EAI Endorsed Transactions
on Security and Safety

Research Article EAI.EU

How Stakeholders Perceived Security Risks? A New Predictive Functional Level Model and its Application to E-Learning

N. Rjaibi[1,*] and L.B.A Rabai [2]

[1, 2] Institut Supérieur de Gestion de Tunis, Université de Tunis, Bardo 2000 Tunisia

Abstract

A new predictive functional level security risk management model is proposed in order to quantify the security level perception and the level of risk involved. It helps in defining the assets, measuring economically the risk, managing the risk toward decisions making. It is out of implementation and based on a functional level architecture.
The paper defines a simple predictive model, it relies on a few number of inputs which form the system's security specifications and provides one output which is the average loss per unit of time ($/H) incurred by a stakeholder as a result of security threats. The obtained values represent how stakeholders perceived economically security risks and predict how it will change over time to implement in advance the needed security strategies.
Our model is useful in any security context. We report it in practice originally to the level of e-Learning systems for current architectures because they lack a common measurable value and evidence of cyber security. Our model assists security experts from the early phases of system's development to implement future safe and secure platforms.

Keywords: Security perception, Risk Measurement, Stakeholders, Security metric, CyberSecurity, E-learning systems.

Received on 26 January 2018, accepted on 27 August 2018, published on 15 October 2018

doi: 10.4108/eai.15-10-2018.155738

*Corresponding author. Email: Rjaibi_neila@yahoo.fr

1. Introduction

Some years ago, developers and researchers focused on the improvement of the aspect of web application design integrating multimedia components and managing content for industry and services. On the same line, the internet introduced more economic and social on-line activities, for a variety of system's organizations, government agencies, defense industries, industrial projects and school environments. This represents a real change in technological habits when conducting everyday business.

In another context, the emergence of internet and computing paradigms such networking, distributed computing and mobile computing developed an exponential increase of malwares and attacks like spam, data loss and email threat. Besides the knowledge, the identity and the finances are threatened. In this digital age, we need to put attention on the newest advances in information security, privacy and ethics. When we talk about security this implies the cyber security and implies security metrics.

The term "security metrics" is a standard term; it refers to security level, security performance, security indicators or security strength [31]. Security metrics denote the maturity level of the security of system and denote the extent to which security characteristic is present in a system, it denote the security level perception. They are defined as quantifiable measurements of some security aspects and attributes of a system. In another facet, they are tools designed to facilitate decision making. The corrected actions are done according to the observed measurements [40].

Security metric refers to measure the product or service quality. In the open literature a variety of security metrics

are discussed such as the MTTF, MTTD, and MTTE to measure reliability and safety of a given system [5, 6, 33]. Other metrics focus on the correctness, availability, effectiveness and other system's security characteristics [35]. Security metrics for cost benefit analysis are highly recommended when we intend to assess and manage the risk objectively [34] such as SLE [8], ALE, MFC [2, 3, 5]. Metrics are useful in security assurance, auditing activities and in security risk management. They should be meaningful, contextually specific and represent real system's features [35]. They offer a quantitative as well as objective basis for security assurance. In the open literature, criteria for defining security metrics are specified. But in practice, they are relatively reported.

In security a risk is measured in terms of its likelihood of happening and the consequences if it should happen. It is a challenging task if we intend to measure it objectively. Security metrics for cost benefit analysis toward management leads to answer the question: How stakeholders perceived economically security risks and predict how it will change over time?

The proposal is to address the problem of quantifying (assessing, measuring) the security of large scale systems with proper financial analysis of the risk. In the open literature, a financial security metric that quantify the risk in economic term of cost, taking account of a functional specification instead of an architectural specification is not illustrated.

Therefore, a security predictive model needed to be created. It is out of implementation and based on a functional architecture. A new functional security risk management (FSRM) model compatible to the variety of architectures needed to be illustrated, in order to underscore its utility in earlier phases of software development. The model is parameterised in the input using the system's security specifications namely the system's stakeholders, the security requirements, the functional components and the security threats to obtain one output which is the average loss per unit of time ($/H) incurred by a stakeholder as a result of security threats.

Moreover, the risk analysis model requires allowing users and experts to update data. It would also be serving as an explanation tool of the structural relation between security specifications and security cost. It would also be serving as a decision support tool in which it expands security investments. In addition, it needs to be useful for other systems.

In research and practice, little attention has been given to the security of e-learning systems. Indeed, they are threatened by a variety of vulnerabilities attacking examination, certification and privacy. It is strongly recommended to quantify the security and compromised risk of e-learning environments [21, 29].

This paper is organized as follows. In section 2, we present a brief description on security and perceived security. In section 3, we illustrate a background of measuring and managing the risk. In section 4, discuss the functional specification concept. In section 5, we illustrate the novel model's characteristics. In section 6, we present a formulation of the FSRM Model. In section 7, we illustrate an application of the FSRM model to e-learning systems. In section 8, we discuss how this metric can be specialized for a software verification metric. Finally we conclude by summarizing our results and sketching directions of further research.

2. Perceived security: Background

2.1 Security, cybersecurity

The cybersecurity is emerged; its concern is to examine the security of industry, public administration, commerce, and others to protect them against their online presence. For this reason, this current knowledge has grown tremendously. It is defined as the body of policies, emerging measures, metrics and strategies designed to protect networks, computers, and programs from threats.

2.2 What is perceived security?

Perceived security refers to the degree to which an individual feels protected against security threats resulting from the use of specific technology; it is the extent to believe that we are free of risk. Moreover it is the "customers' perception of the degree of protection against these threats. In the literature, they are several perceived factors such perceived usefulness and perceived ease-of-use. Later, trust and perceived risk was introduced by Venkatesh & Bala [19]. According to the Technology Acceptance Model (TAM) the perceived factors such perceived usefulness and perceived ease-of-use affect the behavioral intention consequently the user behavior.

