Vulnerability Assessment in Quantitative Risk Management Methodologies
State-of-the-Art and Challenges

Raed Labassi and Mohamed Hamdi
Engineering school of communications, Techno-parc El Ghazala, Route de Raoued, Ariana, 2083, Tunisia

1 STAGE OF THE RESEARCH

The ubiquitous use of information and communication technologies has resulted in more dependency on digital infrastructures. The proliferation of information systems and communication networks had certainly enabled a substantial progress in many aspects of the daily life but it also had opened the possibilities for malicious users to exploit their weaknesses. Thus, there are new risk factors that have huge implications such as economic dependency on the information and communication systems security (CSI, 2010). Vulnerability assessment is one key step in the quantitative risk management approach. Nowadays, analyzing information system vulnerabilities is one of the main operations in a day-to-day workload of security professionals and a crucial step in a quantitative risk management lifecycle. Mitre's CVE/CWE databases (Mitre, 2012) and OSVDB database (OSVDB, 2013) are examples of libraries whose large use among security products, aimed at big companies and organizations, shows the importance of vulnerability assessment in the risk management task.

Assessing information system vulnerabilities enables security professionals to design accurate threat scenarios based on concrete data. The complexity of several risk analysis tasks is due to the identification of security weaknesses and vulnerabilities. This operation is either disregarded, leading to a wide spectrum of threats that are very complex to assess and quantify, or relies on complex methodologies which are rarely assisted by a software solution.

The present paper provides a state-of-the-art of the vulnerability assessment step in quantitative risk analysis methods. These methods have been using different vulnerability assessment techniques. It should be noted that some methods do not even have a vulnerability assessment step. The techniques proposed by risk analysis methodologies have several shortcomings: (a) a limited vulnerability spectrum, (b) reliance on mathematical abstractions which may fail to translate the reality of the security level of an information system, (c) approximations which may not provide an accurate quantification of risks.

2 OUTLINE OF OBJECTIVES

The objectives of the paper are structured as follows: First, the vulnerability assessment step of several quantitative risk management methodologies is analyzed using state-of-the-art Sahinoglu's Security Meter model and NetRAM's vulnerability assessment techniques, in addition to other quantitative approaches found in the literature. Second, some shortcomings in these approaches are investigated. Then, a vulnerability assessment technique, which may correct these shortcomings, is proposed. Finally a conclusion suggests further research in the field.

3 RESEARCH PROBLEM

3.1 Evolution of IT Vulnerabilities

Classical security audits or penetration tests do not provide the best evaluation of security weaknesses and vulnerabilities of a system or a network. Their results may no longer be valid when the target is modified (a new element is added, a change in the architecture is performed, etc.). They only provide a static picture of the security level at a given moment. They are only a snapshot of the security level by evaluating parameters supposed to be static, such as software and hardware configurations, source codes of applications and procedures and processes.

Labassi R. and Hamdi M..
Vulnerability Assessment in Quantitative Risk Management Methodologies - State-of-the-Art and Challenges.

Besides, some evasion techniques are used by attackers to bypass security protections like firewalls, IPS/IDS, application firewalls and other security measures. Such old and conventional techniques keep changing to adapt themselves to the new security features implemented by the targets. Several vulnerability scanners have evasion techniques embedded in them.

It seems that a new vision is needed to accurately represent and model security weaknesses and vulnerabilities. Indeed, these parameters; the key elements of a risk analysis process, are no longer persistent as they have formerly been represented in most paradigms. Vulnerabilities could be dormant; they cannot be detected by the security analysts during the audit or the penetration tests but still could be exploited by attackers. Moreover, attackers exploit vulnerabilities affecting vital services of companies or organizations or even individuals. White list security principles, allowing only what is needed to the right profile, are still pertinent but not sufficient. For instance, some companies cannot disable services such as their VPN remote access or some of their vital applications used in their internal network. Thus, attackers, most of the time, target these vital services.

Therefore an adaptive security model that takes into consideration this aspect of vulnerability assessment in a risk analysis process can provide better results. These results are used as inputs for the next step of the risk analysis.

