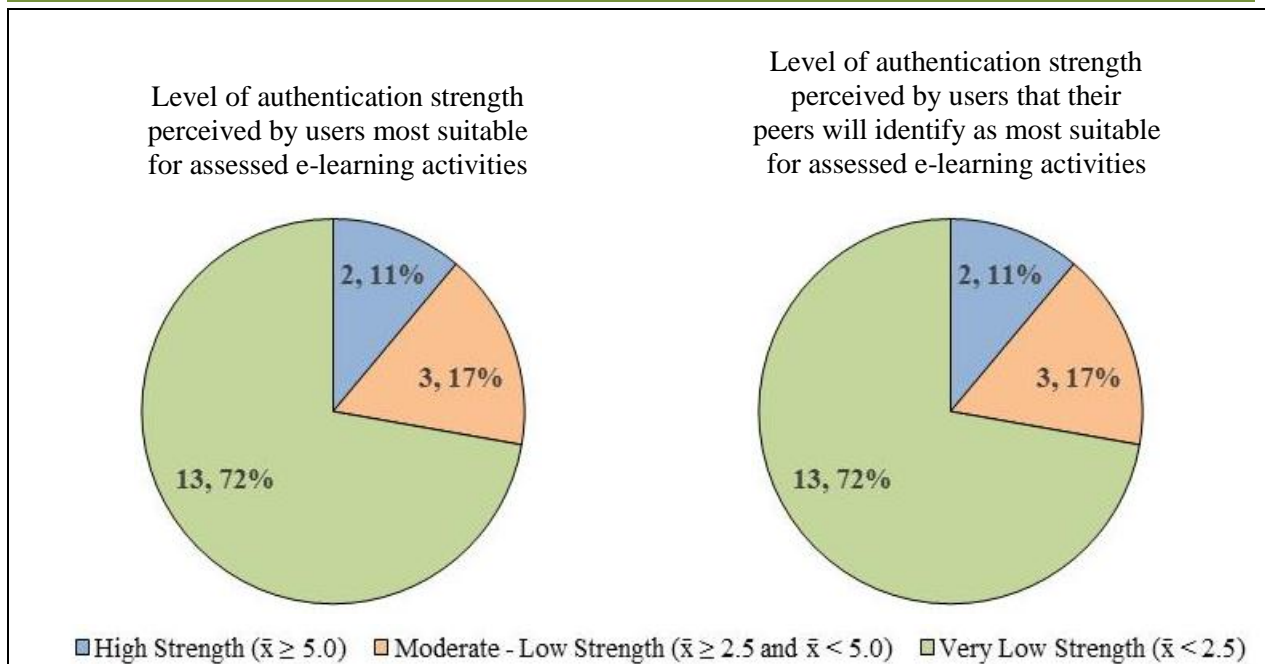


Figure 4. Grouped Means for RQ2a and RQ2b (N=1,070)

These results indicate that e-learners do perceive that suitable levels of authentication must vary in strength based upon the activity being considered. The five e-learning activities that were identified as having the highest potential of threat of impersonation were perceived to need a stronger authentication method than a single-factor authentication username/password. In order to better secure the e-learning system at the activity level, e-learning providers would be interested in these results to know which e-learning activities are perceived to need a suitable level authentication other than a 'one size fits all' username/password system approach to reduce the risk of deliberate impersonation. There is a perception that summative e-assessments need a stronger authentication method, which includes at least a biometric and/or live-proctor authentication. To answer RQ2c, the means and standard deviations results for each group, RQ2a and RQ2b, were compared using a paired sample t-test to see if there were significant differences between the two groups as it relates to levels of authentication strength for assessed e-learning activities. The results of the paired sample t-test indicated that nine out of 18 activities had means that were significantly different between the groups and are presented in Table 10.

