INTEGRATING INFORMATION SECURITY IN AN E-LEARNING ENVIRONMENT

«INTEGRATING INFORMATION SECURITY IN AN E-LEARNING ENVIRONMENT»

by Cezar Vasilescu; Ecaterina Livia TATAR; Aura CODREANU

Source:
Conference proceedings of "eLearning and Software for Education" (eLSE) (Conference proceedings of "eLearning and Software for Education" (eLSE)), issue: 02 / 2011, pages: 70-75, on www.ceeol.com.

The following ad supports maintaining our C.E.E.O.L. service
INTEGRATING INFORMATION SECURITY IN AN E-LEARNING ENVIRONMENT

Cezar VASILESCU, Livia TATAR, Aura CODREANU
Regional Department of Defense Resources Management Studies, 160 Mihai Viteazul Street, Brasov, Romania
caesarv@crmra.ro, livia@crmra.ro, aura@crmra.ro

Abstract: During the latest period of time, e-learning becomes one of the most interesting trends in computer science. It is based on information and communication technologies and provides integrated learning services anytime and anyplace. The main focus of this paper is on e-learning domain and the need to ensure that proper information security measures are in place, to protect the information within the e-learning environment. Also presents possible information security risks regarding e-learning and ways to tackle e-learning security challenges by adopting proper measures in this respect.

Keywords: e-learning, information security, countermeasures, information security risks.

I. INTRODUCTION

During the latest period of time, e-learning becomes one of the most interesting trends in computer science based education. It is based on information and communication technologies and provides integrated learning services anytime and anyplace. There is a large variety of e-learning systems in the world, but there isn’t a universally accepted definition for an e-learning system. In this respect, before starting the main discussion of this paper, let us define some terms that will be used from now on: e-learning and information security.

One possible definition states that e-learning is a “technology-based learning in which learning material is delivered electronically to remote learners via a computer network” [1]. A second definition could be that one given by Wikipedia: “E-learning comprises all forms of electronically supported learning and teaching. The Information and communication systems, whether networked or not, serve as specific media to implement the learning process” [2]. Finally a third source defines e-learning in a shorter and general way as “methods of learning that involve the use of computers and the Internet” [3].

In conclusion, e-learning can be defined as a learning process that involves a wide set of applications, uses available electronic media and tools to deliver education and training no matter the geographical location of teachers and students. Lately, e-learning was adopted by most of public and private universities, institutes and companies to improve the quality of learning and to deliver education anytime and anyplace. Furthermore, e-learning users could use not only “traditional” desktop computers, but also portable devices such as PDAs, notebooks or even mobile phones to access the online content.

In the same time, because all those portable devices could access the e-learning systems almost anytime and anywhere, one of the biggest challenges is to how to effectively solve or prevent the security and privacy concerns generated by this kind of access and not only. One aspect that has not received much attention is the role that information security plays within the e-learning environment. The primary reason why information security is so important is that e-learning is mainly dependent on information as well as information and communication technologies.

In the military, information security is defined as “The protection of information and information systems against unauthorized access or modification of information, whether in storage,
processing, or transit, and against denial of service to authorized users” [4]. Another definition states that information security means “protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide: (a) integrity, (b) confidentiality and (c) availability” [5].

II. SECURITY AND PRIVACY CHALLENGES IN E-LEARNING

E-learning is an interdisciplinary field, including educational science and, informatics (including information security). In order to achieve a proper notion of the impact of information security and privacy in e-learning, both disciplines must be considered and analyzed. Due to the vast amount of specialized topics covered by these disciplines, research must be limited accordingly to achieve a manageable subset.

Generally speaking, the degree of e-learning security and privacy is decided by two factors: policy and technology. While policy can impact on the selection and implementation of security technologies, technology itself assists security and privacy policy by providing best practices and lessons learned.

The relevance of information security in e-learning systems is given by several reasons, such as e-assessments, confidential information, stability of electronic communication and so on [6]. In case of e-exams it is very important to provide a secure e-examination system in order to avoid cheating. One important aspect of e-learning systems is their security and stability. For example, it is very important to know exactly who is logged into the system and who is authorized of doing something, because some people could try to hack the system to modify their grades.

If information security is neglected in this context, we could easily regress to situations like in traditional learning, when a physical contact must be established between the student and lecturer. Currently not much research has been conducted to secure the e-learning environment.

The security and privacy in e-learning environments could be defined as follows: “The goal of security in e-learning is to protect authors’ e-learning content from copyright infringements, to protect teachers from students who may undermine their evaluation system by cheating, and to protect students from being too closely monitored by their teachers when using the software” [7]. In this respect, security of e-learning is not only about the security of technical systems. It is necessary to cover the entire environment, including the organizational process of teaching, system’s administration and examining, in other words it is a combination of objectives, people, procedures, and tools.

