Abstract – As for the relevance of using E-learning as a kind of modern education for schools and business throughout the world, the support of the newest technological components is important. In contrast, the integrity of this cyber system has become more critical. Security of E-learning systems is a current issue that needs to be highlighted to guarantee educational process with higher quality and to maintain its well running. Nevertheless, considering a total secure system is really a challenge. Security assessment policy and metrics are recommended, they serve as a guideline to the issues related to the availability, reliability, integrity, and confidentiality of the online teaching/learning system. In this paper, we illustrate a rigorous cyber security measure to quantify security threats which is the Mean Failure Cost for E-learning systems and then we propose an extension of its formula to measure the critical security requirements. Our focus is to enrich the MFC measure in order to develop a comprehensive science of cyber security and to get more safe and effective systems.

Keywords: Critical security requirements, cyber security metrics, risk management, E-learning, Mean Failure Cost.

1 Introduction

In today's Internet age, education requires the share and the distribution of information. E-learning has become a popular way of learning for schools and business and has increased exponentially in recent years [1]. According to Derek Stockley [2], it is the delivery of a learning, training or education program by electronic means like computers or electronic devices (e.g. mobile phones).

Nickolova and Nickolov [3] suggest that there was a great progress in the use of E-learning as a new way of distributing knowledge, this is justified from the perspective of developing E-learning software applications and portals with no constraint of time and space resulting expansion of mobile learning this day. Among the advantages of E-learning systems we note the rapid and efficient distribution of learning resources, the flexibility in communication and collaboration without time force.

E-learning systems are vulnerable; the serious security threats include software attacks (virus, worms, macros, denial of service), data espionage, acts of theft (illegal equipment or information) and intellectual property (piracy, copyright, infringement) [4]. Cyber security is emerging as a major concern for researchers and practitioners, dealing as it does with privacy, confidentiality, user authentication, etc.

Given the exponential increase of security threats, to guarantee educational process with higher quality [5, 6], to maintain the perfect running of the system and to learn in safe, we need strong security risk management approaches. Actually, these approaches are fundamental in assessing security risk and provide us with good plan for risk mitigation.

Quantitative models are provided to measure reliability and safety of a given system [7, 8 and 9] like the mean failure cost (MFC), the Mean Time to Failure (MTTF), the mean time to detection of vulnerability (MTTD), and the mean time to exploitation of vulnerability (MTTE). These models are adopted to measure security dependability.

To the best of our knowledge, the MFC measure presented in [7, 10 and 11] is a rigorous suitable cyber security measure which presents several benefits. In fact the MFC is advantageous in comparison with other known approaches of security threat metrics, it reflects variance between system stakeholders, one user can attach different stakes regarding the same security requirement [13]. It considers the variance in failure cost from one sub-specification to another, the variance in failure probability from one sub-specification to another and the variance in failure cost from one stakeholder to another [9]. The MFC takes into account complex system specifications, and considers variations by stakeholder, requirements, components, and threats in order to adopt a good quantified security threat measure.

The MFC model provides excellent knowledge about the loss that each stakeholder stands as a result of security breakdowns [8, 12 and 14].

The MTTF has some inconveniences comparing to the MFC system reliability measure [7]:

- Independence of failure cost with respect to sub specificities: The MTTF makes no distinction between requirements
- Independence with respect to stakeholders: It is not dependent on the stakeholder but depends exclusively on the system under observation.
• Independence of failure probability with respect to sub specificities: any failure with respect to any sub specificity is a failure with respect to the whole specificity

The MTTD and the MTTE present the same shortcomings, they form an abstract measure of the failure rate of the considered system. In front of the proposed limits of the MTTF measure, the MFC is the best solution to measure system security reliability; It can be applied to manage and quantify security threats of all E-systems like E-Commerce, E-learning, and E-Government. It is independent from the system but varies from a stakeholder to another [13]. We illustrate in this paper a simple E-learning application to compute it in a practical case study.

Results of security threats analysis may also be useful in a practical plan to provide us with pertinent information in order to implement a secure environment. In the science of cyber security except the assessment of the risk, other challenges are required, especially in a complex system we need the knowledge of the critical security requirements in quantitative way. Hence, we propose in this paper an expansion of the MFC formula to underline the estimation of critical security requirements.