Table 10: Paired Sample T-test Between Groups to Address RQ2a & RQ2b (N=1,070)

Item	RQ2a		RQ2b		Paired Means		
	Mean	SD	Mean	SD	t	Sig.	*
1	1.54	0.925	1.55	0.939	-1.859	.0633	
2	2.60	0.868	2.57	0.875	2.441	.0148	*
3	1.85	1.078	1.83	1.070	2.226	.0262	*
4	1.62	1.111	1.62	1.104	0.000	1.0000	
5	1.59	1.067	1.60	1.066	-1.874	.0612	
6	1.32	0.799	1.34	0.815	-2.021	.0435	*
7	1.35	0.817	1.37	0.849	-3.414	.0007	***
8	1.37	0.831	1.40	0.854	-3.482	.0005	***
9	1.23	0.653	1.28	0.711	-3.871	.0001	***
10	2.02	1.108	2.05	1.116	-2.808	.0051	**
11	2.05	1.116	2.06	1.122	-1.521	.1284	
12	1.55	0.962	1.58	0.974	-2.460	.0140	*
13	1.57	0.974	1.59	0.987	-1.238	.2161	
14	2.80	0.992	2.80	1.009	-0.194	.8461	
15	5.43	1.265	5.43	1.253	-0.988	.3234	
16	5.36	1.252	5.36	1.253	0.738	.4604	
17	1.10	0.442	1.11	0.463	-1.213	.2254	
18	3.25	1.093	3.27	1.109	-2.324	.0203	*

*** p < 0.001, ** p < 0.01, * p < 0.05

The only two activities that were significant based upon the responses from RQ2a and RQ2b were item 2 ‘Participate in text-chat sessions with the professor’ and item 18 ‘Submit projects online’. Item 2 had indicated a stronger authentication in RQ2a, whereas, item 18 had indicated a stronger authentication in the RQ2b group. For the other three items identified in RQ2a and RQ2b there was no significant differences indicating that users believed their peers would perceive the same level of authentication strength is necessary for those summative e-assessments.

To answer RQ3a and RQ3b, the significant components of the levels of authentication strength perceived by users and those users perceived that their peers would identify to be most suitable against the threats of impersonation for assessed e-learning activities were identifying using Exploratory Factor Analysis via Principal Component Analysis (PCA). The analysis for RQ3a and RQ3b had very consistent results. Both PCA analyses initially suggested eight components sets, each having two items, along with two individual items. Item 14 and item 18 did not load well with the other components. An investigation revealed that although both were identified as having a high potential for impersonation, the literature had some contradictions in terms of how these items were categorized. For example, Fry (2001) categorized both items as formative, low-stakes e-assessments, whereas, Levy (2008) categorized both items as summative e-assessments. In contrast, the other 16 items were consistently categorized as collaborative (communication, formative), practice (ungraded, informal) or assessment (formal, summative) in the literature. This investigation explained why item 14 and item 18 are susceptible to various interpretations in

terms of authentication. Following this conclusion and based on the low loadings values for the items, it was determined that removing the items from the analysis provided the best loading of items retained. After the items were removed, eight components were identified. A Cronbach's Alpha analysis on all components was completed to review reliability of the retained components with more than one item. Four components with a Cronbach's Alpha of 0.70 or higher indicating a very high reliability were described by categories used from prior studies as *Collaborative: Voice Chat; Practice: Share Assignments; Assessment: Quizzes and Exams; Collaborative: Sending E-mail* (Fry, 2001, Levy, 2008). Three components that had a moderate Cronbach's Alpha of $0.50 \geq$ or < 0.70 were described as *Collaborative: Text-Chat, Collaborative: Discussion Post, and Collaborative: Discussion Reply*. Yoon, Guimaraes, and O'Neal (1995) stated that in exploratory research values 0.50 and above were acceptable. One component set containing item one and item 17 had an extremely low Cronbach's Alpha of < 0.50 and was removed. The removed component often represents ungraded or informal activities such as practice quizzes or setting up online profile and was identified as highly unlikely to be susceptible to impersonation. Upon completion of the two PCAs, 14 of the 18 items with a factor loading of at least 0.50 were retained in seven components, accounting for more than 80% of the variability. Table 11 lists the items along with their category and activity description (Fry, 2001; Levy, 2008).

