International Journal of u- and e- Service, Science and Technology
Vol.8, No.5 (2015), pp.105-128
http://dx.doi.org/10.14257/ijunesst.2015.8.5.10

Quantitative Risk Management: a Survey of Adaptive Approaches to Risk Management for Information and Communication Systems

Raed Labassi[1], Mohamed Hamdi[1] and Tai-Hoon Kim[2]

[1] *Sup'Com, University of Carthage, Tunisia*
raed.labassi@supcom.tn, mmh@supcom.tn
[2]*Department of Convergence Security Sungshin Women's University, Korea*
taihoonn@daum.net

Abstract

Over the last few years, perspectives in information security have been drawn, to a large extent, by risk management. The extensive use of risk management methodologies in organizations relying on an IT infrastructure proves the potential of the practice. In this survey we discuss the characteristics of the quantitative risk management methodologies, compare them and provide an overview on how these methodologies are entwined with the concept of adaptive security. We also discuss the challenges of quantitative risk management and adaptive security models and propose reliable criteria to compare the different approaches in the literature.

Keywords: *adaptive security models, quantitative risk management, information security, risk assessment, risk analysis, security metrics, risk models.*

1. Introduction

The intensive use of information and communication technologies has created an economic, and in certain critical cases, a vital dependency. Some security issues have resulted from this dependency. How could a secure functioning of organizations and institutions which rely heavily on these technologies be ensured? This question has been efficiently tackled by the risk management approach in industrial and economic environments. Methodologies and models allowing efficient risk management have been developed in order to identify and cope with risks (treat, reduce, eliminate or accept). Measuring risks and their attributes has become the main option in managing the security of a system, a company or a particular investment.

The success of the risk based approach in several fields inspired information technology experts in their quest to manage the security of their systems, applications, organizations, and investments. Several institutions and organizations have been using established norms and regulations. First, experts had mainly used qualitative approaches to manage risks affecting information and communication systems. These approaches rely heavily on the opinion of experts. Experts resorted to qualitative approaches because of the lack of a common view on the definition of risks in information technologies field and the facility they offer. Most experts do not obtain the same results using a qualitative risk assessment on one scope. Nevertheless this approach has advantages such as simplicity and rapidity with quite reliable results.

Several quantitative risk management approaches have been developed in the field of information and communication technologies (ICT). These approaches are not widely used yet mainly because of the complexity level of their implementation, and in spite of the fact that they present many advantages when compared to the qualitative approaches. When risks are objectively quantified with metrics, and measures precisely defined,

ISSN: 2005-4246 IJUNESST

adaptive security models could rely on these measures in order manage security efficiently and in real time.

Surveys about quantitative and adaptive risk management / assessment / analysis approaches are traced in the literature [1, 2, 3]. This survey paper provides an overview of the state of the art models applied to different domains, from software security to networks and communication, and establishes the link between quantitative risk management and adaptive security models. It also presents a detailed and comparative state of the art of the quantitative approaches to ICT risk management, as well as the mathematical models used to define the security metrics while measuring the risks.

In section II we give an overview of the state of the art of quantitative risk assessment methodologies. A variety of models, their application fields, requirements and shortages are presented. In section III we present the abstract mathematical models developed to measure risks and their properties in the IT fields. The objectives and conditions of each model are proposed. In section IV, state of the art of various security metrics, used to quantify risks, are given. These metrics are the parameters that are defined in order to provide a reliable method.

We argue that experts in the discipline do not agree on fundamental issues and definitions [4]. Although standard organizations have set concepts and methods for risk management, it seems that there is a lack of consensus on terminology. Thus, the standardization effort that took place was aimed at the qualitative approaches underlying the claim made by researchers in the 1980s that the risk management discipline cannot be considered as a scientific discipline because of uncertainties affecting the procedure. Approaches based on weak estimations of probabilities and impacts may not be reliable and could even be misleading [4]. The scientific community has kept on trying to develop methods to calculate as objectively as possible the risk values through quantitative approaches and models, in spite of the absence of a systematic terminology and divergence in definitions.

2. Quantitative Risk Assessment Methodologies: State of the Art

This section discusses a selection of quantitative risk assessment methodologies in the literature. A critical and comparative approach is used to assess these methodologies.

