ISSN 1864-6168
UDK 62

SIGURNOST SUSTAVA ZA E-UČENJE

SECURITY OF E-LEARNING SYSTEMS

Davor Levanić, Lana Križarić

Stručni članak

Sažetak: *Današnje doba modernih tehnologija omogućava učenje na daljinu ili e-učenje podržano odgovarajućim sustavima. Sustavi za e-učenje izloženi su prijetnjama i napadima kao i drugi informatički sustavi. Kako bi se projektirao sigurniji sustav koji je manje izložen napadima, potrebno je napraviti analizu modela prijetnji i identificirati što je više moguće ranjivosti. Kontrola pristupa sustavu za e-učenje omogućava da pristup imaju samo ovlašteni korisnici sustava te definira korisničke razine dozvola u pristupanju određenim objektima sustava.*

Ključne riječi: *e-učenje, sigurnost, prijetnja, napad, rješenje, kontrola pristupa*

Professional paper

Abstract: *The contemporary era of modern technologies has allowed for distance learning or e-learning supported by suitable systems. E-learning systems are subjected to threats and attacks, just as other IT systems. In order to design a safer system less subjected to attacks, it is necessary to make the analysis of the model of threats and identify as many vulnerabilities as possible. Access control for e-learning systems grants access only to authorized users of the system and defines levels of user permissions in accessing certain system objects.*

Key words: *e-learning, security, threat, attack, solution, access control*

1. INTRODUCTION

The key feature of the contemporary information economy is the need for life-long learning. Industrial and professional changes, global competitiveness and the explosive development of information technologies have set up a standard that requires new skills, abilities, knowledge and learning [1]. In order to be able to deal with demanding problem solving and use their innovativeness for this purpose, employees are required to engage in life-long learning, especially the ones employed in the area of information technologies.

One of the ways of meeting the aforementioned requirements for acquiring new skills is distance learning or e-learning. From the corporative perspective, staff training equals raising the employees' competitiveness level. Online learning or e-learning has become an important tool for achieving these objectives. Naturally, the application of e-learning is much broader and involves education via its systems and students at faculties and schools. E-learning systems allow for upgrading classes, schools, teachers' work and teaching methods. Information technology provides us with the possibility of applying knowledge in a creative and efficient manner.

The role of e-learning system security is to allow for secure performance of interaction from one point to another between students and the computer network of the e-learning system of an educational institution. The application of the e-learning system at many institutions (schools, faculties, economy) has shown that the importance of information security is increasing, while the software support of the e-learning system is vulnerable and subjected to security risks regarding unauthorized changes and access to the system, as is the case with most of other information systems.

In the e-learning system environment students and teachers use the Internet in order to track and receive courses, ask questions and answer them, send and receive grades. This makes it clear that e-learning systems face security issues in the same way as computer networks and network access.

If the e-learning system within an institution gets compromised due the lack of security, the institution's reputation will decrease. Therefore, it is important to determine capacities of the e-learning system security and define potential threats.

Nowadays most of the e-learning systems is a web-based application that requires Internet browser as the access to the content. Such systems are mostly made as a three-tier architecture (Figure 1), just as any other web application.

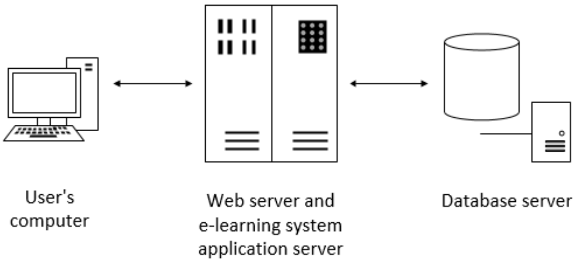

Figure 1. Three-tier architecture of e-learning systems

2. SECURITY CRITERIA OF E-LEARNING SYSTEMS

2.1. Particularities of e-learning systems from the aspect of security

E-learning systems provide a certain number of users with the possibility to send, upload and download data. The technique of communication between end users and e-learning portals is very important in these systems, as they as defined by widely spread elements in terms of network topology and physical geographical position. Furthermore, systems often have to provide a large information flow between users, which requires high system capacity and provides various network nodes with the same communication at any moment.

