Quantifying Security Threats for E-learning Systems

Latifa Ben Arfa Rabai[1], Neila Rjaibi[1], Anis Ben Aissa[2]
[1]Department of Computer Science
ISG, Tunis, Tunisia
[2]Department of Computer Science
ENIT, Tunis, Tunisia
latifa.rabai@gmail.com, {rjaibi_neila, anis_enit}@yahoo.fr

ABSTRACT: *As the reach of the internet expands to cover ever broader aspects of our economic and social welfare, cyber security is emerging as a major concern for researchers and practitioners, dealing as it does with privacy, confidentiality, user authentication, etc. E-learning systems epitomize computing systems and networks of the internet generation, since they involve multiple stakeholders, geographically distributed resources and data, and special requirements for confidentiality, authentication, and privacy. In this paper, we discuss the application of a cyber security metric to E-learning systems, in light of their standard architecture, their well-defined classes of stakeholders, and their specific security requirements.*

Keywords: Formatting, Risk Management, Information Security, E-learning, Threats Analysis, Mean Failure Cost, Quantification

Received: 25 October 2012, Revised 29 November 2012, Accepted 6 December 2012

1. Security issues in e-learning : A litterature review

E-learning concept is the use of technology to deliver information for training. This modern education is useful and interesting as it creates interactions between learners and instructors, or learners and learners regardless of time and space [2]. Also, it is an educational system where the instructor and the learner are at distance, collaborate and communicate using the technology. E-learning is the delivery of a learning, training or education program by electronic means as it involves the use of a computer or electronic device in some way to provide training, educational or learning material [3]. Nowadays, E-learning has become a popular way of learning for schools and businesses, it has increased exponentially in recent years [4].

The E-learning has gone through a spectacular development during the past years. In today's internet age, education requires the share and the distribution of information. We need a system or a platform, and then we call this an E-learning system or distance learning system or the E-learning platform which supports the online and / or the live and / or the blended learning processes. When they support only live learning process they can be an electronic support for course.

A variety of E-learning systems are widespread, the number of commercial E-learning is more than 250 sources and 45 of them are Open Source Software (OSS) [5].These standard systems support either a partially or completely the on line education. We cite WebCT (1997) [6], Ilias (1997), Blackboard (1997) [7], Claroline (2000), Moodle (2002) [5, 8] and SAKAI (2004) as the most used E-learning systems [5, 6, 9 and 10]. Moodle is popular and recommended among the variety of open source free product of the

market, the teacher can produce high quality on-line courses and he/she is well assisted by its rich documentation and support.

E-learning system is complex as it guarantees the satisfaction of the learner and the good image of the learning process. Fundamental assessment dimensions are discussed, they form the content, the human resources and the learning platform which covers network equipments and security. Other external dimensions cover financial, culture, policy and standards. This aspect is essential to make E-learning system successful. By the openness, the heterogeneity and the widespread of an E-learning system, dangerous threats increase and security issues become an important challenge to guarantee a safe environment. It is of our interest to focus on the security of E-learning platform in order to study its integrity, confidentiality and availability. In consequence having a stable platform without technical problems leads to have a learning process with higher quality [11, 22], an important increase in adequate cash, profitability and commercial image.

E-learning systems are large, dynamic with a variety of users and resources. The top three types of security attacks according to a security survey are: insider abuses of network access, viruses and laptop/mobile device theft [12]. The focus reclines on vulnerabilities and risks specific to e-learning, all the components of E-learning system such as web services, server computer systems, client computer systems, database systems can be threatened. Possible vulnerabilities that may affect the security of the online teaching learning system are summarized as follows [13]:

• DDOS (Distributed Denial of Service): the attacker tries to lock the server using a high-speed connection, it jams the network card, or blocks the legit traffic.

