Author's Security in Electronic Learning Systems

Ali Naserasadi
Industrial and Mining Faculty at
Shahid Bahonar University
Kerman, Iran

ABSTRACT

One of the most effective parameters in Electronic Learning or E-Learning systems' success is the security of these systems. But this feature is ignored in the most of cases. An E-Learning system has different user groups such as authors, teachers and students. Each of these groups has special and unique security requirements. In this paper, we distinguished security importance in E-Learning systems from authors' point of view. We investigated security requirements and the manner of authors' security risk analysis. Also, we suggested some approaches for educational content protection.

General Terms

Electronic Learning Security

Keywords

Electronic Learning, Security, Author, Educational Content

1. INTRODUCTION

Although E-Learning comes back to 19th century and correspondence-based learning, but using of computers and electronic devices in learning belongs to personal computers era [1, 2]. Since introducing of computer networks, E-Learning had a great improvement, and a suitable platform for distribution of educational content via internet, intranets and extranets by virtual universities is created. Nowadays by convergence of industries and universities at education process, E-Learning importance is increased too. In fact, E-Learning systems became change into special type of Electronic Commerce systems which require creation, distribution, maintenance and updating of information in the digital educational content format [1].

Despite the costs of above processes, people and parties who involve in these processes such as authors, teachers, students and managers ignore security of educational content; and security consideration are just restricted to user names and passwords or other simple security processes. But these simple processes are not used properly, too and have many problems and weaknesses [3]. In E-Learning system's security policy design, both of technical features of security consideration and mutual relations between people and parties, who present in the system, should be paid attention. Because of difference between these people and parties requirements, their special security mechanisms should be different. For example, in an E-Learning system, an author needs copy right but a teacher needs mechanism for protection from plagiarism [1]. So, despite the uniqueness of security terms such as confidentiality, integrity, accessibility, and non-repudiation in an E-Learning system but from different people point of view they are some different. In this paper, we investigated an E-Learning system security form an educational content author or producer point of view and presented some approaches for meeting his or her requirements and encountering with associated risks and threads.

2. AUTHOR'S SECURITY

Nowadays, knowledge is a very important tool for organizations' and human's success. So, need to education is a continuous and permanent requirement so that this process is became changed into a very important part of human routine life. To achieve this goal, E-Learning with many advantages such as costs deduction and time and location obstacles elimination, play an important role in this process. On the other hand, knowledge is a product, too; that is created via some complex human processes; and machinery systems have a weak role in these processes. Therefore, in the last two decades, knowledge became changed into a tool for business. So it extended business and industry of information technology in an ever-increasing manner [2, 4]. Therefore, security of this tool that is being used as educational content in E-Learning system is very important from author or producer point of view.

Against traditional approaches of security that be used extensively at military and commercial organizations for data confidentiality, author's security goal in E-Learning is not restricted just to data confidentiality and prevent of unauthorized access to data and information but the way of information presentation is important too [1]. In fact, in the most cases, knowledge that exist in E-Learning systems is accessible for each person; so author's assets is not restricted to information but the hypermedia that be used for information presentation has a vital role, too. Therefore, we define author's security in electronic learning as a secure environment for creation and presentation of educational content, without of concern about special threads of electronic communication system based educational platforms.

One of the most important aspects of E-Learning systems is usability of these systems [5]. On the other hand, security mechanisms of each information system have reverse relation with usability of that system [6]. So, using of many security mechanisms for author's security in an E-Learning system, because of high costs and reduction of system's usability is not acceptable as like as using no security mechanism. So, for establishment of author's security in an E-Learning system we need security requirement analysis and security risk analysis about threads and risks of such a system. Then with combining of this two analysis results, we can decide about suitable security mechanisms.