The system may be attacked only through access points and designers of most of the systems may set up a high security level by reducing the number of access points. An attacker may use access points for unauthorized access to numerous resources of the e-learning system. One of access points involves open internet sockets, which are the end point of communication between computers within a networked. Along with open internet sockets, RPC interfaces, configuration files, hardware ports and file system read/write may be mentioned as access points [2]. As, according to the definition, the e-learning system exists in several physical and logical locations at the same time, access points prevail to such extent that the system cannot be defined without them. It is obvious that e-learning system designers cannot apply the model based on the reduction of access points.

Another significant problem is the fact that one never knows in advance which process is going to be run in the system not at which moment. We notice that the potential of access points in the system is large, so it is impossible to know how or even where access points appear. It is also possible that a malicious process gets involved in the interaction via user's computer or the Internet and in this way controls attacks within the system.

Furthermore, the security of the entire system depends not only on the security of the computer network within the system, but also on the security of each individual process member, computer and server where the process is carried out and communication protocols between the participating processes. From the standpoint that the identity of e-learning course attendants is not tightly connected with a certain computer, the implementation of strict access and authorization criteria is required for the purpose of controlling intruders and malicious processes as a possible loss of privacy and confidentiality. The later could cause a decrease in process efficiency, as the percentage of legitimate processes and users would be reduced.

Numerous access points force learning systems to rely on security encoding schemes, but if they are not carefully implemented, they may lead to additional system vulnerability. The difficulties related to access point identification control suggest that it is better to make additional efforts regarding the restriction of attacker's possibilities to carry out any undesired actions at each of the access points.

2.2. The role of defining threats in the security system

The design of a secure e-learning system is not achieved only by using strong authentication and cryptographic systems, but also by implementing new safety solutions as an answer to attacks that had happened a second ago. The technology for designing a secure e-learning system is achieved by solving security issues as early as in the planning phase.

A system cannot be completely secured, but only ensured in a case of a specific attack. This points to the fact that system designers need to bear in mind potential threats and technical options of potential attackers while developing the system.

The aforementioned facts are to be considered and a model of threats, a collection of hypotheses on who and how may attack the system, is to be made.

The model of threats has three main purposes [3]:

a) to upgrade the security of a project by recognizing specific attacks and to implement countermeasures in advance
b) to anticipate possible outcomes of successful attacks
c) to allow for making suitable plans that shall oppose frequent attacks if and when they happen

The purpose of the model of threats is to identify as many vulnerability issues as possible by the system designer, in order to leave as little space for doing so as possible for the attackers. Upon defining the model of threats security demands may be defined and various security mechanisms may be developed.

2.3. Security areas of e-learning systems

There are three fundamental security areas (Figure 2) [4]. Hardware security involves all aspects of physical security and emanation. Compromising of emanation security relates to unintended signals such as electromagnetic waves emitted from cathode monitors that may disclose information by being intercepted and analyzed.

Information security includes computer security and communication security. These two security issues often focus on methods such as cryptography and network protocols. There are many other requirements that are to be met, such as authentication, data validity, access control, intellectual property rights and detection of unauthorized access. Technologies such as digital signature and watermark help in meeting these requirements. Observing it as a whole, computer security deals with prevention and detection of unauthorized actions that come from computer system users. Communication security involves measures and control in order to prevent unauthorized access to information.

Administration security is very important although it is often neglected in comparison with advanced technological solutions. This security area includes staff and operative security.

