Deploying Suitable Countermeasures to Solve the Security Problems within an E-learning Environment

Rjaibi Neila
Institut Supérieur de Gestion (ISG)
University of Tunis
Tunis, Tunisia
rjaibi_neila@yahoo.fr

Latifa Ben Arfa Rabai
Institut Supérieur de Gestion (ISG)
University of Tunis
Tunis, Tunisia
latifa.rabai@gmail.com

ABSTRACT

In earlier works, we present the quantification of security threats of e-learning systems using an economic measure abridged by MFC (Mean Failure Cost). It allows an analyst to estimate the security of a system in terms of the loss that each stakeholder stands to sustain as a result of security breakdowns. This paper provides an understanding of the security problems and risks related to e-learning systems. Then to control the MFC matrix, in particular its first matrix (the stake matrix) and to reduce its values we propose a classification of security problems versus the security requirements taxonomy of the MFC cyber-security model. The strength of the paper is in designing and deploying security measures and solutions to requirements.

Categories and Subject Descriptors

D.2.8 [Software Engineering]: Metrics; H.4 [Information Systems Applications]: Miscellaneous; K.6.5 [Management of Computing and Information Systems]: Security and Protection.

General Terms

Management, Measurement, Security, Reliability, Economics.

Keywords

Cyber Security Metrics, Security Risk Management, Mean Failure Cost Model, e-learning systems, Security requirements, Security problems, Security threats, Security measures, Security Countermeasures, Information Security.

1. INTRODUCTION

E-learning systems are open, distributed and interconnected, ensuring security is recommended for the interested actors mainly students, instructors, teachers and learners in order to have access to the right information at the appropriate time [1, 2, 3, 4].

SIN '14, September 09 - 11 2014, Glasgow, Scotland Uk

http://dx.doi.org/10.1145/2659651.2659721

The main aim of security management is to control and ensure enough security information. Therefore, assessing, managing and controlling the risks associated with e-learning systems such as identity, privacy, and data integrity are vital. But e-learning security risk is an important issue which was not seriously taken into account in the actual educational context.

In earlier works, we present a computational infrastructure that allows an analyst to estimate the security of a system in terms of the loss that each stakeholder stands to sustain as a result of security breakdowns which is the Mean Failure Cost model (MFC) [5, 6, 7].

The MFC is the product of several factors (the stakes matrix ST, the dependability matrix DP, the impact matrix IM, and the threat vector PT) [8]. It is possible to control the MFC through its factors in order to minimize its values.

The beginning of our study, investigates various security issues, problems and their risks involved in e-learning systems with an aim to suggest solutions and possible security measures.

In the actual step we investigate in a practical case study additional advantage of adopting security measures to reduce and control the risks values presented in the first matrix (the stakes matrix) of the MFC model. Therefore we propose a classification of security problems versus the security requirements taxonomy of the MFC cyber-security model [9].

Then we envisage exploring the needed security countermeasures versus the security requirements taxonomy of the MFC model. This family of security solutions named mitigation measures designates measures which we take to reduce the impact of failures on costs incurred by users.

This paper presents a comprehensive analysis of security problems then converges and put into relation with the possible security solutions and technical implementations through the classification of security requirements.
Our strength is to provide insight into the analysis of risks and security problems of e-learning systems; the presented risk analysis is not exhaustive and only gives an overview of possible solutions according to the security requirements taxonomy.

2. SECURITY PROBLEMS OF E-LEARNING SYSTEMS

In the e-learning context, the well known security problems are:

2.1 Unauthorized Use of Digital Content

The unauthorized access to e-learning network resources such the use of digital content is a big problem in e-learning environments. We found users with legitimate access and other without [11, 12]. The problem is the unauthorized access to digital content such unauthorized copying and modification of data, unauthorized physical access to servers, Sharing of unauthorized file during e-learning exams, Unauthorized access to e-learning network resources. This is caused by the spoofing of valid user identity [10].

- Users who access the content without authorization, can access to different layers of the e-learning architecture such the database system, the solution is to provide mechanisms of access control in order to prevent the authorization and it can includes the physical access to the servers [11].
- Users who have legitimate access to e-learning resources can diffuse contents on the internet, this problem and threat is harder to control, solution are digital rights management, distribution using the exchange standard PDF in order to limit modification [11].

2.2 Trust

Trust and intention to use e-Learning is essential. Instructors and students need to trust e-learning contents and resources and their accuracy, the integrity of content and the author's identity need to be established. Solutions are protection of e-learning content against unauthorized modifications. Also confidentiality between e-learning system and others users is essential for example for discussion when it is an essential component of courses. Security mechanisms are suggested such backups and archive of discussion, measures to delete contents, synchronous discussion using pseudonyms [11].