Table 11. List of Reliable E-learning Activities Grouped by Category

Item	Category	E-learning Activity
2	Collaborative: Text-Chat	Participate in text-chat sessions with the professor
3		Participate in text-chat sessions with other students
4	Collaborative: Voice-Chat	Participate in live voice-chat sessions with the professor
5		Participate in live voice-chat sessions with other students
6	Collaborative: Discussion Reply	Post in new discussion forum message with to the professor
7		Post in new discussion forum message with other students
8	Collaborative: Discussion Post	Reply to discussion forum messages to the professor
9		Reply to discussion forum messages with other students
10	Collaborative: Sending E-mail	Send e-mails to other students
11		Send e-mails to the professor
12	Practice: Share Assignments	Share assignments with other students (via discussion forum)
13		Share assignments with other students (via e-mail)
15	Assessment: Quizzes & Exams	Submit exams online
16		Submit quizzes online

To answer RQ3c, it was determined that there were no differences between the significant components for RQ3a and RQ3b. In fact, the factor loadings and the Cronbach's Alpha were very consistent among the two groups. This demonstrated a high reliability in the results for the

level of authentication most suitable for the 14 retained activities. Demographic data collected on gender, age, and e-learning experience. Table 12 shows the demographic distribution of the results of the 1,070 study participants. The rate of responses from females was slightly higher than males at: 58% females versus 42% males. A similar distribution of gender frequencies has been in a number of studies on e-learning and, therefore, is a representative of the population of e-learners (Chua & Montalbo, 2014; Ong & Lai, 2006; Suri & Sharma, 2013). The age of most of the respondents were between 20 and 49 accounting for approximately 90% of the sample. The population mean for e-learners is an average of 34, therefore, the sample mean age was also a representation of the population (Ong & Lai, 2006). Finally, over half of the respondents had completed at least six to 10 courses in e-learning. The population mean of e-learners was 10 completed courses, therefore, the sample mean e-learning experience was also a representation of the population (Ong & Lai, 2006).

Table 12. Descriptive Statistics of Study Participants (N=1,070)

Item	Frequency	Percentage (%)
Gender		
Male	445	41.6%
Female	625	58.4%
Age		
Under 20	51	4.8%
20 - 29	344	32.1%
30 - 39	291	27.2%
40 - 49	326	30.5%
50 - 59	27	2.5%
60 or over	31	2.9%
E-learning Experience (in # online courses)		
1 - 5	484	45.2%
6 - 10	472	44.1%
11+	114	10.7%

Demographic responses were analyzed using the mean responses for the 18 e-learning activities to see if there were significant differences between the perceptions of high potential for threats of impersonation resulting for RQ1a and RQ1b using an analysis of covariance (ANCOVA). With gender as the control variable, two items showed a significantly difference in means; item eight and item 17. With age as the control variable, only item nine showed a significantly difference in means. Finally, with e-learning experience as the control, no items showed any significant differences. As seen in the results, only a few items showed a significant difference, therefore, a large majority of responses showed no significant differences on any of the demographic variable for the items assessed between RQ1a and RQ1b.

