JOURNAL OF APPLIED
COMPUTER SCIENCE
Vol. 19 No. 2 (2011), pp. 7-18

Security of Information in University Elearning Systems

Rafał Grzybowski

Technical University of Łódź
Institute of Information Technology
Wólczańska 215, 90-924 Lodz, Poland
rafalg@p.lodz.pl

Abstract. *The increase in popularity of university eLearning platforms, supporting traditional methods of education, as well as new communication tools development, make the security issues of information stored in these systems becoming increasingly important. The general discussion on security issues in e-learning was inaugurated by M. K. Littman [1] already in 1996. This document has been prepared to identify data security threats existing in a very specific group of computer systems - university eLearning platforms. As a result of the security incidents database analysis and user behavior described in the literature, thirteen security areas have been defined. Activities undertaken in particular areas, described during the data analysis, have a significant impact on at least one of three basic elements of information security.*
Keywords: *eLearning, security, university elearning software.*

1. Introduction

The global market for e-learning is growing very intensively, and thus the number of e learning systems in use is increasingly high. However, despite this significant increase, little attention is paid to security issues of e-learning, in both research and practice.

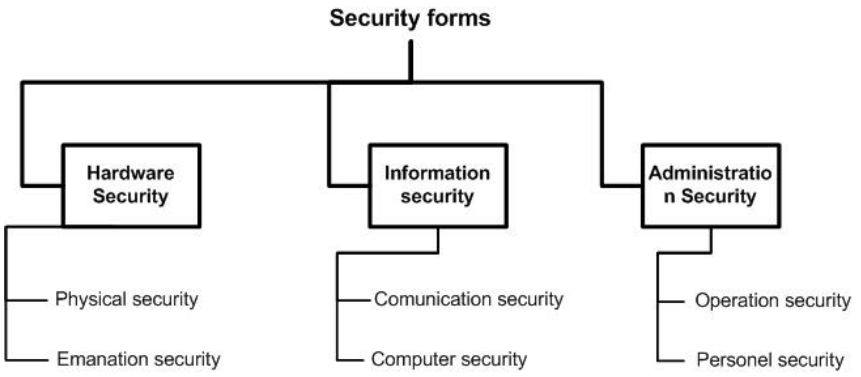

Figure 1. Forms of security [2]

The definitions of computer system security and basic categorization has been introduced by Tomas Olovsson [2], as a three-layer model, presented on Figure 1. In the model presented by Olovsson [2], the computer system security has been divided into three categories, among them:

Hardware security, consisting of:

- Physical security, as a set of activities protecting computer equipment against the external threats such as sabotage, theft, earthquake or flood,
- Emanation security, as a set of activities protecting against an unauthorized signal emission from the computer hardware.

Information security, consisting of:

- Computer security, as a set of activities protecting against vulnerabilities in computer systems architecture,
- Communication security, as a set of activities protecting the security of information in transit.

Administration-related security, consisting of:

- Personnel security, as set of activities protecting components of a computer system against attacks by authorized users,

- Operation security, as set of activities protecting components of a computer system against security vulnerabilities in work organization (procedure errors).

From a security point of view, eLearning systems have several unique characteristics. Edgar R. Weippl wrote about this in [3]. According to him: "E-learning can be considered a special form of e-business. The good involved is digital content that has to be distributed, maintained, and updated. Moreover, the value of this good has to be adequately protected from unauthorized use and modification, without preventing students from using it in a flexible way".

The discussion on security issues in e-learning was inaugurated by M. K. Littman [1] already in 1996. She mentioned that "Internet access to online information can enhance a classroom instruction. However, network connectivity generates security risks for the learning environment". So far, this discussion has taken place in three domains: policy [4, 5, 6], broadly defined access management [3, 7, 8] and the intellectual property [9, 10, 11]. The analysis of publications in each discussion threads indicates, that most of the authors tends to points out an advanced access control as a universal remedy to ensure the safety of eLearning systems.