• Search-SPAM: similar to the DDOS attack, a hacker may submit a lot of "*dummy*" searches using our internal search engine, using two or three letter words with high frequency (such as "*of* ", "*for*", "*and* ", "*in*" etc) The result pages being a lot, these searches consume the most CPU time, both by Apache web service, PHP page generator and the MySQL database server

• Key loggers may be installed by students who can steal teachers' passwords and modify their own grades.

Mohd Alwi et al. [14] present issues related to the security of E-learning environment which are legal and ethical issues, piracy and the accessibility, security with the learning platforms and technologies, authentication of students and copyright and ownership of institution material.

Organizations are exponentially threatened; security is a current issue for them. Some statistics show that organizations are currently investing on security resources. Through 2005, the total global revenue for security products and service vendors amounted to $21.1 billion, from 1999 to 2000, the number of organizations spending more than $1 million annually on security nearly doubled, it represents 12% of all organizations in 1999 to 23% in 2000 [15]. Organizations are obliged to put emphasis on security risk management in order to measure and assess security risk and provide a good plan for risk mitigation.

One very important question that may be asked in security management is: why should we quantify security threats? It is clear that by quantifying variables, meaningful indication about risk assessment and good business decision makers are provided. Furthermore Mohd Alwi et al. [16] also suggest that security information management is useful in increasing competition, adequate cash, profitability and commercial image. Results of analysis security threats may also be useful in a practical plan to provide us pertinent information in order to implement a secure environment.

This paper is organized as follows. In section 2, we review related research on security risk management approaches in order to give a proper context to our work. In section 3, we present the metric for cybersecurity. In sections 4 and 5 we discuss how this metric can be specialized to E-learning systems in light of specific attributes of such systems, such as: their standard architecture, their standard deployment over the internet infrastructure, their typical stakeholders, and their specific security requirements. Finally, in section 6 we conclude by summarizing our results, highlighting strength of the cybersecurity measure and sketching directions of further research.

2. E-Learning Security Risk Management

E-learning shares similar characteristics with other e-services according to Mohd Alwi et al. [16], there are three main characteristics which are: the accessibility of service via internet, the consumption of service by a person via internet and the payment of a service by the consumer. Therefore, management security approaches to quantify security threats in E-learning are common with other e-services. However, some particularities are noted according to Nickolova et al. [17], we found in E-learning system:

• A variety of users, multiple applications and information to download and upload.

• An important communication between the computer users and E-learning portal

• A dynamic nature of the E-learning system

• A complex architecture.

In the first step it is necessary to define the terms '*risk*' and '*threat*' in order to emphasize on their different features. According to Bruce Schneier [18] a threat is defined as: "*a potential way an attacker can attack a system*". Commonly known, threats for computers are viruses, network penetrations, theft and unauthorized modification of data, eavesdropping, and non-availability of servers. A threat is also defined as a category of object, person or other entities that present a danger like spam, trojan horse and fishing [19, 20].

A risk is the product of the probability that a particular threat will occur and the expected loss. According to Bruce Schneier [18], when we talk about risk, it is the likelihood of the threat and the seriousness of its successful attack. For example a threat is more serious because it is more likely to occur. The risk of security threat as a quantitative measure is a suitable input to decision making [21]. Therefore, the purpose of considering risk as a financial measure leads to making decision from business perspective. For example, the return on security investment: ROI measure [22, 23] and the mean failure cost (MFC) measure presented in [22, 24].

It is of our need to adopt a security risk management process to determine the worthiest attack and the ignored one, it is one way to focus on the serious attacks, to better manage the budget and find the best way to use it [18, 21]. In a quantitative security risk management there are two input variables that needed to be fixed but they are difficult in the priori phase: the probability that a threat may occur and the loss suffered from a successful attack [22].

E-learning security management is a hot topic which coincides with the development and the use of E-learning by schools and businesses throughout the world. Much research has been conducted in this perspective but we noted a lack in quantitative approaches. Recently, the strength of Mohd Alwi et al. model resides in presenting a full recent qualitative model depending on vulnerabilities categories, threats, the 22 system applications, whereas the second which is Nickolova et al. qualitative model only depends on threats [17, 16].

