Information Security Trends and Issues in the Moodle E-Learning Platform: An Ethnographic Content Analysis

Christopher Schultz
Information Systems Management
University of Maryland University College
Adelphi, Maryland 20783

ABSTRACT

Empirical research on information security trends and practices in e-learning is scarce. Many articles that have been published apply basic information security concepts to e-learning and list potential threats or propose frameworks for classifying threats. The purpose of this research is to identify, categorize and understand trends and issues in information security in e-learning as reflected in the discussions on a 'Security and Privacy' discussion forum of the Moodle learning management system. Four primary themes were identified, as two-thirds of the security related threads on the discussion board addressed the following topics: authentication, permissions, attacks and Moodle configuration. This study should be of interest to educators in information systems management on several levels. First of all, as users and in some cases ad-hoc administrators of learning management systems, the themes and trends identified should increase awareness of security issues inherent in the platform. Secondly, this article serves as a descriptive case study on how security issues are described, discussed and dealt with by developers, users and administrators within the open source software development paradigm.

Keywords: Information Assurance and Security, Learning Management System (LMS), Online communities, Qualitative research & analysis

1. INTRODUCTION

The problem statement for this study resides at the intersection of two recent and timely phenomena: e-learning and information security. According to an annual study commissioned by the Sloan Consortium (Allen and Seaman, 2010), e-learning has grown massively over the last decade (see Figure 1) and this growth appears to be continuing; recent projections suggest that by 2015, 86% of post-secondary students will take some or all of their classes online (Nagel, 2011, January 26).

An e-learning platform connected to the Internet is susceptible to the same types of attacks and human error as any other site, however, researchers (Furnell, Onions, Knahl, et al., 1998; Furnell and Karweni, 2001; Warren and Hutchinson, 2003; Raitman, Ngo, Augar, and Zhou, 2005; Mohd Alwi and Fan, 2010a, 2010b, 2010c) discussing these issues over the last decade have repeatedly asserted that the issue of e-learning security has not been adequately addressed. Furthermore, considering human beings are widely cited as the weakest link in any information security program (Curry, 2011), this brings the focus on several major categories of participants in the online learning process: developers, teachers, students and administrators. Lack of attention to information security in e-learning is a problem because important issues of student and staff privacy are at stake, but also online learning credibility is at stake due to proper authentication of students and attribution of student work.

Exploits on vulnerabilities of a learning management system could have devastating consequences to accessibility, availability, and reliability of the platform, thus impacting both everyday operations of the educational institution and to its long term reputation. In September 2011, Australian researchers (Pauli, 2011) discovered several zero-day security vulnerabilities in Blackboard Learn, a platform used by thousands of universities around the world. These vulnerabilities could potentially allow students to change grades and download future assignments, including exams and also exposed personal information to theft. As with any information system, internal threats are also possible. In 2008, staff and student workers at the University of Texas Brownsville used an admin access to the university Blackboard system to steal exams (Tillman, 2009) and a breach by a student of a similar Blackboard system at Baylor University compromised personal data of over 500 students, staff and faculty (Daily, 2008). A 2010 study by the Ponemon Institute (Miller, 2010), which included several educational institutions, estimated that the average cost per record of personal information stolen in a data breach was $204.

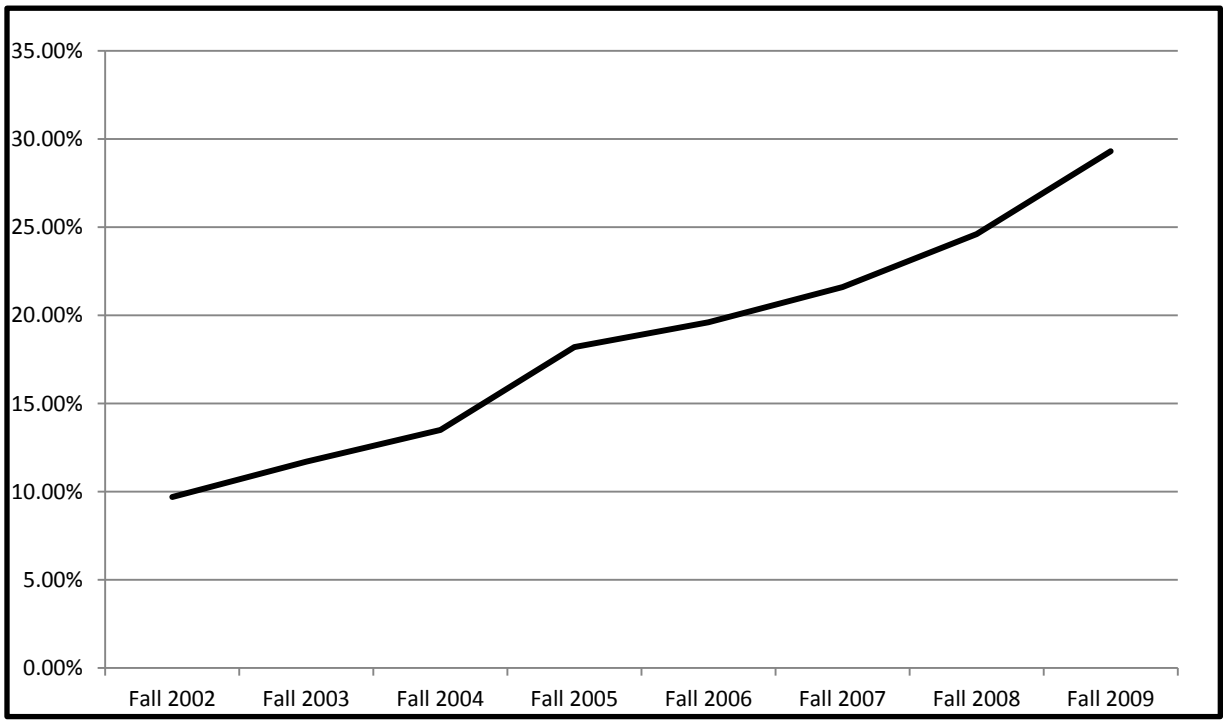

Figure 1: Online Enrollment as a Percent of Total Enrollment in Degree-granting Post-secondary Institutions (Allen and Seaman, 2010)

The open source Moodle platform is not at all immune to vulnerabilities and the vast number of implementations, over 67,000 sites in 217 countries (Moodle.org, 2012), makes it a prime target for attack. In October 2011, Moodle posted comprehensive updates to all three branches of the learning management system which addressed fifteen security vulnerabilities (Nagel, 2011, October 19). Several of these vulnerabilities were identified as "serious" and included the possibility for users to modify form contents, authentication vulnerability, exposure of user names in the chat functionality, cross-site forgery, cross-site scripting, database injection and denial of service vulnerability.