2. Specificity of university elearning systems

Many universities offers a computer eLearning platforms. These platforms expands the traditional educational process by offering educational materials, a places for discussions and information exchange, examination systems for checking the knowledge, virtual libraries, and others. University e-learning platforms were built as open, multiserver, distributed computer systems. These systems are often integrated with the computer systems of university administration. This integration is performed in order to pass to the eLearning application, the informations about students and their permissions, as well as data transmission about a learning outcomes in the reverse direction. Access to such sensitive data as:

- Personal data unambiguously identifying the student or teacher,
- faculty, specialization, year and semester,
- e-mail address,
- partial and final assessments

means that the security has become an important challenge in order to ensure that only authorized people have an access to the right information at the appropriate time. The significance of this assumption is also stressed by Cárdenas and Sanchez in [12], as well as Wang, Zhang and Cao in [13]. Academic centers also have a specific organization of work. It is here, the computer systems are used by people focused on acquiring the knowledge and skills, scientific researches and development of new technologies. People who have flexible hours of work. People very often forgetting about how valuable are the informations stored in their computers. Students who passed the exam and received the privilege of studying in the university, very often forget about this fact, and infected by idea of the open world, commonly copying the teaching materials as well as sharing them illegally to colleagues from other universities.

The designers and administrators of university e-learning platforms should remember, that for these type of e-learning systems, there is a tendency for security principles (such as data confidentiality) to be overlooked. Unlike in case of business computer systems, educational platforms are usually subjected to internal attacks consisting in the attempt to capture the identity in order to the unauthorized access to information (e.g. to pass the exam on behalf of another student or to steal the exam questions) [14]. The threats coming from outside are mainly the attempts to illegally obtain personal information and email addresses. Such data are often used to distribute illegal advertising, ie. spam. In computer systems that support the university eLearning platforms, supporting traditional forms of learning (blended learning), practically do not occur the security risks concerning the Financial Crimes.

3. Security areas in university elearning system

Taking into account the factors presented in the previous chapter, structure of the university eLearning system safety was developed. It is represented in Figure 2. In developing this structure the database of security incidents (DSI) was analyzed. This database was created during five years of operation, of the Technical University of Lodz eLearning platform. This platform currently supports approximately 20 thousands of active student accounts and covers the scope of its operations, all units of university teaching.

The basis for developing the structure presented in Figure 2 was the analysis of the extended model presented in [2]. During the analysis, the model was

