

A BASIC SECURITY REQUIREMENTS TAXONOMY TO QUANTIFY SECURITY THREATS: AN E-LEARNING APPLICATION

Neila Rjaibi *

Department of computer science,
ISG, Tunis, Tunisia
rjaibi_neila@yahoo.fr

Latifa Ben Arfa Rabai

Department of computer science,
ISG, Tunis, Tunisia
latifa.rabai@isg.rnu.tn

Anis Ben Aissa

Department of computer
science, ENIT, Tunis, Tunisia
anis_enit@yahoo.fr

Abstract—In this paper, we go on to define and refine a basic security requirements taxonomy adapted to all context and systems, then our hierarchical model is used to enrich the first matrix (stake matrix) of the Mean Failure Cost (MFC) cyber security measure. 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 compute the Mean Failure Cost for a given system. This expansion gives us more precise estimation, clear refinement and useful interpretation for security related decision-making using MFC. Moreover, the proposed taxonomy of security requirements forms a unified model of security concepts because security lacks a clear taxonomy of attributes, requirements, and standard controls. This taxonomy leads to the improvement of the system's software quality and its well running.

Keywords- *Basic Security Requirements; information security; e-learning; Security Requirements Taxonomy; software engineering, threats analysis; mean failure cost; quantification .*

I. INTRODUCTION

Nowadays, security requirements become an important issue in Information Systems, they improve the quality of software process and products. Security requirements are considered as levels protection, necessary for equipment, data, information and applications to meet security policy [1].

According to Charles et al. [2] security requirements are defined as “constraints on the functions of the system, where these constraints operationalize one or more security goals”. Security

requirements are considered as non functional requirements and a constraint on the system's functional requirements.

According to Firesmith [3], security requirement is considered as a quality requirement or a quality factor (i.e., attributes, characteristics, or aspects). Security requirements are a subset of the most important quality subfactors related to security (e.g., integrity and privacy). Every sub-factor forms a specification of a minimum amount of a security criterion.

Security issues are primordial to be considered for the development of all online systems. This concept is an emerging trend in software engineering. A well defined security process is advantageous and a well defined security requirements plan is recommended. All we need first, is to clarify and identify the needed security requirements as well as the sub security requirements and the whole security requirement taxonomy.

E-learning or other e-systems needed to be safe and secure, to maintain the perfect running of the system and to learn in safe [28, 29], we require the illustration of the Mean failure Cost (MFC) as a strong cyber security risk measure [4, 5, 26, 27]. It is of our need to adopt a security risk management process in order 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 [6, 7].

In this paper, we intend to define a basic security requirements tree or taxonomy, and to

illustrate it on the refinement of the Mean Failure Cost model. We discuss the application of this cyber security metric to E-learning systems.

This paper is organized as follows. In section 2, we present the basic security requirements for e-learning systems. In section 3, we illustrate the proposed basic security requirement taxonomy. In section 4, we discuss and compute the MFC for the basic security requirements taxonomy for An E-learning application. Finally, in section 5, we conclude by summarizing our results, and sketching directions of further research.

II. THE BASIC SECURITY REQUIREMENTS FOR E-LEARNING SYSTEMS

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 [8, 9].

We can classify the following basic security requirements of the e-learning platform into six aspects; Confidentiality, Integrity, Availability, Non-repudiation, Authentication and Privacy.

Authentication: The authentication mechanism is required to identify the application user of the platform and give him the right to access to the system with his own account [10, 11, 12, 13].

Confidentiality: is required to ensure that data and resources available on the platform are accessible only by those with rights of access. Confidentiality of Platform is guaranteed by ensuring a secure data environment [10, 11, 13].

Integrity: Integrity of data and resources in the open source software e-learning platform is required to ensure that the information available on the platform can be modified only by authorized entities [10, 11, 13].

Availability: Availability of the application is required to ensure that the web application is always

available and operational when the user needs it [10, 11, 13].

Non-repudiation: ensures that no party in an operation can deny participating in the operation. We can also define the mechanism of Non-repudiation as the mechanism focus on the fact that the sender of the message cannot deny having sent the message in the future [13].