The diversity of approaches toward quantitative risk assessment is due to the absence of an established terminology in the discipline. Besides, there is a lack of a core model that integrates a wide spectrum of security issues regarding information and communication systems. Quantitative methodologies usually concentrate on one aspect of security, for example application security, project management security, network security. The main challenge is modeling all the aspects of security in creating quantitative parameters that cover all the aspects of security (like the ISO sub-categories). Hybrid risk assessment methodologies like [5, 6, 7] use a quantitative approach in their core framework. However when the quantification metrics are taken into consideration, these methods use scales and approximations in order to quantify the attributes or metrics.

The main indicators used in this survey are:

- The risk coverage: This criterion shows whether the methodology covers different aspects of security when applied to a scope or developed for only one aspect.
- Cyclic risk management: This indicates whether the assessment methodology is designed to be used in a risk management cycle, or it is an independent risk assessment technique.
- Complexity: It indicates the methodology can be used immediately in an enterprise environment or if it is too complex and time consuming to be put in practice.
- Quantification parameters: This category lists the different parameters used to quantify the risks and how these parameters are used in the process.

- Adaptive character: This indicates if the methodology was designed for use in a dynamic adaptive process.

2.1. Risk Coverage

A variety of risk assessment methodologies focus on certain aspects of security. The two methodologies that cover the largest risk spectrum are CORAS [5] and NetRAM [6]. CORAS proposes a model that measures and models quantitatively the risk parameters. NetRAM covers the whole technical side of security except the organizational and financial sides.

Other quantitative approaches like [7, 8, 9] deal only with the organizational side of risk assessment. This aspect is hardly quantifiable due to its nature. Procedures and responsibilities are in fact hardly measurable. Therefore, most quantitative approaches deal with the technical security and tend to ignore this aspect. In [7] the Delphi technique compiles the different answers through multiple rounds of questionnaires in order to obtain more accurate results. In [8] organizational security is defined as the capacity to respond and the ability to recover. These two elements allow measuring the adaptive capacity of an organization. In [9], a structuration of the organizational security in risk management deployment is covered, enabling a better granularity in the quantification of the organizational security parameters.

Other risk assessment approaches focus only on one subject. They are developed for the purpose of assessing risks that are inherent to a technology or a layer or only a certain type of risks (black or gray swan risks). For example in [10], an approach that defines attributes of gray swan risks (risk with low probability and high impact) is proposed. In [11], only the risks concerning reengineering operations are considered and divided in five components which are quantified by measures of impact metrics that are also defined. This methodology extends the capabilities of the ISO standard by defining various impact metrics.

2.2. Cyclic Risk Management

The cyclic aspect of security management was standardized by the majority of the fields in which security and risk management were deployed: industrial, financial and in the ICT field, even though this could be done through managing risks or security processes. NetRAM shows a cyclic risk management approach in the sense that managing risks in an ICT infrastructure is a continuous and adaptive exercise. In fact the cyclic risk management criterion is important when classifying these methodologies in order to know which frameworks can be modified in order to integrate adaptive parameters.

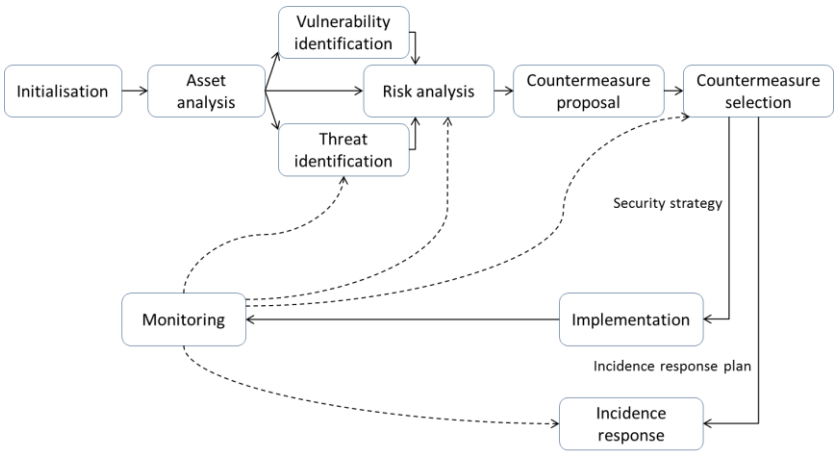

Figure 1. The NetRAM Risk Management Cycle

Indeed, the quantitative risk assessment methodologies studied here are, or, can be used in a cyclic risk management process, such as the one defined by NetRAM as shown in Figure 1.

