Vladimir I. Zuev

E-Learning Security Models

Article Info:

Management Information Systems,
Vol. 7 (2012), No. 2,
pp. 024-028

Received 12 September 2011
Accepted 24 April 2012

UDC 37.018.43:004.738.5 ; 371.322:004

Summary

The article looks into methods and models that are useful when analyzing the risks and vulnerabilities of complex e-learning systems in an emergency management context. Definitions of vulnerability and emergency response capabilities, such as "VLE/PLE attack surface", are suggested.
The article provides insight into some of the issues related to analysis of risks and vulnerabilities of e-learning systems, but more research is needed to address this difficult and comprehensive task.

Keywords

implementation of innovation in education, information technologies, single informational and educational environment

1. Introduction

Modern education is often characterized by transfer of e-learning technologies into practice of traditional brick-and-mortar universities (Kultan, 2011). Thus, the complexity of Education 3.0 technologies inevitably leads to the increase of university vulnerabilitiy. The process is greatly influenced by transfer of system features of e-learning into traditional learning environment. Moreover, there occurs a certain kind of interference between traditional educational risks (psychological, pedagogical, etc.) and a special kind of IT-risks. So in order to create an adequate protection scheme special metrics and e-learning security models are needed.

2. E-Learning 2.0

In the e-Learning field, Web 2.0 has revolutionized the way instructors and end-users interact with learning content and each other. e-Learning 2.0, similar to Web 2.0, is the facilitation of learning through collaboration and sharing ideas and content with other learners.

Let us define specific features of e-Learning 2.0:

- user-generated content,
- social/collaborative/network learning environments,
- aggregating (RSS) and tagging,
- knowledge sharing,
- personal learning environments,
- collective intelligence (wisdom of crowds),
- using a network of diverse technologies,
- creativity and innovation.

The chain of e-learning knowledge flow includes computers, as physical information depositories and both Intranet and Internet as communication and storage medium. In addition, one must take into account VLE and PLE specific architecture. Actors are faculty, multimedia designers, IT-experts, etc. (See Figure 1).

The modern educator participates in online educational communities along three dimensions: interactivity, connectivity, and sharing (See Figure 2).

The first dimension of collaborative behavior measures the degree of the educator's interactivity. The more interactive online users, the better for educational process in which they participate. Highly interactive teachers are responsive, usually replying to e-mails the same day they were received. They also make themselves available via online chat.

The second dimension measures a person's degree of connectivity. Within an online community, team members should be highly connected so that everyone responds to messages from everyone else within the group. A wide and active social network that results from being highly connected is crucial for getting the educational task done, whatever the task is. The more connected people are, the better for the educational community of which they are members.

The third dimension of collaborative behavior measures the degree of group connectivity and knowledge sharing. The more team members are willing to share what they know, the higher the quality of their shared deliverables.

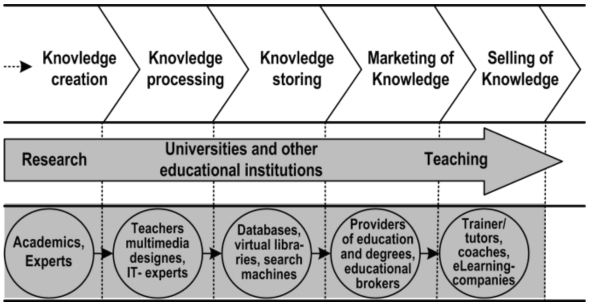
Knovledge creation
Knovledge processing
Knovledge storing
Marketing of Knowledge
Selling of Knowledge
Research
Universities and other educational institutions
Teaching
Academics, Experts
Teachers multimedia designes, IT- experts
Databases, virtual libra- ries, search machines
Providers of education and degrees, educational brokers
Trainer/ tutors, coaches, eLearning- companies

Figure 1 Value chain of knowledge management
Source: Hilse, 2000.