Privacy: Is necessary to ensure non-disclosure of information given for each user. Privacy is required to ensure the security of information related to each user. [13].

III. THE PROPOSED BASIC SECURITY REQUIREMENTS TAXONOMY

Considering the logical relationship between security requirements, we propose in this section a variety of taxonomy of primary and secondary security requirements. As presented in the definition, security requirements are constraints on the functional requirements of a given system, the primary one is abstract, its refinement on sub factors give us more clarity and pertinence. This refinement process is recommended to provide more details about security guidelines and it is need in other cases when specification is related to the system such as the technical one [14].

To the best of our knowledge, security requirements cover a variety of quality criteria. They are formed as an hierarchical taxonomy of quality sub-factors presented by Firesmith [3], Calderón & Marta [15] and Lasheras [1]. Also other approaches are proposed to present the basic security requirements like ISO 7498 -2:1989 [16, 17, 18], The CIA triad (confidentiality, integrity and availability) [19] and other proposed categorization. The primary focus is to facilitate the specification and presentation of security requirements.

Table 1, presents the proposed basic taxonomy of security requirements. It is based on a variety of investigations; we studied 5 security requirement criteria and their relative sub criteria.

- **Access control:** is considered among the principal security requirements and it is called access control. It means that only a trusted user can have an access to the system security [3, 20, 21, 22, 23].
 - **Authorization:** is “the degree to which access and usage privileges of authenticated externals are properly granted and enforced”. [3]
 - **Identification:** is “the degree to which the system identifies (i.e., recognizes) its externals before interacting with them”. [3]
 - **Authentication :** is “the degree to which the system verifies the identities of its externals before interacting with them”. [3, 23].
- **Availability:** System content must be available, for example when a user takes a course, obtains data or a service through an online e-learning system, this service needs to be available in reasonable time [16, 19, 24, 20].
 - **Resource allocation:** the resources of the system in consideration such as memory, disk space and CPU time allocated need to be restricted to guarantee unavailability for anonymous users. For example: “The system shall not assign a single user more than 100 MB in hard disk”. Example: “The system shall not assign more than 50% of all work memory available for user requests”. [15]
 - **Expiration:** Is when the system is time out, and it seems useful when the user forgets to log out. Example: “The system shall reduce the time connection requests take to time-out to 1 minute when the number of connection requests exceeds 10,000 per hour”. [15]
 - **Response time:** the system should be available for a period of time, we can measure it on the percent of requests. Example: “The system shall provide student information within 1 hour for 99% of requests”. [15]
- **Non-repudiation:** is the possibility to deny the transaction or the transmission of data [3, 15, 16, 21, 22].
- **Integrity:** is the ability to protect data from being altered or destroyed in an unauthorized or accidental manner [16, 3, 19, 20, 23, 24].
 - **Software Integrity:** is the protection of software components from intentional corruption (e.g., via unauthorized addition, modification, deletion, or theft). [3]
 - **Personal Integrity:** is the protection of human components from intentional corruption (e.g., via bribery or extortion). [3]
 - **Hardware Integrity:** is the protection of hardware components from intentional corruption (e.g., via unauthorized addition, modification, or theft). [3]
 - **Data Integrity:** is the protection of data including communications from intentional corruption (e.g., via unauthorized creation, modification, deletion, or replay) [3, 15].
- **Privacy :** Personal information should not be disclosed to unauthorized individuals, entities, or computer software processes [3, 16, 19, 20, 23, 24].
 - **Traces:** the system should provide traces on previously accessed information. Mutual exclusion constraints may be required. Example: “The system shall not provide organization information access to any person who previously accessed information about another organization within the same conflict of interest class. [15]