All the information security risks related to computer networks are also applicable to an e-learning system. These risks are not unique to the e-learning environment, but should be addressed as if it were. Many e-learning information systems have been designed with security flaws, because the accent was more on the functionality and less on the software’s security. Consequently, the security which can be achieved through technical means is limited and should be supported by appropriate management and procedures.

If the e-learning application of educational institutions is compromised in any way because of a lack of information security, this might have serious impact on the credibility and status of such institutions. It is therefore important that all necessary steps be taken to ensure information is properly secured within the e-learning environment.

Investigating the privacy protection in universities that extensively use e-learning systems we can identify one of the bigger information security issues: the openness academic culture that is promoted by most of those institutions. That means the academic culture often puts a lower priority on information security in relation to openness [8]. This “culture of openness” often considers security and privacy as hindering technologies, although numerous incidents underlined the need for privacy protection and its implied organizational value.
III. POSSIBLE INFORMATION SECURITY RISKS REGARDING E-LEARNING

In a typical e-learning scenario, the system allows students and professors the access it from remote locations. Usually, professors can do the following actions [9]:

1. Load course material onto course web sites for students to retrieve;
2. Store assignment marks on the course web site;
3. Store tests to be written directly on the course web site.

While learners can:

1. Retrieve course material and lectures;
2. Submit assignments to the course web site from where professors retrieve and mark such assignments;
3. Access the course web site to retrieve their marks for assignments;
4. Write different types of tests directly on their work stations with results marked by the system and stored on a course database;
5. Access course web sites to get the results of tests.

From the above mentioned scenario we can identify several potential information security risks, such as [10]:

- Course material may be altered by unauthorized people;
- Bogus course material may be loaded on course web sites, or web sites may be defaced;
- Submitted assignments can be copied from course web sites by unauthorized parties;
- Submitted assignments can be changed or deleted by unauthorized parties;
- Marks can be changed/deleted;
- Access to test papers may be gained, test contents can be changed, or the test can be deleted before the scheduled test date;
- People may masquerade as students and write tests on behalf of such students;
- Students may get unauthorized help during the writing of tests;
- The destruction of course web sites and course databases containing marks;
- Denial of service attempts against course web sites preventing authorized students from accessing the web site;
- Logon information of professors and students can be intercepted and misused.

The information security risks identified above could be grouped in three general security categories: a) unauthorized release of information, b) unauthorized modification of information and c) unauthorized denial of resource use and should be addressed by ensuring that the e-learning information security countermeasures are in place. Today those security categories are widely described using three short words “confidentiality”, “integrity”, “availability” and “access control”.

Generally, before addressing the issues is necessary to understand what it means. Let’s explain the meaning of those four terms [11] in our case of e-learning systems’ security (described as “ensuring availability, integrity, and confidentiality for all users in combination with access control”).

- **Availability** - An e-learning server is called available if it is reachable over a network almost every time it is needed with sufficient resources. Service intervals must be kept short and announced adequately in advance. Failures, if any, should only lead to short interruptions.

- **Integrity** - Modifications of transmitted or stored data must be detectable. If reasoned by technical defects, fault tolerance and error correction can be applied. If reasoned by fraudulent usage, originator and context should be disclosed.

- **Confidentiality** - For individual information security like learning progress, data must be kept secret. It is in the decision of the learners themselves to discard or submit their solutions and problems while learning to other parties like teachers.

- **Access control** - Users cannot transfer or increase the received privileges even if they collaborate without the perpetrator being identified.

The information security risks are generated by at least two factors: the learning management system (LMS) used to provide e-learning content and the behavior of the system’s users (professors and learners). While the second is somehow beyond the purpose of this paper, the security weaknesses of LM systems worth a closer look.
An excellent practical analysis of threats in two widely used learning management systems was conducted in [13]. For the analysis were chosen MOODLE and ILIAS, because it follow rather different approaches concerning security, and therefore, enable the comparison of even contradictory conceptual deliberations.

As criteria for choosing appropriate LMS as objects of comparison were used:
1. availability of source code - open-source software was preferred;
2. publicity of LMS - size of community and reputation;
3. diversity - LMS considered are not too similar.

Besides the fact of mostly being available for free, open-source learning management systems offer the advantage of allowing the source code to be analyzed. The openness of the source code is important for understanding extendibility and implementation quality. Closed-source and commercial systems can only be regarded in a very restrictive way, since their source is not available, and therefore, cannot be included in the comparison process. The second criterion of publicity and application in numerous institutions aims at ensuring practical relevance of the comparison in the following.

