International Review of Research in Open and Distributed Learning

Security Risks and Protection in Online Learning: A Survey

Yong Chen and Wu He

Volume 14, Number 5, December 2013

URI: https://id.erudit.org/iderudit/1066886ar
DOI: https://doi.org/10.19173/irrodl.v14i5.1632

See table of contents

Publisher(s)

Athabasca University Press (AU Press)

ISSN

1492-3831 (digital)

Explore this journal

Cite this article

Chen, Y. & He, W. (2013). Security Risks and Protection in Online Learning: A Survey. *International Review of Research in Open and Distributed Learning*, *14*(5), 108–127. https://doi.org/10.19173/irrodl.v14i5.1632

Article abstract

This paper describes a survey of online learning which attempts to determine online learning providers' awareness of potential security risks and the protection measures that will diminish them. The authors use a combination of two methods: blog mining and a traditional literature search. The findings indicate that, while scholars have identified diverse security risks and have proposed solutions to mitigate the security threats in online learning, bloggers have not discussed security in online learning with great frequency. The differences shown in the survey results generated by the two different methods confirm that online learning providers and practitioners have not considered security as a top priority. The paper also discusses the next generation of an online learning system: a safer personal learning environment which requires a one-stop solution for authentication, assures the security of online assessments, and balances security and usability.

IRRODL
THE INTERNATIONAL REVIEW OF RESEARCH IN OPEN AND DISTANCE LEARNING

Security Risks and Protection in Online Learning: A Survey


Yong Chen and Wu He
Old Dominion University, USA

Abstract

This paper describes a survey of online learning which attempts to determine online learning providers' awareness of potential security risks and the protection measures that will diminish them. The authors use a combination of two methods: blog mining and a traditional literature search. The findings indicate that, while scholars have identified diverse security risks and have proposed solutions to mitigate the security threats in online learning, bloggers have not discussed security in online learning with great frequency. The differences shown in the survey results generated by the two different methods confirm that online learning providers and practitioners have not considered security as a top priority. The paper also discusses the next generation of an online learning system: a safer personal learning environment which requires a one-stop solution for authentication, assures the security of online assessments, and balances security and usability.

Keywords: Online learning; security; risk; threat; protection; e-learning

Introduction

Due to the development of the Internet, more and more people are taking online courses. According to a recent SLOAN-C annual report (2011), a survey conducted in 2011 among 4,523 degree-granting institutions of higher education in the United States reveals that over 6.1 million students were taking at least one online course during the fall 2010 term and 31% of current higher education students have taken at least one course online. Furthermore, 65% of higher education institutions now say that online learning is a critical part of their long-term strategy (SLOAN-C, 2011; Floyd, Schultz, & Fulton, 2012). Meanwhile, in the business world, numerous online courses for job and skill training are offered, to allow professionals to increase their competency and to upgrade their skills (Oncu & Cakir, 2011).

Online learning is "a type of delivery method used in distance education that allows synchronous and asynchronous exchanges of resource over a communication network" (Khan, 1998). It uses content repositories to store content and uses Web-based technologies to help learners interact with instructors and with other learners (Sasikumar, 2013). For example, a number of Web 2.0 tools such as blogs, podcasting, and wikis have been widely used in online learning to facilitate learning, collaboration, and knowledge sharing (Zuev, 2012). Newer web-based technologies such as social media have inspired educators to think differently about the ways in which learning occurs (Neville & Heavin, 2013) because the social media allow learners to create their own content freely and to form learning communities as the media support collaboration among learners and teachers (Redecker, Ala-Mutka, & Punie, 2010). More recently, massive open online courses (MOOCs) have received a lot of attention among institutions of higher education across the world (Meyer & Zhu, 2013); they are expected to change the learning landscape of higher education during the next decade.

As an Internet-based learning method, online learning depends on the Internet for its execution (Alwi & Fan, 2010). However, there are any number of illegal activities and security threats taking place on the Internet. Consequently, the e-learning environment is inevitably exposed to constant security threats, risks, and attacks. Unfortunately, many educational institutions are rushing into adopting online learning management systems without careful planning and without a thorough understanding of the security aspects of online learning (Alwi & Fan, 2010). A recent survey conducted by Campus Computing (campuscomputing.net) and WCET (wcet.info) found that almost 88% of the surveyed institutions have adopted a learning management system (LMS) as their medium for offering online courses.

In online learning, security means that "learning resources are available and unimpaired to all authorized users when they are needed" (Adams & Blandford, 2003). Since online learning takes place via the Internet, every element in an online learning system can be a potential target of hacking or attacks. This may lead to unauthorized modification and/or destruction of educational assets (Zuev, 2012). Online learning must consider the inherent security risks on the Internet, such as identity theft,

impersonation, and inadequate authentication (Ayodele, Shoniregun, & Akmayeva, 2011). Online learning systems have attracted the attention of cybercriminals who thrive on their ability to hack into such systems. The risk is great; as the functionalities and features of online learning systems become more complex, online learning is increasingly exposed to security threats (Alwi & Fan, 2010).