Little is known, however, about what security concerns and issues are central to those who use learning management systems. Most research discusses security issues on a rather high and conceptual level. The aim of this study is to return to primary sources, the Moodle learning management system (LMS) Security and Privacy forum, in an attempt to identify, categorize and understand trends and concerns among learning management system users.

The primary research questions of this study are:

- What are the main themes and issues discussed by the Moodle LMS developer and user community on the Security and Privacy forum?
- What trends can be identified? How have the themes and issues discussed on the Moodle LMS Security and Privacy forum evolved over time, if at all?

A secondary research question of this study is:

- What is the impact, if any, of the open source nature of the Moodle LMS on the content or process of discussion board conversations?

2. REVIEW OF THE LITERATURE AND RESEARCH

The majority of published work on the topic of information security and e-learning involves applying basic security concepts to e-learning and making general policy-level suggestions for securing e-learning platforms (see Table 1).

It seems important to note that there have been several (six as of December 2012) Workshops on E-Learning Security, also known by the acronym, ELS-2012 (for the latest "Sixth Workshop on E-Learning Security"). These workshops are run as a special track of the International Conference for Internet Technology and Secured Transactions (ICITST, 2009, 2010, 2011a, 2011b), a conference which is co-sponsored by the Institute of Electrical and Electronics Engineers (IEEE). According to the website (ICITST, 2011a), all articles are fully indexed IEEE Xplore and the DBLP databases. However, it appears that in either database only the 2009 and 2010 conferences are indexed. Although full text of the articles is not readily available, of approximately 250 articles from 2009 and 2010, two from 2009 appear to be related to e-learning and security, including a version of the Mohd Alwi and Fan (2010a) article, mentioned previously. There were no articles related to e-learning and security in 2010. In the ELS-2011: Fifth Workshop on E-learning Security there were two papers on e-learning and security. One article (Hirsch and Ng, 2011) discussed basic issues facing educational institutions wishing to implement cloud computing. Another entitled "A Process Framework for Securing an e-Learning Ecosystem" (Eswari, 2011); shows the continuing trend towards applying security frameworks to e-learning systems. A call for papers was issued for the

Article	Authors Assert / Describe	Type of Article / Research Questions or Methodology	Models, Frameworks, Concepts Discussed	Recommendations for Future Research/ Practice
Furnell, Onions, Knahl, Sanders, Bleimann, Gojny and Roder (1998)	Important to address security issues which have not been widely dealt with to date	Conceptual; No Research Questions or Methodology	SDLearn security framework	None
Furnell and Karweni (2002)	Information security is definitely needed in online distance learning	Conceptual; No Research Questions or Methodology	Information security/ information assurance 'foundations' discussed	None
Warren and Hutchinson (2003)	Information security in e-learning environments is often ignored	Conceptual; No Research Questions or Methodology	Fundamental information security issues relevant to the e-learning environment as a guide for future research and practice	Development of comprehensive security guidelines for both users and developers of e-learning application
Kritzinger and von Solms (2006)	Information security is important to e-learning because e-learning is contingent on both information technologies and communication technologies—and both of these technologies are susceptible to security risks and threats	Conceptual; No Research Questions or Methodology	CIA triad (confidentiality, integrity and availability); counter-measures; security policy; risk management	None
Jalal and Zeb (2008)	The Internet is an open access network which allows hackers to analyze a portal's design and identify weaknesses	Technical/ Conceptual; No Research Questions or Methodology	Various technical safeguards discussed	None
Rabuzin, Baca, and Sajko (2006)	The issue of security in e-learning has hardly been dealt with in the literature	Technical/ Conceptual; No Research Questions or Methodology	Biometrics discussed;	None
Castella-Roca, Herrera-Joancomarti and Dorca-Josa (2006)	Exam management discussed--while much of e-learning takes place online, exams are still typically completed in a face-to-face environment	Conceptual; No Research Questions or Methodology	Model for the submission of exams online, in a proctored but perhaps off-site and distant, test taking facility	None
Chudá (2009)	General problems involved in security and evaluation are "difficult or even impossible to manage"	Conceptual; No Research Questions or Methodology	General administration and security features of the Moodle LMS; biometrics	Additional research on keystroke dynamics
Tsiantis, Stergiou and Margariti (2007)	Security should be user-centric; the typical culture of security is based on restricting access and information flow which does not mesh with the openness of an educational ethos	Conceptual; No Research Questions or Methodology	Basic information security concepts; authentication, privacy	None