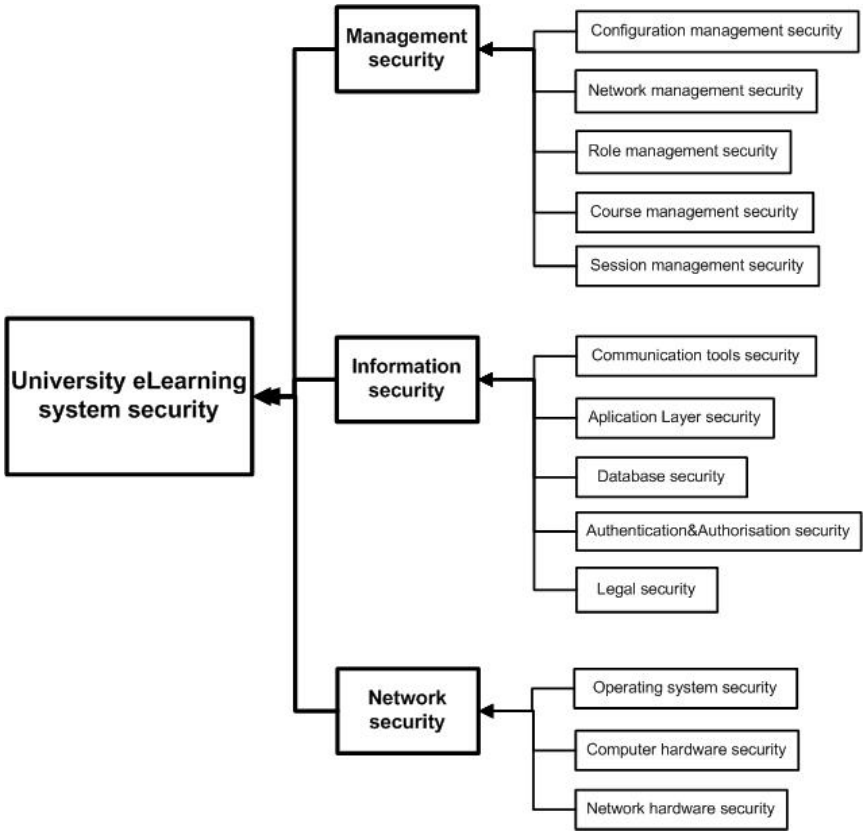

Figure 2. Security areas in university elearning system

progressively simplified in the way that it eliminated all the categories of risks, which effect on the computer system security, about specificity described in Chapter 2, was considered negligible, and this assertion was confirmed by the absence of reported security incidents in the DSI. Threats of the individual layers, such as prepared structure, was defined as follows:

3.1. Network security

Network security area has been divided into three layers. Activities that eliminate the security risks in each of them have been identified as:

Network hardware security – a set of activities designed to ensure the continuous operation of the hardware responsible for the data flow in a computer network. This area of security applies to all network devices installed in the academic campus. E-learning platform has become popular among the universities because it gave a lot of benefits to people such as guaranteed 24-hour response to student questions, education taking place anytime and everywhere. Given these requirements, the need to ensure the continuity of data transmission, is one of the most important tasks of the eLearning system administrators. The causes of data transmission discontinuity are both, hardware failures resulting from normal use and accidents, provoked by the intention to interrupt the transmission (e.g. delay of the exam). Unauthorized modifications to the structure of the network, in order to gain unauthorized access to information, due to the costs and the specificity of applications (application-layer authentication) practically do not occur in a university e-learning systems.

Computer hardware security - a set of activities designed to ensure the continuous operation of the computers that provide educational information. This area concerns the security of both data storage servers and client computers in the campus computer network. While in case of the network hardware security, the causes of malfunction are both, hardware failures resulting from normal use and accidents provoked by the intention to disruption the normal system operation (e.g. Denial-of-service attacks).

Operating system security - a set of activities designed to ensure the continuous operation of the computer operating systems that provide educational information. This area concerns the operating systems security, of all computers connected to the educational platform. The causes malfunction of operating systems can be both, incorrect installations and configurations as well as malicious software (viruses, worms, etc.), that has been installed without user's knowledge. Within this area of security, it should be also considered the elimination of system software installed on purpose to gain unauthorized access to information (keylogger, sniffer, etc.).

3.2. Information security

Information security area has been divided into five layers:

Legal security concerns the implementation and updating, the current internal normative acts within the university so as it always be compatible with the law applies in the country. This is one of the most important tasks of information security administrator. Properly implemented regulations and mechanisms, allowing in an unequivocal way to identify any attempt to breach of these regulations, can replace many a technical solution.

Authentication and Authorisation security concerns the implementation and continuously monitoring of precise mechanisms for eLearning platform users authentication and assigning them the appropriate permissions. The intention to log on as someone else, see mails or achievements are the most common incidents reported to the DSI database. Therefore this area of eLearning university system should be particularly well designed. This thesis has been also confirmed in [13].

Database security concerns the all activities to ensure the reliable operation of the system databases and to protect them from damage. Databases are the heart of the functioning of each eLearning system. The protection against the direct access to these resources is organised by activities undertaken in the next layer (Aplication Layer security). Therefore, the activity of administrators in the "Database security" area, should be focused on ensuring an optimal performance and reliability of the data storage systems.

Aplication Layer security concerns the activities undertaken during the designing, implementation, deployment and use of applications that support university eLearning platform. Properly designed and implemented software allows you to eliminate many risks, e.g. destruction of databases, or steal the user data. Particular emphasis in this security area has been stressed by Shadi Aljawarneh in [15]. In his proposed methodology, security needs to be built into all phases of the System Development Life Cycle.

Communication tools security concerns the proper selection of communication tools and the implementation of appropriate information exchange policies within the elearning platform. That is why the electronic communication tools, e.g. communicators, chat, e-mail, are the weakest point of the confidentiality of information. Electronic mail is the most popular channel of illegal distribution of educational materials . Designing and implementing a communication system,

which does not restrict access to information, yet eliminate existing risks is a very difficult task. For this reason, these tasks should be isolated as a separate security layer in the university elearning platforms information system.