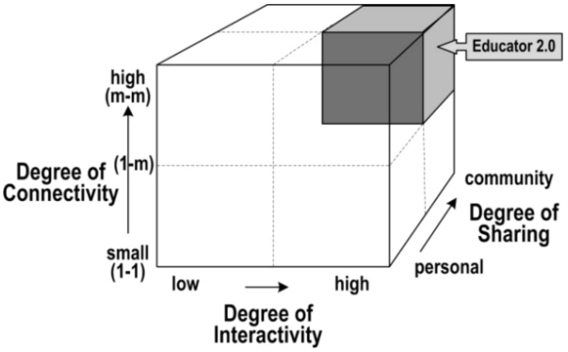

Figure 2 Degree of Educator's 2.0 online involvements.
Source: Author

3. Vulnerabilities of VLE and E-learning Security Policy

Virtual learning environment (VLE) may be described as a collection of integrated tools enabling the management of online learning, providing a delivery mechanism, student tracking, assessment and access to resources.

VLE of a modern university must therefore provide:

- access to adequate educational multimedia resources,
- updating and verification of the latter,
- reusability of learning objects,
- flexibility of student's learning path,
- accurate student's assessment,
- reliable feedback,
- protection of data, etc.

All of the above mentioned elements of the educational technological chain are potential targets of hacking attacks, followed by unauthorized modification, and even destruction of educational assets. In addition, e-university has to solve issues related to student authentication, unfair task performance, plagiarism, as well as the protection of the copyrighted material, placed on the web. So both the integrity of e-resources and smooth functioning of the educational computer systems must be protected.

E-learning security policy must be based on the following assumptions:

- Protection should be, primarily, focused on the reflection of the most probable and destructive attacks;
- The protection system should provide continuous control of VLE, revealing the slightest unauthorized modifications;
- An adequate and rapid response to threats should be as automated as possible;
- Elements of business intelligence should be used for the monitoring of security breaches in the entire set of e-Universities in order to identify potential malicious trends;
- Special metrics should be assigned to measure quantitative characteristics of risks.

The traditional approach to e-learning security includes the following components (Weippl, 2005):

- Information security of e-learning;
- Psychological security of e-learning;
- Didactic security of e-learning;
- Physical security of e-learning.

Meanwhile, there is a possibility of integral handling of the problem involving the selection of the most common specific elements of e-learning security.

Generally, all e-learning security requirements can be reduced to basic four, slightly different from the AIC information security triad. They are:

- to ensure privacy (the user can access only those objects where he is allowed),
- to ensure the integrity of assets (only authorized users can modify data and programs),
- to ensure availability (efficiency of applications and programs is reduced as a result of attacks),
- to provide regular work of application according to the algorithm laid down.

We can list the following vulnerabilities of e-learning system as:

- vulnerability of the hardware infrastructure,
- vulnerability of software,
- vulnerability of human resources,
- vulnerability of databases,
- vulnerability to natural occurrence.

In this case, the security of e-learning system should be provided at several levels:

- the network infrastructure level,
- the operating system and basic services level,
- the applications tevel,
- the database level.

The typical e-learning threats are listed below:

- unauthorized access to digital content (unauthorized copying and modification of data), including physical access to servers,
- loss of integrity, and inadequacy of educational resources (often electronic manuals, with Internet resources, are the main sources of educational information for students),
- violation of assessment procedures (the problem of students identification, cheating, plagiarism and the proper functioning of the knowledge evaluation system),
- violation of the normal functioning of the e-University's departments and services,
- violation of the law (in particular, the laws governing copyrights and other rights).

4. Specific Aspects of E-Learning Security Model

Considering the security of e-learning, one should take into account all the risks and vulnerabilities of such a structure.

In this case, the characteristic feature of this system is the dualism "subject/ object of attack." The same actor (or element) of the educational scene can act as a source or as an object of attack.

In the work (Zuev, 2010) an attempt was made to view this dualism through the prism of "the e-learning cube" model (See Figures 3&4 below). One of the axes of the model shows levels of interaction (student's or teacher's PLE, university's VLE or global network), the others – types of digital resources (software, information objects, learning objects) and – categories of actors (students, faculty, staff).