In response to increasing threats, researchers have developed a number of countermeasures and solutions to improve security in online learning. The purpose of this paper is to synthesize the related discussions in the literature, to provide an in-depth review of the security aspects of online learning, and to identify the future trends and challenges to security in online learning. Currently, the discussion of security risks of online learning is disparate, fragmented, and distributed among different outlets such as academic articles, white papers, educational reports, and news articles. This paper hopes to coordinate this information and to aid administrators and providers of online learning and online learning systems to understand the state of the art in this fast-moving field. This paper will offer necessary insights and tips so that online learning providers can become proactive and knowledgeable as they mitigate the security risks found in online learning.

Background

Security in online learning refers to protection from malicious or accidental misuse of resources in online learning (Adams & Blandford, 2003; Neumann, 1994). Previous literature indicates that security has three basic requirements: confidentiality, integrity, and availability (Adams & Blandford, 2003; Serb, Defta, Iacob, & Apetrei, 2013; Weippl & Ebner, 2008). Confidentiality refers to the protecting of sensitive information from being accessed by unauthorized persons (Serb, Defta, Iacob, & Apetrei, 2013; Adams & Blandford, 2003) and the absence of unauthorized disclosure of information (Weippl & Ebner, 2008). Since there are a large number of users in any online learning environment (among them students, visitors, instructors, tutors, and administrators), both a login system and a strong delimitation marking registered users and user groups are needed to safeguard the access to the appropriate user (Serb, Defta, Iacob, & Apetrei, 2013). In order to protect personal information, security safeguards such as authentication and encryption are usually implemented. Integrity, a critical element of security, refers to “the protection of data from intentional or accidental unauthorized changes” (Serb, Defta, Iacob, & Apetrei, 2013) and “the absence of improper system alterations” (Weippl & Ebner, 2008). It assures that “information and data have not been accidentally or maliciously modified or destroyed, and are in accurate, correct, and complete original form” (Raitman, Ngo, Augar, & Zhou, 2005). Access control is the key to maintaining integrity in the online learning environment (Serb, Defta, Iacob, & Apetrei, 2013). Availability means the readiness for correct service (Weippl & Ebner, 2008). It connotes that an online learning system can be accessed by authorized users whenever needed (Serb, Defta, Iacob, & Apetrei, 2013). And it assures that “information

and communication resources are readily accessible and reliable in a timely manner by authorized persons" (Raitman, Ngo, Augar, & Zhou, 2005). Availability can mainly be damaged by denial of service and/or loss of data processing capabilities (Serb, Defta, Iacob, & Apetrei, 2013).

According to Graf (2002), applications of information communication technology in online learning can cause many security risks, such as loss of confidentiality and availability, the exposure of critical data, and vandalism of public information services. Usually, online learning security issues have been attributed to users' poor knowledge of security measures, improper behaviors, and lack of education, because security protection mechanisms have been adopted in online learning programs. For example, in almost all institutions, the main online learning providers have installed firewalls and anti-virus software to protect their learning resources (Weippl & Ebner, 2008). Furthermore, they continue to enhance the content and technology in their online learning systems to secure online learning (Alwi & Fan, 2010; Srivastava & Sinha, 2013). But in recent years, even though users' security knowledge and skills have grown, security issues such as information manipulation by outsiders and insiders (by students or insiders) and loss of confidentiality still happen from time to time (Dietinger, 2003).

Security is essential as a means to retain users' trust in the online learning environment because any risk can dramatically affect students' perceptions of a system's reliability and trustworthiness (Adams & Blandford, 2003). As a result, it is crucial to identify the underlying factors that can cause security issues in online learning and to identify the limitations of the current security protection methods. Then, counter-measures can be developed to mitigate the security risks inherent in online learning.

Method

This study adopts two approaches to carrying out the review of security risks and protection in online learning.

First, an extensive literature search was conducted, via academic databases including the Web of Knowledge, the ACM Digital Library, the AACE Digital Library, and a web search engine (Google Scholar), using queries regarding security risks, threats, and protection in online learning. Since security has been a hot topic in the domain of online learning for some time, many articles were discovered. However, the discussions of security in online learning are disparate and fragmented.

Second, blog mining, a novel research method, was employed in this study, in order to further identify security risks and threats in online learning and to explore effective security protection strategies available to online learning. Blogs allow self-motivated bloggers to freely and easily post ideas, individual experiences, and opinions (Rubin, Burkel, & Quan-Haase, 2011; Furukawa, Ishizuka, Matsuo, Ohmukai, & Uchiyama,

2007). As blogs have a “high degree of exophoricity, quotation, brevity, and rapid of content update” (Ulicny, Baclawski, & Magnus, 2007, p. 1), running a blog mining analysis can improve the currency and relevance of this study (Chau & Xu, 2012).

However, blog posts can have an inherent bias. For example, the information on blogs is not peer-reviewed; the authorship of some blog pages is either not clear or unknown; and some blog information might be posted for commercial purposes. Therefore, researchers need to be aware of these drawbacks as they carry out blog mining analysis. Overall, this study combines blog mining with an extensive literature search to overcome these shortcomings, in order to engender a comprehensive understanding of the current state of security risks and protection in online learning.

Below is a description of how the blog mining was conducted.

Step one: Keywords, such as “online learning”, “ elearning”, “distance learning”, “security”, and “risk”, were typed in the advanced search option of Google Blog Search (http://www.google.com/blogsearch), a search tool specially designed to retrieve content from blogs that are freely and publicly available on the Internet. To identify the latest blog content discussing security risks and protection in online learning, the query time period was set from January 01, 2010 to June 20, 2013. Next, the query was performed. During this process, Google filtered similar blog posts first and then returned 312 posts that were relevant to the keywords.