Nowadays, security requirements become an important issue in information systems, it improves the quality of software process and products. Security requirements are considered as the level of protection necessary for equipment, data, information and applications to meet security policy.

Measuring in a structured way the critical security requirements regarding the complexity of a given architecture system is beneficial to make more effective system in the development phase and in earlier phases. A well defined security process is advantageous and a well defined security requirements plan is recommended.

This paper is organized as follows. In section 2, we present the MFC cyber security metric, in section 3, we illustrate the threats quantification of the MFC for E-learning systems. In section 4, we discuss and compute the critical security requirements using an extension of MFC formula. Finally, in section 5, we conclude by summarizing our results, and sketching directions of further research.

2 The mean failure cost as a measure of cyber security

The Mean failure Cost is a recent value based measure of cyber-security, presented in [9, 11 and 9], it 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 addition, Anis et al [15] implemented a tool that automatically computes the MFC for a given system, it calculates MFC metrics. They define the MFC as:

\[ \text{MFC} = \text{ST} \cdot \text{DP} \cdot \text{IM} \cdot \text{PT} \]  

Where ST, DP and IM are three matrixes, PT is a vector:

• The stake matrix (ST) is filled by stakeholders according to the stakes they have in satisfying individual requirements;
• The dependency matrix (DP) 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;
• The impact matrix (IM) is filled by analysts according to how each component is affected by each threat;
• The vector of threat 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.

The whole details of the MFC features are presented in the summarized table 1.

3 Computing mean failure cost for E-learning system

3.1 The stakes matrix (ST)

The stakes matrix composed with the list of four stakeholders and the list of security requirements [15]. The four needed actors that interact with each other are presented as follows:

• The system administrator: provides the file-level access for each teacher, the one course should have a single directory on the server. It is the person who maintains and operates the system. In consequence, he forms a technical director of the platform and the network administrator [16].
• The teacher: guides and tutors learners to meet educational goals. He varies the knowledge using different formats. He also needs to communicate with the learner using synchronous or asynchrony communication tools [5, 17].
• The student: is the engine of the learning process. He searches to learn, communicate, discover and analyze knowledge [5, 16].
• The technician: is the responsible for the minor change of the site like the update of themes, the installs of modules, and the upgrade of system software [18].
<table>
<thead>
<tr>
<th><strong>MFC</strong></th>
<th>• Is a vector</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Entries = system stakeholders</strong></td>
<td></td>
</tr>
<tr>
<td><strong>MFC(H)</strong></td>
<td><strong>Is the mean failure cost of stakeholders= cost ($/H)</strong></td>
</tr>
<tr>
<td><strong>ST: Stake matrix</strong></td>
<td>• Is a matrix</td>
</tr>
<tr>
<td><strong>Rows= stakeholders</strong></td>
<td><strong>ST(H,R)</strong></td>
</tr>
<tr>
<td><strong>Columns= security requirements</strong></td>
<td>• Is the stake that stakeholders H satisfy a requirement R</td>
</tr>
<tr>
<td><strong>Is quantified in terms of cost per unit of operation time:</strong>$/Hour**</td>
<td></td>
</tr>
<tr>
<td><strong>DP: Dependability matrix</strong></td>
<td>• Is a matrix</td>
</tr>
<tr>
<td><strong>Rows= security requirements</strong></td>
<td><strong>DP( R,C)</strong></td>
</tr>
<tr>
<td><strong>Columns= system components</strong></td>
<td>The probability that the system fails to meet requirement R if component C is compromise</td>
</tr>
<tr>
<td><strong>IM : Impact matrix</strong></td>
<td>• Is a matrix</td>
</tr>
<tr>
<td><strong>Rows= system components</strong></td>
<td><strong>IM(C,T)</strong></td>
</tr>
<tr>
<td><strong>Columns= security threat</strong></td>
<td>The probability that Component C is compromised if Threat T has materialized</td>
</tr>
<tr>
<td><strong>PT : Vector of probability</strong></td>
<td>• Is a vector</td>
</tr>
<tr>
<td><strong>Entries: Threat</strong></td>
<td><strong>PT(T)</strong></td>
</tr>
<tr>
<td></td>
<td>The probability that threat T materialized for a unit of operation time (one hour of operation)</td>
</tr>
</tbody>
</table>

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 [3, 4]. According to [19], we can classify the following basic security requirements of the E-learning system 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 to give him the right to access to the application with his own account [17].