Table 1: Literature Review on Information Security and E-Learning

Article	Authors Assert / Describe	Type of Article / Research Questions or Methodology	Models, Frameworks, Concepts Discussed	Recommendations for Future Research/ Practice
de Medeiros Gualberto, Abib and Zorzo (2009)	E-learning research has concentrated on content rather than security	Conceptual; Case Study; No Research Questions or Methodology	Concepts of integrity, non-repudiation, confidentiality and authenticity, described as INCA	None
Mohd Alwi and Fan (2010a)	In the rush to put materials online, many institutions have not adequately considered the security implications of their e-learning initiatives	Conceptual; No Research Questions or Methodology	Evolution of security issues in e-learning; specific threats discussed	Institutions should use an information security management (ISM) framework to better understand and combat the security threats present on the Internet
Mohd Alwi and Fan (2010b)	No significant relationship between respondent job role, institution type or self-reported level of information security awareness and perception of information security threats	Empirical study addressing awareness and perceptions of security in e-learning among four job roles; quantitative; online questionnaire		Currently there is no explicit model or framework for eLearning information security; a model should be developed
Mohd Alwi and Fan (2010c)	There is a common supposition that e-learning environments do not need to be secured as much as e-commerce or e-banking applications and that the (mis-)conception is that e-learning operates within a safe environment	Conceptual; No Research Questions or Methodology	Categorize security threats within the e-learning environment	Additional work on countermeasures for the threats identified and the development of a framework for security in e-learning
Kumar and Chelikani (2011)	There are several advantages to cloud-based e-learning, but with accompanying specific security issues.	Empirical; Key research question to identify main security issues in cloud-based e-learning; questionnaires were sent to several companies	Discuss the role of security management standards for cloud computing	Additional research on both cloud-based e-learning and mobile e-learning.
Laisheng and Zhengxia (2011)	Storage and transmission of personal data in a cloud-based environment represents a security risk; security challenges can be overcome by encrypting important data	Conceptual; No Research Questions or Methodology	Discuss seven challenges related to cloud computing and e-learning, one of which is security	None
Ugray (2009)	General security and privacy issues involved in mobile learning, or m-learning	Conceptual; No Research Questions or Methodology	Basic definitions of electronic learning and mobile learning given	Need for academic research in the specific area of security vulnerabilities facing m-learning

Table 1: Literature Review on Information Security and E-Learning (continued)

7th Workshop on E-Learning Security in 2012 (WikiCFP, 2012) but a list of articles was not available from the ICITST website. While earlier proceedings of the Workshop on E-learning Security are also not readily available, this does confirm an interest within the research community for the intersection of information security and e-learning and a need for additional work in this area.

To summarize this literature review, of the sixteen papers discussed, only two are empirical in nature. The remaining articles discuss security issues at a conceptual level and apply frameworks or basic information security concepts to e-learning or advocate the use of a particular technology such as cloud computing or encryption. Most of the papers do not propose research questions and only three give recommendations for future academic research. Other papers call for the development of a framework or model to better understand the security issues involved in e-learning.

3. RESEARCH METHODOLOGY

As shown in the literature review, much of the published work on information security and e-learning has focused on applying basic concepts of information security to the e-learning environment. The empirical study cited above (Mohd Alwi and Fan, 2010b) was inconclusive in terms of its results and suggested even a low level of knowledge of specific security threats and their impact among e-learning professionals. The aim of this study is to return to primary sources in an attempt to identify, categorize and understand trends and concerns among several different types of learning management system users.

3.1 Place, Participants and Materials

Moodle is an abbreviation for Modular Object-Oriented Dynamic Learning Environment, an open source e-learning platform which is managed by the Moodle Trust, a non-profit organization headquartered in Australia, but with developers and users around the world. There are 67,136 registered sites in 217 countries with nearly 60 million users of which 1.28 million are instructors (Moodle.org, 2012). The Moodle.org community, where users share content and engage in discussions about the use of the Moodle platform, also has over 1 million users. One of the discussion forum topics within the Moodle.org community is the 'Security and Privacy' topic, which will be the focus of this study.

In terms of security issues and the Moodle platform, there are three media of communication between the Moodle Trust and users:

- Security Announcements
- Security Documentation
- Security and Privacy discussion forum

The first two media are one-way media, users can submit potential security vulnerabilities to the Security Announcements board, but submissions are either validated or not by Moodle staff and there is no ensuing discussion in the Security Announcements area. The Security Documentation area is frequently updated by Moodle staff, but there is no way for users to edit or contribute and there is no comments functionality enabled. Thus the third medium, the Security and Privacy discussion forum is the only official area for communication between developers and mainstream users regarding these issues.

Members of the Security and Privacy discussion forum include developers, teachers, administrators, security professionals and students. All discussion posts from the 'Security and Privacy' conference are public and readily available. All posts from August 2004 to November 2011 of the Moodle Security and Privacy discussion forum were analyzed using content analysis techniques; no sampling techniques were employed. All in all, the data set consisted of 485 threads. Each thread consisted of an initial post plus reply posts, if any. Some initial posts garnered no reply posts, while one thread garnered 74 reply posts. The total number of posts, initial posts plus reply posts was 2099.

3.2 Procedure and Data Analysis

Content analysis has been defined as "a detailed and systematic examination of the contents of a particular body of material for the purpose of identifying patterns, themes or biases" (Leedy and Ormrod, 2005, p. 142). According to Krippendorf (2004), "content analysis is context sensitive and therefore allows the researcher to process as data texts that are significant, meaningful, informative, and even representational to others" (p.41). Neuendorf (2002) asserts that the objectives and standards of content analysis are consistent with survey research. Both attempt to measure variables as they naturally occur with no experimental manipulation of independent variables.

Content analysis can be approached quantitatively, qualitatively or using both methods. Altheide (1987) first proposed ethnographic content analysis as a way of combining the qualitative approach of ethnography with the quantitative approach of content analysis. The primary feature of ethnographic content analysis is the "reflexive and highly interactive nature of the investigator, concepts, data collection and analysis" (Altheide, 1987, p. 68). Altheide (1987) further states that ethnographic content analysis entails "reflexive movement between concept development, sampling, data collection, data coding, data analysis and interpretation" (p. 68). Ultimately, "the aim is to be systematic and analytic, but not rigid" (p. 68). A comparison of the distinctive characteristics of quantitative content analysis (QCA) and ethnographic content analysis (ECA) is presented in Figure 2.

Quantitative techniques of content analysis were used, however, primarily through the analysis of word counts and key word in context (KWIC) analysis using MAXQDAplus text analysis software (Verbi GmbH, 2011). The quantitative analysis was followed up by and combined with qualitative coding and analysis of themes and issues using the same software.