Figure 1 shows the attack on the faculty at the level of a VLE. The source of threat originates from the software (it can be alteration, modification, destruction, etc.). Figure 2 – situation is reversed: the attack on the software at the level of the VLE is initiated by faculty.

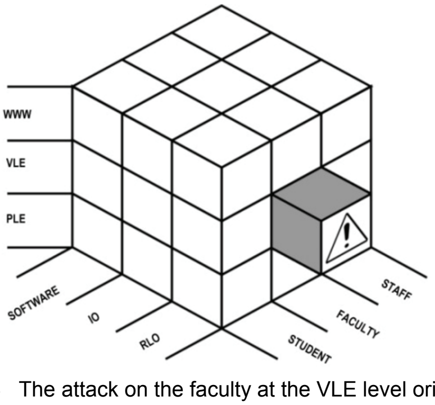

Figure 3 The attack on the faculty at the VLE level origins in software.
Source: Author

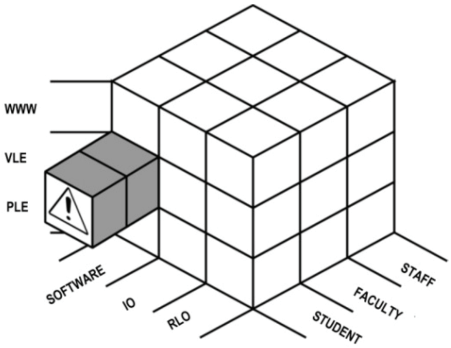

Figure 4 The attack on the software at the VLE level initiated by the faculty.
Source: Author

Let us consider didactic risks of e-learning system. First of all, there are the risks associated with the faculty.

In the first place – those are the risks associated with faculty expertise. There are the following risk levels:

- Didactic risk (occurs when the teacher does not give due attention to updating the training course).
- Technology risk (arises from the inability of teachers to make full use of ICT).
- Scientific risk is associated with the quality of educational material offered by the teacher.
- Risk of delegation occurs when a teacher completely shifts to an electronic learning management system (LMS).

Secondly, these are the risks associated with the organization of educational process. They arise as a result of improper planning and insufficient control of the educational process, consulting and assessment activities. The source of these risks may draw its origins in inadequate student's information system, lack of cooperation between teachers, or lecturing related subjects disciplines.

And finally, the last group of the risks associated with faculty – direct risks of the educational process, appearing as a result of provocative inappropriate student behavior, the low level of professional responsibility of the teacher, and breaches of discipline.

Perhaps even greater amount of risks is associated with the students.

- First, it is the risk associated with the inability to sustain a given rate of learning.
- Second, it is the risk associated with the need of constant student's motivation.
- Third, it is the risk associated with inadequate self-esteem and behavior of the student.

- Fourth, it is the risk associated with the inability to make contact with the teacher.
- And last, it is technology risk, which is associated with high level of student's ICT competence.

There is also certain kind of risks associated with the staff, which can also act either as an object, or as the subject of attacks on e-learning system.

Therefore e-learning security system metrics formalization and creation of adequate model of such a system is quite a difficult task.

5. E-University Security Metrics

Meanwhile, metrics can be an effective tool for university security managers to discern the effectiveness of various components of their security programs, the security of a specific learning management system, product or process, and the ability of faculty and staff to address security issues for which they are responsible. Metrics can also help identify the level of risk in not taking a given action, and in that way provide guidance in prioritizing corrective actions. Additionally, they may be used to raise the level of security awareness within the university.

A complete analysis of the e-learning security systems includes:

- a topological analysis of the structure of e-learning system,
- accounting of software cyclomatic complexity,
- taking into account psychological and educational components of the educational process, etc.

Meanwhile, sometimes it is possible to offer a more simple way of solving this problem.

It is evident that any time the attack occurs, an attacker comes in contact with the e-learning system, using the channels of information, using and imitating the system ways and methods, sending or receiving information from the system. Similar acts are performed by an attacker during the attack on pure "informational" sites. So we use the methodology developed for this case.

Following Howard, Pincus and Wing (2003), let us introduce "VLE attack surface."