Discussion and Conclusions

This study was exploratory and provided recommended levels of authentication for selected e-learning activities that had a perceived high potential for impersonation. Previous studies have indicated that finding suitable authentication is a significant and challenging problem (Apampa

et al., 2010; Jalal & Zeb, 2008). In response, this research explored the need to identify a suitable authentication level specific to an e-learning activity in order to deter IS misuse. Based on descriptive statistics, it was determined that there were a specific set of e-learning activities perceived by users and that users perceived that their peers would identify had a high potential for impersonation. Additionally, the same set of items were identified as needing moderate to high levels of authentication strength in order to reduce the threat of impersonation. A paired sample t-test for means showed that overall there was no significant difference in how the users responded in each group responses (RQa vs. RQb). Significant components were identified and categorized in order to provide a clear list of e-learning activities that are similar in terms of assessment types. The results have made the case that e-learning systems need to authenticate at e-learning activity level for summative e-assessments using suitable authentication strength to ensure the identity of the remote user. The use of stronger multi-factor authentication that involves biometric and/or live-proctor authentication will reduce the opportunity for deliberate impersonation for selected e-learning activities. The results of this study contributes notably to the body of knowledge, and have several implications within the field of IS as well as for future research in the domain of authentication and e-learning. Most relevant is that users do perceive the need for different levels of authentication suitable to the activity being completed, as opposed to a 'one size fits all' systems approach. This is due to the perceived high potential of threat of impersonation on selected summative e-assessments such as exams and quizzes. Although 18 e-learning activities were assessed, many were viewed as having a low potential for impersonation due in part to the formative nature of the activity. Only four activities categorized as summative were consistently identified within an e-learning system as having a high potential for impersonation. The findings in this study are relevant to e-learning providers in both academic and non-academic environments where the possibility of IS misuse due to deliberate impersonation can undermine the value of the system (Apampa et al., 2010). E-learning providers may find it important to incorporate stronger authentication such as biometric and/or live-proctor authentication for summative activities in order to reduce the threat of impersonation fraud.

References

- Alwi, N., & Fan, I. (2010). E-learning and information system management. *International Journal of Digital Society*, 1(2), 148-156.
- Apampa, K. M., Wills, G., & Argles, D. (2010). User security issues in summative e-assessment security. *International Journal of Digital Society*, 1(2), 135-147.
- Bailie, J. L., & Jortberg, M. A. (2009). Online learner authentication: Verifying the identity of online user's. *Journal of Online Learning and Teaching*, 5(2), 197-207.
- Carifio, J., & Perla, R. J. (2007). Ten common misunderstandings, misconceptions, persistent myths and urban legends about Likert scales and Likert response formats and their antidotes. *Journal of Social Sciences*, 3(3), 106-116.
- Chua, C., & Montalbo, J. (2014). Assessing students' satisfaction on the use of virtual learning environment (VLE): An input to a campus-wide e-learning design and implementation. In *Information and Knowledge Management*, 4(2), 108-115.

-
- Fry, K. (2001). E-learning markets and providers: Some issues and prospects. *Education & Training, 43*(4/5), 233-239.
- Furnell, S. (2007). An assessment of Website password practices. *Computers & Security, 26*(7-8), 445-451.
- Gao, Q. (2012). Using IP addresses as assisting tools to identify collusions. *International Journal of Business, Humanities and Technology, 2*(1), 70-75.
- Gathuri, J. W., Luvanda, A., & Kamundi, S. M. M. S. (2014). Impersonation challenges associated with e-assessment of university students. *Journal of Information Engineering and Applications, 4*(7), 60-68.
- Helkala, K., & Snekenes, E. (2009). Formalizing the ranking of authentication products. *Information Management & Computer Security, 17*(1), 30-43.
- Hylton, K., Levy, Y., & Dringus, L. (2016). Utilizing Webcam-based proctoring to deter misconduct in online exams. *Computer & Education, 92-93*, 53-63. doi:10.1016/j.compedu.2015.10.002
- Jalal, A., & Zeb, M. A. (2008). Security enhancement for e-learning portal. *International Journal of Computer Science and Network Security, 8*(3), 41-45.
- Joint Information Systems Committee. (2006). E-assessment glossary (extended). Retrieved from http://www.jisc.ac.uk/uploaded_documents/eAssess-Glossary-Extended-v1-01.pdf
- Kasraie, N., & Kasraie, E. (2010). Economies of elearning in the 21st century. *Contemporary Issues in Education Research, 3*(10), 57-62.
- Kitahara, R., Westfall, F., & Mankelwicz, J. (2011). New, multi-faceted hybrid approaches to ensuring academic integrity. *Journal of Academic and Business Ethics, 3*(1), 1-12.
- Lam, W. (2004). Encouraging online participation. *Journal of Information Systems Education, 15*(4), 345-349.
- Levy, Y. (2008). An empirical development of critical value factors (CVF) of online learning activities: An application of activity theory and cognitive value theory. *Computers & Education, 51*(4), 1664-1675.
- Levy, Y., & Ramim, M. (2007). A theoretical approach for biometrics authentication of e-exams. *Chais Conference on Instructional Technologies Research, The Open University of Israel, Raanana, Israel*.
- Marnell, J. W., & Levy, Y. (2014). Towards a model of factors affecting resistance to using multi-method authentication systems in higher-education environments. *Information Security Education Journal, 1*(1), 36-44.
- Norman, G. (2010). Likert scales, levels of measurement and the “laws” of statistics. *Advances in health sciences education, 15*(5), 625-632.
- O’Gorman, L. (2003). Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE, 91*(12), 2019-2040.