3. REQUIREMENT ANALYSIS

As mentioned before, regardless of using of unhidden information and educational content in E-Learning systems, security plays an important and vital role in these systems. In fact, we should take into consideration that despite of security mechanisms side effects on information systems complexity and reduction of their usability, we can't ignore them. For example, we can't ignore critical and vital role of security mechanisms in electronic banking. Also, in E-Learning, educational content is accessible for numerous people, so they can distort or alter them without informing the author or his or her grant, who is the owner of that educational content. Therefore, in an E-Learning system, author needs some security mechanisms to protect his or her assets (including text, audio, image, video or application that we generally named them educational content). We will investigate the most important author's security requirements in next sections.

3.1 Protection against Unauthorized Change

Many times we saw incorrect and unreal news and information on internet websites. Most of them are result of unauthorized change of contents by hackers or other users. This problem may cause users distrust about integrity of data [1]. Importance of this problem in E-Learning systems is very higher than a website; because user of an E-Learning system is a student who is under graduation and the system should provide correct and valid information for him or her. If not, undesirable results may take place. Therefore, in an E-Learning system, the author should be sure that users receive educational content in a correct and unchanged format.

3.2. Protection against Unauthorized Use

Most of authors and publishers are concerned about unauthorized use of published educational content. In classic and traditional education system, that uses paper-based educational content, users can make unauthorized copy of educational content but at most of times these copies are not economical and have not the quality of original content. On the other hand, make copy from digital educational content that exists on computer networks or storage media such as optical disks, has very lithe cost (almost it doesn't have any cost) and the unauthorized copy has the same quality as like as original copy. We should mention that there is a same problem in video and music industries.

3.3. Protection against Data Destruction

By using of Section 5 approaches, we can protect educational content against unauthorized change but we can't be satisfied with them; because in an E-Learning system if you can't present educational contents to students in suitable time and conditions, these contents loses their value. So, in these systems, author needs some mechanisms to protect data from destruction and prevent from denial of service attacks.

3.4. Gathering Data to Update Information

In an E-Learning system, educational data should updated base on user needs and conditions of the system in special time periods. One of the most effective parameters in this process is the way of using educational data by users. In fact, author can use these data to improve educational content, such as correcting a broken link in a website. In traditional education systems, these data seldom was accessible for author, but in E-Learning systems we can simply track users operations and gather needed data. Anyway, we should concern about user freedom for using educational content in this process. So, author needs some mechanisms to gather needed data while protect user privacy.

Now, we should answer to a very important question: Do the above requirements have similar importance and priority in all E-Learning systems? In other word, are the security mechanisms similar in all E-Learning systems?

The answer of above question is negative. In each E-Learning system, depend on special conditions of that system such as educational content format, used hypermedia for content distribution, importance degree of content based on economical, political, industrial and etc. dimensions, we should use special security mechanisms. To carefully answer the above question we should do the author's security risks analysis in an electronic learning system.

4. SECURITY RISKS ANALYSIS

Risk analysis is an important process in each project. Often, project managers are responsible to do this process. The important point to correctly do this process is that all stakeholders should be considered in the process [7]. As mentioned, authors are one of important groups in each electronic learning system project. Therefore, security risk analysis for this group is necessary to clear up associated risks and threads.

To explain this process, first, we should clearly define security risks and threads in a computer based information system. Thread is defined as each undesirable event in the system [8]. For example, intrusion of unauthorized users into the system, unauthorized change of data, data eavesdropping and denial of system services are instances of threads in an E-Learning system. On the other hand, risk is product of a thread's probability into its expected damage [8].

Security risk analysis should always be done before project outbreak to plan for encountering with risks via countermeasures [9]. All of E-Learning system stakeholders should attend at this process. Authors' attendance in this process limited to security risks analysis sessions for assigning educational content security mechanisms. Of course, depend on authors' experiences and knowledge about information technology, some education for using security tools may be needed, such as setting access right in a network based system or the way of working with cryptosystems.