Let us call a "VLE attack surface" – a lot of (the locus) of the possible vulnerabilities of the e-learning security system. Those are – data transmission channels, elements of the LMS, database, software, e-learning techniques and procedures, points of system's input and output, etc. The more components are included in VLE, the greater is the number of potential vulnerabilities and, therefore, the attack surface.

Meanwhile, not all elements of VLE are parts of the "VLE attack surface", and those that really are the sources of vulnerabilities, are unequal in their breach potential. It is therefore necessary to define criteria by which we assess the vulnerabilities (contribution of each of the possible breach elements).

The element of VLE becomes a part of the "VLE attack surface" if the attacker can use it to disrupt normal system performance. To assess this element's ability it is logical to introduce a criterion based on the ratio:

[The System Recovery Cost / Damage from the Actions of the Attacker].

Another option may be the assessment ratio of system failure time and system repair time.

Thus, the "VLE attack surface" is an integral characteristic of the vulnerability of the system as a whole. It gives an idea about the damage that an attacker can cause the system and at the same time gives notions of the way he must act in order to damage an e-University.

Manadhata and Wing (2004) introduced the concept of "attack vector". Actually "attack vector" characterizes an option of malicious disruption of the system's normal performance.

Thus the set of "attack vectors" is defined by the set of threats and risks of e-learning system as mentioned above.

The larger attack surface is, the more insecure is the e-learning system. Manadhata and Wing (2011) formalized the notion of a system's attack surface using an I/O automata model of the system and introduced an attack surface metric to measure the attack surface in a systematic manner.

One way to minimize the risk is by reducing the attack surfaces of their VLE. A smaller attack surface makes the exploitation of the vulnerabilities harder and lowers the damage of exploitation and hence mitigates the security risk.

6. Conclusion

An adequate evaluation of all vulnerabilities and risks of e-learning system will ensure a creation of a model according to which a strategy of protection can be developed. Thus threat modeling is an integral part of e-learning system planning. Paying attention to the problem at the initial stage of developing a secure e-learning system, we will be able to adequately analyze the system's architecture in order to detect and resolve security problems.

References

Hilse, H. (2000). *Unternehmen, Universitäten und "Corporate Universities": Wissen und Lernen im Wandel der Institutionen.* Retrieved February 22, 2011 from Universität Witten-Herdecke: http://www.uni-wh.de/de/wiwi/index.htm

Howard, M., Pincus, J., & Wing, J. M. (2003). *Measuring relative attack surfaces in Proceedings of WADIS 2003: Workshop on Advanced Developments in Software and Systems Security.* Retrieved March 19, 2011 from School of Compute Science, Carnegie Mellon: http://www.cs.cmu.edu/~wing/publications/Howard-Wing03.pdf

Kultan, J. (2011). Issledovanije ispoľzovanija LMS Moodle v processe obučenija. *Elektronnaja Kazaň 2011 : materialy tret`ej meždunarodnoj naučno-praktičeskoj konferencii* (pp. 295-300). Kazaň: Izdateľstvo Juniversum.

Manadhata, P. K., & Wing, J. M. (2011). An Attack Surface Metric. *IEEE Transactions on Software Engineering, 37* (3), 371-386.

Manadhata, P. K., & Wing, J. M. (2004). *Measuring a System's Attack Surface.* Retrieved March 20, 2011 from SCS Technical Report Collection: http://reports-archive.adm.cs.cmu.edu/anon/2004/CMU-CS-04-102.pdf

Weippl, E. R. (2005). Security in E-Learning. *Advances in Information Security*, *16*, 13-75.

Zuev, V. I. (2010). Bezopasnost electronnogo obuchenia. *Proceedings of Sovershenstvovanie podgotovki IT specialistov.* Moscow: Moscow state university of economics, statistics and informatics - MESI.

Vladimir I. Zuev
Kazan Federal University Kazan
Institute for social sciences and humanities (ISSH)
Dostoevsky Str., 10
Kazan
Russia
Email: vzuev@ksu.ru