3.3. Management security

Security of management area has been also divided into five layers:

Session management security concerns the proper selection of the supervising session management software for all applications with the WEB interface. Theoretically, any activities in this area should be placed in the layer "Authentication and Authorisation". However, a large number of attacks, attempting to exploit the mechanisms of session interception, demonstrate shortcomings of the Web server technology. The intention to draw the administrators and designers attention to the risks associated with mechanisms of the session management, was the main objective of isolating the security of these technologies as a separate security layer.

Course management security concerns the activities undertaken by the teachers during the management of their courses. The main threat in this area is usually poor knowledge of the functionality of the eLearning platform software. Insufficient knowledge, and often also disregard for university safety policy creates errors resulting in unauthorized sharing of copyright material. The most common steps taken to ensure security in this area are intensive training of platform users.

Role management security concerns the activities undertaken by administrators while managing platform roles. Permissions management through the mechanism of inherited roles are today the most popular standard in distance learning systems [13]. This mechanism enables to very flexible permissions allocation. But it has a disadvantage, which is the complexity of management. A small mistake in the definition of the selected role may allocate excessive permissions for too large group of users. The most common mistakes of eLearning platforms administrators are insufficient knowledge of technology and too little care in defining roles.

Network management security concerns the efforts to optimize the data flow in a computer network. In case of eLearning systems these are difficult actions, for the reason that many of the commonly used technologies, such as network congestion avoidance (e.g. reducing the number of concurrent connections between

nodes) cannot be used without affecting on the data integrity (student sitting an examination cannot suddenly be cut off from the server, just because other students started the exam with another course). Working in this area requires a lot of knowledge and should be begun at the design stage of the system.

Configuration management security concerns the activities undertaken during the system functionality configuration. University eLearning platforms are usually constructed as a distributed multiserver environment which integrates many applications. Vast number of configuration parameters requires a lot of attention and diligence. Poor environment configuration is a frequent implementation mistake and the cause of many frustrated users. The solution to this problem can be performing a very thorough analysis of the functionality at the design stage of the system, and also stiffening of the rules modifications at the implementation and operation stage. Ill configuration changes during operation stage are cause of all software malfunction incidents reported to DSI.

4. The importance of each security areas in university eLearning system

Detailed analysis of the database the DSI as well as conditions presented in Chapter 3, allowed to determine the effect of activities undertaken in different security zones on the three basic elements of the data protection: confidentiality, integrity and availability. The results of this analysis have been presented in Table 1. The impact of these activities in each layer is assigned to one of two levels: HI – significant or LO – small effect. Such approach enables quick identification of the suitability of particular administrative action. Apart from classification, Table 1 also contains the numbers, specifying the amounts of security incidents recorded in the various layers, including identification the types of incidents (intrinsic or forced). It is anticipated that due to the impossibility of automatic recording of incidents in areas legal security, application layer and communication tools, the DSI data in these areas are seriously understated.

Discussing the data presented in Table 1 it should be noted that the most important steps to ensure security of the university eLearning system are located in areas Authentication and Authorisation security, Database security and Application layer security. That is why in these areas should be given special attention when designing, implementing and managing the university elearning system. It

Table 1. The importance of security activities in each zones

Security area	effect the performance of information			database of security incidents		
	availability	integrity	confidentiality	intrinsic failure	forced failure	# of registered incidents
Network hardware	HI	LO	LO	91%	9%	46
Computer hardware	HI	LO	LO	81%	19%	127
Operating system	HI	LO	HI	41%	59%	258
Legal	LO	LO	HI	3%	97%	86**
Authentication&Authorisation	HI	LO	HI	14%	86%	361
Database	HI	HI	HI	98%	2%	9
Application layer	HI	HI	HI	60%	40%	138**
Communication tools	LO	LO	HI	0%	100%	72**
Session management	LO	LO	HI	49%	51%	176
Course management	LO	LO	HI	0%	100%	465
Role management	LO	LO	HI	3%	97%	26
Network management	HI	HI	LO	34%	66%	31
Configuration management	HI	LO	HI	3%	97%	68

HI - significant effect
LO - small effect
** - Data not representative due to lack of automatic registration method.

is also important to emphasize that the actions taken in almost all areas have a significant impact on the confidentiality of information.