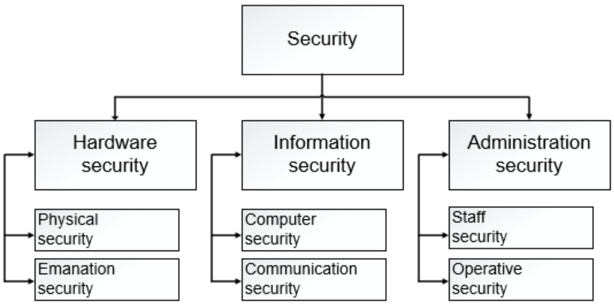

Figure 2. Security area categories

2.4. Basic security requirements

Basic security requirements for a computer network are secrecy, integrity, availability and non-repudiation. All other requirements may be traced to the aforementioned four [5]:

Secrecy – probably the most well-known security criterion. Users may obtain access only to those objects for which they have received authorization. They are not granted access to information they must not see.

Integrity of data and programs is equally important as secrecy, although it may be said that it is often neglected in everyday life. Integrity means that only authorized subjects (users or computer programs) are granted the possibility to alter data or initiate executive files. Secrecy of data is tightly connected with the integrity of programs and operative systems. If the operative system integrity is violated, the reference control will not work properly. Reference control is a mechanism that assures that only authorized subjects may access data and carry out operations. It is obvious that data secrecy cannot be guaranteed if this mechanism that checks and limits access to data does not function. This is why it is necessary to protect the integrity of operative systems with the purpose of protecting data secrecy.

Availability – it was not before the usage of the Internet that many users have recognized that availability is one of the main criteria in computer system security. If web-based applications are not available or the network is too slow, users cannot work effectively. An attack on withholding a service that compromises system availability may dramatically degrade performances of a web-based service of an author using it. Authors require more time to finish their work, and final frustration may make them less productive. There are no effective mechanisms for the prevention of service withholding attack. However, through constant control of applications and network connections it may be automatically detected. Suitable measures against this attack may limit its effects.

Non-repudiation – the fourth significant security criterion is that users are unable to deny having carried out operations. For instance, whenever grades of students are changed, it must be possible to reliably trace who has performed the modification and when it occurred.

3. TYPES OF POSSIBLE ATTACKS ON E-LEARNING SYSTEMS

3.1. Steps in defining threats

In defining threats three steps are to be carried out: characterization of the attacker, identification of access points and identification and classification of threats that simplify the fight against the attacker. The characterization of the attacker involves defining attacker's objectives, motives and possibilities. Identification of access points is carried out by determining entrances through which the attacker would search for system access. Identification and classification of threats describes potential threats that are to be delivered to the risk management department. Furthermore, there are three main terms in e-learning system security: attacker, system functioning means and access points [6].

Attacker – it is actually difficult to answer who the potential attacker of the e-learning system is and what their intentions and possibilities are. Attackers may take many forms. Some of them carry out their actions in a well-thought manner. Some are incompetent, legitimate system users. Attackers who operate in a well-thought way may be classified into several categories: hackers, users who want illegitimate free access to materials, unsatisfied employees or teenagers with a lot of free time. It is impossible to mention all potential attackers without leaving out at least a couple of types. Their basic features are e.g. unlimited attack time (teenagers), sophisticated knowledge (hackers) or the availability of system access for internal attackers (unsatisfied employees).

System functioning means – any element of the e-learning system necessary for the functionality of the system. Any threat may be defined in the part of means that the attacker wants to penetrate. Naturally, the objective of any solution to means security is not to eliminate the means, but to protect it. In order to protect the means, previously they need to be identified. For e-learning systems the following elements may be attacker's targets:

- e-learning content
- content of the cryptographic key
- users' personal data
- messages between users
- data of groups using the system
- network band broadness
- integrity of messages
- availability of messages

For each of these system elements there are elements of lower levels that are also potential targets of attackers, but they depend on specifics of each individual system.