3. Mean Failure Cost: A Measure Of Cyber-Security

In [1], Ben Aissa et al. introduce the concept of Mean Failure cost as a measure of dependability in general, and a measure of cyber security in particular. To compute the values of the mean failure cost for each stakeholder, we need to fill 3 matrixes and a vector as follow:

3.1 Stakes Matrix (ST)

We consider a system S and we let $H_1, H_2, H_3, \ldots H_k$, be stakeholders of the system, i.e. parties that have a stake in its operation. We let $R_1, R_2, R_3, \ldots R_n$, be security requirements that we wish to impose on the system, and we let $ST_{i,j}$, for $1< i < k$ and $1< j < n$ be the stake that stakeholder H_i has in meeting security requirement R_j.

3.2 Dependency Matrix (DP)

We consider the architecture of system *S*, and let *C*1, *C*2, *C*3,…*Ch*, be the components of system S. Whether a particular security requirement is met or not may conceivably depend on which component of the system architecture is operational. If we assume that no more than one component of the architecture may fail at any time, and define the following events:

• E_i, $1< i < h$, is the event: the operation of component C_i is affected due to a security breakdown.

• E_{m+1}: No component is affected.

Given a set of complementary events $E_1, E_2, E_3, \ldots E_h, E_{h+1}$, we know that the probability of an event *F* can be written in terms of conditional probabilities as:

$$P(F) = \sum_{k=1}^{h+1} P(F \mid E_k) \times P(E_k) \qquad (1)$$

We instantiate this formula with F being the event: the system fails with respect to some security requirement. To this effect, we let F_j denote the event that the system fails with respect to requirement R_j and we write (given that the probability of failure with respect to R_j is denoted by PR_j:

$$PR_j = \sum_{k=1}^{m+1} P(F_j \mid E_k) \times P(E_k) \quad (2)$$

3.3 Impact Matrix (IM)

Components of the architecture may fails to operate properly as a result of security breakdowns brought about by malicious activity. In order to continue the analysis, we must specify the catalog of threats that we are dealing with, in the same way that analysts of a system's reliability define a fault model. To this effect, we catalog the set of security threats that we are facing, and we let T_1, T_2, T_3, … T_p, represent the event that a cataloged threat has materialized, and we let T_{p+1}, be the event that no threat has materialized. Also, we let PT be the vector of size p +1 such that:

• PT_q, for 1< q < p, is the probability that threat T_q has materialized during a unitary period of operation (say, 1 hour).

• PT_{p+1} is the probability that no threat has materialized during a unitary period of operation time.

$$PE_k = \sum_{q=!}^{p+1} P(E_k \mid T_q) \times PT_q \quad (3)$$

• We introduce the Impact (IM) matrix, which has h + 1 rows and p + 1 columns, and where the entry at row k and column q is the probability that component C_k fails

$$PE = IM \circ PT \quad (4)$$

Matrix IM can be derived by analyzing which threats affect which components, and assessing the likelihood of success of each threat, in light of perpetrator behavior and possible counter-measures. Vector PT can be derived from known perpetrator behavior, perpetrator models, known system vulnerabilities, etc. We refer to this vector as the Threat Configuration Vector or simply as the Threat Vector.

3.4 Summary of MFC formula

Given the stakes matrix ST, the dependency matrix DP, the impact matrix IM and the threat vector PT, we can derive the vector of mean failure costs (one entry per stakeholder) by the following formula:

$$MFC = ST \circ DP \circ IM \circ PT \quad (4)$$

Where matrix *ST* is derived collectively by the stakeholders, matrix *DP* is derived by the systems architect, matrix *IM* is derived by the security analyst from architectural information, and vector *PT* is derived by the security analyst from perpetrator models.