Krippendorf (2004) describes six components of content analysis that offer a step-by-step process to "partition, conceptualize, talk about and evaluate" content analysis (p.83). The first four steps are further sub-divided into a rubric known as "data making"—the process of transforming raw text into analyzable data:

- Unitizing – the process of defining the unit of text, message or document that will be the subject of analysis,
- Sampling – the process of determining a statistically representative subset, if necessary, of a larger population of documents or text,

	QCA	ECA
Research Goal	Verification	Discovery; Verification
Reflexive Research Design	Seldom	Always
Emphasis	Reliability	Validity
Progression from Data Collection, Analysis, Interpretation	Serial	Reflexive; Circular
Primary Researcher Involvement	Data Analysis and Interpretation	All Phases
Sample	Random or Stratified	Purposive and Theoretical
Pre-Structured Categories	All	Some
Training Required to Collect Data	Little	Substantial
Type of Data	Numbers	Numbers; Narrative
Data Entry Points	Once	Multiple
Narrative Description and Comments	Seldom	Always
Concepts Emerge During Research	Seldom	Always
Data Analysis	Statistical	Textual; Statistical
Data Presentation	Tables	Tables and Text

Figure 2: A Comparison of Quantitative (QCA) and Ethnographic (ECA) Content Analysis (Altheide, 1987)

- Recoding/Coding – the dual process of capturing and saving text, documents, images or sound, that might otherwise be transient, and rendering the text in a format that is more conducive to analysis,
- Reducing – the process of transforming masses of text, data and codes into a more manageable format, such as frequency counts or other aggregations.

In this study, the **Unitizing** step involved determining the unit of analysis which was a single message, with associated replies, in the discussion forum. In situations in which a single message contains multiple themes, the message may be broken down into multiple parts before analysis. Weber (1990) suggests this technique for complex content and adds that "this form of coding is labor-intensive, but leads to much more detailed and sophisticated comparisons" (p. 22). **Sampling** was not relevant to this study since all messages from the Security and Privacy discussion forum will be analyzed. **Recording/Coding** and **Reducing** took place once the data collection process has begun according to the timeline at the end of this document. The final two steps were **inferring** and **narrating**. The step of abductively inferring requires that the researcher move the analysis beyond the text and data to evoke broader meaning. Again according to Krippendorf (2004) "abductively inferring contextual phenomena...is unique to content analysis and goes beyond the representational attributes of the data" (p.83). Narrating is the step in which the researcher translates and packages his or her analysis into a format that is understandable to external audiences. The final step might also include clarifying any practical significance of the analysis.

In terms of this study, as stated previously the recording unit was one post to the discussion conference, including all reply posts, if any. The categories were determined after an initial reading of the data and were continually refined through the test coding phase. Reliability was assessed via a second coder who was trained and re-coded a subset of the data before proceeding to later stages of the research design. Twenty-five posts were chosen at random and recoding achieved a 96% reliability rating after one round of coding; after discussion with the second coder, 100% reliability was achieved after the second round.

Julien (2008) has noted that "Identifying themes or categories is usually an iterative process, so the researcher spends time revisiting categories identified previously and combining or dividing them, resolving contradictions, as the text is analyzed over and over" (p.120). Krippendorf (2004) concurs that content analysis may include iterative loops—"the repetition of particular processes until a certain quality is achieved" (p. 85). Krippendorf (2004) also asserts that "there is no single 'objective' way of flowcharting research designs" (p. 85).

4. ANALYSIS AND RESULTS

The coding process did not begin with hard and fast terms and themes with precise definitions. Instead the coding process began in an open-ended manner, with the researcher reading through the data, noting recurring concepts and themes; a second, third and fourth reading through the data allowed for themes to be narrowed or combined or new themes added. A new theme, 'training' only emerged in the

fourth reading of the data. After this fourth reading of the data, actual coding began with a list of forty-eight codes.

This section on results of the coding and frequencies directly address the first research question:

What are the main themes and issues discussed by the Moodle LMS developer and user community on the Security and Privacy forum?

4.1 Results of the coding with frequency of terms and themes

Of the 485 threads coded in this study, the vast majority of threads were coded with a single code. Initial posts tended to ask a specific question or express a specific concern and follow-up posts tended to keep this narrow focus. As I will discuss more in detail later, the vast majority of threads were opened and closed within one month. As mentioned in the "Good Practice Guide and Etiquette Tips: Moodle Chat, Forum and Blog" (Dvorak, 2011), good practices for posting in any Moodle classroom include writing short messages, staying on topic and refraining from opening inactive threads. These practices are evident in the Security and Privacy discussion forum. However, in several instances, either in the initial post or in subsequent reply posts, a given thread did overlap more than one code. As a result, for 485 threads coded, 500 total codes were employed.

The raw frequencies are given in the Table 2 from most to least used. Note that certain 'header codes' with subcodes, such as Configuration, Permissions and Security Warnings were not used as individual codes per se, thus these codes have a zero frequency. Each of these header codes does have subcodes that are represented in the table. Other 'header codes' such as Authentication and Attacks were used as general codes, that is, the coded text did not correspond to one of the subcodes, but did refer generally to the header code.

When subcodes are grouped with their respective header code, a visual representation of the frequencies can be found in Figure 3. Thus the top four themes of authentication, permissions, attacks and Moodle configuration amount to 59% of all coded threads in the Moodle 'Security and Privacy' discussion board. Since 10% of the coded threads are not explicitly about security at all, the weight of the top four teams increases to nearly two-thirds of all coded threads that address security issues. The next eight themes account for an additional 24% of codes (when 'not security' posts are removed). When combined with the top four themes, these twelve themes represent 90% of all threads on the discussion board:

- Authentication
- Permissions
- Attacks
- Moodle configuration
- User Profile/Privacy/Policy
- Security Warnings
- General Security Advice
- Security Reporting/Logs
- Anti-Virus
- PHP
- Training (Moodle or Security)
- Update/Upgrade Issues

4.2 Additional Discussion of themes, trends and patterns identified

In the previous section, a broad overview of identified themes was presented in a list of the forty-eight codes and frequencies of those codes over the existence of the Moodle Security and Privacy discussion board. In this section, an analysis of several longitudinal trends and patterns will be presented. This section directly addresses the second primary research question of this study:

> What trends can be identified? How have the themes and issues discussed on the Moodle LMS Security and Privacy forum evolved over time, if at all?