2.3 Exams

Critical risk related to examination is directly associated with cheating and plagiarism. This is a real danger threaten the e-learning environments and its good image, and exam is directly attached to security policy in order to reduce cheating.

- In E-learning context, the violation of access control is critical in the assessment phases, we are front a critical security problem of student's identification which causes cheating and plagiarism. This threats the proper functioning of the evaluation system.
- Sharing of unauthorized file during e-learning exams [12].
- Teachers must be concerned about availability and non repudiation of assessments. It's a challenge task, the teacher must control that answers are stored in an unaltered way [13].
- The Repudiation is when a person's deny the participation in any transaction of documents [13]. The non repudiation is the elimination of a refuted activity performed by a user. In the e-learning context, it is interesting mainly in an e-assessment context, the student who finished his evaluation tasks must not be able de deny that. The main solution that provides non deniability is authentication.
- Other problem when the students begin by the identification (Id, password) and then other friends collaborate with them and answer the exam. In this case authentication mechanism should been verified and the physical contact between student and the teacher is fundamental [11]. The core of any e-learning system is authentication techniques, it is vital because it provides confidentiality. The student's personal space includes e-mail, a discussion, marks, assignments and assessments that must be available to the concerned person.

2.4 The Personal Privacy of the User

Privacy is the ability of individuals to control, collect and distribute the personal information for example (user ID, passwords, and marks)**.** The privacy of Internet users is considered as the key risk in security, for the case of e-learning systems the danger is about the privacy and personal data of students and teachers, all about them are digitally recorded and stored in archives, this is critical and presents a real danger [13].

The main risk is that institution does not control these services and worse they are not aware about this fact. Given the widespread of servers in different country, they do not belong to the educational institution [14].

Privacy laws differ from country to another, government worldwide works on the development of privacy awareness and on the development of privacy policies.

The advancement of attackers targeting the personal privacy of the user such [14]:

- The misuse of login information (user ID and passwords) may also prevent the authorization of learner to access the server.
- Confidentiality violation is a related term of privacy: We can talk about: "An unauthorized party gaining access of the assets present in E-Learning system" [13]. The student needs to keep his marks and information private and confidential.

2.5 E- Learning System is not Available

The related threat is the Denial of Service (DoS) which is the "Prevention of legitimate access rights by disrupting traffic during the transaction among the users of E-Learning system". E-Learning system can be threatened by natural disasters like fire, storm, volcanic eruption, earthquake, floods etc [13].It is a set of physical threats such as theft, tampering, or destruction of equipment, accidents and disasters.

In an e-learning context, availability of e-learning platform:

- Is essential for students when they submit their assignments on time.
- Is also critical is assessment phases, student could launch an attack on the e-learning server to make such computers unavailable
- Also extends to the e-learning software used. They must be available. All this is the responsibility of the system administrator.

Availability is the accessibility and reliability of the systems and its resources in a timely manner by the authorized persons.

2.6 Non Detection of Attacks

The non detection of attacks means that the system is not able to detect or notify about successful attacks. It is needed to provide an active or passive monitoring of behaviors and conditions for evidence of an attack [15, 16].

2.7 Integrity Violation

Integrity means that data have not been accidentally or maliciously modified or destroyed. In the e-learning context we talk about Integrity Violation security problem, for example reading and/or altering e-mails sent to someone else [12].

"An unauthorized party accessing and tempering with an asset used in E-Learning system"[13].

"Students need the assurance that their assignments arrive to the intended examiner in its original and 'unedited' state." [17].

In e-learning systems, they are three cases of integrity violation, in the: [10]

- **Assessment integrity**: "A misuser tries to intercept and copy a message sent by the user to the system during an assessment".
- **User's message integrity**: "A misuser tries to create a false user's message and sends it to the system intending to modify the database or initiate a denial of service attack".
- **System's message integrity**: "A misuser tries to corrupt a message that is sent from the system to a user".

2.8 Non-repudiation security problems

The Repudiation is when a person's deny the participation in any transaction of documents [13]. The non repudiation is the elimination of a refuted activity performed by a user.

In the e-learning context, it is interesting mainly in an e-assessment context, the student who finished his evaluation tasks must not be able de deny that. The main solution that provides non deniability is authentication.

2.9 Physical attack

It is a set of physical threats such as theft, tampering, or destruction of equipment, accidents and disasters.