2.3 Perceived security risk

In a system, we need to provide an answer to the question: What degree or level of security does it have now? Perceptions refer to the degree instead of objective measurement and extensively used in e-commerce [19]. A weakness of the colobran's model rises from the subjective measuring. Two professionals could not have the same perception of security [19].

Objective (quantitative) assessment metrics of security risk are continuously recommended and a financial analysis of the risk is required to quantify the security level perception and justify the security improvements [39]. The economic point of view with a financial analysis is included in the security quantification [39]. This concept is called the cost effectiveness metrics. It is studied by Rathbun, Böhme and Freiling, Kanoun et al., Henning et al., Jaquith [35]. The key advantage is to provide an actual dollar amount of security breakdown. Security is monetized in terms of cost which may be lost due to security failure [2, 3, 9]. Thus, we seek a definition of the security risk in monetary terms which is the average loss per unit of time ($/H) incurred by a stakeholder as a result of security threats.

3. Quantifying security, measuring and managing the risk: Background

3.1 Risk

The risk is measured in terms of its likelihood of happening and the consequences if it should happen. It arises out of uncertainty. A risk refers to the possibility of suffering loss. This loss may or may not happen. A risk is the chance of something going wrong as a result of a hazard or a threat which has an impact on operations [14].

3.2 Risk assessment

Risk assessment is the process of estimating the probability of occurrence of an undesirable event and the magnitude of its consequences over a specified time period. Risk assessment is a "hybrid discipline" in which the current state of scientific and technological knowledge is made accessible to society as input to risk management decisions [38].

3.3 Metrics

Metrics are defined as quantifiable measurements of some aspects of a system. It is compared to a scale or benchmark to produce a meaningful result. The term metrics describes a broad category of tools used by decision makers to evaluate data in many different areas of an organization. Thereafter, corrected actions are done according to the observed measurements [40]. Security metrics denote the maturity level of the security of system. And denote the extent to which security characteristic is present in a system. Performance and accountability are improved using collection and analysis of data.

According to Jansen main merits of security metrics are [40]:

- Strategic support: decision making is supported by the assessment of security features. For example, product, service selection and resource allocation.
- Quality assurance: the software development cycle is supported by security metrics, in order to eliminate vulnerabilities. Examples fall into different perspectives such as during code production, during the identification of vulnerabilities and tracking security flaws.
- Tactical oversight: the monitoring and report of security status, the evaluation of the effectiveness of security measures and the management of risk. For example, we provide a practical area improvement.

3.4 Security risk management (SRM) MODELS

Security risk management model are needed to identify risk. Managers focus on minimizing security costs and maximizing security benefits. Comparison of costs among alternative security architectures is significant [36].

Nevertheless, considering a totally secure system is really a challenge. Regarding the real danger, its complex property and the scale of the system [30] implementing security is costly and sometimes ineffective [39].

However, when the system is large, measurement became a challenging task. We are faced to a wide security gap quite difficult to control. Risk quantification is a challenge work, it requires a very big knowledge and it depends on a variety of empirical work collection [22]. The quantification model must take into consideration the variability between the system's stakeholders, the security requirements, the architectural components and the security threats [1, 12, 10, 43]

4. Functional specification

Functional specification is advantageous in risk management when we address a complex system [13]. A system is secure with respect to its functional architecture. For a decision maker, it is interesting to diagnose how important functional variables are or what their value mean for the system's security. In addition, on more complex systems multiple levels of functional specifications may typically resemble each other.

A functional specification contains simpler components, referring elementary functional properties [13] and what has to be implemented. It does not include details of implementations. Functional specification leads to support risk assessment of large systems or complex real-time software systems during early development phases such as analysis and design phases [7, 15]. The representation of risk is more comprehensive.

In the open literature, a financial security metric that quantify the risk in economic term of cost, taking account of a functional specification instead of an architectural specification is not illustrated. In consequence, a quantitative security risk management model that take account of the system's typical stakeholders, their specific security requirements, threats and the functional specification is not illustrated and reported in practice.

This contribution supports the software development; it leads to improve product quality. Developers can identify and handles risks before happening. They can produce an efficient development process [7]. A functional level risk assessment is useful for cost and time reduction. Functional security risk analysis provides useful illustrations on the system project. Stakeholders may negotiate a cost effective process to achieve the needed requirements in order to show:

- The developers how to build.
- The testers how to run a tests.
- The stakeholders how to exploit their stakes

In order to obtain sufficient and credible security evidence during different phases of the system lifecycle, the paper proposes a new approach for measuring security and quantifying the security risk level's perception. The model to be defined shares several characteristics with existing models namely the system's stakeholders, the security requirements and the security threats. The new model distinguishes on the characteristics of perceived security level out of implementation or system's architecture. It is based on a functional specification instead of an architectural specification.

5. The novel model's characteristics

A new predictive functional security risk management model is proposed in order to quantify the security level's perception and the involved level of risk. The model is simple and defines an economic measure that quantifies this risk in terms of financial loss per unit of operation time (for example dollars per hour ($/h)) due to security threats for each stakeholders of such a system.

It is out of implementation and based on a functional architecture. The model is parameterised in the input using the system's security specifications namely the system's stakeholders, the security requirements, functional components and the security threats, to obtain one output which is the average loss per unit of time ($/H) incurred by a stakeholder as a result of security threats.