- **Cardinality:** the system should verify the number of simultaneous connections for a user. Example: “The system shall not allow more than two simultaneous connections to a user”. [15]
- **Consent and notification:** is important in medical information systems, the system should notify users when they access to the system. Example: “ The system shall not allow medical center physicians to have access to medical records of a patient unless the patient has approved the access”. [15]
- **Attribution:** this is specific to verify access to logs, then only the system administrator can delete records from the account access log. Example: “The system shall record user identification, date, and time each time a user prints a customer list”. [15]
- **Aggregation:** the system must not be able to provide user access a large number of records which form the aggregate information such as daily sales reports and monthly customer purchase reports. Example: “The system shall not allow tellers to access daily sales reports before they execute the end day drawer process (in a Point of Sales system)”. [15]
- **Encryption:** the system must guarantee that sensitive data are encrypted. Example: “The system shall not allow users to transmit credit card numbers using an easily understandable format”. [15]
- **Confidentiality:** Personal information should not be disclosed to unauthorized individuals, entities, or computer software processes. For examples trade secrets, business plans, education records, credits card numbers. Confidentiality is usually ensured by encryption [3, 23].
- **Anonymity:** is the possibility to conserve the identity of users from unauthorized storage or disclosure [3].

TABLE 1. THE PROPOSED BASIC TAXONOMY OF SECURITY REQUIREMENTS

Security requirements	Security Requirements Sub factor
Access control	Authorization
	Identification
Availability	Authentication
	Resource allocation
	Expiration
Non-repudiation	Response time
	Non-repudiation
Integrity	Software Integrity
	Personal Integrity
	Hardware Integrity
	Data Integrity
	Traces
Privacy	Cardinality
	Consent and notification
	Attribution
	Aggregation
	Encryption
	Confidentiality
	Anonymity

IV. COMPUTING THE MFC FOR THE BASIC SECURITY REQUIREMENTS TAXONOMY: AN E-LEARNING APPLICATION

The Mean Failure Cost is a recent value based measure of cyber-security, First of all, on the theoretical side; Anis et al. developed the mathematical infrastructure to estimate the MFC using failure cost and failure probabilities [4, 5, 25, 26, 27]: They define the MFC as :

$$\text{MFC} = \text{ST} \circ \text{DP} \circ \text{IM} \circ \text{PT} \quad (1)$$

The MFC computes for each stakeholder of the given system his loss of operation (\$/H). This quantitative model is a cascade of linear models to quantify security threats in term of loss that results from system vulnerabilities.

In the practical side, they applied the proposed MFC to an e-commerce sample application [25] and to a cloud computing systems [31, 32, 33] using an implemented tool which computes the MFC for a given system, it calculates MFC metrics.

Our proposed improvement is on the ST' and DP' matrix, Where ST', DP' and IM are three matrixes, PT is a vector:

- The stake matrix (ST') presented in table 2 is filled by stakeholders according to the stakes they have in satisfying individual requirements; it is composed with the list of four stakeholders and the list of security requirements. Each cell expressed in dollars monetary terms and it represents loss incurred and/or premium placed on requirement. Our contribution in this paper resides on improving the stake matrix and presenting the basic taxonomy of security requirements. To fill ST Matrix we did a survey for ENT1. ST (Hi, Rj): Is the stake that stakeholders Hi has in meeting requirement Rj.
- The dependency matrix (DP') presented in table 3 is filled in by the system architect (i.e., cyber security operations and system administrators) according to how each component contributes to meet

each requirement; each cell represents probability of failure with respect to a requirement given that a component has failed. DP (Rj, Ck): The probability that the system fails to meet requirement Rj if component Ck is compromise. To fill this matrix we have used the values from [30].

- The impact matrix (IM) presented in table 4 is filled by analysts according to how each component is affected by each threat; each cell represents probability of compromising a component given that a threat has materialized, it depends on the target of each threat, likelihood of success of the threat. To fill this matrix we have used the values from [30]. IM (Ck, Th): The probability that Component Ck is compromised if Threat Th has materialized.
- The vector of threat presented in table 5 emergences probabilities (PT) that represents the probability of emergence of the various threats is done empirically, by simulating and/or operating the system for some length of time and estimating the number of threats that have emerged during that time. Each cell represents the probability of realization of each threat, it depends on perpetrator models, empirical data, known vulnerabilities, known counter-measures, etc. PT (Ti): The probability that threat Ti materialized for a unit of operation time (one hour of operation).