Besides the security issues and problems that may threaten e-learning systems, we present an overview of the possible well known security threats classified by security requirements [8, 20]:

- **Authentication attacks**
  1. Broken authentication and session management.
  2. Insecure communication.
- **Availability attacks**
  1. Denial of service.
- **Confidentiality attacks**
  1. Insecure cryptographic storage.
  2. Insecure direct object reference.
  3. Information leakage and improper error handling.
- **Integrity attacks**
  1. Buffer overflow.
  2. Cross Site Request Forgery.
  3. Cross Site Scripting.
  4. Failure to restrict URL access.
  5. Injection flaws.
  6. Malicious file execution.

3. CONTROLLING THE STAKE MATRIX AND MINIMIZING ITS VALUES

The Mean Failure Cost is the product of several factors (the stakes matrix ST, the dependability matrix DP, the impact matrix IM, and the threat vector PT) [5, 6, 7]. It is possible to control the MFC through its factors in order to minimize its values. This leads to set security priorities in the risk management process.

$$MFC = ST \circ DP \circ IM \circ PT$$

The stake matrix defines the list of system's stakeholders and the list of security requirements, it is used to express each cell in dollar monetary terms, it represents loss incurred and/or premium placed on requirement.

In order to control the stakes matrix we need to define the mitigation measures: This family designates measures which we take to reduce the impact of failures on costs incurred by users [18].

Table 1. The Stakes matrix (ST)

ST		**Requirements**							
		R_1	**…R_i…**						**R_n**
Stakeholders	**H_1**								
	…H_i…		**Stake that stakeholders H_i has in meeting requirement R_j**						
	Hm								

To control the MFC matrix, in particular its first matrix: the stake matrix (ST) and to reduce its values we propose a classification of security problems versus the security requirements taxonomy of the MFC cyber-security model.

4. CLASSIFYING SECURITY PROBLEMS VERSUS SECURITY REQUIREMENTS

After presenting the security issues and problems of the e-learning systems, we present a classification of security problems versus security requirements, this help to design the mitigation security measures in order to reduce the risk in the stake matrix of the MFC model.

Table 2. Classifying Security problems versus Security Requirements

Security Problem	Sub Security Problem	Security requirements	Security requirement Sub factor
Unauthorized Use of Digital Content		Access control	Authorization
Trust	Integrity of content	Integrity	Data integrity
	Student's identification	Access control	Identification
Exam	Student's identification	Access control	Identification
	Sharing of unauthorized	Access control	Authorization
	Availability of assessment	Availability	Response time
	Non repudiation of assessment	Non-repudiation	
	Non verification of the user's identity	Access control	Authentication
Privacy problems	Pb11: the misuse of login information	Access control	Authorization
	Pb12: confidentiality violation	Privacy	Confidentiality
E- learning system is not available		Availability	Resource Allocation
			Expiration
			Response time
Non detection of attacks		Attack/ Harm Detection	
Integrity Violation	Pb21:Assessment integrity	Integrity	Data integrity
	Pb22: User's message integrity		
	Pb23:System's message integrity		
Non-repudiation problem in an e-assessment		Non-repudiation	
Physical attack		Physical Protection	

5. CONTROLLING THE STAKE MATRIX THE POSSIBLE SECURITY SOLUTIONS VERSUS SECURITY REQUIREMENTS

Different ways are presented to control the Stakes Matrix by mean of adopting security measures that reduce the impact of failures on costs incurred by users/stakeholders for each security requirement.

5.1 Privacy Security Requirements

A number of security policy and measures against the violation of privacy are developed to provide the high level of protection:

Security policy [16]

- Administrative privileges
- Malware detection
- Multilevel security
- Reference monitor
- Secure channels
- Security session
- Single access point
- Time limits
- User permissions

Securing Privacy Control [19]

- Protecting Your Privacy
- Effectively Erasing Files
- Supplementing Passwords
- Install and Use Anti-Virus Programs
- Use Care When Reading Email with Attachments
- Install and Use a Firewall Program
- Make Backups of Important Files and Folders
- Use Strong Passwords
- Use Care When Downloading and Installing Programs
- Install and Use a File Encryption Program and Access Controls
- Safeguard your Data
- Real-World Warnings keep you safe online.
- +Keeping Children Safe Online

5.2 Integrity Security Requirement

Integrity is considered to be among the most vital security requirements. Authentication technique is the best way to protect the e-assessment task. In order to avoid plagiarism of student's response, another technique is to block the retrieval of the student's response. The e-learning security management should include the following possible solutions and security mechanisms to guarantee the integrity security requirement [16]:

- Administrative privileges
- Logging and auditing
- Reference monitor
- Biometrics
- Certificates
- Multilevel security
- Passwords and keys
- Reference monitor
- Registration
- Time limits
- User permissions

5.3 Non-repudiation

Possible solutions to the non repudiation are [16]:

- Administrative privileges
- Logging and auditing
- Reference monitor

5.4 Availability

The system recoveries are services that minimize the effects of a security failure; the solution is to restore the system to a secure state during or after an attack or accident [16].