4. Illustration: An E-Learning Application

4.1 List of stakeholders

E-learning system as a popular online learning environment adapts a variety of stakeholders. The list of the needed actors includes the system administrator, the teacher, the student and the technician [10, 11, 25 and 26].

4.2 E learning system architecture

The Online environment involves several dimensions in their architecture in order to support the various needs of stakeholders. The architecture is the integration of several technological components. According to [10] they are not a unique architecture for E-learning system. Consequently, there is no independent architecture, but we recognize for Moodle and WebCt the two popular and well known E-learning systems that actors are common like teacher, student, knowledge manager and administrator. Also, architectural components are common like browser, database server and web server.

Based on the architecture diagram presented by Selvi et al. [27], we recognize six architectural components which are:

• The browser as the client user interface [27],

• The Web server which hosts the Content Management System (CMS) Applications for managing students and their academic

and financial situations [25, 27],

• The application server which incorporates the E-learning platform; the request sent by the web server is forwarded to the application server; therefore the database concentrates on the storage, retrieval and analysis of data. It hosts online courses and is considered as the web server application programming interface which forms a standard web browser related to the organization [25, 27].

• The database server: is the core database and some extension tables of the E-learning system [27],

• The firewall server secures internet input and output traffic and filters high-risk codes, such as viruses [25],

• The mail server covers email application and user's mail boxes [25].

4.3 List of requirements

E-learning systems share similar security requirements with other e-services related to the accessibility of service via internet, the consumption of service by a person via internet and the payment of a service by the consumer [16, 17]. The basic security requirements are classified into six aspects [28]:

• **Authentication:** is required to identify the application user of the platform and to give him the right to access to the application with his own account [25].

• **Confidentiality:** is required to ensure that data and resources available on the platform are accessible only by those with right of access [5].

• **Integrity:** is required to ensure that the information like data and resources are available on the platform and can be modified only by authorized entities [29].

• **Availability:** is a very important subject, it is required to ensure that the web application is always available and operational when the user needs it [5, 29].

• **Non-repudiation:** is needed to ensure that no party in an operation can deny participating in the operation. We can also define the mechanism of non-repudiation as the mechanism that ensures that the sender of the message can't deny having sent the message in the future [28].

• **Privacy:** is necessary to ensure non-disclosure of information. It is required to ensure the security of information relating to each user [28].

4.4 List of threats

E-Learning systems allow multiple users or applications to download, upload and exchange distributed information.

Communication issues between end-users' computers and E-learning site in these systems are very important, as the systems are defined by widely dispersed elements in terms of network topology and physical geography. Additionally, the systems often allow many-to-many communication which provides powerful capabilities and allows many systems nodes to have the same communication at any given time. As noted in [16] a system can be attacked by a lot of threats that we can summarize the most important as follows:

• Viruses (VS),

• Denial of service (DoS),

• Acts of human error or failure like accidents (AH),

• Unauthorized access and/or data collection (DST),

• Deliberate acts of sabotage or vandalism (destruction of information or system) (DSV),

• Deliberate acts of theft (illegal confiscation of equipment or information) (TH),

• Compromises to intellectual property (piracy, copyright, infringement) (CIP),

• Quality of Service deviations (QoS),

• Blackmail for information disclosure (BID).

5. Computing Mean Failure Cost For E-Learning System

5.1 The stakes matrix (ST)

Each row of the matrix presented in Table I below is filled by relevant stakeholders who have internal or external usage for the platform, each cell expressed in dollars monetary terms and it represents loss incurred and/or premium placed on requirement. To fill ST Matrix we did a survey for EVT.

ST (H_i, R_j): Is the stake that stakeholders Hi has in meeting requirement R_j.

5.2 The dependency matrix (DP)

Each row of the matrix presented in Table II below is filled by system architects; each cell represents probability of failure with respect to a requirement given that a component has failed.