2.3. Complexity

This criterion is defined on the basis of three parameters: (1) The scalability of the model, (2) the existence of a framework ready to use and (3) the easiness of applying the methodology on a classic information system of an average size organization containing multiple DMZ separated by a firewall. This third parameter is defined as a comparison with the easiness of deploying a qualitative standard such as ISO on the same scope. The CORAS framework needs a configuration before use. Its semantics need to be mastered beforehand, and then the diagrams between the components of the process need also to be set. Once the core diagrams are set, it is easier to manipulate and scale to variable scopes. The NetRAM methodology needs setting up the matrixes containing the values by analyzing first the data used for quantifying the risk attributes as probabilities and impacts. The complexity in using it is due mainly to the collection of the values used in the matrixes. The more specific methodologies [7, 11, 10, 8], applied only to a field or a type of risks, are less complex, since they create attributes of risks or environments that can be easily integrated in the risk management operations, with more accurate means of collecting and assigning values in the process.

2.4. Quantification Parameters

In this part the quantification parameters of the risk assessment methodologies are analyzed. These parameters allow us to know how the risks are measured, and whether their attributes can be used in a fully or partially quantitative process. In addition, knowing how these parameters are measured is crucial, as this indicates how the quantification of risks is achieved.

Felani and Dwiputra define a scale in their organizational risk management methodology. Nevertheless, the values are collected in a more objective way by doing several rounds of the questionnaire and comparing the results with the Delphi method. This constitutes one approach, where the quantification parameters are not applied directly on the classic attributes of risks (probability and impact), but it is applied in the process of calculating these values. NetRAM and CORAS and Rajavat and Tokekar follow the same process by applying values from a scale, but inserts quantification in the process of choosing these values for attributes such as probability, impact and residual risk values. Liu et al. define another way of risk quantification by defining components and subcomponents for resilience and adaptive capacities. These components aim at quantifying vulnerabilities; considered as the key factor to risk management.

2.5. Adaptive Character

This criterion was selected in order to reflect the capacity to integrate adaptive security in these quantitative risk assessment methodologies. A methodology that can be qualified as adaptive is one that can be used in a dynamic environment with values that vary in time, and a possibility to automatically cope with the change in the scope. Usually adaptive security models predict risks and change security parameters accordingly in an optimized way [12]. Adaptive security models could be one solution to resolve the complexity of ICT risk management [3].

The adaptive capacity is assessed in order to evaluate the quantitative methodologies studied in this survey. This is carried out by analyzing the mechanisms of each methodology, and showing how the model can be used in an adaptive manner by

integrating dynamic risk parameters. These parameters allow predicting the behavior of the system during runtime, and adapting its security level accordingly.

In [6, 10, 8] the methodologies can be used with adaptive models of risks and environments. In fact these methodologies offer a capacity of using models that can predict risks. Liu et al. rely heavily on the capacity of adaptation as a main feature to measure the level of security of an ICT system. In NetRAM it is possible to use variable parameters like resources values, probabilities and impacts. Despite the fact that Holes methodology concerns only gray swans, predicting these risks is vital to stakeholders.

2.6. Summarizing Table

Methodology	**Risk spectrum**	**Cyclic risk management**	**Complexity**	**Quantification parameters**	**Adaptive character**
Felani and Dwiputra	Not defined	Integrated into a risk management cycle	Not complex	Risk factors dened and measured with Delphi technique	No
NetRAM	Technical threats only (no organizational threats)	Yes	Complexity grows with the scope of the analysis	Classical metrics: impact and probability (quantified subjectively)	Yes
CORAS	Methods for risk assessment are not specied, but the risk spectrum is large	Yes	Semantics and diagrams are complex to use and design	Quantification is applied through a scale (similar to MEHARI)	No
Hole	Only gray swans (hid- den risks with great impact and low probability)	Yes			Yes
Rajavat and Tokekar	A good coverage with 5 risk components but still confined to reengineering legacy projects	Yes	Not complex to implement	A scale is defined, no quantification metrics	No
Liu et al.	Organizational vulnerabilities	Yes through resilience and adaptive capacity	Not complex	Indicators and parameters of resilience and adaptive capacity are defined	Organizational adaptive capacity is defined