- **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 [20].

- **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 [21].

- **Availability:** Availability of the application is a very important subject, so it is required to ensure that the web application is always available and operational when the user needs it [20, 21].

- **Non-repudiation:** Needs 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 [19].

- **Privacy:** Is necessary to ensure non-disclosure of information given and for each user. [19]

Each row for the matrix presented in table 2 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 EVT1. ST (Hi, Rj): Is the stake that stakeholders Hi has in meeting requirement Rj.

### 3.2 The dependability matrix (DP)

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 [16] they are not a unique architecture for E-learning system, so, 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. [22] we recognize six architectural components as follow:

The browser: is the interface used by the client [22].

The Web server: hosts the Content Management System (CMS) Applications for managing students and their academic and financial situations, it covers the module of the related E-learning system, it includes themes, activities, interface languages, database schemas and course formats. It also includes the management and labeling of objects. Other modules can incorporate the learner registration component which forms the administration components, then, it covers the tools that assist the creation of objects (content) [17, 22].

Application server: incorporates the E-learning system 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. It covers the Learning Activity Management System (LAMS), it is used for designing, managing and delivering online collaborative learning activities. Therefore this is the useful environment for creating sequences of learning activities [17, 22].

Database server: is the core (default) database and some extension tables of the E-learning system as the user administration data base [22].

Firewall server: is the component that secures Internet input and output traffic, it also filters high-risk codes, such as viruses or worms [17].

Mail server: considering the increase number of users and stored message, the mail server covers the email application, user’s mail boxes [17].

Each row for the matrix presented in table 3 is filled by System Architects; 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 [23].

3.3 The impact matrix (IM)

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 (portal) 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 system nodes to have the same communication at any given time. As noted in [4] a system can be attacked by a lot of threats that we can summarize the most important as follow:

- Viruses (VS),
- Denial of service (DoS),
- Acts of human error or failure (accidents, employee mistakes) (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 from service providers (QoS),
- Blackmail for information disclosure (BID).

Each row for the matrix presented in table 4 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. To fill this matrix we have used the values from [23]. IM (Ck, Th): The probability that Component Ck is compromised if Threat Th has materialized.

3.4 The threat vector (PT)

Each row for this vector presented in table 5 is filled by Security Team; each cell represents the probability of realization of each threat, it depends on perpetrator models, empirical data, known vulnerabilities, known countermeasures, etc.

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

<table>
<thead>
<tr>
<th>Stakeholders</th>
<th>Confidentiality</th>
<th>Integrity</th>
<th>Availability</th>
<th>Non-repudiation</th>
<th>Authentication</th>
<th>Privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>System administrator</td>
<td>40</td>
<td>30</td>
<td>60</td>
<td>10</td>
<td>10</td>
<td>50</td>
</tr>
<tr>
<td>Teacher</td>
<td>20</td>
<td>20</td>
<td>60</td>
<td>20</td>
<td>30</td>
<td>40</td>
</tr>
<tr>
<td>Student</td>
<td>0</td>
<td>5</td>
<td>5</td>
<td>0</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>Technician</td>
<td>10</td>
<td>7</td>
<td>15</td>
<td>5</td>
<td>5</td>
<td>15</td>
</tr>
</tbody>
</table>
Using this data, we compute the vector of MFC presented in table 6 using the formula: $\text{MFC} = \text{ST} \times \text{DP} \times \text{IM} \times \text{PT}$

The MFC for stakeholders can appear insignificant but for a failure to long-term they are significant. While our focus so far has been on measuring mean failure cost, we discuss in the next section how to found and compute the critical security requirement using an extension of MFC formula.

Using this data, we compute the vector of MFC presented in table 6 using the formula: $\text{MFC} = \text{ST} \times \text{DP} \times \text{IM} \times \text{PT}$

The MFC for stakeholders can appear insignificant but for a failure to long-term they are significant. While our focus so far has been on measuring mean failure cost, we discuss in the next section how to found and compute the critical security requirement using an extension of MFC formula.
4 MFC Extension: computing critical security requirements

In the stake matrix \( ST \), we have introduced the costs that can be lost by the stakeholders. The stakes depend on the stakeholders and the security requirements. The MFC vector is the mean failure cost of system / stakeholder during a unit of operating time. The values of MFC don’t distinguish between the low and the high cost of security requirement for the global system. In this section we introduce a new extension of the MFC formula to define which requirement is more critical than the others.