Security risk analysis is accomplished in several serial steps: assets identifications, estimation or calculation of threads, identification of risks and countermeasures, identification of risks priority based on system conditions, implementation of controls and countermeasures and monitoring of risks and used countermeasures' performance [7, 8].

As mentioned at section 3, in an E-Learning system, author's assets are information or educational content; and associated threads are unauthorized use, unauthorized change, data destruction, denial of system services and copyright violation. So, we had done the first two steps of security risks analysis process. For doing the third step, we should estimate risk of each thread. Priority of each risk is calculated via relation (1) and base on its expected damage.

$$e = v \, .p \qquad (1)$$

In the above relation, e is the expected damage of a risk, v is asset's value and p is probability of thread occurrence [7, 8].

Due to lake of a standard and general way to determine priority of each risk by calculating the assets' value and the associated thread probability, we normally use expert judgment or brainstorming based on previous projects' information. For example, to determine author's assets' value we should pay attention to some parameters such as information gathering costs, information selling revenue, recovering destructed or changed data costs, private information leak costs, the value of information for competitors and so. Also, each thread probability is calculated via system conditions and infrastructure such as distribution hypermedia type, user access to educational content type, user level of knowledge and experience about using educational content, user familiarity with used tools, legal and regular features about computer crimes and copyright protection.

After determining of risks priority, due to limited security budget in each E-Learning system, we should select countermeasures so that the system we can protect system against high priority risks. Of course, in implementation of countermeasures we should pay attention to the cost of implementation and the cost of alternative plans [1].

5. COUNTERMEASURES

As mentioned, in an E-Learning system, content is created via complex human process. On the other hand, presenting on this content to users in a digital format causes many security problems. Based on researches, 80% of attacks in an E-Learning system are done by internal users [2]. So, use of some techniques such as cryptography, digital signature and VPNs, despite protection of system against external attacks, don’t have enough performance to protect against authorized users’ attacks, lonely. Therefore, we should use mechanisms that protect system against both internal and external attacks. For example, we can use client/server architecture and force the user to use educational content online. But this technique, due to unsafe client side scripting methods has not enough performance. Thus, protecting each type of educational data separately and via special techniques is better.

5.1. Text Protection

Text is one of the most usual formats of educational contents, which should be protected against external and internal attacks. To protect text against external attacks we can use authentication, authorization and access control techniques such as username and password, smart identification card or biometric identification methods [10]. Of course, each of these techniques has special strengths and weaknesses. For example, username is a very simple mechanism with low security level, while smart cards or biometric identification systems have higher security level but have some special problems such as lake of global standard or risk of privacy violation. A quick look comparison of different types of identification and authentication methods is provided in Table 1. In this comparison, different types of identification and authentication methods have been compared on the following eight criteria: information source, accuracy, reliability, maintainability, availability, upgradeability, system integrity and cost [11]. In the table, number 10 is used for the best case and number 1 shows the worst one. We should mention that these techniques do not guarantee complete security. For example, most of text based applications such as word processors; use temporal files that, in some cases, remain on the system even after user withdrawal, and so, unauthorized users can misuse them. To solve this problem, we can use special application such as AutoClave, to omit temporary files.

On the other hand, the authorized internal users can cause system a lot of loss via inadmissible content change or present them to external parties. To encounter with this threads, we can use digital certificates in cryptosystems or unchangeable text formats such as PDF. Figure1 shows the way of using digital certificates to protect educational content in an E-Learning system. Of course, we can use copyright protection methods, too (see section 5.4). At all, we should use a combination of above techniques to protect texts in all modes.