Table 1. Comparative Table of Quantitative Risk Assessment Methodologies

3. Quantitative Security Models: the Mathematical Representation

In this section, the mathematical models on which the quantitative security paradigms rely are analyzed. There are steps between collecting data and expressing a risk or threat or loss or any other security attribute quantitatively in a risk management process. The final values of these attributes are calculated from inputs. The quantitative models of the literature are diverse in terms of mathematical models. Some mathematical models are often used in quantitative risk methodologies like the Markov chain [13] or the attack graph [14, 6, 15] due to their use in many similar processes. Others proposed by Alhazmi and Malaiya model the evolution of the rate of vulnerabilities discovery in time [16]. Many models are inspired by physical phenomena like the exponential model, the logarithmic model or the thermodynamic model. In this section, the models of the quantitative risk methodologies are analyzed using the following criteria:

- The input data: This indicates what data is taken into account as input for the mathematical model. The input can have several forms. The data used as input and the manner with which it is collected are important factors in order to have an objective and quantitative result in the end.
- The output data: This indicates how the final result of the mathematical model is represented. In fact, having a multi-dimensional vector with different values and attributes can be an accurate and objective measure of the risk, but it differs from a simple quantitative value that can be used in a risk management cycle. Furthermore, some methodologies can go further by exactly calculating the loss of security objectives or economic loss if the risk occurs.
- The security vectors representation: During the different steps of risk management, vectors like vulnerability, threat, risk and impact are used. Their representation depends heavily on the mathematical model.
- The risk spectrum: It specifies the covered risk spectrum of the analyzed methodology.

3.1. Quantifiable Input Data

The input data, used in the different mathematical models, is collected from the context of the assessed scope. The manner in which this data is collected is important to the accuracy and objectivity of the final results of the risk assessment. If the data is collected from network sensors or security equipment like IDS or firewalls, certain preventive measures have to be taken, such as verifying if the alerts or the log do not contain false positives. The results of penetration tests or audits can also be used after putting them in the right format for the mathematical security model.

There are different definitions of “quantitative”, since there are different models and different approaches to quantitative risk assessment. Some authors use the word to describe the core of their risk assessment approach. They use a mathematical model to calculate risk values or security attributes, so their model is quantitative [16, 17, 11]. However, other researchers [6, 5, 18, 19, 20, 21] estimate that a quantitative model has to be accurate in all its cycles, and use quantifiable parameters systematically, starting from data collection to the final steps of decision making.

The risk assessment methodologies, covered here, use many approaches in collecting the set of input data. The type of data and the manner in which it is collected depend on the mathematical model that processes it. Abdelmoez et al. in [17] enumerate the different components of the system to calculate the probability and the impact of change on the security of a component. Unconditional probabilities of change are estimated then the conditional probabilities on the rest of the components are calculated. In this case, a

system of conditional probabilities and propagation is used to calculate the risk attributes. The Astrolab methodology [18] of identifying risks is based on the HAZOP method that is also used by CORAS [5]. The quantifiable input data for this model is the goal of each component, the evidence of achieving the goal and the inter-relation between those two parameters. Each of these three parameters is given a value between 0 and 1 according to its importance. This data is collected qualitatively and given values depending on the evaluation of the expert. Falcon et al. in [19] use live data as input for their framework of risk management for wireless sensor networks. But, in their context this live stream of data is split into discrete snapshots of risk features in order to feed the rest of the cycle. Sun et al. use the same paradigm as collecting live data from the network, by using sensors installed on each host that detect intrusion and report it as antigen [20]. This analogy between a network and a human body functioning with lymphocytes and antigens has also been used by Liu *et al*. in [8] in their risk management model. The input data is the level of antigens detected by a network sensor. Keramati and Akbari use a statistical paradigm for input data [14]. Probabilities and impacts of vulnerabilities, used in the attack graph, are calculated from the CVSS databases. The cumulative values of these parameters, when used in the attack graph, are then calculated using the probability and impact values from the CVSS.

As presented previously, the input data is not uniform for all these methodologies. They depend heavily on many factors, and mainly on the design of the framework and the field for which the methodology was designed.

3.2. Quantifiable Output

The output data of the quantitative risk assessment methodologies vary depending on the quantitative model used by the framework and the risk spectrum covered. The main goal of quantitative risk assessment is to make decisions depending on an accurate and objective assessment of the threat. Then, by measuring precisely the risk, decisions can be taken with confidence. Therefore, the output data of a quantitative risk assessment methodology is the key: what it indicates and how it is performed, are the main features of the following analysis. Furthermore, the maturity of each methodology is a crucial parameter in what the methodology provides as output data and how it is formatted.