¹ <http://ent.uvt.rnu.tn/>

TABLE 2. THE EXTENDED STAKES MATRIX (ST')¹ (cost of failing security requirement stakes in \$)

Access control	Authorization	10	30	5	5
	Identification	10	30	5	5
	Authentication	10	30	5	5
Availability	Resource allocation	30	30	2	10
	Expiration	30	30	2	5
	Response time	20	20	1	5
Non-repudiation	Non-repudiation	10	20	0	5
Integrity	Software Integrity	30	20	5	7
	Personal Integrity	40	30	10	10
	Hardware Integrity	20	20	10	10
	Data Integrity	30	20	5	5
Privacy	Traces	10	0	0	5
	Cardinality	20	0	0	10
	Consent and notification	5	0	0	3
	Attribution	40	0	0	0
	Aggregation	20	0	0	10
	Encryption	30	15	5	7
	Confidentiality	40	20	0	10
	Anonymity	40	20	0	10
Security requirements	Security Requirements Sub factor/	Administrator	Teacher	Student	Technician
		Stakeholders			

TABLE 3. DEPENDENCY MATRIX (DP')

Security requirements	Security Requirements Sub factor	Components						
		Browser	Web server	Application Server	DB server	Firewall server	Mail server	No failure
Access control	Authorization	0	$4.2 \cdot 10^{-3}$	$4.2 \cdot 10^{-3}$	$4.2 \cdot 10^{-3}$	$4.2 \cdot 10^{-3}$	$4.2 \cdot 10^{-3}$	$9.79 \cdot 10^{-1}$
	Identification	0	$4.2 \cdot 10^{-3}$	$4.2 \cdot 10^{-3}$	$4.2 \cdot 10^{-3}$	$4.2 \cdot 10^{-3}$	$4.2 \cdot 10^{-3}$	$9.79 \cdot 10^{-1}$
	Authentication	0	$4.2 \cdot 10^{-3}$	$4.2 \cdot 10^{-3}$	$4.2 \cdot 10^{-3}$	$4.2 \cdot 10^{-3}$	$4.2 \cdot 10^{-3}$	$9.79 \cdot 10^{-1}$
Availability	Resource allocation	0	$3.3 \cdot 10^{-3}$	$3.3 \cdot 10^{-3}$	$3.3 \cdot 10^{-3}$	0	$3.3 \cdot 10^{-3}$	$9.868 \cdot 10^{-1}$
	Expiration	$3.3 \cdot 10^{-3}$	$3.3 \cdot 10^{-3}$	$3.3 \cdot 10^{-3}$	$3.3 \cdot 10^{-3}$	$3.3 \cdot 10^{-3}$	$3.3 \cdot 10^{-3}$	$9.802 \cdot 10^{-1}$
	Response time	$3.3 \cdot 10^{-3}$	$3.3 \cdot 10^{-3}$	$3.3 \cdot 10^{-3}$	$3.3 \cdot 10^{-3}$	$3.3 \cdot 10^{-3}$	$3.3 \cdot 10^{-3}$	$9.802 \cdot 10^{-1}$
Non-repudiation	Non-repudiation	$2 \cdot 10^{-2}$	$3.3 \cdot 10^{-2}$	$3.3 \cdot 10^{-2}$	0	$1 \cdot 10^{-2}$	$3.3 \cdot 10^{-2}$	$8.71 \cdot 10^{-1}$
Integrity	Software Integrity	$7 \cdot 10^{-3}$	$7 \cdot 10^{-3}$	$7 \cdot 10^{-3}$	$7 \cdot 10^{-3}$	$7 \cdot 10^{-3}$	$7 \cdot 10^{-3}$	$9.58 \cdot 10^{-1}$
	Personal Integrity	0	0	0	0	0	0	1
	Hardware Integrity	0	$7 \cdot 10^{-3}$	$7 \cdot 10^{-3}$	$7 \cdot 10^{-3}$	$7 \cdot 10^{-3}$	$7 \cdot 10^{-3}$	$9.65 \cdot 10^{-1}$
	Data Integrity	0	$7 \cdot 10^{-3}$	$7 \cdot 10^{-3}$	$7 \cdot 10^{-3}$	0	$7 \cdot 10^{-3}$	$9.72 \cdot 10^{-1}$
Privacy	Traces	0	0	0	0	$3.33 \cdot 10^{-2}$	0	$9.667 \cdot 10^{-1}$
	Cardinality	0	0	0	0	0	0	1
	Consent and notification	0	0	0	0	0	0	1
	Attribution	0	0	0	0	0	0	1
	Aggregation	0	0	0	0	0	0	1
	Encryption	0	0	0	0	0	0	1
	Confidentiality	$2 \cdot 10^{-2}$	$3.33 \cdot 10^{-2}$	$3.33 \cdot 10^{-2}$	$5 \cdot 10^{-2}$	$1 \cdot 10^{-1}$	$3.33 \cdot 10^{-2}$	$7.3 \cdot 10^{-1}$
	Anonymity	0	0	0	0	0	0	1