3.2 Challenges

3.2.1 Correlating Vulnerabilities

Once the vulnerability assessment step is complete, vulnerabilities are used as the input of the next step, which is the threat assessment. The correlation of the different vulnerabilities in a model is one of the major challenges during this transition. This model is often represented in the quantitative risk analysis methodologies as the attack tree model. The difficulty of the task consists in building the threat or attack scenarios related to the vulnerabilities. Specific mathematical operators can be used depending on the mathematical representation of the vulnerabilities and their relationship, which lead to the threat scenarios. In most of the quantitative risk analysis methodologies the security expert is responsible for the vulnerabilities correlation. This could lead to different diagnostics and threat scenarios with different experts.

3.2.2 Monitoring Vulnerabilities

This challenge has two aspects: the first consists in monitoring the target to discover its vulnerabilities and the second in keeping the vulnerability databases up to date. Quantitative risk analysis is applied on an existing operating environment and continually sensitive to attacks or security incidents. A permanent monitoring of the target's weaknesses and vulnerabilities is needed to feed the risk management cycle, so that a pertinent evaluation is achieved. This task raises issues in a quantitative risk management approach: what resources to monitor, how to select these resources (which metrics to use) and what means to use in the monitoring operation (security monitoring solutions). The choice of the vulnerability database to be used is crucial. The vulnerabilities should cover the largest spectrum possible. Security experts generally use those present in vulnerability scanners, which cover the technical spectrum, and those in security norms such as ISO27000, which cover the organizational aspects of security. Nevertheless, the vulnerability databases need to be kept up to date. An update mechanism must be defined on the database design phase. This rule applies for every vulnerability database especially the technical ones.

3.2.3 Real-time Reaction

The real-time reaction is another major challenge of the vulnerability assessment techniques; applied to quantitative risk management methodologies. Security experts sometimes face incidents and discover vulnerabilities that need instant reaction. This challenge raises the following questions: What triggers the security alert? Which reaction is suitable for which alert level? How to reduce the false positive and false negative rates of alerts in the information system? When performing monitoring tasks, security experts use alert levels that are often defined by default by the security monitoring solution. These levels classify security incidents according to the service level agreements (SLA) of the monitored resources and the security incident or vulnerability detected. Most of the time, this approach leads to arbitrations made by security experts on the priority of the measures taken to stop the attack or the incident and limit its impact. Security experts face false positive security alerts daily. They are not inherent in the monitoring or scanning solutions, but they often depend, not only on the way these solutions are configured and used, but also on the resources they monitor or scan.

4 STATE OF THE ART

The analysis covers the Security Meter model developed by Sahinoglu, the NetRAM methodology, and other quantitative methodologies that lack a fully qualified vulnerability assessment step. These quantitative risk management methodologies, applied to information and communication systems, are not normalized and have many differences in their core steps.

4.1 State-of-the-Art of Vulnerability Assessment Techniques

The vulnerability assessment step shapes the threat scenarios and the following steps of the risk management cycle. In the methodologies under study, hypotheses and approximations are set in order to t in the quantitative risk management mathematical model.

In this section, the vulnerability assessment step of several quantitative risk management methodologies is analyzed.

Sahinoglu defines vulnerability in the following terms:

"A vulnerability is a weakness in any information system, system security procedure, internal controls, or implementation that an attacker could exploit. It can also be a weakness in a system, such as a coding bug or design flaw. An attack occurs when an attacker with a reason to strike takes advantage of a vulnerability to threaten an asset." (Sahinoglu, 2005).

A wider definition would include flaws, misconfigurations and weaknesses that could result (exploited by an attacker or accidental events) in a security flaw. The absence of redundancy of the electricity source of an information system is an example of a vulnerability that is not included in the definition of Sahinoglu. In case of unavailability (due to an incident on the electricity providers part) of the electricity source, the availability of the information system is corrupted. This is an example, among others, which is not exploited by attackers. Nevertheless vulnerabilities lead to a loss in the security level of the information system.

A company may have its own methods of assessing the vulnerabilities affecting its information system. This may include security equipments placed on the network (IDS, log analyzers, etc.), or regular audits and penetration tests, as well as vulnerability scanners performing planned scan. The result of such tasks constitutes the output of the vulnerability assessment step in a risk analysis cycle.

In the quantitative risk management approach, only exploitable vulnerabilities are taken into account and combined with threats to build risk scenarios. This means that these vulnerabilities can lead to a security level downgrade if exploited in an attack or an incident.