-
- Ong, C. S., & Lai, J. Y. (2006). Gender differences in perceptions and relationships among dominants of e-learning acceptance. *Computers in Human Behavior*, 22(5), 816-829.
- Penteado, B. E., & Marana, A. N. (2009). A video-based biometric authentication for e-learning web applications. *Enterprise Information Systems*, (24)4, 770-779.
- Peres, P., Lima, L., & Lima, V. (2014). B-learning quality: dimensions, criteria and pedagogical approach. *European Journal of Open, Distance and e-Learning*, 17(1), 56-75.
- Prince, D. J., Fulton, R. A., & Garsombke, T. W. (2009). Comparisons of proctored versus non-proctored testing strategies in graduate distance education curriculum. *Journal of College Teaching and Learning*, 6(7), 51-62.
- Ross, A. A. (2007). An introduction to multibiometrics. *Proceedings of the 15th European Signal Processing Conference (EUSIPCO)*, pp. 20-24, Poznan, Poland.
- Ross, A. A., Nandakumar, K., & Jain, A. K. (2006). *Handbook of multibiometrics*. New York, NY: Springer.
- Rovai, A. P. (2000). Online and traditional assessments: What is the difference? *The Internet and Higher Education*, 3(3), 141-151.
- Sadler, R. (1989). Formative assessment and the design of instructional systems. *Instructional Science*, 18(2), 119-144.
- Song, K. S., Lee, S. M., & Nam, S. (2013). Cognitive biometrics application for e-learning security enhancement. *International Journal of Bio-Science and Bio-Technology*, 5(3), 143-152.
- Suri, G., & Sharma, S. (2013). The impact of gender on attitude towards computer technology and e-learning: An exploratory study of Punjab University, India. *International Journal of Engineering Research*, 2(2), 132-136.
- Velleman, P. F., & Wilkinson, L. (1993). Nominal, ordinal, interval, and ratio typologies are misleading. *The American Statistician*, 47(1), 65-72.
- Yoon, Y., Guimaraes, T., & O'Neal, Q. (1995). Exploring the factors associated with expert systems success. *MIS Quarterly*, 19(1), 83-106.

Authors' Biographies

Dr. Shauna Beaudin is a Lecturer in the Computer Information Systems department of the School of Business at Southern New Hampshire University. She joined the University in 2002 as an adjunct professor and subsequently became a Visiting Professor in 2013, then a Lecturer in 2016. She earned her Bachelor's degree in Business Administration from New Hampshire College, a Masters of Business Administration and Masters in Computer Information Systems from Southern New Hampshire University, and her Ph.D. in Information Systems at Nova Southeastern University. Her research interests include information system security and e-learning. She is also a member of Americas Conference on Information Systems (AMCIS) and Upsilon Pi Epsilon Honor Society (UPE). During the mid-1990s, Dr. Beaudin worked as an

independent Process Consultant then as an IT Director whose primary focus was to develop and deploy system solutions for organizations to streamline their business processes.

