Knowledge horizons – Volume 5, no. 2/2013

INFORMATION SECURITY MANAGEMENT IN E-LEARNING

Professor Aurel ȘERB PhD.
"Dimitrie Cantemir" Christian University, Bucharest
Faculty of Finance, Banking and Accountancy
E-mail: aurelserb@yahoo.com
Lecturer Costinela - Luminița DEFTA, PhD. candidate
"Dimitrie Cantemir" Christian University, Bucharest
Faculty of Touristic and Commercial Management
E-mail: lumi.defta@yahoo.com
Junior Lecturer Nicoleta Magdalena IACOB, PhD.
"Dimitrie Cantemir" Christian University, Bucharest
Faculty of Finance, Banking and Accountancy
E-mail: nicoleta.iacob_2007@yahoo.com
Lecturer Marius Cristian APETREI, PhD. candidate
"Dimitrie Cantemir" Christian University, Bucharest
Faculty of Foreign Languages and Literature
E-mail: marius.apetrei@gmail.com

Abstract:
The security risks introduced by the e-learning represent an important issue which was not seriously taken into account in the actual educational context, where increasingly more people are taking online courses. Also, universities and other organizations are resorting to e-learning to provide instruction on-line. The e-learning platforms are today production systems that need to be secured. In this paper we will discuss the security elements required to be implemented within e-learning environments. Also we paper presents the most popular e-learning standards to determine their provisions and limitations for privacy and security.

Keywords: *e-learning, security, confidentiality, administration.*

JEL Classification: *C88*

Introduction

E-learning is a learning environment supported by continuously evolving, collaborative processes focused on increasing individual and organizational performance. E-learning refers to the use of internet or wireless technologies to deliver a broad array of training solutions. E-learners access the learning from computers via the internet or an intranet, or through a hand held device.

Because the marketing of e-learning is continuing to grow, fuelled by new institutions entering into the online arena combined with a continuous student demand for online learning, the need to understand it and also to understand the security issues associated with it will also increase.

As a consequence of e-learning having to depend on the Internet, which is continuously exposed to security threats, the e-learning environment has also become affected by these threats. Considering these aspects, in this paper we will try to explore the wider context of information security issues and threats, and the potential of information security management in reducing them.

In the first part of this paper we will present the security elements that are required to be implemented in e-learning environments. We will discuss the potential of information security management to be implemented in the context of e-learning, in order to prepare a secured e-learning environment. Many institutions are rushing into adopting e-learning platforms without carefully planning and understanding the ever-present security concerns. Issues such as legitimate users, course content reliability and accessibility (including the admissibility and availability), as well as other considerations, all need to be carefully addressed in order to ensure the learning process can effectively take place.

The second part is dedicated to the e-learning standards in order to determine their provisions and limitations for privacy and security.

Security requirements

Online e-learning environment is different from tradition learning environment. The main change is submission of assignments by students to teachers. In the traditional learning environment, students submit their assignments in hard copy format to their teachers directly in class rooms. Whereas in online e-learning environment, students need to upload their soft copy of assignment. So, this kind of methods in e-learning technology brings the threats and vulnerabilities from internet to e-learning systems. To overcome these problems, basic security requirements such as the integrity, confidentiality and availability are to be observed.

Availability in e-learning is the assurance that the e-learning environment is accessible by authorized users, whenever needed. Two facets of availability are typically discussed, which are denial of service and loss of data processing capabilities. The e-learning users are dependent on the information on the Internet; therefore, the availability of materials and information to be accessed at any time and any location is crucial. If, for example, an e-learning platform is slow, users do not only require more time to do their work, but they also become frustrated, increasing the negative effect on productivity. Failing to fulfill this will have a major impact on e-learning users and e-learning providers. There are no effective mechanisms for the prevention of denial of service, which is the opposite of availability. However, through permanent monitoring of applications and network connections one can automatically detect when a denial-of-service attack occurs.

Integrity in e-learning is the protection of data from intentional or accidental unauthorized changes. Integrity depends on access controls; therefore, it is necessary to positively and uniquely identify all persons who attempt access. Integrity can be compromised by hackers, masqueraders, unauthorized user activity, unprotected downloaded files, LANs, and unauthorized programs (e.g., Trojan horses and viruses), simply because each of these threats can lead to unauthorized changes to data or programs. Ensuring the availability and integrity of information is the main goal in relation to e-learning security. Secrecy of data is closely connected to the integrity of programs and operating systems.