Access points – may be defined as essential for the attacker while they are trying to penetrate the system. There is a long list of potential access points of a general e-learning system:

- used network protocols
- used communication channels
- computers of past, current and future attendants of courses
- physical network infrastructure
- data being collected for access into interactions within the system

3.2. Models of threats in the e-learning system

The four main security aspects (Table 1) in any computer system are availability, integrity, dependability and authenticity [6]. Each attack relates to at least one of these aspects.

The attack on the availability tends to make e-learning system services and data unavailable for legitimate users for a defined period of time. Attacks on integrity tend to actively alter or destroy data in the e-learning system without a suitable authorization. Attacks on confidentiality disclose confidential data to unauthorized users do not alter the contents of the e-learning system, but only affect the level of content security and users' personal data. Attacks on authentication appear when attackers represent themselves as legitimate users by means of a stolen password or credential. Attackers' objective is to gain free access to the e-learning system.

Table 1. Summary of security aspects independent on the performance of the e-learning system

Availability	Integrity	Confidentiality	Authentication
Denial of service	Malicious code attacks	Interception of group interactions	Attacks by force
Attacks on nodes	Encouraging messages	Analyzing traffic of group interactions	Attacks by vocabulary
Attacks on links	Traffic modification	Disclosing group identity	Application interference
Attacks on network infrastructure	Traffic erasing		Attacks on key control
	Traffic re-routing		Attacks by reproduction
	Re-routing traffic with delivery error		Attacks man in the middle
	Attacks by forging		Attacks by interaction extortion
	Congestion attacks		Attacks by non-acknowledging

Denial of Service – DoS is one of the dangerous methods of attacking e-learning systems, as one message or package may be replicated to numerous receivers over a large number of connections that appear in the system (Figure 3). This type of attack may be malicious, but may also be initiated undeliberately or by lack of caution. Some attacks are very complicated, while there are also very simple ones, and may be presented in a few ways:

Attack by a masked sender – the attacker may gain access into the system by attacking authentication. Once being authenticated, the source may overflow traffic for all users in order to usurp current and future interactions.

Attack by a masked receiver – once being authenticated, the attacker may cause problems through traffic by creating a large number of processes that are used by end users. In this way they overload the capacity of the system itself, but not the traffic of interactions. Due to this, the capacity of interactions increases for the purpose of accomplishing more traffic and consumption of resources.

DoS attack from the inside – a legitimate end user becomes a threat by overloading traffic for all users by usurping the system with signalization or by creating many processes for the receiver.

Transit DoS attacks – without authentication the attacker may insert unauthorized transit traffic through the network for the purpose of disturbing communication.

Current availability – a specific user is prevented to use the interaction through targeted DoS attacks.

Reception availability – a specific user is prevented to receive information through a targeted DoS attack.

SYN flood attacks – work on the principle of "bombarding" the e-learning system by means of the SYN (Synchronize) packages that are used for opening connections with other computers [7]. They cause unavailability problems or e-learning system overload.

Smurf attacks – use the ICMP package (Internet Control Message Protocol) that was sent by the user with a forged return address of the victim [8]. The ICMP package is emitted to a large number of other users and if many computers answer by sending the ICMP package to the victim, it may result in strong network congestion.

Distributed DoS attacks – multiplying common DoS attacks by initiating attacks from several different addresses at the same time. The attacker gains access to a certain number of end users' computers in advance and places a code into each computer for the purpose of attacking at the current moment or a defined signal. In this way the attacker becomes invisible, so such attacks are difficult to track and prevent.