DP (R_j, C_k): is the probability that the system fails to meet requirement R_j if component C_k is compromise. To fill this matrix we have used the values from [30].

Using this data, we can now compute the vector of mean failure costs using the formula: $MFC = ST \circ DP \circ IM \circ PT$

ST Matrix	***Security Requirements***					
Stakeholders	***Confidentiality***	***Integrity***	***Availability***	***Non-repudiation***	***Authentication***	***Privacy***
Administration	40	30	60	10	10	50
Teacher	20	20	60	20	30	40
Student	0	5	5	0	5	0
Technician	10	7	15	5	5	15

Table 1. The Stakes Matrix (ST)

DP Matrix	***Components***						
Requirements	***Browser***	***Web server***	***Application server***	***DB server***	***Firewall server***	***Mail server***	***No failure***
Confidentiality	0.2	0.333	0.333	0.5	1.0	0.333	0.0
Integrity	0.2	0.333	0.333	0.0	1.0	0.333	0.0
Availability	1	0.333	0.333	0.0	1.0	0.333	0.0
Non-repudiation	0.2	0.333	0.333	0.0	1.0	0.333	0.0
Authentication	0.2	0.333	0.333	0.5	1.0	0.333	0.0
Privacy	0.2	0.333	0.333	0.5	1.0	0.333	0.0

Table 2. The Dependency Matrix (DP)

5.3 The impact matrix (IM)

Each row of the matrix presented in Table 3 below is filled by 5&5 Team; each cell represents probability of compromising a component given that a threat has materialized, it depends on the target of each threat, and likelihood of success of the threat. To fill this matrix we have used the values from [30].

IM (C_k, T_h): is the probability that Component C_k, is compromised if Threat T_h has materialized.

5.4 The threat vector (PT)

Each row of the vector presented in Table 4 is filled by security team; each cell represents probability of realization of each threat, it depends on perpetrator models, empirical data, known vulnerabilities, known counter-measures.

PT (T_i): The probability that threat T_i materialized for a unit of operation time (one hour of operation).

IM Matri	*Threats*									
Components	***VS***	***DoS***	***AH***	***DST***	***DSV***	***TH***	***CIP***	***QOS***	***DIE***	***No Threats***
Browser	0.004	0.005	0.100	0	0	0.300	0	0.200	0.200	0
Web Server	0.004	0.001	0	0	0	0	0.001	0.500	0	0
Application server	0.054	0.010	0.030	0.200	0.200	0.300	0.001	0.400	0	0
Database server	0.054	0.010	0.030	0.200	0.200	0.300	0.030	0.400	0	0
Firewall server	0.010	0.050	0.010	0	0	0.01	0	0.010	0	0
Mail server	0.054	0.010	0.030	0.200	0.200	0.300	0	0.400	0.400	0
No Failure	0.600	0.700	0.500	0.600	0.500	0.300	0.300	0.300	0.700	1

Table 3. The Impact matrix (IM)

Threats	**Probability/hour**
VS	5.04 10-3
DoS	3.08 10-3
AH	0.1 10-3
DST	0.42 10-3
DSV	2.31 10-3
TH	2.5 10-3
CIP	0.7 10-3
QOS	2.5 10-3
BID	1.4 10-3
No Threats	0,9819

Table 4. The Vector Of Probability (PT)

Table 5. presents the MFC for each stakeholder, therefore the system administrator stand to lose 0.785 $ / hour if the system is threatened, also the teacher lose about 0.743 $ / hours. For student and technician it can appear insignificant but for a failure to long-term they are significant.

Stakeholders	**Mean Failure Cost $ /hour**
System administrator	0.785
Teacher	0.743
Student	0.056
Technician	0.223

Table 5. The Mean Failure Cost for e-learning system

6. Conclusion

As distributed systems, E-learning systems epitomize the security concerns that such systems raise, including:

• Privacy of student and teacher personal records,

• Confidentiality (protection from exposure) and integrity (protection from alteration) of student performance records and transcripts,

• Authentication and access rights to course materials, grade records, etc.