Confidentiality is the protection of information in the system so that unauthorized persons cannot gain access. Because an e-learning application can have a large number of users that can be either visitors, students, tutors or administrators who can access different information regarding one another, it is necessary to have a higher level of confidentiality. It is necessary to have a login system and a strong delimitation between each registered user and user groups. In this way, the user will have access only to the information which regards him directly. The traffic encryption between the e-learning platform and the user's computer may help to improve confidentiality.

The following are some of the most commonly encountered threats to information confidentiality:

hackers, masqueraders, unauthorized user activity, unprotected downloaded files, local area networks (LANs), and Trojan horses.

Security management

Many information systems have not been designed to be secure. The security which can be achieved through technical means is limited and should be supported by appropriate management and procedures. The security management includes policies, process, procedures, organizational structures, and software and hardware functions. There are four main elements of information security within e-learning environments, including ensuring e-learning information security governance, creating e-learning information security policy and procedures, implementing e-learning information security countermeasures, and monitoring the e-learning information security countermeasures. The elements suggested here include the management aspect to ensure that the security implementation achieve its objective.

The security management in e-learning can be stated as similar to other e-services; however, there are some different emphases based on the services being offered. E-learning offers flexibility to the user as a learner, whilst simultaneously ensuring availability, integrity and confidentiality of information. The behaviors of users in users in e-learning are also different from the users in other e-services; therefore, security management is specifically needed for e-learning.

Security management is an important part of the whole secure system process. A system whereby security cannot be managed is not secure, no matter how excellent the controls suggested. Furthermore, the users (lecturer and students) will also benefit with the secured e-learning environment.

Implementing information security measures are becoming more difficult due to the huge number of possible information security threats connected to the use of the Internet. Below we will describe these security threats.

When it is implemented, an e-learning platform should be tested for external intrusion issues using methods like:

- XSS (or Cross Side Scripting)
- SQL injection in the site address (URL SQL injection)
- performing different searches using search engines to retrieve personalized web-site information like password, username
- password cracking using decryption systems
- session hijacking
- guessing the web site session id (session prediction).

Cross Site Scripting (or XSS) is one of the most common application-layer web attacks. XSS commonly targets scripts embedded in a page which are executed on the client-side (in the user's web browser) rather than on the server-side. XSS in itself is a threat which is brought about by the internet security weaknesses of client-side scripting languages, with HTML and JavaScript as the prime culprits for this exploit.

SQL injection is a relatively simple type of attack, and can be avoided with strict adherence to some basic coding practices. Using this method, a hacker can pass string input to an application with the hope of gaining unauthorized access to a database. Hackers enter SQL queries or characters into the web application to execute an unexpected action that can then act in a malicious way. Such queries can result in access to unauthorized data, bypassing of authentication or the shutdown of a database even if the database resides on the web server or on a separate server.

Session hijacking is the exploitation of a valid computer session, sometimes also called a session key to gain unauthorized access to information or services in a computer system. This basically means stealing the magic logon hash from the session cookie. This is achieved by handing a unique and difficult-to-guess identity value (session id) to the browser (either in a cookie or the URL) which the browser submits with every new request.

Session prediction means guessing a valid session id using various tools and methods (like brute force technique). The attack is possible when session id is weakly encrypted, too short or assigned sequentially. Sessions that do not expire on the HTTP server can allow an attacker unlimited time to guess or brute-force a valid authenticated session id and eventually gain access to that user's web accounts.

To mitigate all these security threats, the e-learning security management should include the following mechanisms:

- passwords, tokens and biometrics – for identification and authentication

- access control list, directory list and access control matrix – for authorization
- encryption, effective identification and authentication service - for confidentiality
- message authentication code, encryption, effective authorization service, effective identification and authentication service – for integrity
- effective backup system, effective business continuity management process – for availability.

Security standards

To develop an online e-learning solution there are number of factors and standards of distance learning in education to be considered, which will influence its survival and the growth in the future market. For different online learning vendors the main factors which are vital to sell the products in the markets are standardization and compatibility. There is also a factor to check whether different e-learning systems are compatible with one another or not. There are several working groups which are seeking to develop the standards for the e-learning sources. Those groups suggest the principles and standards concerned mostly on the sharable components and other resources. Principles involved in them also suggest the privacy and the security issues involved in the e-learning solutions.