We consider a system \( S \), we let \( H_1, H_2, \ldots, H_K \) be stakeholders of system and \( R \) one of the security requirements of system. Let \( MFC_R \) be the random variable that represents the mean failure cost of the requirement \( R \). We let \( PR \) the probability that the system fail to meet the requirement \( R \).

We quantify this random variable in term of financial loss per unit of operation time. If we suppose that we have \( k \) stakeholders the stake matrix can be presented as a vector.

\[
\begin{array}{c|c}
\text{Stakeholders} & \text{Stake that stakeholders} \\
\text{H}_1 & \text{H}_i \ldots \text{H}_m \text{ has in meeting} \\
\text{requirement } R & \\
\end{array}
\]

We consider the architecture of system \( S \) and let \( C_1, C_2, \ldots, C_h \) be the components. Using the same principle of dependency matrix and under the constraint that we have one requirement \( R \), the stake matrix can be presented as a linear vector.

\[
\begin{array}{|c|c|}
\hline
\text{DP'} & \text{Components} \\
\hline
\text{C}_1 & \ldots \text{C}_k \ldots & \text{C}_{h+1} \\
\hline
\text{R} & \text{Prob of failing requirement } R, \text{ once component } C_k \text{ has failed} \\
\hline
\end{array}
\]

Taking the same impact matrix \( IM \) and the threat vector \( PT \), the mean failure cost of the requirement \( R \) can be written as:

\[
MFC_R = \left( \sum_{i=1}^{f} MFC_i \right)
\]

Applying the above formula, we can define the MFC for each security requirement and which requirement is more critical than the others.

<table>
<thead>
<tr>
<th>Security Requirements</th>
<th>Mean $/hour</th>
<th>Failure Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality</td>
<td>0.294</td>
<td></td>
</tr>
<tr>
<td>Integrity</td>
<td>0.359</td>
<td></td>
</tr>
<tr>
<td>Availability</td>
<td>0.580</td>
<td></td>
</tr>
<tr>
<td>Non-repudiation</td>
<td>0.099</td>
<td></td>
</tr>
<tr>
<td>Authentication</td>
<td>0.210</td>
<td></td>
</tr>
<tr>
<td>Privacy</td>
<td>0.441</td>
<td></td>
</tr>
</tbody>
</table>

As it’s appearing in table 7, the availability and the privacy are the most important security requirements in the proposed E-learning system.

When we talk about availability, the most known concerned attack is the denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services in the platform. There are two types of DoS attack: logic and flooding attacks. Logic attacks (e.g. ping) exploit existing LMS flaws to crash remote server or significantly decrease its performance. Flooding attacks overloads LMS with a high number of requests to disable legitimate users from accessing E-learning resources [21]. According to the MFC metric and especially the IM matrix the application server, the firewall server and the database server need more precious practical instruments of security.

About privacy, it is the non-disclosure of information for each user [19]. Security guidelines in the development phase are required to protect the privacy of student and teacher personal records, the protection of their personal information when using E-learning services is primordial.

5 Conclusion

E-learning becomes a popular way of learning for schools and business and has increased exponentially in recent years. To guarantee educational process with higher quality, to maintain the perfect running of the system and to learn in safe, we require the illustration of the MFC as a strong cyber security risk measure.

The MFC is advantageous in comparison with other know metrics of security, reliability and safety:
• It reflects variance between system stakeholders, one user can attach different stakes regarding the same security requirement

• It considers the variance in failure cost from one sub specification to another, the variance in failure probability from one sub-specification to another and the variance in failure cost from one stakeholder to another.

• It takes into account complex system specifications, and considers variations by stakeholder, requirements, components, and threats in order to adopt a good quantified security threat measure.

In addition, our extension of the MFC formula to measure the critical security requirements is beneficial to a better management, assessment and control of the non secure system. These theoretical and practical improvements lead to the enrichment of the MFC application, to provide more comprehensive science of cyber security and their related metrics, especially to interpret in the deep and to get more safe and effective systems. Besides, the quantification of security threats and their impact throughout a financial measure open a wide range of further interpretation.

6 References