NetRAM is one of the rare quantitative methodologies that goes as far as indicating which decision to make after assessing risks. This is the output data given in the end of the cycle as a countermeasure selection depending on the risk values calculated before with the attack graph model. Abdelmoez et al. in [17] provide as output data values of risks concerning each component of the project, since their methodology concerns only maintainability risk for software products. These values are expressed as raw data represented by the product of cumulative probability and impact on the components.

Bagheri and Ghorbanis model and CORAS use the HAZOP method to calculate a parameter defined as hazard. Once it is calculated, the risks are estimated based on the analysis of goals, evidence, capabilities, resources, threats and significance [22]. These parameters constitute the output of the Astrolab methodology applied to each goal as identified in the initial step of the process. Values of these vectors are represented in a table listing all the goals and the values of each of these parameters. The output data of the Falcon et al. methodology for wireless sensors networks is an overall measurement of the risk at any point in time [19]. A live risk measurement requires real time evaluation carried out in the model. Risks can be dismissed and others treated proactively depending on the weights of each member of the WSN. The sensor based risk assessment used by Sun et al. provides the same overall risk vision by giving a live feed of the antigens concentration in the system, and then correcting the antibody concentration by creating lymphocytes with memory [20]. Thus, this system is more complete than the one applied

for the WSN since it is auto regulated. It also has an adaptive side that is absent in the Falcon et al. system which relies on the users updating grades of the nodes in order to evaluate risks. The lymphocyte and antigens model is a whole model used to represent the scope like a biological body when reacting to the intrusion of virus or bacteria, its immunity mechanisms and reaction to counter the attack and adapt itself with memory lymphocytes and vaccines.

The study of the output data provided by the different quantitative models shows a variety and the absence of homogeneous understanding of risk quantification. A detailed comparative table shows the characteristics of these models and the variety of their outputs.

3.3. Mathematical Representation of Security Vectors

In this section, the models presented above are analyzed in order to identify their security vectors. The two main goals here are: the security indicators that are taken into account when calculating risks and how they are represented by each model. The nature and the mathematical representation of security vector depend mainly on the mathematical model used by the methodology.

One of the most widely-used models for risk management and representation of the security factors that build the risk is the attack tree model based on threat scenarios. This representation is used by many quantitative risk management methodologies [6, 14, 15] [23, 24]. However, there are different approaches to the concepts of threat, vulnerability and attack scenario. Generally, these models use the same mechanisms and processes to calculate risks in terms of probabilities and impacts. The level of detail differs from one methodology to another. For example, in NetRAM the main vectors of security are vulnerabilities, threats and risks [6]. In addition to those parameters, the attack graph model used by Keramati and Akbari uses a more granular vision based on the exploit-based attack graphs which are developed to cover the scalability issue of state-based attack graphs (hosts and vulnerabilities interrelations) [14]. New nodes are added to the graphs: exploit nodes and condition nodes to check whether the vulnerability can be used by an attacker and on which conditions.

The Astrolabe methodology developed in [22] is based on a model representing the goals and objectives of the studied system. Three main vectors are expressed in the first step of the iterative process: goal, evidence and the interrelation between them. These three vectors are given values between 0 and 1. Then the HAZOP method is used to identify hazards characterized by their causes and the conditional probability of each cause.

The methodologies using the antibody representation [8, 20] of security mechanisms use the same vectors as they are similar to the functioning of a human like biological system. These vectors of the immunity-based security model are: functions of the concentration of antigens (generally by analyzing IP packets), antibody, lymphocyte, self tolerance (threshold), lifecycle of mature lymphocyte, immune memory, *etc* [8]. These vectors are functions or expressions of real time indicators of the network state. These vectors follow a set of rules in order to follow the evolution of the system state by detecting intrusion in the packets circulating in the network. Methodologies that are developed for a specific environment like [19], have security vectors that are inherent to their environment. For example, in [19], a wide range of vectors covering the security of the wireless sensors network and its nodes are defined and measured from a live feed of data.