To track Internet users’ search interests regarding “online learning security” in recent years, we applied Google Trends, a web-based search tool that provides the frequency of some specific search terms or keywords queried over a specific period of time. The result generated by Google Trends (see Figure 1) indicated that although the search frequency of online learning security has fluctuated in a narrow range since 2010, the overall attention paid to it has not changed much. This was consistent with the result we got via a Google Blog search.

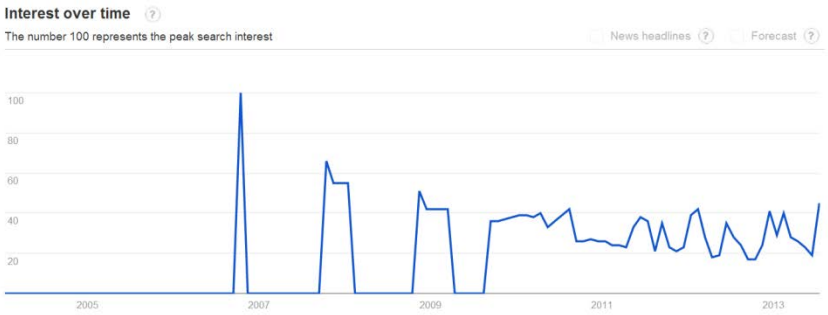

Figure 1. Search frequency of "online learning security" shown by Google Trends.

Step two: The authors read through each page of the 312 blogs generated, removed 62 irrelevant and repetitive posts, and saved the content of the rest of the posts in a single Word document as the sample data set. The sample data set provided a glimpse into the ongoing concerns and discussion regarding security risks and protection in online learning.

Step three: A concept analysis and mapping (CAAM) technique was applied to the data by loading the data file into a special CAAM software tool called Leximancer (http://www.leximancer.com), which extracted and classified the key concepts and themes in the data, and further identified the patterns and the relationships between concepts and themes. Leximancer has been adopted in quite a few studies in recent years (Cretchley, Rooney, & Gallois, 2010; Smith & Humphreys, 2006; Watson, Smith, & Watter, 2005). The Leximancer system is "a method for transforming lexical co-occurrence information from natural language into semantic patterns in an unsupervised manner" (Watson, Smith, & Watter, 2005). It uses word frequency and co-occurrence data to identify which concepts (words that occur very frequently) exist in a set of texts (Cretchley, Rooney, & Gallois, 2010). The technology behind the system is based on Bayesian theory, which argues that fragmented information can be used to predict what happens in a system (Watson, Smith, & Watter, 2005). Cretchley, Rooney, and Gallois (2010) describe in detail the way in which Leximancer works:

> The software includes an interactive concept-mapping facility, which provides an overview of the conceptual structure of the data set that assists the researcher in interpretation. Concepts that co-occur often within the same two-sentence coding block attract one another strongly when the map is clustered, so that similar concepts tend to settle together in close proximity. Clusters of concepts are grouped by theme circles to summarize the main ideas in particular clusters. Each theme is named after the most prominent concept in that

group, which is also indicated by the largest dot in the theme cluster. (p. 319)

Figure 2 is a screenshot of the interface of Leximancer 4.0. The map in the middle indicates the importance of the concepts. Red is the most important, followed by orange and so on, according to the color wheel.

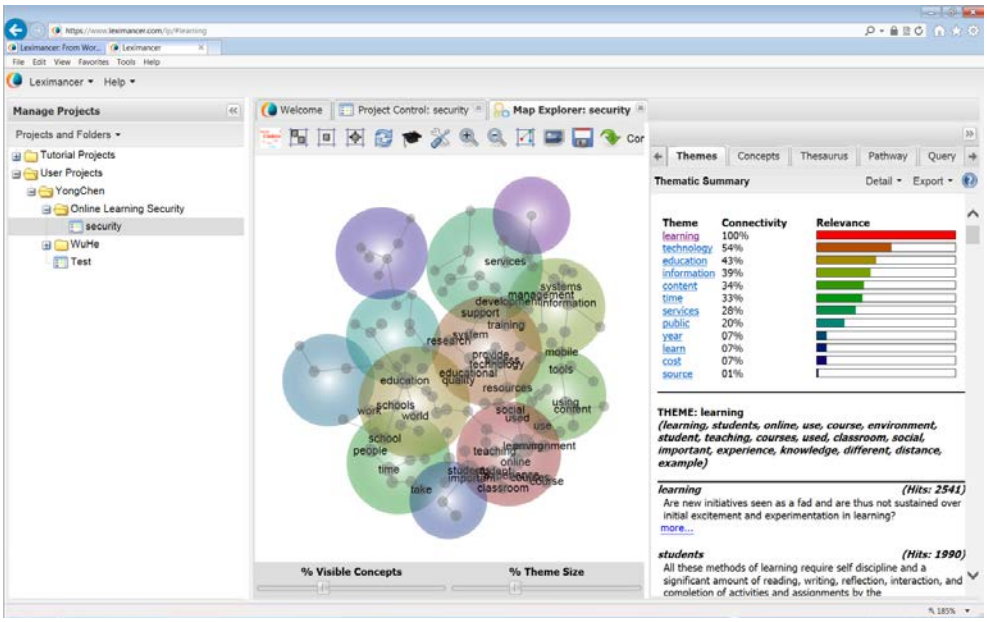

Figure 2. A screenshot of the interface of Leximancer 4.0.