The obtained values represent how stakeholders perceived economically security risks and predict how it will change over time to implement in advance the needed security strategies. It helps in defining the assets, measuring economically the risk and managing the risk toward decisions making. There is a lack of a quantitative standard model that will assess and analyse risk. Our contribution is a new model of functional level risk assessment which is based on the mean failure cost metric [3, 27, 28] to assess economically the risk:

Quantification will take into account the respective stakeholders, security requirements, security threats and functional components. We proceed as follows as illustrated in Figure 1:

- Step 1: The stake matrix (STR): it is composed with the list of stakeholders and the list of security requirements. Each cell represents loss incurred on requirement.
- Step 2: Elaborating the dependency matrix (RFC): each cell represents probability of failure with respect to a requirement given that a functional component has failed instead of an architectural component.
- Step 3: Elaborating the impact matrix (FCT): each cell represents probability of compromising a functional component instead of an architectural component given that a threat has materialized.
- Step 4: The vector of threat emergences probabilities (T). Each cell represents the probability of realization of each threat, it depends on perpetrator models, empirical data, known vulnerabilities, known counter-measures, etc.

6 Formulation of the FSRM Model

ST is the set of stakeholders, R is a set of requirements, FC is a set of system's applications (functions) and T is a set of threats. We define the functional security risk management FSRM as follow:

$$FSRM = STR^{\circ} RFC ^{\circ}FCT ^{\circ} T$$

1. We denote by ° the matrix multiplication operation.
2. STR is a matrix of size ($|ST|$; $|R|$) that each entry (i; j) represents the value of the stake that stakeholder ST_i has in meeting a requirement R_j. we denote by $|ST|$ (resp: $|R|$) the size of the set ST (resp: $|R|$).
3. RFC is a matrix of size ($|R|$; $|FC|$) that each entry (i; j) represents the probability of failing requirements R_i due to a failure originating from elements FC_j.
4. FCT is a matrix of size ($|FC|$; $|T|$) that each entry (i; j) represents the probability of failing FC_i once the threat T_j has materialized.
5. T is a column vector of size $|T|$ that each entry i represents the probability that threat T_i has materialized during unitary period of time.

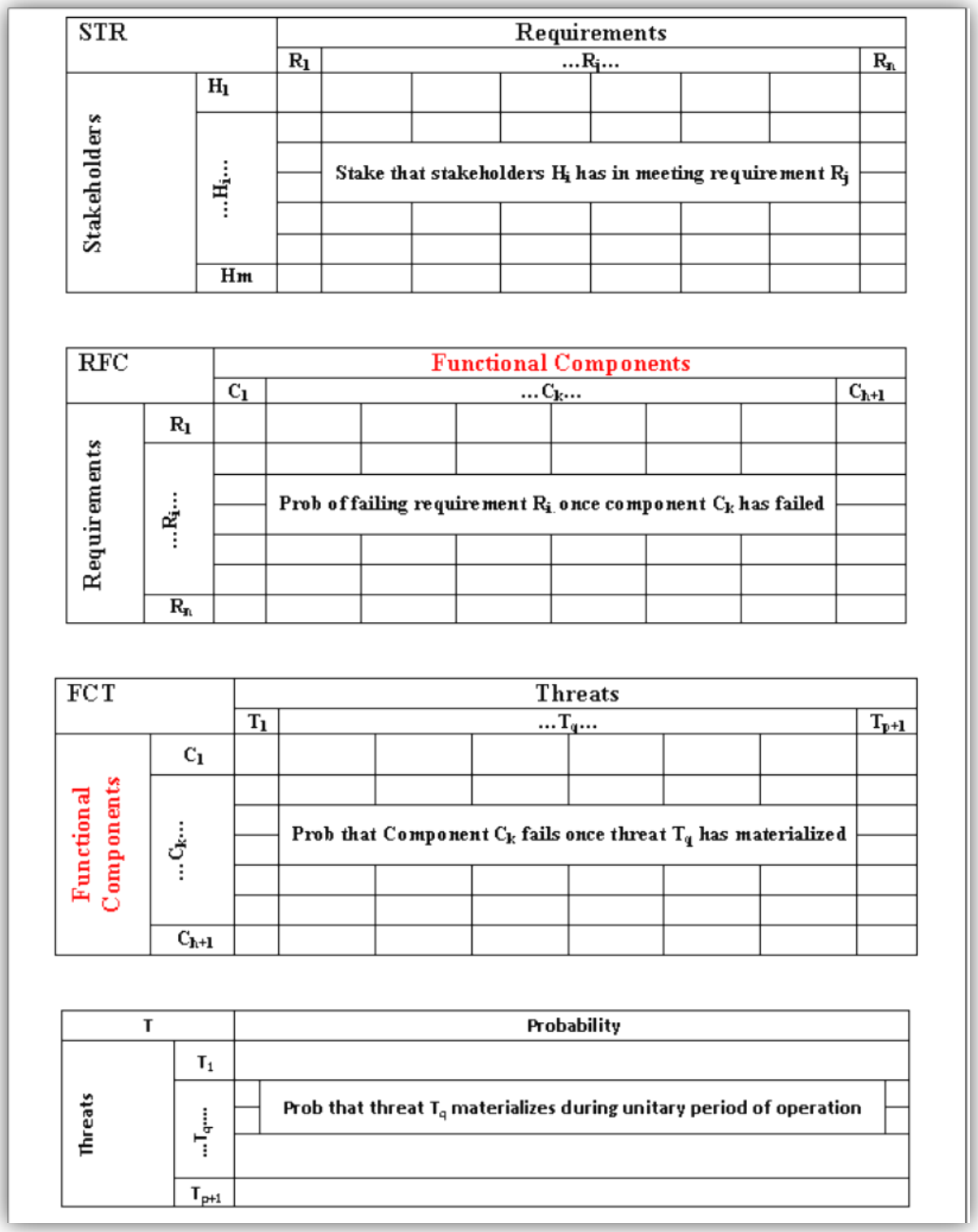

Figure 1. Illustration of the FSRM Model

7 Computing the Functional Security Metric (FSRM): Application in e-learning

In practice, in the e-learning context a variety of e-learning implementations are used such as:

- WebCT: 1997 [11]
- Ilias:1997
- Blackboard: 1997 [20]
- Claroline : 2000
- Moodle : 2002 [1, 37]
- SAKAI : 2004.