Table 1.The comparison of different types of identification and authentication methods

Method	Information Sources	Accuracy	Reliability	Maintainability	Availability	Upgradeability	Integrity	Cost
Username & Password	9	9	7	10	10	9	7	10
Smart Card	5	10	10	6	5	5	10	6
Hand-Held Password Generator	4	10	10	3	3	4	10	2
Biometrics	5	7	8	5	5	3	8	3
Cryptography	8	9	9	9	8	8	8	10
Place-Based	7	2	2	6	9	9	3	9

5.2. Audio and Video Protection

Audio and video files form another important part of educational content in E-Learning systems, too and have problems as like as text files. We can use same methods to protect these files. In any case, we can use methods such as digital watermarking to place imperceptible information on audio and video files. Of course, this information which placed in areas with different color patterns in video files and high frequency areas in audio files can be detected by detection systems. But this information can only protect copyright of audio and video files and can’t protect educational content against making unauthorized copies [12, 13].

5.3. Application Protection

In the last decades, to encounter with unauthorized copies of applications, floppy disks were made so that making copy form them was impossible. Nowadays, also, same methods are used in optical disks. In spite of this, there are tools to bypass this mechanism [14]. At all, it seems that encountering with unauthorized copies is impossible. But, using hardware protection mechanism (such as serial or USB hardware lock) or software protection mechanisms (such as serial numbers) can be effective. Certainly, software protection mechanisms often are cracked by professional hackers. Hardware mechanisms are more reliable but undertake more costs.

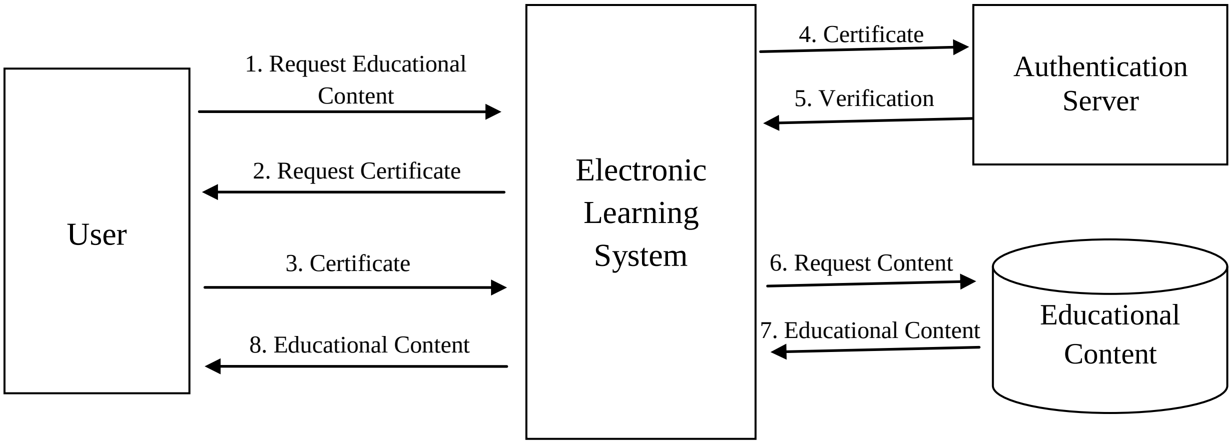

Figure 1.Using Digital Certificate to Protect Educational Content

In addition, because E-Learning normally use network infrastructure, we can use online of offline software keys to protect applications. In online software key method, user introduces himself or herself to server and receives a key to start the application. After that, the application continuously check the validity of key with server prevent form user usage in the case of key invalidity. In this technique, because each user has his or her own key and there is a permanent relation between the application and the server, different user can't use a same key concurrently. Of course, the most important problem of this technique is need to continuous relation between user and server that reduces system usability, especially in cases that the network bandwidth is low [1].

The above problem will be solved via offline software key system. In this system, user after connecting to server and receiving the key disconnects from server. Server locks the key and don't give in to other users. When user connects again to server, the server unlocks the key. In this system, for more protection, the keys have expiration time [1].