Results

According to an extensive literature search via academic databases and Google Scholar, online learning faces various security risks (shown in Table 1), which mainly come from external intruders.

Table 1

Security Risks and Protection Measures in Online Learning

Security risks	Protection measures
• ARP cache poisoning and MITM attack • Brute force attack • Cross-Site Request Forgery (CSRF) • Cross Site Scripting (XSS) • Denial of Service (Dos) • IP spoofing • Masquerade • Rootkits • SQL Injection • Session Hijacking • Session Prediction • Stack-smashing attacks (Serb, Defta, Iacob, & Apetrei, 2013; Costinela-Luminita & Nicoleta-Magdalena, 2012; Barik & Karforma, 2012; Srivastava & Sinha, 2013)	• Installing firewalls and anti-virus software (Weippl & Ebner, 2008) • Implementing Security Management (ISM) (Adams & Blandford, 2003; Alwi & Fan, 2010) • Improving authentication, authorization, confidentiality, and accountability (Cardenas & Sanchez, 2005; Agulla, Rifon, Castro, & Mateo, 2008) • Using digital right management and cryptography (Barik & Karforma, 2012) • Training security professionals (Srivastava & Sinha, 2013)

To mitigate these risks, scholars have offered quite a few protection proposals (shown in Table 1). In contrast, in the concept map generated by Leximancer, neither the risks nor the protection measures can be easily identified. Figure 3 shows the concept map that Leximancer generated after the blog data was loaded. The large circles represent the clusters of concepts and the dots represent the main concepts. Leximancer can generate many concept terms using its text analytics algorithms. For our study, those clusters and concepts that appear with the highest frequency are listed in Table 2. It should be noted that compared with Table 1, Table 2 shows quite different content.

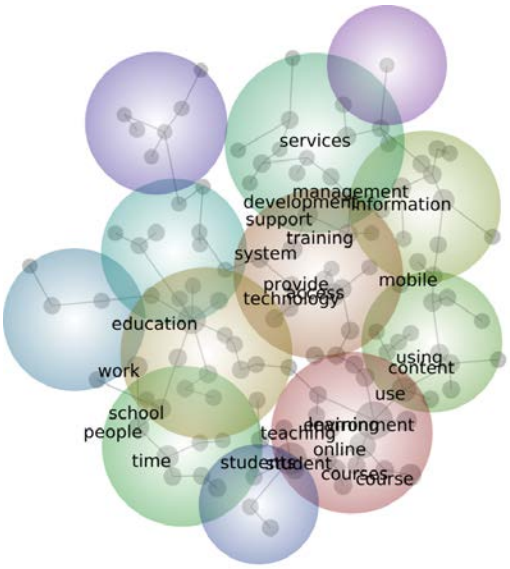

Figure 3. An example of the concept map generated by Leximancer with the sample data.

Table 2

Cluster of Concepts Associated with Security in Online Learning in Blog Posts

Cluster of concepts	Concept
Learning	learning, students, online, use, course, environment, teaching, courses, used, classroom, social, important, experience, knowledge, different, distance, example, virtual
Technology	technology, support, system, development, access, training, provide, research, resources, educational, quality, skills, institutions, developed
Education	education, work, world, schools, community, higher, better, program, become, life, group, programs, making
Information	information, management, mobile, systems, software, data, design, based, web, include, applications, performance, network, provides
Content	content, using, tools, available, process, technologies, e-learning, digital, level, computer, communication, offer, assessment

Discussion

Based on our extensive literature search and blog mining, we would like to provide a more detailed discussion on the causes of security threats, security protection measures, and the status of existing security protection for online learning.

Causes of Security Threats

Security threats in online learning can be examined from two aspects: the user side and the management side. As far as the user side is concerned, emerging ICT applications and imprudent human behavior are the main causes that lead to security issues in online learning. Besides, of the security risks inherent in the Internet, the development of new learning technologies such as Web 2.0 and social media have allowed for many new security breaches and a much larger security impact (Adams & Blandford, 2003; He, 2012). The amount of malicious content and the number of cyber-attacks on these new Web applications is rapidly increasing in both frequency and sophistication. Nowadays, many instructors are using social media sites such as Tumblr, Facebook, Wikis, online forums, and Twitter to support collaborative learning in their online courses (He, 2011; Camarero, Rodríguez, & José, 2012; Patel et al., 2012). However, for unwary instructors and students, these social media sites pose a variety of serious security risks and threats. For example, as a collaborative learning environment, a wiki also becomes a ripe environment for hacking, deception, abuse, and misuse (Patel et al., 2012). Personal data posted on social media sites can be misused in many ways (e.g., for virtual insult or, worse, for financial gain). Furthermore, recent studies show that social media sites are more likely to be used for delivering malware than were previously popular methods of email delivery (Kaspersky, 2009; He, 2013).