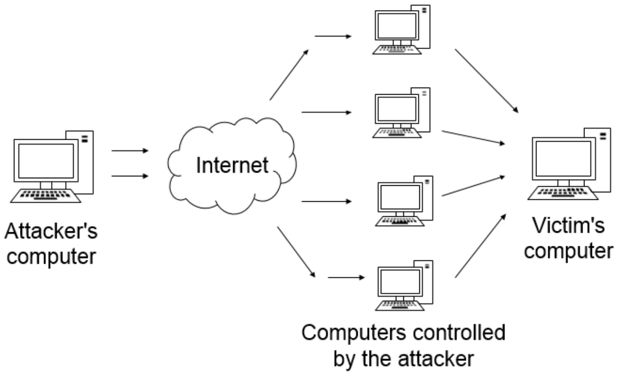

Figure 3. Representation of a DoS attack

4. SOLUTIONS THAT RESULT IN THE DESIRED LEVEL OF SECURITY

4.1. Access control

Access control is used for granting access (reading and writing) to certain objects or files provided by the authorized user [4]. Access control requires dependable authorization and only if user's identity may be determined for sure, it is possible to check access rights as well.

Access control may be carried out on several levels, and in operative systems it generally relates to permissions to read, write and execute. In database systems access control may be more precisely defined than in operative systems.

4.1.1. Discretionary Access Control

The main idea of the Discretionary Access Control (DAC) is that all users may independently decide who shall be granted access to objects created by them. Most users are familiar with DAC through their daily work with files. In operative systems only a small amount of mouse work is necessary for allowing a certain user to read and write in a file or that these rights are abolished.

DAC is very flexible. Its disadvantage is that administering it is quite complicated in large user groups. Moreover, the system is safe only if each user follows instructions and correctly sets up access rights.

The following example shows another disadvantage. The author creates confidential course materials and asks a colleague to check the content. For this purpose the author grants access to the colleague who copies it into their own folder in order to be able to work on it. This means that they move it from the place where the author is able to control the access to contents. The reliability of data may at this moment be ensured only if the colleague, in this case the reviewer, has correctly set up the access rights.

4.1.2. Compulsory access control

As opposed to Discretionary Access Control, compulsory access control does not allow an individual user to decide who may access certain data. Most of common ways of carrying out this control are multi-level security systems. These systems are usually used in military sectors. However, multi-level methods are recommended in the case that security of private data is guaranteed in mobile applications or in e-learning systems.

In multi-level systems data are categorized according to the level of secrecy. They can be public, confidential, secret or classified. Similarly, users are classified by a process that is characterized as determining users for access to allowed level. Users are authorized and see all documents positioned on their level or below. It means that it can be guaranteed that users are not able to access information on a higher, confidential level. Access to writing is allowed only on equal or higher level. It means that users who are authorized for accessing confidential data may create documents on the level of secret or classified data. In this case users cannot copy confidential data on the public level.

4.1.3. Basic web server access control

For granting access to files on a web server for certain users only, access limitations are defined for each folder, so all data in a folder may be accessed by the same group of people. In order to achieve controlled access to a web server, the first step is to group data that are to be protected, in the folder. For instance, the folder "lesson security through literature" may contain literature for a security course. Similarly, folders for other courses may be opened as well. The next step is the identification of individual user groups, e.g. students lv0079: all students participating in the course 0079, as in Table 2.

Table 2. Web server access control matrix

Objects / subjects	**Students Course 0079**	**Finished students**	**Teachers**
/security lesson/ literature	reading	reading	reading/writing
/security lesson/ exam model	reading	/	reading
/security lesson/ model solution	reading	/	reading

User name and password protected by some of the encrypting methods are to be assigned to each user. This mechanism provides relatively good protection that is sufficient in most cases. A big advantage of this security solution is simplicity.

4.1.4. Role-based access control

Role-based access control – RBAC is a widely spread access control form that is mostly used in operative systems, databases and web services. This access control may be understood as a logical successor of DAC. Access rights are not granted to users but to roles. For instance, the role "reading course registration" may be granted reading rights for objects "student", "course" and "course registration". These roles are also called roles with tasks, because they describe certain activities and determine which rights are required for which tasks. RBAC allows for assigning roles to other roles and determines authorization hierarchy.

Tasks are usually assigned to job roles. Figure 4 shows that mentor may comprise tasks such as course registration management, course registration reading, grading students and altering course description. Finally, users are assigned with certain job roles. For instance, user Ivo is the mentor, Ana is a mentor, but also a student (in a different course).