4.3 Themes, issues and trends by year

The Moodle Security and Privacy discussion board did not exist as a separate board with that name until 2008. There are posts on the discussion that pre-date 2008, in fact the first initial post on the board dates to August 2004. However, these earlier posts regarding security issues were posted in a different Moodle discussion board and were subsequently moved by moderators when the

Code	Frequency	Percentage
Permissions: Platform Permissions	63	12.6%
Authentication: Passwords	43	8.6%
Configuration: Server Configuration	41	8.2%
Attacks: Hacking/Hacked	31	6.2%
User Profile/Privacy/Policy	24	4.8%
Authentication	21	4.2%
Authentication: LDAP	20	4.0%
Authentication: Certificates	18	3.6%
General Security Advice	16	3.2%
Not Security: Installation/Configuration	15	3.0%
Not Security	14	2.8%
Permissions: Locked out	14	2.8%
Security Warnings: Moodle Security Warnings	14	2.8%
Security Reporting/Logs	13	2.6%
Attacks: Spam	12	2.4%
Anti-Virus	10	2.0%
Not Security: Functionalities	10	2.0%
PHP	9	1.8%
Training (Moodle or Security)	9	1.8%
Update/Upgrade Issues	9	1.8%
Attacks: Viruses, Trojans	8	1.6%
Vulnerabilities	8	1.6%
Not Security: Enrollment	7	1.4%
Configuration: Block Access	5	1.0%
Configuration: Platform Configuration	5	1.0%
Javascript	5	1.0%
Security and Privacy Board/Mailing list	5	1.0%
Authentication: Cookies	4	0.8%
Backup/Restore	4	0.8%
Databases (MySql + others)	4	0.8%
Intellectual Property/Proprietary	4	0.8%
Not Security: Registration	4	0.8%
Pornography	4	0.8%
Security Warnings: External Security Warnings	4	0.8%
Encryption	3	0.6%
Module (3rd Party) Security	3	0.6%
Open Source	3	0.6%
Permissions: Server Permissions	3	0.6%
Attacks	2	0.4%
Attacks: XSS	2	0.4%
Authentication: Logout	2	0.4%
General Security Advice: Keeping informed	2	0.4%
Attacks: SQL injection	1	0.2%
Change Management	1	0.2%
Risk Assessment	1	0.2%
Configuration	0	0.0%
Permissions	0	0.0%
Security Warnings	0	0.0%

Table 2: Raw Frequencies of Code Use (subcodes not grouped by header code)

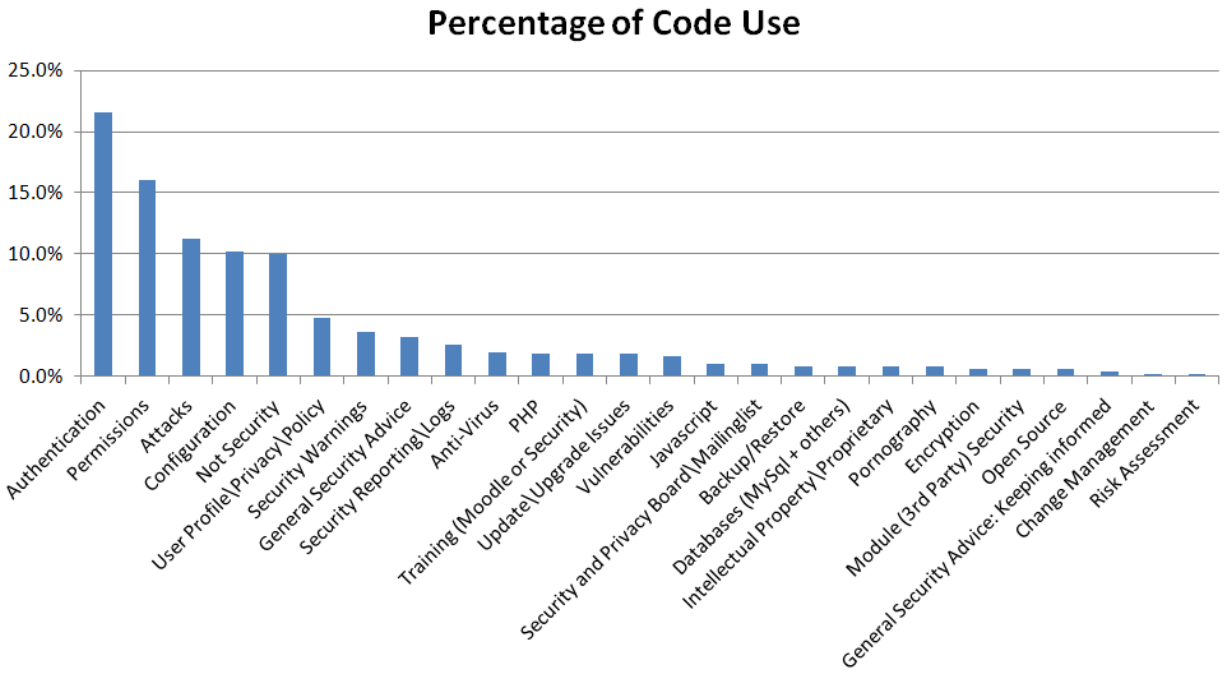

Figure 3: Percentages of Code Use (subcodes grouped by header code)

Security and Privacy discussion board was created. Table 3 provides an overview of number of posts per year; the date of post is based on the date of initial post. The year 2011 is an incomplete year as the data set was obtained on November 18, 2011, thus the final six weeks of 2011 are not included in this analysis.

Year	Number of threads
2011 (through Nov 18)	155
2010	151
2009	159
2008	15
2007	1
2006	2
2005	1
2004	1

Table 1: Number of discussion threads by year

The content analysis software MaxQDA was used to mine the data and codes to determine the most prevalent themes and issues by year in hopes of identifying trends in the data. Due to the small number of threads from 2004-2008, this data was combined in this analysis. Table 4 shows the top five themes discussed in each year.