Other scholars analyze security issues from the standpoint of the user. For example, Adams and Blandford (2003) argue that threats to online learning security are caused by two main reasons: 1) The security mechanisms used in online learning programs lack usability; and/or 2) security discipline is not user-centered and therefore can lead the user to overlook serious security risks. They point out that the need-to-know principle (restricting information only to those who need to know) coupled with the unwillingness of security departments to know their users can cause a low usability of security mechanisms. Due to the lack of usability, many online learning systems do not provide users with adequate feedback or with the control rights that would allow them to protect their data (Adams & Blandford, 2003). Furthermore, poor user-centered design of security mechanisms and policy can contribute to insecurity and to users' low motivation to seek security (Adams & Sasse, 1999).

From the perspective of management, online learning providers have made some mistakes. In the domain of online learning, threats not only come from outsiders, but also from insiders (Alwi & Fan, 2010). Many scholars argue that security risks are caused by online learning providers' underdeveloped security policies and immature security measures. For instance, Serb, Defta, Iacob, and Apetrei (2013) note that

although more people are currently taking online courses, the security risks inherent in online learning have not been seriously taken into account in the actual educational context. Alwi and Fan (2010) point out that many online learning providers rush into adopting information communication technology without fully understanding the related security concerns. Yao and Ji (2011) note that online learning system designers consider the quality of online course content a considerably bigger issue than the security of their online systems. Furthermore, Weippl and Ebner (2008) indicate that even though almost all institutions have firewalls and anti-virus software to protect their campus resources, they often fail to perform adequate information system security management. Unfortunately, content and technology are still the focuses of online learning (Srivastava & Sinha, 2013). We feel that more attention should be put on the security aspect of online learning. In fact, security is very important for online learning because lacking security in online learning will cause a number of serious problems. For example, as Adams and Blandford (2003) point out, any security risk in online learning can dramatically affect students' perception of reliability and trustworthiness about learning via the Internet. As such, online learning will be less attractive and the development of online learning will be hindered. In addition, ICT applications make user authentication a big challenge for student assessment in online learning. When assessing students' asignments, as Alwi and Fan (2010) argue, it is very hard to verify whether an assignment is completed and/or submited by a valid student. If student assessment is not conducted correctly, the quality of online learning will be harmed greatly.

Security Protection Measures

Scholars have discussed security protection from the user side and management side as well. From the user side, protection motivation theory (PMT), a theory originally from social psychology, is introduced into the field of information system security. Based on this theory, information is perceived and evaluated, and then provides supports for users to take actions (Crossler, 2010). This theory explains the cognitive mediating process and coping modes when users encounter information sources. The PMT theory is helpful for understanding security protection measures adopted by online learning users.

From the management side, general deterrence theory (GDT), a theory from criminal justice, is adopted by information system security scholars to explain how security countermeasures can increase the perceptions of members in an organization regarding the severity and certainty of punishment for any misuse of information (Straub, 1990).

Security policies and mechanisms in online learning must support authentication, authorization, confidentiality, and accountability (Cardenas & Sanchez, 2005; Agulla, Rifon, Castro, & Mateo, 2008). Authentication refers to the validation of a person's identity before the access is assigned. Authorization defines what rights and services a person can access after the authentication process is passed. Confidentiality means that some specific information or data cannot be disclosed to anyone who is not authorized.

Accountability refers to the methodology by which users' resource consumption information is collected for billing, auditing, and capacity-planning purposes (Song, Lee, & Nam, 2013).

To mitigate security threats and risks in online learning, researchers have proposed many remedies from a variety of points of view. For example, Alwi and Fan (2010) propose information security management (ISM) for online learning providers, in order to build an effective security architecture that can fight existing and emerging information security threats. They argue that ISM should include policies, process, procedures, organizational structures, and software and hardware functions, in order to enhance the execution of security measures. Furnell and Karweni (2001) depict a framework that includes five aspects: 1) authentication and accountability; 2) access control; 3) protection of communications; 4) non-repudiation issues; 5) learning resource provider server protection. Srivastava and Sinha (2013) highly recommend that information security professionals improve their security knowledge and skills by using the Virtual Training Environment (VTE), a web-based knowledge library launched by the Carnegie Mellon Software Engineering Institute.

Security Protection Status

By comparing the results from the two research methods (Table 1 and Table 2), it is obvious that security is not a prime focus of blog posts discussing online learning, even though the topic has attracted much attention in the academic domain. Given the analysis of the causes of security risks in online learning, security is not at the top of the priority list in distance learning providers' hands. As long as a decade ago, Furnell and Karweni (2001) noted, "Security represents an aspect that may not suggest itself as a high priority in an education environment." The differences between the results generated by the two research methods confirm the scholars' conclusions, as mentioned above: The security risks inherent in online learning have not been seriously taken into account in an educational context. It may be that security issues have not caused as much damage in the realm of distance learning as they have in the business world. Since nothing serious about security has yet happened in the realm of online learning, not much attention has been paid to it in blog posts so far.

Research Trends

During the past decade, online learning has quickly grown. It has grown, perhaps, too quickly – too little attention has been paid to its security. Online learning will become more user-centered and more secure with the help of new technologies.