Some of the groups which work in the proposal and in development of these standards are: IEEE LTSC (IEEE Learning Technology Standards Committee), IMS GLC (IMS Global Learning Consortium), AICC (Aviation Industry Computer-Based Training Committee), ARIADNE (Alliance of Remote Instructional Authoring and Distribution Networks for Europe) and ADL-SCORM (Advanced Distributed Learning-Sharable Content Object Reference Model).

In the following paragraphs we will present the standards that have privacy and security implications in e-learning.

IEEE P1484

IEEE P1484 is the model which was proposed by IEEE LTSC. It involves the specification of Public and Private Information (PAPI) which effectively describes all the variances that deal with the privacy and the security features using the learner's information. They may create, store, retrieve the users information by using specific entities. It categorizes the views related to security from the different stakeholders involved in the system like developer, regulator etc. It also chooses the different entities involved in the customer management like their contact information, preferences, performance, personal information and portfolios.

As explained above it does not explain about a specific structure or a model or a technology but it explains all the security issues implemented in order to provide privacy factor. Also it does not provide any privacy or a security policy. It only explains that the administrators and the learners will act as the policy makers by applying the policy factor of privacy using certain security techniques and technologies. It uses a factor of logical division of learner information. Once if the learner information gets accredited in server it will become de-identified, partitioned and compartmentalized which will cover most of the privacy and security factors related to the user.

IMS LIP

The IMS global learning consortium (IMS GLC) is an organization intended to develop open specifications for distributed learning. This is involved in addressing the key challenges and problems in distributed learning environments with a series of reference specifications which include Meta-data specifications, Enterprise specification, content & packaging specification, question and test specification, Simple sequencing specification, and learner's Information Package specification. Among all the specifications mentioned above IMS Learners Information package deals with the interoperability of the Learner's Information systems with other systems which are supported by the internet learning environment.

It employs different ways to capture Learners' information which includes his education record, training log, professional development record, and life-long learning period, community service record (e.g. work and training experience). With the help of the learner's information the system can be made to respond to specific needs of the user or learner. By employing the learners' Information server the Learning system can be efficiently utilized by the user. For maintaining privacy and security for the learners, information for providing better support to the learner, enable certain mechanisms in the IMS LIP specification. A learner information server is responsible for sending and receiving learner's data to other information systems or other servers. The server is

administered or monitored by a special authorized person.

Data Privacy and integrity are considered to be the most vital requirements for the IMS LIP specification. Nevertheless the IMS LIP specification does not avail the facility of having a look at the details of Implementation mechanisms or architectures that are employed for providing security and integrity to the Learners Information.

The core structures of the IMS LIP are based upon: accessibilities, activities, affiliations, competencies, goals, identifications, interests, qualifications, certifications and licenses, relationship, security keys and transcripts.

Conclusions

The main aim of security management is to control and ensure enough information security. The ultimate aim of information security is to save information/data from the security attacks. Usually these goals were presented in this paper in terms of assuring the confidentiality, integrity and availability. We also described some information security threats that need to be taken for an e-learning platform.

In the last part of this paper we briefly present the main security standards used in e-learning environments. Even if the security can increase the complexity of an e-learning platform, it should be taken seriously into account - after all the people only use a system if they trust it. The development of the e-learning systems should be done using safety methods and internationally recognized standards. The system needs to implement security services such as authentication, encryption, access control, managing users and their permissions.

BIBLIOGRAPHY

[1] Iacob N. *Distributed Queries in the E-learning Environment*, World Conference on Educational Technology Researches, Volume 28, pp. 241–245, 2011.

[2] Edgar R. *Security in e-learning*. Springer. Vienna University of Technology, Austria, 2005.

[3] Defta L. *Information security in E-learning Platforms*, Proceedings of the 3rd World Conference on Educational Sciences, Istanbul, Turkey, 2011.

[4] Defta L. *Security Issues in E-learning Platforms*, World Journal on Educational Technology, Vol 3, issue 3, 153-167, 2011.

[5] Assefa S. *An Information Security Reference Framework for E-learning Management Systems*, University of Johannesburg, 2009.

[6] Kumar G, Chelikani A. *Analysis of Security Issues in Cloud Based E-learning*, University of Boras, 2011.

[7] Hayaati N, Ip-Shing F. *E-learning and Information Security Management*, International Journal of Digital Society, 2010.

[8] Clements I. *Virtual Learning Environment Comparison*, Progress through Training, 2003.