- Backup and restoration
- Configuration management
- Connection service agreement
- Disaster recovery
- Off-site storage
- Redundancy

5.5 Access Control

Is considered among the most important and fundamental security requirement; it means "the access to a resource that is restricted to those who are authorized". Access control is also related to the three security requirements sub factor: identification, authentication, and authorization of actors [16].

Possible security solutions for access control

- Biometrics
- Certificates
- Multilevel security
- Passwords and keys
- Reference monitor
- Registration
- Time limits
- User permissions

Possible security measures to ensure students authentication:

- Passwords
- Challenge response questions
- E-token authentication
- Smart card authentication
- Biometric authentication
- Digital signature and digital certificate [13].

We could guarantee the access control security requirement using Firewall : A firewall may be is hardware or software security tool, it is used to prevent unauthorized access to a corporate network from outside the organization[13].

5.6 Physical Protection

According to Firesmith [15], physical protection security requirement is the degree to which the system protects itself and its components from physical attack. It is recommended to secure the e-learning platforms and its related services from physical threats. Such policies of physical protection are [16]:

- Access cards
- Alarms
- Equipments tagging
- Locks
- Offsite storage
- Secured rooms
- Security personal

5.7 Attack/Harm Detection

We present these countermeasures [16]:

- Administrative privileges
- Alarms
- Incident response
- Intrusion detection systems
- Logging and auditing
- Malware detection
- Reference monitor

6. CONCLUSION

An adequate security problems interpretation and risk analysis of e-learning regarding the security requirements taxonomy give us full guidelines about the needed developed strategy of protection and security. This family of security solutions named mitigation measures designates measures which we take to reduce the impact of failures on costs incurred by users. Our Future works focus on controlling the other factors (matrix) of The MFC model.

7. REFERENCES

[1] Rjaibi, N. and Rabai, L. B. A. 2010. On the assessment of quality teaching processes in informatics, *Proceedings of the Second Meeting on Statistics and Data Mining (MSDM 2010)*, March 11-12, 2010 Hammamet, Tunisia. Pp 104-110. http://tasa-online.com/msdm2010/proceeding.swf.

[2] Rabai, L. B. A., Rjaibi, N. 2013. Assessing Quality in E-learning including learner with Special Needs. *Proceedings of The Fourth National Symposium on Informatics, Technologies for Special Needs*, April 23-25, 2013. King Saud University, Riyadh, Saudi Arabia, http://nsi.ksu.edu.sa/node/2.

[3] Rjaibi, N. and Rabai, L. B. A. 2011. Toward A New Model For Assessing Quality Teaching Processes In E-learning, *Proceedings of 3rd International Conference on Computer Supported Education, CSEDU'2011*, Vol.2, (www.csedu.org), Noordwijkerhout, The Netherlands; 6-9 May 2011, page 468-472. SciTePress, 2011, ISBN: 978-989-8425-50-8.

[4] Rjaibi,N. and Rabai, L. B. A. 2012.Modeling The Assessment of Quality Online Course: An empirical Investigation of Key Factors Affecting Learner's Satisfaction", *IEEE technology and engineering education (ITEE)*. Vol 7, No.1, edited 23 March 2012, ISSN 1558-7908, 2012.

[5] Rabai,L. B. A., Rjaibi, N., and Aissa, A.B. 2012. Quantifying Security Threats for E-learning Systems. *IEEE Proceedings of International Conference on Education & E-Learning Innovations- Infrastructural Development in Education* (ICEELI' 2012- http://www.iceeli.org/index.htm), July 1-3, 2012, Sousse,Tunisia, Print ISBN: 978-1-4673-2226-3, Digital Object Identifier : 10.1109/ICEELI.2012.6360592.