In Sahinoglu's Security Meter model, vulnerabilities are inputs to the probability model. Each vulnerability is determined by a probability of occurrence and the sum of all the vulnerabilities' probabilities is one (Sahinoglu, 2005). In this model, the risk analyst is responsible for defining the vulnerabilities to be included in the risk analysis process (Sahinoglu, 2008). The parameters used to calculate the vulnerabilities' probabilities are the presence or absence of countermeasures and the number of cyber attacks witnessed by the target. In fact a vulnerability probability is calculated as a percentage of the cyber attacks that harmed the information system of the target of the risk analysis operation.

The NetRAM approach is different. The vulnerability identification step is based on pre-built vulnerability libraries that are checked (Hamdi *et al.*, 2003). These libraries should be as exhaustive as possible in order to cover most of the vulnerabilities that can affect information and communication systems. Bugs, misconfiguration, physical, conceptual and procedural vulnerabilities are the types listed in the NetRAM methodology. The set of vulnerabilities can be collected from scanners databases for the technical ones, and from the risk analyst's expertise for the organizational ones. Contrary to the Security Meter model, NetRAM does not assign a probability to each vulnerability, but probabilities are assigned to the attacks based on expert's opinions and on statistics provided by security institutes.

Security Assurance is another methodology of assessing a system's security level. It allows measuring quantitatively the efficiency of the existing security measures at the design phase (of software for example) and at the runtime. The methodology is based on five steps which are: modelling; metric specification; assurance evaluation; aggregation; and display and monitor (Moussa et al., 2013) (Haddad et al., 2011). The assurance evaluation and the monitoring depend on the metric specification step, which consists of collecting data from logs, configuration files and dedicated network probes (Haddad et al., 2011). The measurement is constantly taking place via the network probes and the operation assurance. The metrics used in this methodology are:

- Coverage: This is related to the nature of the verified key functionality of the assessed security mechanism.
- Depth: This is related to the level of detail to which the security mechanism is assessed. This metric depends on the presence of a document detailing the security mechanism's key properties.
- Rigour of verification: This metrics measures whether the verification follows a systematic process and to which extent this process is sophisticated.
- Independence of verification: This metric denotes the independence of the persons performing the verification from the ones that deployed the security mechanism.

The Adaptive Security Management approach was developed to provide a paradigm that provides learning, anticipation, evolution and adaptation to a changing environment at runtime (Savola et *al.*, 2010). It proposes metrics that respond to the security requirement of the target's scope. Managerial and operational nodes are defined by this methodology. The managerial nodes conduct the following tasks: runtime monitoring (anomaly monitors, QoS managers, logging tools), control (audit tools) and decision-making (Blasi et *al.*, 2010). The vulnerability discovery and anomaly detection in this approach is performed with a set of detectors placed on the operational nodes of the scope. The Adaptive Security methodology offers a vulnerability assessment approach that responds to the operational need of the target in terms of security and offers a constant monitoring of the security level.

The present study addresses another quantitative risk analysis methodology presented by Felani and Dwiputra. Their work aims at developing an information system solution for risk analysis, which may resolve some of the drawbacks of the qualitative risk analysis methodologies (Felani and Dwiputra, 2012). This methodology relies on the same steps as ISO International Standard, thus it is based on risk identification with questionnaires. Thus, vulnerability assessment is assimilated with risk identification through a series of questions. The main difference with qualitative risk analysis methodologies is the use of the Delphi method. This method relies on several rounds of the same questionnaire where experts revise their answers based on the answers of their peers in order to reduce the subjectivity of the answers.

Game theory is used in many risk analysis approaches (Bier and Azaiez, 2008) (Abie and Balasingham, 2012) (Cox, 2012). Manshaei et al. (Manshaei *et al.*, 2013) made a survey about the game theoretic approaches of security for privacy and intrusion detection. There are advantages of using game theory to model a security approach, which mainly are the quantitative nature of strategies used by the attacker and the defender, the abstraction of security policies as probabilities, formal decision-making and behaviour prediction for risk analysis (Manshaei *et al.*, 2013). Hamdi and Abie in (Hamdi and Abie, 2013) state that security games is a quantitative framework for modelling the interactions between malicious users and defence systems. This definition takes into account the mathematical modelling of the conflict between the two parties in an attack and defence vision of the network security, the players. Abie and Balasingham implemented this model in risk-based adaptive security applied to a specific context, which is Internet of Things for e- Health (Abie and Balasingham, 2012). The data produced by this model allows a measure of threat level and a prediction of risk damages based on data collected and analyzed in security games fashion applied to the context of IoT in e-Health. The process of the developed framework is aligned to the ISOs Plan-Do-Check-Act (PDCA) cycle in an adaptive security fashion.