Some popular and recommended architecture used the content management system and learning management system (LMS) like Moodle, mooKIT platform for MOOC, Blackboard, LRN and Sakai [1, 11, 37]. Other used the technology of Web Services to solve the problem of interoperability between different e-learning systems [42] such as the iMOOC platform.

The on-line learning management systems or e-learning systems are adopted but without a thorough understanding of the security aspects [29]. Bloggers, practitioners and researchers did not discuss the security as a big issue. In the practice of security risk assurance for e-learning platforms, there was not a quantitative standard model that will effectively assess risks in economic term of cost.

Thus, following the research plan this section proposes new components identification for e-learning systems. It leads to develop a functional security risk management model based on educational assets. We proceed as follows:

1. We define a set of primary stakeholders that are administrator, teacher, student and technician which are applicable to any e-learning product/technology [17].
2. We define all security requirements for any software technology; these have been defined in such a way to encompass all product security requirements. For example, privacy, integrity and availability and their related sub requirements. The mapping of the taxonomy of security requirements in the functional model [26, 27].
3. For the functional components we have studied five primaries inspired by the qualitative risk analysis model [29] which are as the following: virtual library, on-line course administration, course management, registration and communications tool (Table 1).
4. We define security threats and components, values are inferred from the MFC model [23]. The probabilities that a given threat has materialized during a unitary period of operation time are available in Table 3 and Table 5.
5. We derive an original quantitative security risk management metric of current e-learning systems. The FSRM model along with numeric values is presented in Table 6.
6. To validate our model that we obtain, we have used an independent empirical study of the RFC matrix from Mohd Alwi and Fan [29] and used an empirical study of the FCT matrix (Table 4) from [26, 27].

The Functional Security Metric 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 as:

$$FSRM = STR° RFC °FCT ° T$$

Where STR, RFC and FCT are three matrixes, T is a vector

The following empirical data of the STR, RFC matrix and FCT vector are determined from [4]. Values collected to fill them are a combination of collected empirical data and survey from antivirus reports. They used various antivirus security reports like Kaspersky (Kaspersky Security Bulletin The overall statistics), AVG (avg threat report 2012), etc. The data collection took 1 research year to construct the used data base available at [41].

❖ The Stakeholders - Requirements Matrix (STR)

The STR matrix forms the list of the system's stakeholders and the list of security requirements. Each row 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 in dollars incurred and/or premium placed on requirement.

To fill ST Matrix we did a survey for EVT†, which is a Tunisian Virtual School that uses a distant platform to provide coaching and academic support.

In order to collect empirical data related to the used e-learning platforms, each stakeholder estimates and put the stake satisfying a given requirement in quantitative terms of cost per unit like $/hour.

For example, the system administrator estimates his loss as 40 dollars / hour when the system fails to meet the security requirement conformance as shown in Table 2.

We rely on an online survey for data collection available at:

https://docs.google.com/forms/d/1NPT64kSdJhXaWDeBhXft5WQiPYZNHutW5WL2CpU7Fmw/edit?usp=sharing

STR (Hi, Rj): Is the stake that stakeholders Hi has in meeting requirement Rj

† http://www.evt.edunet.tn/

❖ **The Requirements – Functional Components Matrix (RFC)**

Each row for this matrix is filled by System Architects; each cell represents probability of failure with respect to a requirement given that a component has failed.

RFC (Rj, Ck): The probability that the system fails to meet requirement Rj if component Ck is compromise.

❖ **The Functional Components - Threat Matrix (FCT)**

Each row for this matrix is filled by V&V Team; each cell represents probability of compromising a component given that a threat has materialized, it dependent on the target of each threat, likelihood of success of the threat.

FCT (Ck, Th): The probability that Component Ck is compromised if Threat Th has materialized

❖ **The Threat Vector (T)**

Each row for this matrix is filled by Security Team; each cell represents probability of realization of each threat, it dependent 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).

Table 1. Case study of an e-learning functional architecture

Virtual library	Online course admin	Course Management	Registration	Communications tool
VL_1	OCA_1	CM_1	Re_1	COT_1
…				
VL_n	OCA_n	CM_n	Re_n	COT_n

The FSRM model can underline security risk assessment and management of large scale systems and consider all its security sub specifications. It is possible to control the FSRM through its factors in order to minimize and reduce its values. We need to choose the right measures for security priority and decide whether the considered solution is profitable or not.

Our contribution can be generalized to other practical e-systems because an E-learning systems share similar characteristics with other e-systems:

- The accessibility of service via internet,
- The consumption of service by a person via internet,
- The payment of a service by the consumer

In e-learning systems, we are facing a great number of applications such registration, finance, examination, certification, communication tool and others. These applications can be a potential target of hacking or attacks on other online systems. It is crucial to discover the critical assets and to identify the limitations in current systems and to underline factors that affect their quality.

8 Deep analysis about quantification

A recent value based measure of cyber-security is presented, it computes for each stakeholder of the given system his or her loss of operation ($/H). This metric forms a cascade of linear models to quantify security threat in term of loss that results from system vulnerabilities. The financial security measures are the estimation of system security using the loss of a given stakeholder as a result of security breakdown.