Of note is the fact that the theme of platform permissions is the number one discussed topic in each year. Configuration issues are also ever-present. Also significant is that there seems to be a progression from general security issues, also training, in earlier years to more technical issues in 2011. The sudden rise of installation/configuration as a point of discussion might be due to a major upgrade of the Moodle platform that made installation and configuration considerably more complex.

4.4 Additional analysis of themes and issues: Replies and overall 'life of thread'

A content analysis program like MaxQDA also allows analysis beyond simply counting word frequencies. Two other areas of analysis that can shed light on longitudinal trends and patterns of themes in the discussion board involve analyzing threads by number of replies and the overall life of a thread.

2004-2008	2009	2010	2011
1 (tie). Platform Permissions	1. Platform Permissions	1. Platform Permissions	1. Platform Permissions
1 (tie). Training (Moodle or Security)	2. Hacking/Hacked	2. Passwords	2. Installation/ Configuration
3 (tie). Server Configuration	3. Passwords	3. Server Configuration	3. Server Configuration
3 (tie). Hacking/Hacked	4. Server Configuration	4. User Profile/Privacy/Policy	4. Passwords
3 (tie). General Security Advice	5 (tie). Moodle Security Warnings	5. Hacking/Hacked	5. LDAP
3 (tie). Platform Configuration	5 (tie). User Profile/Privacy/Policy		

Table 4: Top 5 most frequent discussion topics by year, 2004-8, 2009, 2010, 2011

Theme	Dates	Months open	Total number of replies
Passwords	May 2009 - Oct 2011	29	16
Passwords	July 2009 - Feb 2011	19	6
Passwords	Jan 2010 - Jan 2011	12	3
General Security	Feb 2009 - Jan 2010	11	9
User Profile/Privacy/Policy	July 2009 - May 2010	10	11
Hacked/Hacking	Feb 2009 - Nov 2009	9	23
Certificates	March 2009 - Sept 2009	7	3
Not Security: Registration	July 2009 - Feb 2010	7	3
Server Configuration	Apr 2010 - Oct 2010	6	5
Platform Permissions	May 2011 - Nov 2011	6	4

Table 5: The ten discussion topics that spanned six months or more

As mentioned previously, the vast majority of threads were opened, discussed, and became inactive within one month. When a person replies to a post the thread is put back on the front page of the discussion forum, along with other recent replies or any newly created threads. Inactive threads, those that no longer receive replies, remain in the system but are no longer as easily accessible as they will fall further and further from Page 1. It is common practice in discussion forums to make a specific comment or ask a specific question. Subject lines should be informative and although some background to the issue or problem should be given, it should remain as brief as possible. Replies work in a similar fashion. Also 'hijacking of a thread', replying to a thread and changing or derailing the original topic towards a new and different topic, is discouraged. Common netiquette requires that a new topic be started.

Of 485 main threads, 427 or 88%, were inactive within one month. This does not necessarily mean that the topic or question was resolved, just that there were no additional reply posts. Threads are never really 'closed', however, because if a person conducts a search using keywords, older posts could appear and if a person replies, any post would become active again and appear on Page 1 (which may encourage more replies). Of those that remained open for more than one month, only 10 or 2%, were open for six months or more. Topics that remained 'current' for more than six months and continued to garner replies are clearly topics that remained active and timely for the Moodle security community. Table 5 presents the ten topics that remained open and active for six months or more.

It is important to note here that the length of time a thread remained active does not necessarily correspond to a high number of reply posts. Another measure of a popular or hot topic, is sheer number of replies, whether these replies come over a short or long period of time. Of 485 main topics, 105 or 22% had no replies at all. While one might think that non-security related topics would top the list of posts with no replies, the code 'not security' was ranked ninth, behind eight security-related topics (see Table 6).

The average number of replies per post was 3.3, with 30 or 6% garnering ten or more reply posts. The post that had the most replies, 79, was among the first posted on the discussion board in October of 2008 and fell under the topic of training. The top five topics discussed in those thread were hacking/hacked, training (Moodle or security), server configuration, passwords and platform permissions.

Topics
1. Platform Permissions
2. Server Configuration
3. Passwords
4. LDAP
5. Installation/Configuration
6. User Profile/Privacy/Policy
7. Authentication
8. General Security Advice
9. Not Security
10. Anti-virus

Table 6: Top ten discussion topics with no replies

4.5 Open source and the discussion board process

As mentioned previously, this study was conducted with a secondary research question in mind:

> What is the impact, if any, of the open source nature of the Moodle LMS on the content or process of discussion board conversations?

The existence of an open and freely accessible discussion forum on security issues, sponsored, maintained and moderated by the Moodle organization, is already a divergence from the common practice in closed source learning management systems. However, beyond this fact, this study did not uncover any additional insight into what open source means to the users or developers who use the site. Indeed, 'open source' as a code or topic of main thread discussion ranked 35th in frequency and comprised only three of 485 threads in the Security and Privacy discussion board.

5. CONCLUSION

5.1 Significance of the Study

The purpose of this research was to identify, categorize and understand trends and issues in information security in e-learning as reflected in the discussions on a 'Security and Privacy' discussion forum of a major learning management system. The study of information security and e-learning is a relatively new area of inquiry, thus this exploratory study has laid the groundwork for future studies by identifying trends and issues facing e-learning developers, administrators and users.

Four themes were of primary importance to members of the Moodle Security and Privacy community, as two-thirds of their security related threads addressed these four topics:

- Authentication
- Permissions
- Attacks
- Moodle configuration

A year to year analysis also revealed that 'platform permissions' was consistently an important concern for community members. 'Platform permissions' is a subcode of the 'Permissions' code in the above list; other subcodes within Permissions are 'Locked out (of Moodle)' and 'Server permissions'. This combination of authentication, issues of access control and configuration of the platform show the concern that administrators, developers and users have with properly setting up the Moodle platform to protect against threats to security and minimize potential vulnerabilities.

In terms of discussions that maintained interest of the community over the long term, in addition to the four themes above, passwords generated quite a lot of discussion, in particular, how best to encourage and/or require users to implement hardened passwords and to change them often. Training for Moodle or regarding security issues in general was also an important theme. So at the same time while there was considerable interest in discussing elements of configuration in order to ward off threats and protect against vulnerabilities, there was also an acute awareness among the community that security is also very much in the hands of the users and that education and training are also critical success factors to creating and maintaining a secure learning management platform.