1. Personal Learning Environment and Biometric Authentication

Authentication has been widely adopted in online learning as a tool to improve confidentiality. Generally speaking, there are three ways to authenticate a user: 1)

knowledge-based authentication that requires that users provide something that only they know (e.g., type in a password, answer a secret question, or submit a personal identification number); 2) token-based authentication that requires that users show something that only they own (e.g., a key card, a mobile device, or a security token); 3) biometrics that require that users provide something for measurement (e.g., a fingerprint, a palm print, a retinal image, or a face gesture) (Garfinkel & Spfford, 1996; Alotaibi & Argles, 2011). Among these authentication methods, passwords and personal identification numbers (PINs) are most widely used (Adams & Blandford, 2003). As Raitman, Ngo, Augar, and Zhou (2005) note, user logins are the simplest means for providing identity and access services.

The next generation of online learning system is a personal learning environment (PLE), "a learning environment where the student is able to customize his/her learning environment based on pedagogical and personal choices" (Kolas & Staupe, 2007). As a new way of using the web or Web 2.0 for learning, the PLE focuses on the individual and "presents learners with learning resources based on individual interests, education level, attitude and cultural, social and other factors" (Li & Gu, 2009). It is a framework that integrates Web 2.0 and social tools, such as blogs, wikis, Facebook, podcasting, and videocasting, according to the choice of learners (Alotaibi & Argles, 2011; Kompen, Edirisingha, & Mobbs, 2008). As Alotaibi and Argles (2011) point out, the widespread authentication mechanism of username and password is out of date for use in the PLE, because learners have to sign on to multiple systems, each of which may involve a different username and password. As intruders and hackers become smarter and more technologically savvy (Science News, 2002), easy passwords make intrusion very achievable for malicious users, even as long and complex passwords are impractical for learners to remember (Gligor, 1993). According to a survey carried out in Alotaibi and Argles (2011), the average internet user has to remember 15 access control passwords.

Thus, a one-stop solution that is not dependent on a series of characters but on a technology, which is unique and can only be possessed by a specific individual, is needed for PLE. As such, Alotaibi and Argles (2011) have proposed a biometric authentication system, FingerID, which requires a fingerprint scan and human interaction to utilize a service. Meanwhile, Song, Lee, and Nam (2013) have proposed another method that uses brain wave and eye movement to authenticate users of online learning systems. Biometrics refers to the use of identification mechanisms, such as a fingerprint and retina scan, to certify that a person in front of a computer is indeed the intended person (Sasikumar, 2013). Biometric authentication seems to be the option for the next generation of authentication (Wang, Ge, Zhang, Chen, Xin, & Li, 2013).

2. Security for Online Assessments

As a major component in online learning, online assessments are important, both to ascertain students' progress and because they can be carried out flexibly in different locations and at different times (Reeves, 2000; Meyer & Zhu, 2013). According to a study carried out by King, Guyette, and Piotrowski (2009), 73.6% of students think that

it is easier to cheat in an online environment than in a conventional one. Methods of cheating on online assessments include online communication, telecommunication, internet surfing (Rogers, 2006), copying and pasting from online sources (Underwood & Szabo, 2003), obtaining answer keys in an illegitimate way, taking the same assessment several times, and getting unauthorized help (Rowe, 2004).

Other means of cheating on online tests include someone other than the actual student taking the online test and the copying of answers from elsewhere (Sasikumar, 2013). Ndume, Tilya, and Twaakyondo (2008) argue that preventing cheating in online course assessments is much harder than in traditional classrooms and that secure assessment of online courses requires the improvement of system security, the registration of learners with unique identification, and the overall administration of the online assessment. Therefore, improving the security of online learning will improve the security of online assessments, and this should not be neglected. The one-stop security solution for the next generation of online learning needs to assure the security of online assessment, as well.

3. The Goal of Security for Online Learning

Online learning is built on trust, information exchange, and discussion. However, a secure environment can rely on distrust, restricted information flow, and autocratic rules (Adams & Blandford, 2003). These attributes can make online learning and security mutually exclusive concepts. In addition, Weippl and Ebner (2008) indicate that no system can ever be totally secure while still remaining usable. What level of security does online learning need? Needless to say, the goal of security in online learning is definitely not to limit its usability. However, currently, online learning providers are facing a difficult balance, as they try to provide sufficient security to protect online learning resources while not inhibiting the appropriate use of these resources. Maintaining such a balance is challenging due to diversity – the diversity of computers and devices as well as a large number of diverse users (Pendegraft, Rounds, & Stone, 2010). Although this study shows that security is not a top priority for many online learning providers right now, serious efforts are needed to improve the security in online learning. The goal of security for online learning is to maintain the confidentiality, integrity, and availability of the resources in online learning at a certain level while keeping their usability acceptable for learners.

Conclusion

The growing availability of the Internet and the number of diverse end user devices facilitate the demands of online learning. The application of Web 2.0 and MOOCs are heralding a new era in education. Online learning brings with it all of the security risks inherent to the use of the Internet. However, although more people are taking online courses, online learning providers have not been seriously taking security risks into

account. Many of them rush into adopting information communication technologies without fully understanding the related security concerns. Scholars have identified diverse security risks and have proposed solutions to mitigate the security threats in online learning. To our surprise, our study found that security is not a hot topic among blog posts which discuss online learning. So far, online learning providers and practitioners have not considered security as a top priority, possibly because few serious security incidents have happened in the realm of online learning. As more and more people are studying online, more attention and efforts are needed from online learning providers and practitioners to prevent possible security breaches in online learning before it is too late.

References

Adams, A., & Blandford, A. (2003). Security and online learning: To protect or prohibit. *Usability Evaluation of Online Learning Programs*, 331-359.