TABLE 4. THE THREAT MATRIX (IM)

Threats Components	BroA	InsC	DoS	CryptS	DOR	InfL	Buff	CSRF	CSS	FURL	InjecF	MFile	No Threats
Browser	0.4	0.1	0.005	0	0	0	0	0	0	0.333	0	0	0
Web server	0.4	0.2	0.001	0	0	0	0.5	0.01	0.02	0.333	0	0	0
Application server	0.4	0.2	0.01	0	0	0	0.5	0.01	0	0.333	0.02	0.005	0
DB server	0.4	0.2	0.01	0.33	0.33	0.33	0.5	0.01	0	0	0.02	0.005	0
Firewall server	0.01	0.01	0.05	0	0	0	0	0	0	0	0	0	0
Mail server	0.4	0.2	0.01	0.03	0.03	0.03	0	0.01	0	0.333	0.02	0.005	0
No Failure	0.6	0.4	0.7	0.8	0.8	0.8	0.7	0.8	0.8	0.6	0.8	0.8	1

TABLE 5. THE PT VECTOR (PT)

Threats	Probability
Broken authentication and session management (BroA)	4.20 10 ⁻⁵
Insecure communication (InsC)	3.00 10 ⁻⁵
Denial of service (Dos)	3.08 10 ⁻⁵
Insecure cryptographic storage (CrypS)	7.00 10 ⁻⁴
Insecure direct object reference (DOR)	7.00 10 ⁻⁴
Information leakage and improper error handling (InfL)	7.00 10 ⁻⁴
Buffer overflow (Buff)	1.00 10 ⁻⁴
Cross Site Request Forgery (CSRF)	4.20 10 ⁻⁴
Cross Site Scripting (CSS)	1.80 10 ⁻⁴
Failure to restrict URL access (FURL)	9.80 10 ⁻⁵
Injection flaws (InjecF)	2.17 10 ⁻⁵
Malicious file execution (MFile)	5.04 10 ⁻⁴
No Threats	974.44 10 ⁻⁵

Using this data, we compute the new vector of the Mean Failure Cost using the formula, as shown in table 6:

$$MFC' = ST' \circ DP' \circ IM \circ PT \quad (2)$$

TABLE 6. THE MEAN FAILURE COST ' FOR E-LEARNING SYSTEM USING NEW TAXONOMY

Stakeholders	Mean Failure Cost' \$ /hour
System administrator	418.178
Teacher	301.872
Student	50.595
Technician	118.125

Given the fact that security lacks a clear taxonomy of security requirements, the new basic taxonomy of security requirements forms a unified model of security concepts, therefore it is useful in many directives:

- Ensuring an orthogonal decomposition of the security requirements sub factor.
- Empirical value of the first matrix (stake matrix') became more precise, near to the reality and useful in practice.
- Reducing the redundancy of stakes values in ST matrix.

The Mean Failure Cost formula is a stochastic function, the major focus is to optimize the classic MFC metric and its quantitative value. In [4, 26, 27] Rjaibi et al. have implemented the classic MFC formula for the same system, value are presented in table 7.

As a validation of the extended MFC cyber security model, we compare the result of table 6 (MFC application for e-learning systems based on the new taxonomy of security requirements) and

result of table 7 (MFC application for e-learning systems using some listed security requirements)

The first interpretations of the new results of the MFC metric are more significant. So, the refinement of the basic security requirements is beneficial to better estimate the matrices that are needed to compute MFC, and explore the best opportunities for security related decision.