Finally, analysis of the discussions also pointed out that while the lifespan of certain topics is limited, others are more persistent and still others re-emerge after having been ostensibly absent from the forum. Among the primary, persistent themes discussed on the forum, the challenges of developing an interactive software system are evident. There is a constant tension between creating a usable, functional system while providing the highest level of protection regarding issues of system security and user privacy. As evidenced in the forum, discussions of 'highest levels' of protection quickly transform into discussions of 'sufficient' levels of protection. As in all software development, this tension between usability and security may never be resolved.

5.2 Limitations of the Study

Any content analysis study must limit the scope of the material to be analyzed. Moodle is a learning management platform that is growing rapidly. The Nagel (2011, October 19) article mentioned earlier credited Moodle with 48 million users via 58,000 sites around the world. Six months later, these figures stand at nearly 59 million users via 67,000 sites (Moodle.org, 2012). The study drew a somewhat arbitrary, albeit practical, line on November 18, 2011 as the cutoff date for data collection—thus any analysis is a snapshot in time of a moving target—and one moving very quickly.

Another limitation is the choice of Moodle itself. There are many learning management systems, including other open source alternatives (Dawson, 2011; Sampson, 2009). While most of these alternatives do provide openly available discussion boards, none of them could provide the breadth and depth of data specifically on security as Moodle. As these other platforms gain momentum and provide more specialized listservs and discussion boards geared towards security issues, other interesting and plentiful points of comparison will be available to researchers.

The choice of ethnographic content analysis also includes a significant limitation to the study. The themes and trends identified remain at a descriptive level and statistical significance cannot be inferred, nor are the results generalizable in a conventional quantitative sense. However, as was established in the literature review, previous research in this area remained at a highly conceptual level and the present article represents a significant qualitative step towards adding an empirical element which has, to date, been lacking in the literature. This ethnographic content analysis study provides valuable groundwork for additional empirical work on this subject.

5.3 Recommendations for future research

This content analysis merely scratched the surface of the types of dialogue that exist among developers, administrators and users of the Moodle learning management system. Opportunities to study the Security and Privacy community are vast, whether online on allied listservs and discussion boards or offline at face-to-face conferences, trainings and workshops. Content analysis could be supplemented with quantitative methods by sending a questionnaire to members of the community in an attempt to confirm some of the results of the analysis of this study. A quantitative approach could fill some of the gaps and address the limitations on reliability and generalizability inherent in the ethnographic content analysis approach adopted by the present study. Alternatively, keeping within the qualitative paradigm, in-depth interviews could be arranged with members of the community to delve deeper into the concerns and challenges that community members face in using the Moodle learning management system. Finally, for those who are interested in open source 'process' and e-learning security issues, since the current content analysis was not particularly revealing in this area, there remains much research to be done.

6. REFERENCES

Allen, I.E., & Seaman, J. (2010). Class Differences: Online Education in the United States, 2010. Retrieved from http://www.sloanconsortium.org/publications/survey/pdf/class_differences.pdf

Altheide, D. L. (1987). Ethnographic content analysis. *Qualitative Sociology, 10*(1), 65-77.

Castella-Roca, J., Herrera-Joancomarti, J., & Dorca-Josa, A. (2006). A secure e-exam management system. First International Conference on Availability, Reliability and Security (ARES '06), 864-871.

Chudá, D. (2009). Evaluation and security features in e-learning. *Communication & Cognition, 42*(1 & 2), 63-74.

Creswell, J. (2006). *Qualitative Inquiry and Research Design: Choosing Among Five Approaches.* London: Sage.

Curry, S. (2011, May 25). The weakest link is the human link. *Security Week.* Retrieved from http://www.securityweek.com/weakest-link-human-link

Daily, S. (2008, January 28). BIN breached over break, ITS still recovering. Retrieved from http://www.baylor.edu/lariat/news.php?action=story&story=48754

Dawson, C. (2011, February 1). There are alternatives to Blackboard and Moodle: Instructure Canvas goes open source. ZDNet Education. Retrieved from http://www.zdnet.com/blog/education/there-are-alternatives-to-blackboard-and-moodle-instructure-canvas-goes-open-source/4475

Dvorak, R. (2011). Good practice guide and etiquette tips: Moodle chat, forum and blog. Retrieved from http://media.wiley.com/product_ancillary/22/04709494/DOWNLOAD/MoodleGoodPracticeandEtiquette.pdf

Eswari, P.R.L. (2011). A process framework for securing an e-learning ecosytem. International Conference for Internet Technology and Secured Transactions (ICITST 2011), 403-407.

Furnell, S.M., Onions, P.D., Knahl, M., Sanders, P.W., Bleimann, U., Gojny, U., & Roder, H.F. (1998). A security framework for online distance learning and training. *Internet Research, 8*(3), 236.

Furnell, S.M., & Karweni, T. (2001). Security issues in online distance learning. *VINE: The Journal of Information and Knowledge Management Systems, 31*(2), 28-35.

Hirsch, B., & Ng. J.W.P. (2011). Education beyond the cloud: Anytime-anywhere learning in a smart campus environment. International Conference for Internet Technology and Secured Transactions (ICITST 2011), 718-723.

ICITST. (2009). Workshop on E-learning Security. Retrieved from http://www.icitst.org/Workshop_on_Elearning%20Security.pdf

ICITST. (2010). ICITST-2010 final programme. Retrieved from http://www.icitst.org/ICITST-2010%20Final%20Programme

ICITST. (2011a). ICITST-2011: List of accepted papers [Data file]. Retrieved from http://www.icitst.org/ICITST%202011%20List%20of%20Accepted%20Papers.xlsx

ICITST. (2011b). ICITST-2011: The International Conference for Internet Technology and Secured Transactions. Retrieved from http://www.icitst.org/

Jalal, A., & Zeb, M.A. (2008). Security enhancement for e-learning portal. *International Journal of Computer Science and Network Security, 8*(3), 41-45.