[6] Rjaibi, N., Rabai, L. B. A., Omrani, H., and Aissa, A.B. 2012. Mean failure cost as a measure of critical security requirements: E-learning case study. *Proceedings of The 2012 World Congress in Computer Science, Computer Engineering, and Applied Computing (WORLDCOMP'12, Las Vegas, Nevada, USA)*, pp. 520-526, July 16-19, 2012, The 11 th International Conference on e-Learning, e-Business, Enterprise Information Systems, and e-Government (EEE'12: July 16-19, 2012, USA), http://www.world-academy-of-science.org/, Session: Novel Algorithms And Applications: E-Learning, E-Business, Eis, And E-Government, Copyright © 2012 CSREA Press U. S. A., ISBN: 1-60132-209-7

[7] Rjaibi,N., Rabai, L.B. A., Aissa, B.A. and Mili, A. 2013. Mean failure Cost as a Measurable Value and Evidence of Cybersecurity: E-learning Case Study. *International Journal of Secure Software Engineering (IJSSE)*. 4(3), 64-81, July-September 2013, Website: http://www.igi-global.com/ijsse. doi:10.4018/jsse.2013070104.

[8] Rjaibi,N., Rabai, L.B. A., and Aissa, B.A., and louadi,M. 2012. Cyber security measurement in depth for e-learning systems. International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE). Vol 2, No 11, pp 107-120, November-2012, ISSN (Online): 2277 128X, ISSN (Print): 2277 6451, Website:www.ijarcsse.com.

[9] Rjaibi,N., Rabai, L.B. A., and Aissa, B.A. 2013. A basic security requirements taxonomy to quantify security threats: an e-learning application. *Proceedings of The Third International Conference on Digital Information Processing and Communications (ICDIPC2013)*, Session: Information security, Islamic Azad University (IAU),Dubai, United Arab Emirates (UAE), pp. 96-105, ISBN: 978-0-9853483-3-5 ©2013 SDIWC, Jan. 30, 2013 - Feb. 1, 2013, http://www.sdiwc.net/conferences/2013/Dubai/

[10] Webber, C. G., Lima, M. D. F. W., Casa, M. E., Ribeiro, A. M. 2007. Towards Secure e-Learning Applications: a Multiagent Platform. *Journal of Software*, 2007, vol. 2, no 1, p. 60-69.

[11] Weippl, E. 2005. Security In E-Learning, *eLearn Magazine, Association for Computing Machinery (ACM)*, article from, 2005, vol. 16, p. 03-05.

[12] Levy, Y. and Ramim. M. M. 2010. Students' Perceived Ethical Severity of e-Learning Security Attacks, *Proceedings of the Chais conference on instructional technologies research*, 2010: Learning in the technological era.

[13] Barik, N., and Karforma, S. 2012. Risks and remedies in e-learning system, *International Journal of Network Security & Its Applications (IJNSA)*, Vol.4, No.1, January 2012, DOI : 10.5121/ijnsa.2012.

[14] Weippl, E. R. and Ebner, M. 2008. Security Privacy Challenges in E-Learning 2.0. *In World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education Healthcare, and Higher Education*. 2008. p. 4001-4007.

[15] Firesmith, D. 2004. Specifying Reusable Security Requirements, *Journal Of Object Technology*, Vol. 3, No. 1, January-February 2004, Online at http://www.jot.fm. Published by ETH Zurich.

[16] Rjaibi,N., Rabai , L. B. A., and Aissa, A.B. 2013. The Mean Failure Cost Cybersecurity Model toward Security Measures And Associated Mechanisms. *International Journal of Cyber-Security and Digital Forensics (IJCSDF)* 2(2): 23-35.

[17] Raitman, R., Ngo, L. , Augar, N.and Zhou W. 2005. Security in the online e-learning environment. *In Advanced Learning Technologies, 2005. ICALT 2005. Fifth IEEE International Conference on. IEEE*, 2005. p. 702-706.

[18] Aissa, A. B. 2012, "Vers une mesure économétrique de la sécurité des systèmes informatiques, " Doctoral dissertation, Faculty of Sciences of Tunis, submitted, Spring 2012.

[19] Ateeq, A. and Elhossiny, M.A. 2012. E-Learning and Security Threats, *IJCSNS International Journal of Computer Science and Network Security*, VOL.12 No.4, April 2012.

[20] Rjaibi, N., Gannouni, N., Rabai, L. B. A., and Aissa, B.A. 2014. Modeling the Propagation of Security Threats: An E-Learning Case Study, *IEEE Proceedings of The Third International Conference on Cyber Security, Cyber Warfare, and Digital Forensic (CyberSec2014)*, Beirut – Lebanon on Apr. 29 – May 1, 2014 , http://sdiwc.net/conferences/2014/cybersec2014/, pp. p. 32-37, ISBN: 978-1-4799-3905-3 ©2014 IEEE