5.4. Copyright Protection

One of encountering methods with unauthorized distribution of educational content and monitoring of documents usage is double cryptography technology. In this process, data is encrypted and stored on user's computer. Each time user wants to use data; they are decrypted and stored on computer's memory. As soon as user stores data once more, they will encrypt again, normally with a new key that extracted from server. Therefore, E-Learning system can monitors user operations and on the other hand, unauthorized user can't use data because of encryption. Also, the authorized user can't change data. This system has some other advantages such as taking tuition based on user usage of educational content, establishing time limit on document usage, customizing of data and easier maintenance [15].

6. CONCLUSION

Despite importance of security, often it is ignored in E-Learning systems. In spite of this, because of knowledge critical role in organizations' success and complexity of knowledge creation and use processes in E-Learning system, we should use mechanism to protect it. Therefore, paying attention to author's security as creator of knowledge in an E-Learning system is very important in system's success. In this paper, we introduced special requirements of an author in an E-Learning system. Also, we introduced an approach for analyzing associated security risks and choosing suitable countermeasures to protect author's assets (text, audio, video and applications) in an electronic learning system

7. REFERENCES

[1] E. R. Weippl, Security in E-Learning, Springer Science and Business Media inc., 2005, pp. 13-75.

[2] F. Graf, "Providing security for e-learning", Computers & Graphics, Volume 26, Issue 2, April 2002, pp. 355-365.

[3] M. Warren and W. Hutchinson, "Information security – an e-learning problem", Advances in web-based learning – ICWL, Springer Berlin/Heidelberg, 2003, pp. 21-26.

[4] E. Turban, D. Leidner and E. McLean, Information technology for management: transforming organizations in the digital economy, 5th edition, Virginia: J. Wiley and sons, 2005, pp. 448-490.

[5] I. Smissen, "Requirements for online teaching and learning at Deakin university: A case study", unpublished.

[6] M. Bishop, Computer security: Art and science, Addison Wesley, 2002, pp. 1-25.

[7] J. Greene and A. Stellman, Applied software project management, O'Reilly Media inc., 2006, pp. 81-95.

[8] B. Schneier, beyond fear: Thinking sensibly about security in an uncertain world, New York: Springer-Verlag, 2003, pp. 59-73.

[9] J. Greene and A. Stellman, Applied Software Project Management, O'Reilly, 2005.

[10] Mahdi Jampour, Ali Naserasadi, Majid Estilayee and Maryam Ashourzadeh , "Extract and Classification of Iris Images by Fractal Dimension and Efficient Color of Iris", International Journal of Computer Applications (IJCA)

18(1), March 2011, pp. 11-14, ISSN: 0975 – 8887, Published by foundation of computer science.

[11] -, An Introduction to Computer Security: The NIST Handbook, National Institute of Standard and Technology, 2001.

[12] J. Seitz, Digital watermarking for digital media, Idea Group inc., 2005, pp. 30-52

[13] D. Zhang, L. Zhou, R. O. Briggs and J. F. Nunamaker Jr., “Instructional Video in E-Learning: Assessing the Impact of Interactive Video on Learning Effectiveness”, Information and Mathematics (43), pp.15-27, 2006.

[14] P. Craig, R. Honick and M. Burnett, Software piracy exposed, Syngress, 2005, pp. 19-63.

[15] Ross J. Anderson and Ross Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 1st edition, Wiley, 2001, ISBN: 0471389226, Chapter 20.

[16] G. S. Mouzakitis, “The E-Learning: The Six Important wh…?” , procedia Social and Behavioral Sciences (1), pp. 2595-2599. 2009.

[17] G. Kambourakis, D. N. Kontoni, A. Rouskas, S. Gritzalis, “ A PKI approach for deploying modern secure distributed e-learning and m-learning environments”, Computers and Education (48), pp. 1-16, 2007.

[18] S. Adibi, “A remote interactive non-repudiation multimedia based m-learning system”, Telematics and informatics (27), pp. 377-393, 2010.

[19] G. Darab, Gh. A. Montazer, “An eclectic model for assessing e-learning readiness in the Iranian universities”, Computers and educations (56), pp. 900-910, 2011.