Adams, A., & Sasse, M. A. (1999). The user is not the enemy. *Communications of the ACM*, *42*(12), 40-46.

Agharazi, M., Song, H., & Rahimi, S. (2011). Microblogging as an educational tool to advance learning: Case studies and recent reports. *EDULEARN11 Proceedings*, 6191-6196.

Agulla, E. G., Rifon, L. A., Castro, J. L. A., & Mateo, C. G. (2008). Is my student at the other side? Applying biometric web authentication to e-learning environment. In *Advance Learning Technologies, 2008. ICALT'08. Eighth IEEE International Conference* (pp. 551-553). IEEE.

Alotaibi, S. J., & Argles, D. (2011). FingerID: A new security model based on fingerprint recognition for personal learning environments (PLEs). In *Global Engineering Education Conference (EDUCON), 2011 IEEE* (pp. 142-151). IEEE.

Alwi, N. H. M., & Fan, I. S. (2010). E-learning and information security management. *International Journal of Digital Society (IJDS)*, *1*(2), 148-156.

Ayodele, T., Shoniregun, C. A., & Akmayeva, G. (2011). Towards e-learning security: A machine learning approach. In *Information Society (i-Society), 2011 International Conference* (pp. 490-492). IEEE.

Barik, N., & Karforma, S. (2012). Risks and remedies in e-learning system. *International Journal of Network Security & Its Applications*, *4*(1), 51-59.

Camarero, C., Rodríguez, J., & José, R. (2012). An exploratory study of online forums as a collaborative learning tool. *Online Information Review*, *36*(4), 568–586.

Cardenas, R. G., & Sanchez, E. M. (2005). Security challenges of distributed e-learning systems. In *Advanced distributed systems* (pp. 538-544). Springer Berlin Heidelberg.

Chau, M., & Xu, J. (2012). Business intelligence in blogs: Understanding consumer interactions and communities. *MIS Quarterly*, *36*(4), 1189-1216.

Costinela-Luminita, C. D., & Nicoleta-Magdalena, C. I. (2012). E-learning security vulnerabilities. *Procedia-Social and Behavioral Sciences*, *46*, 2297-2301.

Cretchley, J., Rooney, D., & Gallois, C. (2010). Mapping a 40-year history with Leximancer: Themes and concepts in the Journal of Cross-Cultural Psychology. *Journal of Cross-Cultural Psychology*, *41*(3), 318-328.

Crossler, R. E. (2010). Protection motivation theory : Understanding determinants to backing up personal data. In *Proceedings of the 43rd Hawaii International Conference on System Sciences*.

Dietinger, T. (2003). *Aspects of e-learning environments* (Unpublished doctoral thesis). Institute for Information Processing and Computer Supported New Media (IICM), Graz University of Technology, Austria.

Floyd, C., Schultz, T., & Fulton, S. (2012, June). Security vulnerabilities in the open source Moodle eLearning system. In *Proceedings of the 16th Colloquium for Information Systems Security Education*. Lake Buena Vista, Florida.

Furnell, S. M., & Karweni, T. (2001). Security issues in online distance learning. *Vine*, *31*(2), 28–35.

Furukawa, T., Ishizuka, M., Matsuo, Y., Ohmukai, I., & Uchiyama, K. (2007). Analyzing reading behavior by blog mining, In *Proceedings of the National Conference on Artificial Intelligence* (Vol. 22, No. 2, p. 1353). Menlo Park, CA; Cambridge, MA; London; AAAI Press; MIT Press.

Garfinkel, S., & Spafford, G. (1996). Practical Unix and Internet security. In *INET 96*. O'Reilly & Associates, Inc.

Gligor, V. (1993). A guide to understanding covert channel analysis of trusted systems. *Technical Report NCSC-TG-030*. National Computer Security Center, USA.

Graf, F. (2002), Providing security for eLearning. *Computer & Graphics*, *26*(2), 355-365.

He, W. (2011). Using wikis to facilitate collaborative website peer evaluation in an online web development course: An exploratory study. *Journal of Information Technology Education*, *10*, 235-247.

He, W. (2012). A review of social media security risks and mitigation techniques. *Journal of Systems and Information Technology*, *14*(2), 171-180.

He, W. (2013). A survey of security risks of mobile social media through blog mining and an extensive literature search. *Information Management and Computer Security*, *21*(5), 381–400.

Kaspersky Labs. (2009). Kaspersky security bulletin: Malware evolution 2008. Retrieved from http://www.securelist.com/en/analysis?pubid=204792051

Khan, B. H. (1998). Web-based instruction (WBI): An introduction. *Educational Media International*, *35*(2), 63-71.

King, C. G., Guyette, R. W., & Piotrowski, C. (2009). Online exams and cheating: An empirical analysis of business students' views. *The Journal of Educators Online, 6*(1), 1-11.

Kolas, L., & Staupe, A. (2007). A personalized e-learning interface. In *EUROCON, 2007*m *The International Conference on "Computer as a Tool"* (pp. 2670-2675). IEEE.