Also, these systems present a relatively uniform architecture, and a common set of system stakeholders (students, teachers, administrators, tech support/ system custodians, etc). As such these systems are prime candidates for the Mean Failure Cost as a measure of cybersecurity, which offers the following attributes:

• **MFC varies by stakeholders:** The mean failure cost is not a characteristic of the system but rather depends on the system and the stakeholder/ user of the system.

• **MFC varies by stakes:** the same stakeholder may have different stakes in meeting different security requirements.

• **MFC is cognizant of the system architecture:** The mean failure cost is calculated by estimating the probability of failure of each component of the system, and the probability that failure of each component may affect each security requirement.

• **MFC is cognizant of the threat configuration:** The mean failure cost is calculated by cataloging the list of threats that the system is vulnerable to, the probability that each one of these threats may materialize within a unitary operation time, and the probability that each threat, if it materializes, will affect each component of the architecture.

• **MFC is quantified in economic terms:** The mean failure cost is computed as a monetary value per unit of operational time, and measure the amount of risk that each stakeholder is incurring as a result of security threats and system vulnerabilities. As such, it provides adequate support for quantitative decision-making.

We envision to broaden the application of MFC to the analysis of the security attributes of E-learning systems, by refining the catalog of threats, collecting empirical information that help us better estimate the matrices that are needed to compute MFC, and explore more opportunities for security related decision-making using MFC.

References

[1] Ben Aissa, A., Abercrombie, R. K., Sheldon, F. T., Mili, A. (2010). Quantifying Security Threats and Their Potential Impacts: A Case Study, Innovations in Systems and Software Engineering, 6 (4) 269–281, Springer London: March 27.

[2] Sun, P. C., Ray, J. T., Finger, G., Chen, Y. Y., Yeh, D. (2008). What drives a successful E-learning ? an empirical investigation of the critical factors influencing learner satisfaction, Computers and Education, Elsevier, 50, p.1183–1202.

[3] Stockley, D. (2008). E-learning Definition and Explanation (Elearning, Online Training, Online Learning), Retrieved November 14th, http://derekstockley.com.au/elearning-definition.html?

[4] Sung, Y. T., Chang, K. E., Yu, W. C. (2011). Evaluating the reliability and impact of a quality assurance system for E-learning courseware, *Computers & Education*, 57 (2) 1615–1627.

[5] Kumar, S., Dutta, K. (2011). Investigation on Security In Lms Moodle, *International Journal of Information Technology and Knowledge Management*, 4 (1) 233–238, January-June .

[6] Ngai, E. W. T., Poon, J. K. L., Chan, Y. H. C. (2007). Empirical examination of the adoption of WebCT using TAM, Computers & Education, Elsevier, 48, p. 250–267.

[7] Machado, M., Tao, E. (2007). Blackboard vs. Moodle: Comparing User Experience of Learning Management Systems, 37th ASEE/IEEE Frontiers in Education Conference, October 10 – 13, Milwaukee.

[8] Al-Ajlan, A., Zedan, H. (2008). Why Moodle, 12th IEEE International Workshop on Future Trends of Distributed Computing Systems, IEEE computer society.

[9] Khanjari, Z. A., Kutti, S., Hatem, M. (2006). An Extended E-learning System Architecture: Integrating Software Tools within the E-learning Portal, *The International Arab Journal of Information Technology*, 3 (1), January.

[10] Caron, P., Couture, M., Grant, A. (2005). Architecture pour le Développement et l'Implantation d'un Environnement de Formation Continue en Ligne (LOLE), Journées Francophones d'Informatique Médicale, Lille 12-13 mai.

[11] Rjaibi, N., Rabai, L. (2011). Toward A New Model For Assessing Quality Teaching Processes In E-learning, Proceedings of 3rd International Conference on Computer Supported Education (CSEDU 2011 - www.csedu.org), Noordwijkerhout, The Netherlands; 6-9 May.