4.2 Shortcomings of existing Techniques

The Security Meter model developed by Sahinoglu is a deterministic model in which the probabilities of all the vulnerabilities add up to one (Sahinoglu, 2005) (Sahinoglu, 2008). This approach assumes a "probabilistic sample space of feasible outcomes" (exploitable vulnerabilities). Vulnerabilities are then represented in a tree diagram as the roots of the scenarios. The following stage is the threat one. In this model, the probabilities of the vulnerabilities are taken from recorded security breach statistics of the target. The condition about the probabilities adding up to one is not realistic because not all vulnerabilities that can be exploited are present in the target security breach statistics. In fact in a real case, there are always vulnerabilities that have not been detected as security breaches and that are discovered by attackers and not figuring in the target's security statistics. Also vulnerabilities taken into account i the Security Meter model are only those that are have been exploited in the past, but there are no details about how to judge if a vulnerability is exploitable or not. In real life scenarios, the exploitable character of a vulnerability comes from the expertise level and skills of the attacker not only from statistics or lack of countermeasures. In some cases, even security equipments can bread vulnerabilities if their configuration is not hardened.

NetRAM has another approach to the vulnerability assessment. It is based on pre-built vulnerability libraries (Hamdi *et al.*, 2003). These libraries can be vulnerability scanners databases for technical vulnerabilities. As for the organizational and human behaviour vulnerabilities, the security expert's opinion could be valid. This approach of vulnerability assessment has some deficiencies: a) The vulnerability scanners on the market have different databases. Sometimes there are huge differences between the vulnerability databases since there are different vulnerability assessment paradigms. Besides, the update level of the vulnerability database is a key issue while performing the vulnerability assessment. b) False-positives and false-negatives need to be assessed in the NetRAM approach which adds a new level of complexity to the process. c) Organizational vulnerabilities and the ones that do not depend on a scanner rely on the expert's opinion.

In the NetRAM methodology the information system's security fields or categories that are to be assessed by the expert are not specified. This can lead to different results with different experts. Nevertheless, expert opinion in risk management is a mandatory component. Carl S. Young stresses this particular issue saying:

"Direct experience is indeed relevant to a security risk assessment process. Both experience and science are crucial to risk decisions in a world that seems to be neither completely deterministic nor entirely random. But rejecting science would be just as foolish as ignoring intuition developed through years of experience. Scientific reasoning and experience are not mutually exclusive in the world of security. Both should contribute to a rational assessment process that informs judgment in assessing the totality of risk." (Young, 2010)

The Security Assurance methodology is used to measure the pertinence of the deployed security mechanisms. It also helps security specialists to organize their process when choosing which tools and which methodologies to use. When applied in a risk assessment process, this methodology is adapted to a scope where security has already been taken into account. Thus, the Security Assurance methodology helps identify vulnerabilities and weaknesses of security mechanisms that are already deployed. In order to identify the gap between the security objectives and the existing security level, or the running security and the deployed security, the Security Assurance methodology (Operational Assurance) is not relevant. The developers of this methodology insist on the fact that to measure these gaps, other methodologies like Common Criteria (ISO/IEC 15408) or BUGYO. Security Assurance is complementary to these two methodologies (Haddad *et al.*, 2011) its the vulnerability assessment is related to operational security mechanisms that are already deployed.

The Adaptive Security Management approach has a vulnerability assessment node that is designed to identify operational anomalies on the technical level of the scope. The difficulty of applicability of such a methodology is that it needs to be deployed on the design step of the solution or scope on which it is applied. This methodology focuses on the process of adaptive security management, especially by monitoring the operational nodes of the scope to meet their security requirements. A monitoring tool defines the security levels to meet and raises alerts whenever an attack that compromises the operational security requirements is detected (Blasi *et al.*, 2010). The organizational side of the vulnerability assessment or monitoring step is not detailed in this approach. Responses to the alerts are not defined and organizational aspects of security are not detailed.