The FSRM metrics is characterized in relation to other measures [5] that it takes into account the functional architecture of the system instead of the architectural. It is compatible to the variety of architectures, implementations and platforms such as (cloud, LMS, web service, mobile technology...). This model can be used in common with the variety of implementations and technical specifications. The risk is easily identified and assessed for one system and between different members' risk management processes. Our functional security risk management model will be also a metric for software verification at the early stages of development of large systems or complex real-time software.

We intend to study such similarities, differences and relations between security measurements.

We suggest studying correlation between the quantification of an e-learning system and the quantification of the different functions of the same systems or in different systems. Likewise, measurements between the whole system's quantification and the different function's quantifications are interesting. They reveal dependencies between them which are nearly the sum for the different stakeholders.

The Functional Security Risk Management Model (FSRM) is an original application in e-learning:

A novel model for security risk assessment and management is proposed, which considers the functional specification of a given system. So far, quantification will take account of the respective stakeholders, security requirements, security threats and functional components are instead of architectural components as considered in our previous models. This model may further be expanded to a security metric for software verification out of implementation at the early stages of software's development. In practice, we conduct this metric to e-

learning systems, it could be used as a security risk management metric for the variety of e-learning systems.

Cyber Security metrics may support:

- **The need for operational risk assessments:**

Assessing risk in the business process layer opens up new opportunities for assurance and attestation functions. The risk assessments project leads to a timely incidence and internal audit reports. The operational risk assessment provides new opportunities over auditors' traditional assurance tasks. These new dimensions of potential accounting involvement enrich the business process outsourcing debate and enrich the traditional security accounting.

- **The need of a common security risk analysis:**

The increase of interoperability between methodologies leads to build up a common risk analysis methodology or common language or repository. We have different security risk assessment models qualitative or quantitative, for example EBIOS for France, CRAMM for UK, ITSG-04 for Canada, MAGERIT for Spain. Our need is a common security risk analysis repository of threat, requirements and vulnerabilities identification. This will ensure the capability to continuously asses and manage the risk, to measure the overall security of a network, a crucial issue is to correctly compose the measure of individual components, then to exchange experiences and risk analysis results.

- **The need of a dynamic risk analysis:**

There is a need for dynamic risk assessment. Dynamic risk assessment refers to a risk assessment that can be updated quickly as the system being assessed changes. Possible changes for example may be due to:

- The operational threat level
- The incremental system development
- The deployment phase.

In addition, the dynamic risk analysis refers to the feedback between threats detection tools. In addition, it refers to the results of the initial risk analysis which may identify potential and generally high level threats.

9 Discussion

We illustrate an original quantitative security risk management model based on a functional specification and report it in practice for current e-learning systems. Our purpose is to assess the risk and identify quantitatively the security risk perceptions for the system's stakeholders [24, 25]

Our proposed functional security risk management model illustrated for e-learning systems can be generalized to a generic model while taking into consideration the functional specification of the system. It will be compatible with all architecture platforms such as (cloud, LMS, web service, mobile technology...).

Hence, security assessment and management are easily justified. The technical or no technical decision makers are strongly supported according to a secure functional roadmap. Quantification, analysis and management of e-learning security network may be done according to the new FSRM model. Moreover, our functional security risk management model will be a metric for software verification at the early stages of development.

In addition, the functional level risk assessment model provides a metric on the effectiveness of Verification and Validation tasks in reducing the risk factors associated with software specification modules at the early stages of development. This risk assessment model leads to provide a metric for software verification [16].

In another perspective functional risk assessment models can support the Software Reliability Engineering (SRE) in designing operational user profiles at the early phases of development based on dynamic simulation [16]. Security assets such threats, components and requirements are identified, then the probability that a threat is compromised is estimated, and at the end the risk is defined as a financial metric. Our need is a common security risk analysis repository of threat, requirements [18, 32] and a standard approach for risk management.

When we compare values between risk quantification using an architectural level risk management model [23] and the functional level risk management model, we note that values are practically similar for all stakeholders. The obtained results validate the architectural derived model. We intend to study such similarities, differences and relations between security measurements.

We suggest studying correlation between the quantification of an e-learning system and the quantification of the different functions of the same systems or in different systems. Likewise, measurements between the whole system's quantification and the different function's quantifications are interesting.

Table 2. The STR Matrix

Conformance	Conformance	40	30	10	20
Secure Information Flow	**Secure Information Flow**	**10**	**10**	**0**	**5**
Freshness	**Freshness**	**5**	**2**	**1**	**1**
Fair Exchange	**Fair Exchange**	**10**	**2**	**0**	**2**
Usability	**Reduce risks**	**20**	**20**	**5**	**5**
	Consistent APTs	**20**	**20**	**10**	**10**
	Available security	**20**	**20**	**1**	**7**
	Manageable security	**30**	**0**	**0**	**10**
Attack/Harm Detection	**Attack/Harm Detection**	**30**	**20**	**0**	**10**
Physical Protection	**Physical Protection**	**20**	**10**	**0**	**10**
Access control	**Authorization**	**10**	**30**	**5**	**5**
	Identification	**10**	**30**	**5**	**5**
	Authentication	**10**	**30**	**5**	**5**
Manageability	**Accountability**	**20**	**10**	**2**	**7**
	Security Auditing	**5**	**0**	**0**	**5**
Availability	**Resource allocation**	**22.5**	**22.5**	**1.5**	**7.5**
	Expiration	**22.5**	**22.5**	**1.5**	**3.75**
	Response time	**15**	**15**	**0.75**	**3.75**
Non-repudiation	**Non-repudiation**	**10**	**20**	**0**	**5**
Integrity	**Software Integrity**	**7.5**	**4.44**	**0.38**	**1.47**
	Personal Integrity	**10**	**6.6**	**1.66**	**2.1**
	Hardware Integrity	**5**	**4.44**	**1.66**	**2.1**
	Data Integrity	**7.5**	**4.44**	**0.83**	**1.05**
Privacy	**Traces**	**3**	**0**	**0**	**1.65**
	Cardinality	**6**	**0**	**0**	**3.3**
	Consent and notification	**1.5**	**0**	**0**	**1**
	Attribution	**12**	**0**	**0**	**0**
	Aggregation	**6**	**0**	**0**	**3.3**
	Encryption	**9**	**17.1**	**5**	**2.31**
	Confidentiality	**40**	**20**	**0**	**10**
	Anonymity	**12**	**22.8**	**0**	**3.3**
Security requirements	**Security Requirements Sub factor/**	**Administrator**	**Teacher**	**Student**	**Technician**
			Stakeholders		