Dr. Yair Levy is a Professor of Information Systems and Cybersecurity at the College of Engineering and Computing, at Nova Southeastern University, the Director of the Center for e-Learning Security Research (CeLSR), and chair of the Information Security Faculty Group at the college along with serving as the director of the Ph.D. program in Information Assurance. He joined the university in 2003, was promoted to an Associate Professor in 2007, and to full Professor in 2012. During the mid to late 1990s, Dr. Levy assisted NASA to develop e-learning platforms as well as manage Internet and Web infrastructures. He earned his undergraduate degree in Aerospace Engineering from the Technion (Israel Institute of Technology). He received his Masters of Business Administration (MBA) with Management Information Systems (MIS) concentration and Ph.D. in MIS from Florida International University. He heads the Levy CyLab, which conducts innovative research from the human-centric lens of four key research areas Cybersecurity, User-authentication, Privacy, and Skills (CUPS), as well as their interconnections. He authored over 60 articles, three book chapters, one book, and his publications have been cited for over 1,400 times by other scholarly research. Dr. Levy has been an active member of the US Secret Service (USSS)'s - Miami Electronic Crimes Task Force (MECTF) and The South Florida Cybercrime Working Group (SFCWG). He was trained by the Federal Bureau of Investigation (FBI) on various topics, and actively serves as a member of the FBI/InfraGard, and consults the FBI/Cyber Task Force (CTF). Dr. Levy serves on the national Joint Task Force of Cybersecurity Education, as well as other national initiatives related to cybersecurity workforce, education, and research. He is also a frequent invited keynote speaker at national and international meetings, as well as regular media interviews as a Subject Matter Expert (SME) on cybersecurity topics. Find out more about Dr. Levy and his research lab via: <http://cec.nova.edu/~levyy/>

Dr. James Parrish is an Associate Professor of Information Systems and the Chair of the Department of Information Systems and Cybersecurity at the College of Engineering and Computing at Nova Southeastern University. He is also the Vice President of Student Chapters for the Association of Information Systems and serves on the board of directors for multiple organizations in industry and academia. His research interests include information systems security, knowledge management and design science.

Dr. Theon Danet is the Chief Enterprise Architect in the Information Technology (IT) Directorate with the Defense Contract Management Agency (DCMA) at their headquarters in Ft. Lee, VA. She is responsible for aligning DCMA's IT investments with the Agency Mission and Vision. She leads and directs a team with diverse functional and technical disciplines to include information technology architects, data analytics specialists, data security specialists and business intelligence analysts.

Past Federal Government assignments include:

- Department of the Army: Deputy Branch Chief, Army G-1, CIO
- NASA Langley Research Center: Lead Enterprise Architect
- Military Traffic Management Command: IT Specialist/Webmaster

In addition to her work with the DoD, Dr. Danet has been a subject matter expert in the private industry as a Lead Enterprise Architect for SRA International and Betac, Inc. Dr. Danet directed high level enterprise architecture analysis of Defense Architecture Framework 2.0 (DoDAF) compliant Human Capital Management (HCM) enterprise architecture products developed using IBM System Architect tool. Dr. Danet received her Ph.D. in Information Systems from Nova Southeastern University and her Professional MBA from Florida Institute of Technology. She earned her BS in Computer Studies from the University of Maryland. Dr. Danet is a graduate of the Federal Enterprise Architecture Certification (FEAC) Institute. The FEAC Institute recognizes the industry trends toward adopting Cloud Computing and Service-Oriented Architecture (SOA), combined with the imperativeness of planning and executing organizational and technology transformation, as well as supporting governance and compliance.