The main advantage of RBAC is the simplicity of authorization process. It means that modifications may be carried out in a simple manner. If Ana finishes her course and becomes only a mentor, her student role will be abolished. In places where individual object access rights are directly allowed, the administrator must know precisely which rights are granted to students, but not to mentors.

In most of RBAC systems it is possible to approve rights directly to individual users as well. This option is available in e.g. databases for the purpose of compatibility. Furthermore, direct assigning of rights is less complicated for smaller user groups (e.g. three users) who rarely change. However, as soon as a larger user group is created, the manner of assigning direct access is not to be used. The utmost complexity of this mechanism inevitably leads to incorrect authorization and results in security holes.

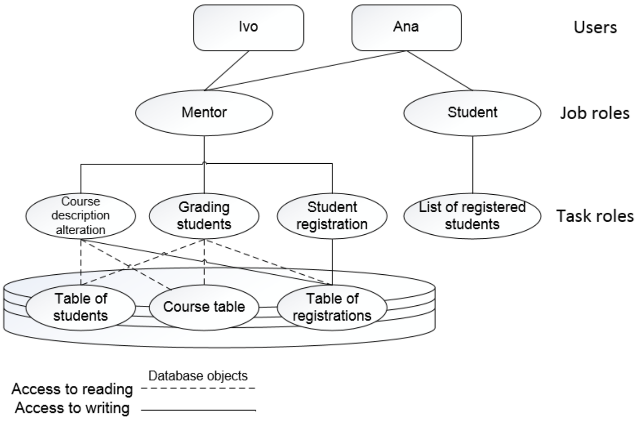

Figure 4. Access control toward assigned roles

5. CONCLUSION

As we currently witness technology advancing in all areas of life, the area of educational technologies advances as well. Along with traditional education, computer technology has been introduced too, as well as e-learning, i.e. distance learning.

E-learning is by no means a substitute for traditional learning, but it serves as a supplement or upgrading of the existing knowledge. As the number of courses and the need for e-learning services grows, it shall be necessary to pay more attention to security. As the number of users attending e-learning courses grows, the number of potential attackers increases as well.

For designers are programming experts the most significant fact is that security in the e-learning system is a problem that should be solved while planning a project. Special attention should be paid to risk analysis, check-ups and ensuring access points. The level of security based on access control is to be maintained during the course period and upgraded in the planned process, especially after attacks if they occur.

6. LITERATURE

[1] El-Khatib, K.; Korba, L.; Xu, Y., Yee, G.: Privacy and Security in E-Learning, International Journal of Distance Education, Vol. 4, No. 1 (2003) 1-19

[2] Myagmar, S; Lee, A. J.; Yurcik, W.: Threat Modeling as a Basis for Security Requirements, In Symposium on Requirements Engineering for Information Security (SREIS), 2005

[3] Swiderski, F.; Snyder, W.; Threat Modeling (Microsoft Professional). Microsoft Press, 2004

[4] Weippl, E. R., Security in E-Learning, Springer, 2005

[5] http://elearnmag.acm.org/featured.cfm?aid=1070943 (Available on: 15.05.2013)

[6] Nicklova, M.; Nickolov, E.; Threat Model for User Security in E-Learning Systems, International Journal "Information Technologies and Knowledge", Vol. 1, No. 4 (2007) 341-347

[7] http://en.wikipedia.org/wiki/SYN_flood
(Available on: 15.05.2013)

[8] http://en.wikipedia.org/wiki/Ping_(networking_utility)
(Available on: 15.05.2013)

Contact:

Davor Levanić, dipl.inf.
Polytechnic of Varaždin
J. Križanića 33, 42000 Varaždin
davor.levanic@velv.hr

Lana Križarić, dipl.iur.
Polytechnic of Varaždin
J. Križanića 33, 42000 Varaždin
lana.korunic-krizaric@velv.hr