Table 3: The RFC Matrix

Security requirements	Security Requirements Sub factor	Functional Components					
		Virtual library	**Online course admin**	**Course Management**	**Registration**	**Communications tool**	**No failure**
Conformance	Conformance	0	$1.66\ 10^{-3}$	$\mathbf{3.32\ 10^{-3}}$	0	$1.66\ 10^{-3}$	$9.93\ 10^{-1}$
Secure Information Flow	Secure Information Flow	$4.2\ 10^{-2}$	$4.2\ 10^{-2}$	$\mathbf{8.4\ 10^{-2}}$	0	$4.2\ 10^{-2}$	$7.9\ 10^{-1}$
Freshness	Freshness	0	$1\ 10^{-3}$	$\mathbf{2\ 10^{-3}}$	0	$1\ 10^{-3}$	$9.97\ 10^{-1}$
Fair Exchange	Fair Exchange	0	$1\ 10^{-3}$	$\mathbf{2\ 10^{-3}}$	0	$1\ 10^{-3}$	$9.97\ 10^{-1}$
Usability	Reduce risks	0	0	**0**	$3\ 10^{-3}$	0	$9.97\ 10^{-1}$
	Consistent APTs	$5\ 10^{-4}$	$5\ 10^{-4}$	$\mathbf{10\ 10^{-4}}$	0	$5\ 10^{-4}$	$9.97\ 10^{-1}$
	Available security	$3\ 10^{-3}$	$3\ 10^{-3}$	$\mathbf{6\ 10^{-3}}$	$3\ 10^{-3}$	$3\ 10^{-3}$	$9.82\ 10^{-1}$
	Manageable security	0	$3\ 10^{-3}$	$\mathbf{6\ 10^{-3}}$	$3\ 10^{-3}$	$3\ 10^{-3}$	$9.85\ 10^{-1}$
Attack/Harm Detection	Attack/Harm Detection	0	$24.4\ 10^{-3}$	$\mathbf{48.8\ 10^{-3}}$	0	$24.4\ 10^{-3}$	$9.024\ 10^{-1}$
Physical Protection	Physical Protection	0	$0.7\ 10^{-3}$	$\mathbf{1.4\ 10^{-3}}$	$0.7\ 10^{-3}$	$0.7\ 10^{-3}$	$9.965\ 10^{-1}$
Access control	Authorization	0	$4.2\ 10^{-3}$	$\mathbf{8.410^{-3}}$	$4.2\ 10^{-3}$	$4.2\ 10^{-3}$	$9.79\ 10^{-1}$
	Identification	0	$4.2\ 10^{-3}$	$\mathbf{8.410^{-3}}$	$4.2\ 10^{-3}$	$4.2\ 10^{-3}$	$9.79\ 10^{-1}$
	Authentication	0	$4.2\ 10^{-3}$	$\mathbf{8.4\ 10^{-3}}$	$4.2\ 10^{-3}$	$4.2\ 10^{-3}$	$9.79\ 10^{-1}$
Manageability	Accountability	$3\ 10^{-3}$	$3\ 10^{-3}$	$\mathbf{6\ 10^{-3}}$	$3\ 10^{-3}$	$3\ 10^{-3}$	$9.82\ 10^{-1}$
	Security Auditing	$3\ 10^{-3}$	$3\ 10^{-3}$	$\mathbf{610^{-3}}$	$3\ 10^{-3}$	$3\ 10^{-3}$	$9.82\ 10^{-1}$
Availability	Resource allocation	0	$3.3\ 10^{-3}$	$\mathbf{6.6\ 10^{-3}}$	0	$3.3\ 10^{-3}$	$9.868\ 10^{-1}$
	Expiration	$3.3\ 10^{-3}$	$3.3\ 10^{-3}$	$\mathbf{6.6\ 10^{-3}}$	$3.3\ 10^{-3}$	$3.3\ 10^{-3}$	$9.802\ 10^{-1}$
	Response time	$3.3\ 10^{-3}$	$3.3\ 10^{-3}$	$\mathbf{6.6\ 10^{-3}}$	$3.3\ 10^{-3}$	$3.3\ 10^{-3}$	$9.802\ 10^{-1}$
Non-repudiation	Non-repudiation	$2\ 10^{-2}$	$3.3\ 10^{-2}$	$\mathbf{3.3\ 10^{-2}}$	$1\ 10^{-2}$	$3.3\ 10^{-2}$	$8.71\ 10^{-1}$
Integrity	Software Integrity	$7\ 10^{-3}$	$7\ 10^{-3}$	$\mathbf{14\ 10^{-3}}$	$7\ 10^{-3}$	$7\ 10^{-3}$	$9.58\ 10^{-1}$
	Personal Integrity	0	0	**0**	0	0	1
	Hardware Integrity	0	$7\ 10^{-3}$	$\mathbf{14\ 10^{-3}}$	$7\ 10^{-3}$	$7\ 10^{-3}$	$9.65\ 10^{-1}$
	Data Integrity	0	$7\ 10^{-3}$	$\mathbf{14\ 10^{-3}}$	0	$7\ 10^{-3}$	$9.72\ 10^{-1}$
Privacy	Traces	0	0	**0**	$3.33\ 10^{-2}$	0	$9.667\ 10^{-1}$
	Cardinality	0	0	**0**	0	0	1
	Consent and notification	0	0	**0**	0	0	1
	Attribution	0	0	**0**	0	0	1
	Aggregation	0	0	**0**	0	0	1
	Encryption	0	0	**0**	0	0	1
	Confidentiality	$2\ 10^{-2}$	$3.33\ 10^{-2}$	$\mathbf{8.33\ 10^{-2}}$	$1\ 10^{-1}$	$3.33\ 10^{-2}$	$7.3\ 10^{-1}$
	Anonymity	0	0	**0**	0	0	1