Analyzing the information security case study it becomes obvious that it did not only focus on the security concept at a specific point in time, but rather compared these systems (Moodle and ILIAS) concerning their development during the run-time of these projects. Besides the practical presentation of weaknesses related to theoretically introduced threats, conceptual shortcomings in these systems were presented to illustrate the necessity for a sound security concept and disadvantages related to an insufficient consideration of user input.

Also, weaknesses and security holes as discovered during this analysis (e.g., sensitive file disclosure exploiting the TEX filter and allowing the deactivation of e-mail addresses - in Moodle), were reported to and discussed with corresponding developers to support them in fixing this issues.

IV. ADDRESSING ISSUES THROUGH AN E-LEARNING INFORMATION SECURITY POLICY

E-Learning Governance can be defined as “The responsibilities and practices carried out with a view to providing strategic direction to an institution’s e-learning initiatives, ensuring that established objectives are achieved and risks managed properly, as well as that resources allocated are used responsibly” [12].

During the last decade, researches proposed the connection of information security and e-learning with different approaches. However, no matter what specific security risk analysis we choose (e.g. Using five steps [7]: identification of assets; estimation or calculation of threats and risks; setting priorities; implementation of controls and counter measures; monitoring of risks and of the effectiveness of counter measures) this sounds very easy for computer practitioners, but for the leadership of educational institutions this is too abstract. Therefore, an e-learning information security policy should be very generic, non-technical, and must be signed by the leadership of the institution.

Ideally, before starting implementing e-learning systems, any institution should have an e-learning policy and in order to manage information security (IS) - an e-learning information security policy in place. Its primary purpose is to protect the institution’s information assets from all possible threats.

Just like any other policy, an e-learning IS policy should be a document that addresses the rules and regulations regarding e-learning within the institution and should directly relate to the institution’s e-learning policy. The e-learning IS policy should be used as a guideline as to what must be managed, how this should be done and should address how security decisions can be made with regard to hardware, software, networks and ultimately information.

It is essential that all institutions ensure that their e-learning IS policy is not only well designed but also properly implemented. If an e-learning IS policy is not implemented within the institution, it is just as bad as not having one at all. Such a policy has no value if it is just a piece of paper in a cabinet and is not used to secure information.
The implementation of the e-learning IS policy should be assured by the IT technicians and e-learning instructors. It is the responsibility of institutions’ leadership and consists of several e-learning IS measures that should enforce the following six IS services:

1. **Confidentiality** - is put in place to protect data from unauthorized access and to ensure that data stored in databases and transmitted over a network, cannot be read by unauthorized parties.
   An example of IS measure for confidentiality is encryption.

2. **Integrity** - ensure that data stored in databases and transmitted over a network cannot be changed by unauthorized third parties, that information is still in its original form and that no tampering or alteration has taken place. An example of an IS measure that helps ensuring integrity is message authentication codes.

3. **Availability** - ensures that all electronic resources and services are available to authorized users when they want to use such services; it means that data is available to authorized parties at any time. An example of an IS measure for availability is regular backups.

4. **Identification and authentication** - ensure that a learner is properly identified and verified during the log-on process (only authorized users can gain access to the e-learning system). The first part of this service is called identification and is usually done by entering the user credentials into the system. The purpose is to determine whether or not a person who is trying to gain access to a system is cleared for access. The second part of the service is called authentication - the system must ensure that the user is truly who he claims to be. It can be done by passwords, access cards or fingerprints. The IS measures for identification and authentication include unique credentials for each user.

5. **Authorization** - ensures that the user has access only to that data which is relevant to him, and not to other data; involves determining whether or not the authenticated user has the right to access the requested information. An example of the IS measures for authorization is logical access control.

6. **Non-Repudiation** - ensure that a user can be held individually responsible for any action performed on the system; ensures that no action taken that affects IS can be denied by the author. It is very hard to enforce, because learners are very inventive in exploiting some security issues and cannot be prevented from sharing their accounts. An example of an IS measure for non-repudiation is digital signatures.

It is obvious that not all security services can be singularly used without applying other ones. A combination of these six secured IS services will have a significant effect on implementing and maintaining a good and secure e-learning environment.

**V. CONCLUSIONS**

Many educational institutions are adopting e-learning systems and techniques without carefully planning and understanding the related security concerns. E-learning (as a relatively new method of learning) greatly depends on the connection to the Internet and as a result the e-learning environment is now exposed to threats specific to the World Wide Web.

The implied need for security and connected requirements by the use of e-learning systems has only been marginally examined up to now.

The trend of moving from traditional education to blended/on-line one make the requirement for a security management framework specific tailored to the e-learning environment to be in the pipeline more than ever. It will act as a guide in helping the e-learning institutions in managing the information security within the e-learning environment.
References