TABLE 7. THE MEAN FAILURE COST FOR E-LEARNING SYSTEMS WITHOUT SUB FACTOR OF SECURITY REQUIREMENTS

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

V. CONCLUSION

Among major concern of software engineering we present the topic of software security. Therefore, Security requirements are useful to discuss in early the software development process, or it is considered as a check list in security management.

Security requirements represent the high level of abstraction of the security architectural mechanism. For the security Sub-factors, only a small number of security quality sub-factors exist.

Our contribution is to provide a basic and refined taxonomy of security requirements adapted to all context and systems. In this case we refer to the variety of proposed models from the literature to drive an aggregate model and move away from the individualistic proposed taxonomy to a hierarchical model of security concepts.

The second contribution of this paper is to use the proposed refined taxonomy to enrich the first matrix of the Mean Failure Cost cyber security measure which is the stake matrix, this expansion give us more precise estimation.

We envision to broaden the application of MFC to the analysis of the security attributes of E-learning systems, by refining the holistic and complete catalog of security requirements, 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 the same measure (MFC).

VI. REFERENCES

- [1] J. Lasheras, R. Valencia-García, J.T. Fernández-Breis and A. Toval, "Modelling Reusable Security Requirements based on an Ontology Framework", *Journal of Research and Practice in Information Technology*, Vol. 41, No. 2, pp. 119-133, May 2009.
- [2] B. H. Charles, L. Robin, D. Jonathan Moffett, and B. Nuseibeh, "Security Requirements Engineering: A Framework for Representation and Analysis", *IEEE Transactions On Software Engineering*, Vol. 34, No. 1, pp. 133–153 January/February 2008.
- [3] D. Firesmith, "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, Chair of Software Engineering ©JOT, 2004.
- [4] N. Rjaibi, L. Ben Arfa Rabai, H. Omrani, A. Ben Aissa, "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), 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.*
- [5] L. Ben Arfa Rabai, N. Rjaibi, A. Ben Aissa, "Quantifying Security Threats for E-learning Systems", *Proceedings of IEEE 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] T. Tsiakis, G. Stephanides, "The economic approach of information security", *Computers & Security*, vol. 24, pp.105-108, 2005.
- [7] A. Ben Aissa, R. K. Abercrombie, F. T. Sheldon, and A. Mili, " Quantifying Security Threats and Their Potential Impacts: A Case Study," *Innovations in Systems and Software Engineering*, vol. 6, No. 4, pp. 269–281, Springer London: March 27, 2010.
- [8] M. Nickolova, E. Nickolov, "Threat Model For User Security In E-Learning Systems," *International*