The third methodology, presented by Felani and Dwiputra, relies heavily on qualitative methodologies. In fact the vulnerability assessment step relies on questionnaires enhanced with the Delphi method. This approach does not provide reliable results as respondents; often prepare their answers in advance. Besides, the output data of the risk identification step -assimilated here to vulnerability assessment- is then qualified on a qualitative scale depending on probability and impact. In fact the vulnerability assessment step in this methodology provides a less subjective output than the one provided by a questionnaire answered in a qualitative approach.

The adaptive security model relying on game theory is very context dependent. The game theory core of the framework is used in the step of analysis and prediction. This step relies on the results obtained from the monitoring step which is dependent on the threat model. The process is inspired from the PDCA cycle but its threat model is not detailed and is heavily dependent on the IoT context, which generates a limited risk spectrum.

4.3 Summary of the existing Methodologies

The following table compares the methodologies cited in the previous section through the three criteria of vulnerability correlation, monitoring and real-time reaction.

Table 1: Comparison of the methodologies.

	Correlating vulns.	Monitoring vulns.	Real-time reaction
Security Meter	++	0	0
NetRAM	++	+	-
Security Assurance	+	++	-
Adaptive Security Mgt	-	++	+
Delphi	-	-	0

Scale: 0 is mentioned but not integrated; + is mentioned and detailed but not fully integrated; ++ is fully integrated; - means absent.

This comparison shows that none of the studied methodologies fully covers the three criteria. In fact this is due to the fact that their conception is not based on an adaptive paradigm. Quantitatively they allow measuring a certain level of the vulnerability but the output data is not exploited in an adaptive fashion.

5 METHODOLOGY

In this section, a framework for vulnerability analysis is presented. This framework is adapted for a quantitative risk analysis approach in order to be integrated in an adaptive security model. Figure 1 details the process of the framework. Inspired from the PDCA cycle, this framework is adapted to classic communication and information networks with various security zones, which make it convenient for most enterprise information systems. Figure 2 details an example of a generic network for which this framework is adapted.

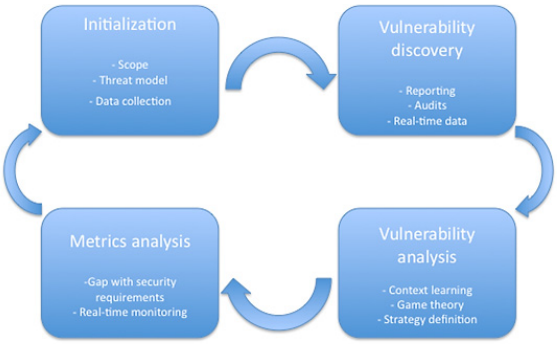

Figure 1: Proposed framework for vulnerability assessment in an adaptive quantitative approach.

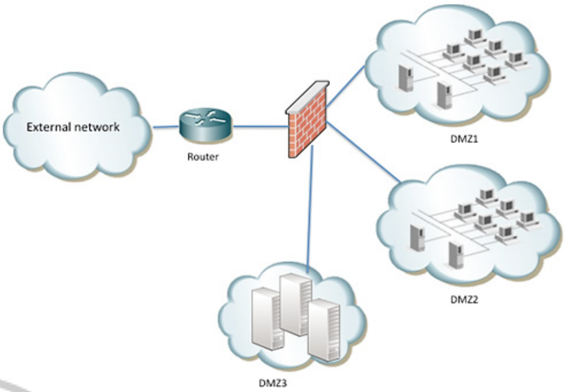

Figure 2: An example of a classical network structure of an enterprise information system.

In the ISMS system, risk management process is a cycle in which vulnerability discovery is a key step to properly estimate risk and threat scenarios. The framework is developed in order to provide quantitative output for the next steps of the risk management process. It follows these four main steps (i) initialization step during which the context is analyzed and data is collected, (ii) the vulnerability discovery step during which the collected data is analyzed and vulnerabilities are extracted, (iii) vulnerability analysis is the phase during which the abstraction and quantitative modeling of vulnerabilities as security vectors and metrics is performed, (iv) and the final step is the metrics analysis in order to extract usable security indicators as values to assess risks.