Table 4: The FCT matrix

Threats Components	BroA	InsC	DoS	CryptS	DOR	InfL	Buff	CSRF	CSS	FURL	InjecF	MFile	No Threats
Virtual library	0,000	0,000	0,0195	0,978	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
Online course admin	0,090	0,231	0,231	0,000	0,099	0,000	0,066	0,002	0,004	0,140	0,132	0,000	0,000
Course Management	**0,206**	**0,103**	**0,135**	**0,000**	**0,135**	**0,069**	**0,135**	**0,005**	**0,000**	**0,191**	**0,010**	**0,022**	**0,000**
Registration	0,108	0,000	0,235	0,231	0,198	0,000	0,023	0,000	0,000	0,000	0,000	0,000	0,000
Communications tools	0,165	0,000	0,176	0,176	0,132	0,012	0,314	0,003	0,000	0,000	0,008	0,002	0,000
No Failure	0,793	0,769	0,764	0,022	0,802	0,930	0,685	0,994	0,995	0,808	0,868	0,997	1,000

Table 5: The T Vector

Threats	**Probability**
Broken authentication and session management (BroA)	$4.20\ 10^{-3}$
Insecure communication (InsC)	$3.00\ 10^{-3}$
Denial of service (Dos)	$3.08\ 10^{-3}$
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)	$9.80\ 10^{-3}$
Injection flaws (InjecF)	$2.17\ 10^{-3}$
Malicious file execution (MFile)	$5.04\ 10^{-4}$
No Threats	$974.44\ 10^{-3}$

Table 6: Mean Failure Cost based on an e-learning functional architecture

Stakeholders	**FSRM** for e-learning systems
System administrator	645,162
Teacher	456,572
Student	81,991
Technician	209,429

10 Conclusion

This paper illustrates an original theoretical and practical contribution which is benefic to the top security managers or providers of e-learning systems. Also, it leads to improve and support the knowledge of measurements and risk management for other systems:

We develop a new functional security risk management model (FSRM). It is compatible with the different architectures, implementations and platforms such as (cloud, LMS, web service, mobile technology and MOOC...). This model can be used in common with the variety of implementations and technical specifications. The risk is easily identified, assessed, managed and perceived for one system and between different members' risk management processes. Our functional security risk management model will be also a metric for software verification at the early stages of development of large systems or complex real-time software.

Our Future works focus on developing a functional security risk analysis model for every system's function. It is useful for future empirical reuse and security asset's identification. This information can also be used to provide feedbacks at the modelling layer.

REFERENCES

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

[2] A. B. 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), ACM International Conference, 2010.

[3] A. B. Aissa, R. K. Abercrombie, F. T. Sheldon, and A. Mili, Defining and Computing a Value Based Cyber-Security Measure, Information Systems and e-Business Management Volume 10, Issue 4 , pp 433-453 , 2012-12-01, DOI: 10.1007/s10257-011-0177-1, Springer-Verlag, 2012.

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

[5] A. Mili and F.T. Sheldon, Measuring Reliability as a Mean Failure Cost, in Proc. HASE, pp.403-404, 2007.

[6] A. Mili, and F. T. Sheldon, 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, pp. 10, 2009.

[7] A.Tangsuksant, and N. Prompoon, Risk assessment using functional modeling based on object behavior and interaction. In The 4th international Joint Conference on Computer Science and Software Engineering, Khon Kaen, 2007.

[8] B. Karabacak, I. Sogukpinar, ISRAM: information security risk analysis method, Computer and Security, Elsevier. Vol 24, pp. 147-159, 2005.

[9] D. L. Nazareth and J. A. Choi: System Dynamics Model for Information Security Management. Information and Management. Elsevier, 2014.

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

[11] E.W.T. Ngai, J.K.L. Poon, and Y.H.C. Chan, Empirical examination of the adoption of WebCT using TAM, Computers and Education, Elsevier vol. 48, pp. 250-267, 2007.

[12] F. Alkhateeb, E. AlMaghayreh, S. Aljawarneh, Z. Muhsin, and A. Nsour. E-learning Tools and Technologies in Education: A Perspective. E-learning, 2010.

[13] F. T. Sheldon, R. K. Abercrombie, and A. Mili, Methodology for Evaluating Security Controls Based on Key Performance Indicators and Stakeholder Mission, IEEE Proceedings of the 42nd Annual Hawaii International Conference on System Sciences (HICSS-42), (CD-ROM), Waikoloa, Big Island, Hawaii, January 5-8, 2009, Computer Society Press, 2009.

[14] Final Report of Task Group IST-049, Improving Common Security Risk Analysis, 2008.