5. Conclusions

The increase in popularity of eLearning systems, with large dependence on the Internet has resulted in the appearance of new threats in the security of information stored in these systems. This document has been prepared to identify data security threats existing in a very specific group of computer systems, university eLearning platforms. As a result of this analysis, 13 areas of security have been defined. Activities undertaken in particular areas, defined during the data analysis (The analyzed data came from the eLearning platform of the Technical University of Lodz.), have a significant impact on at least one of three basic elements of information security. Further work will be devoted to the analysis of tools used to ensure safety in each of the defined areas, with particular emphasis on areas where logging security incidents were defined as intricate.

References

[1] Littman, M. K., *Guidelines for Network Security in the Learning Environment.* Journal of Instruction Delivery Systems, Vol. 10, 1996, pp. 35–40.

[2] Olovsson, T., *A structured approach to computer security.* Tech. Rep. 122, Chalmers University of Technology, Department of Computer Engineering, 1992.

[3] Weippl, E. R., *SECURITY IN E-LEARNING*, Vol. 16 of *Advances in Information Security*, Springer Science+Business Media, 2005.

[4] Boella, G. and van der Torre, L., *Security Policies for Sharing Knowledge in Virtual Communities.* IEEE Transactions on Systems, Man, and Cybernetics Part A: Systems and Humans, Vol. 36, 2006, pp. 439–450.

[5] El-Khatib, K., Korba, L., and Xu, Y., *Privacy and Security in E-Learning.* International Journal of Distance Education Technologies, Vol. 1, 2003, pp. 1–19.

[6] Yang, C., Lin, F. O., and Lin, H., *Policy-Based Privacy and Security Management for Collaborative E-Education Systems.* Proceedings of the 5th IASTED International Multi- Conference Computers and Advanced Technology in Education (CATE 2002), Vol. 1, 2002, pp. 501–501.

[7] Raitman, R., Ngo, L., and Augar, N., *Security in the Online E-Learning Environment.* In: Fifth IEEE International Conference on Advanced Learning Technologies, ICALT 2005, 2005.

[8] Yong, J., *Digital Identity Design and Privacy Preservation for e-Learning.* Shen, W., Yong, J., Yang, Y., Barthes, J.-P.A., Luo, J. (eds.) CSCWD 2007. LNCS, Springer, Heidelberg, Vol. 5236, 2008, pp. 858–863.

[9] Graf, F., *Providing Security for eLearning.* Computers & Graphics, Vol. 26, 2002, pp. 355–365.

[10] Kennedy, G., *E-Learning Intellectual Property Issues in E-Learning.* Computer Law & Security Report, Vol. 18, 2002, pp. 91–98.

[11] Samuels, R., *The Future Threat to Computers and Composition: Nontenured Instructors, Intellectual Property, and Distance Education.* Computers and Composition, Vol. 21, 2004, pp. 63–71.

[12] Cardenas, R. and Sanchez, E., *Security Challenges of Distributed e-Learning Systems*, ISSADS: Springer, Series Lecture Notes in Computer Science, Vol. 3563, 2005, pp. 538–544.

[13] Wang, H., Zhang, Y., and Cao, J., *Effective Collaboration with Information Sharing in Virtual Universities*, Knowledge and Data Engineering, USA: IEEE Transactions, Vol. 6, 2005, pp. 40–853.

[14] Zamzuri, Z. F., Manaf, M., Ahmad, A., and Yunus, Y., *Computer Security Threats Towards the E-Learning System Assets*, Communications in Computer and Information Science, Vol. 180, Software Engineering and Computer Systems, Part 3, 2011, pp. 335–345.

[15] Aljawarneh, S., *A web engineering security methodology for e-learning systems*, Network Security, Vol. 2011, No. 3, March 2011.