5.1 Initialization (Plan)

During this step the context is studied in order to perform accurate vulnerability assessment. The following tasks are performed:

- Scope definition: The analyst and the Chief Security Officer (CSO) limit the perimeter of the vulnerability assessment. This defines the borders of the studied perimeter.
- Threat model: In order to know what to look for when assessing the scope, a threat model must be defined. The threat model is basically the answer to the question: What are we trying to prevent? (Abie and Balasingham, 2012)
- Data collection: The analyst collects Security policy and all the available documents and

data concerning the security of the scope. Example: Service Level Agreements (SLAs), Access Control Lists (ACLs), security procedures in case of incidents, security reports, real-time data if available, etc. For the unavailable data, targeted and redundant vulnerability scans, audits, interviews and penetration tests can be performed by the analyst depending on the scope.

5.2 Vulnerability Discovery (Do)

Collected data is analyzed to extract vulnerabilities: technical and organizational.

- Technical Vulnerabilities are discovered mainly through the assessment of the various reports of security sensors: scan reports cross-checked through redundant scans with different vulnerability scanners, log analysis, IDS reports. False positives must be avoided, so once the vulnerabilities are discovered, they are exploited in false flag operations (or simulated attacks) in order to confirm that they can be used by attackers in real threat scenarios. Technical incidents cannot be simulated; statistics about the equipments failures can be used as data to assess vulnerabilities.
- Organizational Vulnerabilities: these are discovered through analysis of the different procedures (if they exist), interviews are very often the main source of information when an analyst is checking organizational security, the reliability of collected information can be enhanced with cross-checking as described in [?] and material proof.

5.3 Vulnerability Analysis (Check)

Once the previous step is complete, the analyst knows exploitable vulnerabilities affecting the analyzed scope. In order to attack the scope, the attacker (or the incident) has to exploit one or a set of vulnerabilities to cause damage. A rule-based reasoning is applied in this step. Security policy and procedures are modelled into a set of rules against which the vulnerabilities are analyzed. Game theory approach can be used in this step to confront the two sides (defence and attack through vulnerabilities). Rules and context are represented as strategies in game theory. This representation takes into account the technical side as well as the organizational side of security. Collected data in the previous step is used in the security games model as the attackers strategy. The defence strategy is based on vectors like flow matrix, ACLs, SLAs, security policy, filtering rules, etc. These strategies are learned and applied in a continuous monitoring process in order to provide the adaptive and predictive side for the risk management cycle. Changes in these strategies (new rules, a change of the context, new vulnerabilities, etc.) must be easily applied in order to have a flexible framework.

5.3 Metrics Analysis (Act/ Adapt)

Security metrics are necessary in a quantitative approach. They allow measuring as objectively as possible the vulnerability vector used in the risk management process. In this framework, the metrics are linked with security objectives, which are inherent to the context and scope of the analysis. In this step the defined metrics must allow to measure the gap between the assessed vulnerability level and the security requirements of the scope on the technical and organizational levels. The link between vulnerability and security objective is considered in this approach because a vulnerability implictaes a risk only if it lowers a security level of an asset. Practically, before starting the vulnerability discovery, each resource of the assessed scope must be given security objectives values. These values are usually defined by assessing the criticality of the resource in the whole business process and its need to the security services (confidentiality, availability, integrity and authentication). This step is performed quantitatively in the initialization process of the risk management when assessing the resources on the scope (Evesti and Ovaska, 2010). So depending on the evaluation of the security objectives, which are generally defined in a qualitative manner, values are defined by assessing the mechanisms that ensure the objectives. For example a server that has high confidentiality and integrity requirements will have metrics related to these objectives with high coefficients. The vulnerability analysis phase will then take place (scanning, interviewing, penetration testing, monitoring, etc.) then metrics will be affected with values that correspond to the degree of impact of the vulnerability on the security objective. On each round of analysis the metrics' values are updated depending on the counter-measures performed on the next steps of the risk management cycle.

6 EXPECTED OUTCOME

The work on the quantitative vulnerability assessment is a part in the development of an adaptive quantitative security management model. The thesis in which this work is incorporated is entitles “Adaptive Security Models for Information and Communication Systems”. The expected outcome of this thesis is to shed light on the quantitative and adaptive security models, identify the main reasons why they are not widely used in IT as opposed to other fields (industrial and financial for example). Once these reasons identified, a model that can be used in an enterprise environment will be developed. This model should avoid complexity and should allow security analysts to accurately measure their security indicators for risk management and to be able to have a security environment that is adaptive to all sorts of changes in its scope.