Julien, H. (2008). Content analysis. In L. M. Given (Ed.), *The Sage Encyclopedia of Qualitative Research Methods* (pp. 120-121). Thousand Oaks, CA: Sage Publications.

Krippendorf, K. (2004). *Content Analysis: An Introduction to its Methodology* (2nd Ed.). Thousand Oaks, CA: Sage Publications.

Kritzinger, E., & von Solms, S.H. (2006). E-learning: Incorporating information security governance. *The Information Universe: Journal of Issues in Informing Science and Information Technology*, 3, 319-325. Retrieved from http://www.informingscience.org/proceedings/InSITE2006/IISITKrit157.pdf

Kumar, G., & Chelikani, A. (2011). Analysis of security issues in cloud based e-learning. (Unpublished master's thesis). University of Borås, Borås, Sweden. Retrieved from http://bada.hb.se/bitstream/2320/9271/1/2011MAGI23.pdf

Laisheng, X., & Zhengxia, W. (2011). Cloud computing: A new business paradigm for e-learning. Proceedings of the 2011 Third International Conference on Measuring Technology and Mechatronics Automation (ICMTMA), 716-719. DOI: 10.1109/ICMTMA.2011.181

Leedy, P.D., & Ormrod, J.E. (2005). *Practical Research: Planning and Design* (8th Ed.). Upper Saddle River, NJ: Pearson Education, Inc.

Miller, M.H. (2010). The cost of data breaches is rising, study finds. Retrieved from http://chronicle.com/blogs/wiredcampus/the-cost-of-data-breaches-is-rising-study-finds/20809

Mohd Alwi, N.H., & Fan, I.S. (2010a). E-learning and information security management. *International Journal for Digital Society, 1*(2), 148-156. Retrieved from http://infonomics-society.org/IJDS/E-Learning%20and%20Information%20Security%20Management.pdf

Mohd Alwi, N.H., & Fan, I.S. (2010b). Information security in elearning: A discussion of empirical data on information security and elearning. Proceedings of the 5th International Conference on e-Learning, 282-290.

Mohd Alwi, N.H. and Fan, I.S. (2010c). Threats analysis for e-learning. *International Journal of Technology Enhanced Learning, 2*(4), 358–371.

Moodle.org. (2012). Moodle statistics. Retrieved April 8, 2012, from http://moodle.org/stats

Nagel, D. (2011, January 26). Online learning set for explosive growth as traditional classrooms decline. Campus Technology. Retrieved from http://campustechnology.com/Articles/2011/01/26/Online-Learning-Set-for-Explosive-Growth-as-Traditional-Classrooms-Decline.aspx?Page=1

Nagel, D. (2011, October 19). 3 Moodle updates address 15 security vulnerabilities. *THE Journal.* Retrieved from http://thejournal.com/articles/2011/10/19/3-moodle-updates-address-15-security-vulnerabilities.aspx

Neuendorf, K.A. (2002). *The Content Analysis Guidebook.* Thousand Oaks, CA: Sage Publications.

Rabuzin, K., Baca, M., & Sajko, M. (2006). E-learning: Biometrics as a security factor. International Multi-Conference on Computing in the Global Information Technology (ICCGI'06). 64- . DOI: http://doi.ieeecomputersociety.org/10.1109/ICCGI.2006.28

Pauli, D. (2011). Millions of student exams, tests and data exposed. *SC Magazine.* Retrieved from http://www.scmagazine.com.au/News/272215,millions-of-student-exams-tests-and-data-exposed.aspx

Raitman, R., Ngo, L., Augar, N., & Zhou, W. (2005). Security in the online e-learning environment. Proceedings of the Fifth IEEE International Conference on Advanced Learning Technologies (ICALT'05), 702-706.

Sampson, B. (2009, April 8). Open source LMS: 10 alternatives to Moodle. Retrieved from http://barrysampson.com/2009/04/open-source-lms-10-alternatives-to-moodle/

Tillman, L. (2009, August 1). 'Gross academic fraud' at UTB-TSC rocked Office of Distance Education. Retrieved from http://www.brownsvilleherald.com/news/online-100590-utb-employees.html

Tsiantis, L. E., Stergiou, E., & Margariti, S.V. (2007). Security issues in e-learning systems. In T.E. Simos & E. Maroulis (Eds.), Computation in Modern Science and Engineering, Proceedings of the International Conference on Computational Methods in Science and Engineering 2007 (Vol. 2, Part B, pp.959-964). College Park, MD: American Institute of Physics.

Ugray, Z. (2009). Security and privacy issues in mobile learning. *International Journal of Mobile Learning and Organisation, 3*(2), 202-218

Verbi GmbH. (2011). MAXQDAplus [computer software]. Marburg, Germany: Verbi GmbH.

Warren, M., and Hutchinson, W. (2003). Information security: An e-learning problem. In W. Zhou et al. (Eds.), *Advances in Web-Based Learning - ICWL 2003, Volume 2783/2003. Lecture Notes in Computer Science* (pp. 21-26). Berlin: Springer Verlag. DOI: 10.1007/978-3-540-45200-3_3

Weber, R. P. (1990). *Basic Content Analysis* (2nd Ed.). Newbury Park, CA: Sage Publications.

WikiCFP. (2012). ELS 2012: The 7th workshop on e-learning security. Retrieved from http://www.wikicfp.com/cfp/servlet/event.showcfp?eventid=25179&copyownerid=2

AUTHOR BIOGRAPHY

Christopher Schultz is Professor of Information Systems Management at the University of Maryland University College. In addition to e-learning and information security, his research interests include professional culture acquisition and knowledge sharing and transfer in professional communities. He is particularly interested in qualitative research methods and ethnography. He has taught courses at the undergraduate and graduate level in e-commerce, information systems management, information assurance and cybersecurity, ergonomics and interface design, and research methods.

STATEMENT OF PEER REVIEW INTEGRITY

All papers published in the Journal of Information Systems Education have undergone rigorous peer review. This includes an initial editor screening and double-blind refereeing by three or more expert referees.

ISSN 1055-3096