Kompen, R., Edirisingha, P., & Mobbs, R. (2008). Building Web 2.0-based personal learning environments-A conceptual framework. *EDEN Conference.* Paris. Retrieved from http://hdl.handle.net/2381/4398

Li, X., & Gu, X. (2009). A conceptual model of personal learning environment based on Shanghai Lifelong Learning System. In *Proceedings of 17th International Conference on Computers in Education, Asia-Pacific Society for Computers in Education* (pp. 885-889). Hong Kong.

Meyer, J.P., & Zhu, S. (2013). Fair and equitable measurement of student learning in MOOCs: An introduction to item response theory, scale linking, and score equating. *Research & Practice in Assessment, 8*(1), 26-39.

Ndume, V., Tilya, F. N., & Twaakyondo, H. (2008). Challenges of adaptive eLearning at higher learning institutions: A case study in Tanzania. *International Journal of Computing and ICT Research, 2*(1), 47-59.

Neumann, P. G. (1994). *Computer related risks*. Addison-Wesley Professional.

Neville, K., & Heavin, C. (2013). Using social media to support the learning needs of future IS security professionals. *Electronic Journal of e-Learning, 11*(1), 29-38.

Oncu, S., & Cakir, H. (2011). Research in online learning environments: Priorities and methodologies. *Computer & Education, 57*(1), 1098-1108.

Patel, A., Taghavi, M., Júnior, J. C., Latih, R., & Zin, A. M. (2012). Safety measures for social computing in wiki learning environment. *International Journal of Information Security and Privacy (IJISP), 6*(2), 1-15.

Pendegraft, N., Rounds, M., & Stone, R. W. (2010). Factors influencing college students' use of computer security. *International Journal of Information Security and Privacy (IJISP), 4*(3), *51-60*.

Raitman, R., Ngo, L., Augar, N., & Zhou, W. (2005). Security in the online e-learning environment. In *Advanced Learning Technologies, 2005. ICALT 2005. FIFTH IEEE International Conference* (pp. 702-706). IEEE.

Redecker, C., Ala-Mutka, K., & Punie, Y. (2010). *Learning 2.0-The impact of social media on learning in Europe.* Policy brief. JRC Scientific and Technical Report. EUR JRC56958 EN. Retrieved from http://www.ict-21.ch/com-ict/IMG/pdf/learning-2.0-EU-17pages-JRC56958.pdf

Reeves, T. C. (2000). Alternative assessment approaches for online learning environment in higher education. *Journal of Educational Computing Research, 23*(1), 101-111.

Rogers, C. F. (2006). Faculty perceptions about e-cheating during online testing. *Journal of Computing Sciences in Colleges, 22*(2), 206-212.

Rowe, N. C. (2004). Cheating in online student assessment: Beyond plagiarism. *Online Journal of Distance Learning Administration, 7*(2).

Rubin, V. L., Burkel, J., & Quan-Hasse, A. (2011). Facets of serendipity in everyday chance encounters: A grounded theory approach to blog analysis. *Information Research, 16*(3), 16-3.

Sasikumar, M. (2013). E-learning: opportunity and challenges. Retrieved from http://www.cdacmumbai.in/design/corporate_site/override/pdf-doc/e-learning.pdf

Science News (2002). Smart methods for detecting computer network intruders. *Science Daily*. Retrieved from http://www.sciencedaily.com/releases/2002/02/020226075019.htm

Serb, A., Defta, C., Iacob, N. M., & Apetrei, M. C. (2013). Information security management in e-learning. *Knowledge Horizons, 5*(2), 55-59.

Sloan-C. (2011). Going the distance: Online education in the United States. Retrieved from http://sloanconsortium.org/publications/survey/going_distance_2011

Smith, A. E., & Humphreys, M.S. (2006). Evaluation of unsupervised semantic mapping of natural language with Leximancer concept mapping. *Behavior Research Methods, 38*(2), 262-279.

Song, K., Lee, S. M., & Nam, S. C. (2013). Combined biometrics for e-learning security. *ISA 2-13, ASTL, 21*, 247-251.

Srivastava, A. & Sinha, S. (2013). Information security through e-learning using VTE. *International Journal of Electronics and Computer Science Engineering, 2*(18), 528-531.

Straub, D. W. (1990). Effective IS security : An empirical study. *Information System Research, 1*, 255-276.

Ulicny, B., Baclawski, K., & Magnus, A. (2007). New metrics for blog mining. In *Defense and Security Symposium* (pp. 657001-657001). International Society for Optics and Photonics.

Underwood, J., & Szabo, A. (2003). Academic offences and e-learning: Individual propensities in cheating. *British Journal of Educational Technology, 34*(4), 467-477.

Wang, F., Ge, B., Zhang, L., Chen, Y., Xin, Y., & Li, X. (2013). A system framework of security management in enterprise systems. Systems Research and Behavioral Science.

Watson, M., Smith, A., & Watter, S. (2005). Leximancer concept mapping of patient case studies. In *Knowledge-based intelligent information and engineering systems* (pp. 1232-1238). Springer Berlin Heidelberg.

Weippl, E., & Ebner, M. (2008). Security privacy challenges in e-learning 2.0. In *World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education* (Vol. 2008, No. 1, pp. 4001-4007).

Yao, H. & Ji, Y. (2011). Security protection for online learning of music. In *Computer Communication and Networks (ICCCN), 2011 Proceedings of 20th International Conference on* (pp.1-4). IEEE.

Zuev, V. (2012). E-learning security models. *Management, 7*(2), 24-28.

Athabasca University