A mathematical model based on quantitative metric that translate the changes in an IT environment will first be developed and then integrated in a risk management process. Adaptability will then be the core feature of operational security.

ACKNOWLEDGEMENT

This research project has been carried out within a MOBIDOC thesis financed by the European Union through the PASRI program.

REFERENCES

Abie, H. and Balasingham, I. (2012), “Risk-Based Adaptive Security for Smart IoT in eHealth”, *Proceedings of the 7th International Conference on Body Area Networks*, *Oslo, Norway,* pp. 269-275.

Bier ,V.M. and Azaiez, M.N (2008), “Game Theoretic Risk Analysis of Security Threats”, *Springer, International Series in Operations Research & Management Science*, Vol. 128.

Blasi, L., Savola, R., Abie, H. and Rotondi, D. (2010), “Applicability of Security Metrics for Adaptive Security Management in a Universal Banking Hub System”, *European Conference on Software Architecture (ECSA) Companion*, *Copenhagen, Denmark, August 2010*, Vol.2010, pp. 197-204.

Computer Security Institute CSI (2010), *2010 / 2011 CSI* Computer Crime and Security Survey, New York.

Cox, L.A. (2012) “Game Theory and Risk Analysis”, *Risk Analysis,* Vol 29 Issue 8, pp. 1062-1068.

Evesti, A. and Ovaska, E. (2010), “Ontology-based Security Adaptation at Run- time”, *Fourth IEEE International Conference on Self-Adaptive and Self-Organizing Systems*, Budapest, Hungary, pp. 204-212.

Felani, I. and Dwiputra, A. (2012), “Developing Objective-Quantitative Risk Management Information System”, *Proceedings of the World Congress on Engineering 2012, London, UK, 2012*, Vol I, pp.481-484.

Haddad, S., Dubus, S., Hecker, A., Kanstrn, T., Marquet, B. and Savola, R.(2011), “Operational Security Assurance Evaluation in Open Infrastructures,” *6th International Conference on Risks and Security of Internet and Systems (CRiSIS)*, Romania, pp. 100-105.

Hamdi, M. and Abie, H. (2013), “Game-Based Adaptive Security in the Internet of Things for eHealth”, *ACM Computing Surveys (CSUR), ACM NY, New-York, USA*, Vol 45, Issue 3, Acticle No. 25.

Hamdi, M., Krichene, J., Tounsi, M. and Boudriga, N. (2003), “NetRAM: A Framework for Information Security Risk Management,” *Nordic Workshop on Secure IT Systems*, *Gjovik, Norway*.

Manshaei, M.H., Zhu, Q., Alpcan, T., Basar, T. and Hubaux, J.P. (2013), “Game Theory Meets Network Security and Privacy”, *ACM Computing Surveys (CSUR)*, *ACM NY, New-York, USA*, Vol 45, Issue 3, Acticle No. 25.

The Mitre Corporation (2012), “Vulnerability Management”, available at: http://measurable security.mitre.org/directory/areas/vulnerabilitymanagement.html (accessed 16 April 2013).

Moussa, O., Savola, R.M., Mouraditis, H., Preston, D., Khadhraoui, D. and Dubois, E. (2013) “Taxonomy of quality metrics for assessing assurance of security correctness,” *Software Quality Journal*, Vol.21, issue 1, pp. 67-97.

Open Source Vulnerability Data Base (2013), “Vulnerability Entry Standards”, http://www.osvdb. org/vuln standards (accessed 16 April 2013).

Sahinoglu, M. (2005), “Security Meter: A Practical Decision-Tree Model to Quantify Risk”, *IEEE Security Privacy*, Vol. 3, No. 3, pp. 18-24.

Sahinoglu, M. (2008), “An InputOutput Measurable Design for the Security Meter Model to Quantify and Manage Software Security Risk”, *IEEE transactions on Instrumentation and Measurement*, vol. 57, No. 6, pp. 1251-1260.

Savola, R. M., Abie, H.,Bigham, J. and Rotondi, D.(2010), “Innovations and Advances in Adaptive Secure Message Oriented Middleware the GEMOM Project”, *IEEE 30th International Conference on Distributed Computing Systems Workshops*, *Genova, Italy, June 2010*, pp. 288-289.

Young, C.S. (2010), “Metrics and Methods for Security Risk Management”, *SYNGRESS, USA*.