[12] Bojanc, R., Blazic, B. J. (2008). An economic modelling approach to information security risk management, *International Journal of Information Management*, 28 (5) 413–422.

[13] Tugui, O., Funar, S., Cofari, A. (2008). Trends of Integrating the E-Learning Platform in the Graduate Agronomic Educational System in Romania, Computing & e-System, Hammamet, Tunisia.

[14] Mohd Alwi, N. H., Fan, I.S. (2010). Threats analysis for e-learning, *Int. J. Technology Enhanced Learnin*g, 2 (4) 358–371.

[15] Ekelhart, A., Fenz, S., Neubauer, T. (2009). AURUM: A Framework for Information Security Risk Management, Proceedings of the 42*nd* Hawaii International Conference on System Science.

[16] Mohd Alwi, N. H., Fan, I. S. (2010). E-Learning and Information Security Management, *International Journal of Digit Society*, 1 (2).

[17] Nickolova, M., Nickolov, E. (2007). Threat Model For User Security In E-Learning Systems, *International Journal Information Technologies and Knowledge*, V. 1.

[18] Scheier, B. Beyond Fear: Thinking Sensibly about Security in an Uncertain World, Springer-Verlag, New York, Inc.

[19] Whitman, M. E., Mattord, H. J. (2004). Principles of Information Security, Publisher Course Technology Press Boston, MA, United States.

[20] Stoneburner, G., Goguen, A., Feringa, A. (2002). Risk Management Guide for Information Technology, *Computer Security*, July.

[21] Ryan, J. J. C. H., Ryan, D. J. (2006). Expected benefits of information security investments, *Computers & Security*, 25, p. 579–588.

[22] Ben Aissa, A., Mili, A., Abercrombie, R. K., Sheldon, F. T. (2010). Modeling Stakeholder/Value Dependency through Mean Failure Cost, *In*: Proceedings of 6*th* Annual Cyber Security and Information Intelligence Research Workshop (CSIIRW-2010), ACM International Conference .

[23] Cavusoglu, H., Mishra, B., Raghunathan, S. (2004). A model for evaluating it security investments, *Communications of the ACM*, 47, p.87–92.

[24] Mili, A., Sheldon, F. T. (2009). Challenging the Mean Time to Failure: Measuring Dependability as a Mean Failure Cost, *In*: Proceedings of 42nd Hawaii International Conference on System Sciences (HICSS-42), Waikoloa, HI, p. 10.

[25] Naaji, A., Herman, C. (2011). Implementation of an E-learning system: Optimization and security Aspects, *In*: Proceedings of the 15*th* WSEAS International Conference on Computers, Part of the 15*th* WSEAS CSCC Multiconference.

[26] Wagner, N., Hassanein, K., Head, M. (2008). Who is responsible for E-Learning Success in Higher Education? A Stakeholders Analysis, *Educational Technology & Society*, 11 (3) 26–36.

[27] Selvi, R. T., Balasubramanian, N. V., Manohar, G. T. (2008). Framework and Architectural Style Metrics for Component Based Software Engineering, *In*: Proceedings of the International MultiConference of Engineers and Computer Scientists, 1, IMECS, 19-21 March, Hong Kong.

[28] Luminita, D. C. (2011). Information security in E-learning Platforms, Procedia Social and Behavioral Sciences, Elsevier, 15, p. 2689–269.

[29] Stapié, Z., Orehovacki, T., Danié, D. (2008). Determination of optimal security settings for LMS Moodle, *In*: Proceedings of 31st MIPRO International Convention on Information Systems Security, Opatija, 5, p. 84–89.

[30] Ben Aissa, A. (2012). Vers une mesure économétrique de la sécurité des systèmes informatiques, Doctoral dissertation, Faculty of Sciences of Tunis, submitted, Spring.