- Journal Information Technologies and Knowledge, vol.1, pp. 341-347, 2007.
- [9] N.H. MohdAlwi, and I.S. Fan, "E-Learning and Information Security Management," International Journal of Digit Society (IJDS), vol. 1, no. 2, pp.148 – 156, 2010.
- [10] S. Kumar and K. Dutta, "Investigation on Security In Lms Moodle," International Journal of Information Technology and Knowledge Management, vol. 4, No. 1, pp. 233–238, January-June 2011. Francophones d'Informatique Médicale, Lille 12-13 mai 2005.
- [11] Z. Stapié, T. Orehovacki and M. Danié "Determination of optimal security settings for LMS Moodle," Proceedings of 31st MIPRO International Convention on Information Systems Security, Opatija, vol. 5, pp. 84–89, 2008.
- [12] A. Naaji, and C. Herman, "Implementation of an e-learning system: Optimization and security Aspects," Proceedings of the 15th WSEAS International Conference on Computers, Part of the 15th WSEAS CSCC Multiconference, 2011
- [13] D. C. Luminita, "Information security in E-learning Platforms," Procedia Social and Behavioral Sciences, Elsevier, vol. 15, pp. 2689–269, 2011.
- [14] H. Wang, S. Gao, B. Lu, Z. Shen, "A Novel Model for Security Requirements Process", Proceedings of the Third International Symposium on Electronic Commerce and Security Workshops (ISECS '10) Guangzhou, P. R. China, 29-31, July 2010, pp. 029-033.
- [15] C. Calderón, E. Marta, "A Taxonomy of Software Security Requirements", Avances en Sistemas e Informática, vol. 4, núm. 3, diciembre, 2007, pp. 47-56
- [16] ISO 7498-2: 1989, "Information Processing Systems - Open Systems Interconnection - Basic Reference Model", Part 2: Security Architecture, International Organization for Standardization (ISO), Geneva 15.
- [17] A. Ben Aissa, A. Mili, R. K. Abercrombie, and F. T. Sheldon, "Quantifying security threats and their impacts", Proceedings of 5th Annual Cyber Security and Information Intelligence Research Workshop (CSIIRW-2009), ACM International Conference Proceeding Series, Oak Ridge.
- [18] K. C. Sekaran, "Requirements Driven Multiple View Paradigm for Developing Security Architecture," in PWASET, Proceedings of World Academy of Science, Engineering and Technology, 2007, pp. 156-159.
- [19] "Engineering Principles for Information Technology Security". csrc.nist.gov.
- [20] J. Hintzbergen, K. Hintzbergen, B. Hans, S. André, "Foundations of Information Security Based on Iso27001 and Iso27002, Best Practice". (2010), Van Haren Publishing. pp. 13. ISBN 90-8753-568-6.
- [21] A. Mahtab, "Software Security Requirements Checklist", Int.J. of Software Engineering, IJSE Vol.3 No.1, pp. 2. 54, January 2010.
- [22] J. Jurjens, "Secure Systems Development with UML", Springer-Verlog, 2005.
- [23] R. M. Nancy, D. Eric, "Security Quality Requirements Engineering (SQUARE) Methodology", Theodore R. Stehney II, November 2005.
- [24] T. Christian, "Security Requirements Reusability and the SQUARE Methodology", September 2010.
- [25] A. B. Aissa, R. K. Abercrombie, F. T. Sheldon, and A. Mili, "Defining and Computing a Value Based Cyber-Security Measure," Innovations in Systems and Software Engineering, Vol 10, No.4, pp.433-453, December 2012 Springer London: April 23, 2011 (DOI:10.1007/s10257-011-0177, Online First)
- [26] N. Rjaibi, L. Ben Arfa Rabai, A. Ben Aissa and M. Louadi, "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,
- [27] A. Ben Aissa, A. Mili, R. K. Abercrombie, and F. T. Sheldon, " Modeling Stakeholder/Value Dependency through Mean Failure Cost," Proceedings of 6th Annual Cyber Security and Information Intelligence Research Workshop (CSIIRW-2010), ACM International Conference.
- [28] N. Rjaibi, L. Ben Arfa Rabai, "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, 2011.
- [29] N. Rjaibi, L. Ben Arfa Rabai, "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, pp.6-13 edited 23 March 2012, ISSN 1558-7908, 2012.
- [30] A. Ben Aissa, "Vers une mesure économétrique de la sécurité des systèmes informatiques," Doctoral dissertation, Faculty of Sciences of Tunis, submitted, Spring 2012.
- [31] L. Ben Arfa Rabai, M. Jouini, A. Ben Aissa, A. Mili, " A cybersecurity model in cloud computing environments ", Journal of King Saud University-

Computer and Information Sciences, Vol 25, No.1, pp.63-75, January 2013, Available on line at: <http://0-www.sciencedirect.com/precise.petronas.com.my/science/article/pii/S131915781200033X>

- [32] M. Jouini, A. Ben Aissa, L. Ben Arfa Rabai, A. Mili, "Towards quantitative measures of Information Security: A Cloud Computing case study ", International Journal of Cyber-Security and Digital Forensics (IJCSDF) 1(3), pp. 248-262

(2012). Available on line at: <http://sdiwc.net/digital-library/web-admin/upload-pdf/00000315.pdf>

- [33] L. Ben Arfa Rabai, M. Jouini, A. Ben Aissa, M. Nafati, A. Mili, "An economic model of security threats for cloud computing systems", in Proceedings of the International Conference on Cyber Security, Cyber Warfare and Digital Forensic. (CyberSec), June 2012, pp:100-105, IEEE CONFERENCE PUBLICATIONS.