[15] H. H. Ammar, T. Nikzadeh and J. B. Dugan, A methodology for risk assessment of functional specification of software systems using colored petri nets. In Software Metrics Symposium, 1997 Proceedings Fourth International (pp. 108-117), IEEE, 1997.

[16] H. H. Ammar, T. Nikzadeh and J. B. Dugan, A methodology for risk assessment of functional specification of software systems using colored petri nets. In Software Metrics Symposium, 1997 Proceedings Fourth International (pp. 108-117), IEEE, 1997.

[17] L. B. A. Rabai, N. Rjaibi, and A. B. Aissa, Quantifying Security Threats for E-learning Systems, IEEE Proceedings of International Conference on Education and E-Learning Innovations- Infrastructural Development in Education (ICEELI' 2012- http://www.iceeli.org/index.htm), July 1-3, Sousse, Tunisia, Page 482 487, 2012.

[18] L.Wang, A. Singhal, and S. Jajodia, Toward measuring network security using attack graphs. In Proceedings of the 2007 ACM workshop on Quality of protection (pp. 49-54). ACM, 2007.

[19] M. Colobran, Modeling human perceived security: A conceptual framework and its application to health, Computers in Human Behavior, 2016.

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

[21] M. Nickolova, E. Nickolov, Threat Model For User Security In E-Learning Systems, International Journal Information Technologies and Knowledge, 1(1), 341-347, 2007.

[22] N. Rjaibi and A. B. Aissa, The empirical data base for quantifying security threats. Retrieved Jan, 2013, from https://docs.google.com/file/d/0B0Z2laATxEo7Tlk2TGd4elJjNFk/Edit

[23] N. Rjaibi and L. B. A. Rabai, Expansion And Practical Implementation of The MFC Cybersecurity Model via a Novel Security Requirements Taxonomy, International Journal of Secure Software Engineering (IJSSE), 6(4), 32-51, October-December 2015.

[24] N. Rjaibi and L. B. A. Rabai, Functional specification to support security risk assessment of large systems, 7th Computer Science On-line Conference 2018 (CSOC 2018), April 25-28, 2018, the Springer Series: Advances in Intelligent Systems and Computing, Springer

[25] N. Rjaibi and L. B. A. Rabai, New classification of Security Requirements for Quantitative Risk Assessment, Analyzing the Role of Risk Mitigation and Monitoring in Software Development, IGI Global, Analyzing the Role of Risk Mitigation and Monitoring in Software Development. IGI Global, 2018. 100-117. Web. 20 Jun. 2018. doi:10.4018/978-1-5225-6029-6.ch007

[26] N. Rjaibi, L. B. A. Rabai, A. B. Aissa and A. Mili, Mean failure Cost as a Measurable Value and Evidence of Cyber security: E-learning Case Study, International Journal of Secure Software Engineering (IJSSE), Vol 4, Issue 3, September-December 2013.

[27] N. Rjaibi, L. B. A. Rabai, A. B. 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.

[28] N. Rjaibi, L. B. A. Rabai, H. Omrani, A. B. 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, CSREA Press, pp. 520-526, 2012.

[29] N.H. MohdAlwi, and I.S. Fan, E-Learning and Information Security Management, International Journal of Digit Society (IJDS), vol. 1, no. 2, 2010.

[30] P. Feiler, R. Gabrielp, J. Goodenough, et al. Ultra-large-scale systems: The software challenge of the future. Software Engineering Institute, vol. 1, 2006.

[31] R. Böhme, Security Metrics and Security Investment Models, In Advances in Information and Computer Security (pp. 10-24). Springer Berlin Heidelberg, 2010.

[32] R. Bojanc, B. Jerman-Blazic, An economic modelling approach to information security risk management. International Journal of Information Management, 28(5), 413-422, Elsevier, 2008.

[33] R. K. Abercrombie, F. T. Sheldon, and A. Mili, Managing Complex IT Security Processes with Value Based Measures, Proceedings of 2009 IEEE Symposium on Computational Intelligence in Cyber Security (CICS '09), Nashville, TN, April 1, 2009.

[34] R. M. Savola, A Security Metrics Taxonomization Model for Software-Intensive Systems, Journal of Information Processing Systems, Vol.5, No.4, 197-206, December 2009.

[35] R. Savola, On the Feasibility of Utilizing Security Metrics in Software-Intensive Systems, International Journal of Computer Science and Network Security, VOL.10 No.1 230-239, January 2010.

[36] S. A. Butler, Security attribute evaluation method: a cost-benefit approach. In Proceedings of the 24th international conference on Software engineering (pp. 232-240). ACM, 2002.

[37] 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.

[38] S. Myagmar Adam, J. Lee William Yurcik, Threat Modeling as a Basis for Security Requirements, In Symposium on Requirements Engineering for Information Security, 2005.

[39] U.Saluja and N. B. Idris, Information Risk Management: Qualitative or Quantitative? Cross industry lessons from medical and financial fields, Journal of Systemics, Cybernetics and Informatics, 10(3), 2012.

[40] W. A. Jansen, NIST IR 7564: Directions in security metrics research, National Institute of Standards and Technology, US Dept. of Commerce, Gaithersburg, 2009.

[41] Web PAGE : https://docs.google.com/file/d/0B0Z2laATxEo7Tlk2TGd4elJjNFk/edit

[42] X. Liu, A. E. Saddik and N. D. Georganas, An implementable architecture of an e-learning system, CCECE 2003-CCGEI 2003, Montreal, IEEE, 2003.

[43] Z. A. Khanjari, S. Kutti, and M. Hatem, An Extended E-learning System Architecture: Integrating Software Tools within the E-learning Portal, The International Arab Journal of Information Technology, vol. 3, no.1, January 2006.