3.4. Summarizing Table

Methodology	Quantifiable input	Quantifiable output	Vectors representation	Risk spectrum
NetRAM	Assets, vulnerability, attacks, impact, probability	Decision	Vulnerability, threat, risk	Technical
Abdelmoez et al.	Requirements, system architecture Change profile for each component	Risk factor = Probability * Impact	Maturity index, initial change probability, change propagation probabilities, size of change	Maintainability risks
Bagheri and Ghorbani (Astro-labe)	Astrolabe: HAZOP	Hazards	Goals, evidences, impact factors	Risks affecting the proper being of a system infrastructure
Falcon et al.	Sets of risk features that are monitored (live data), Cluster-ing data, Sensors measurement in risk features space	Risk reports	Wide range of vectors proper to WSNs	Risk Management Framework for Wireless Sensor Networks
Feixian Sun and Zhigang Wu	Lymphocyte antigen detection	Antibody con-Centration	-Sets of lymphocytes, antibodies and antigens -Mature and memory lymphocytes -Activation threshold	E-government network security
Keramati and Akbari	Probability and impact (CVSS)	Cumulative values of probability and impact	Exploit-based or compact attack graphs: exploit and condition nodes	Computer net-works

Table 2. Comparative Table of Mathematical Models of Risk Quantification

4. Estimating Security Metrics in Quantitative Risk Management

Aubert et al. in [25] present security metrics as a modeling object defined as the process that allows producing a normalized risk level, and is based on the measurement of various parts/parameters of security functions. Surveys about security metrics were published [26] [27] [28]. They were related to qualitative approaches [28] or measuring metrics related to specific fields. Most surveys do not integrate the risk vision.

Calculating risk values is a task involving parameters and features that need to be defined as the quantification elements of the process. Security metrics need to be defined in order to obtain precise numerical values of risks. The qualitative approaches like the ISO standard or Mehari or EBIOS define two main metrics which are probability and impact. Risks are expressed in terms of probabilities and impacts and many consider the risk measure as the product of these two metrics. Quantitative methodologies made the measurement of these metrics the linchpin of risk calculation. Some of these methodologies improved these classic metrics by developing more accurate methods of estimation. Others created their own new metrics depending on the scope of their methodologies in terms of the contexts and environments for which they were developed. Nevertheless, there is not a unique framework for measuring real-world security data for risk models, neither is there a unique method to collect this data [29]. In this section, a comparison of the major security metrics of the quantitative risk management literature is carried out. The analysis is based on the following criteria:

- Choice of the metrics: The type of the metrics and the reason of choosing them are analyzed. The variety of the existing metrics in the literature is detailed.
- Estimation methods: The methods used to estimate the metrics for each of the analyzed methodologies are given in this paragraph. The importance of this criterion resides in the fact that some quantitative approaches tend to use estimations based on qualitative data.
- Contribution and specificities: In this paragraph, the contribution of each methodology developing or enhancing metrics calculation for quantitative risk management is listed and analyzed.

4.1. Choosing the Metrics

In the absence of a harmonizing framework for risk management, each methodology defines the elements that are necessary to calculate risk values. The steps of the process, the nature of the framework and the context of use determine which parameters are defined as metrics. Many methodologies such as [5, 18] adapt metrics from fields other than the information and communication systems. These metrics are defined by techniques like HAZOP or FMEA and can be adapted to the information and communication settings. Many other quantitative methodologies like [6, 30, 31, 29] use the traditional metrics of probabilities and impacts, and better their measurement in order to provide accurate quantitative data. Each one of these methodologies adds its own new metrics. Others choose to keep the probability and impact metrics but define new ways of computing their values [30, 32].

Chen et al. in [30] define a risk probability estimator framework. This methodology focuses only on the probability of risks. It proposes a technique to calculate accurately risk probabilities, while integrating the interaction feature between the components of the assessed system.

Metrics can also be defined depending on the context and the environment of the risk assessment task. For example, Ebert et al. in [2] focus only on managing risks of global software engineering projects. The metrics defined are risk mitigation actions and project deliveries. These two metrics are the only ones taken in consideration in the context of the global software engineering and cannot be applied to another project, since risks are predefined and measured with these two metrics. [32] is another example of specific metrics, but that has a larger spectrum and can be used in the context of information or communication networks using servers and computers. The metrics defined are related to the activity of the host since the framework in question focuses only on assessing the risks affecting directly hosts in the network. For example, the CPU consumption, memory

resources, OS security indicators and sensors, network traffic, security devices alerts, are the metrics defined in this methodology. These two examples show that the diversity of the scope of the study can trigger a variety of metrics inherent to the environment.

Ryan and Ryan [31] use the traditional metrics of probability and consequence (or impact) as performance metrics for information security risk management. Their core model is based on the calculation of loss expectancy. This value is defined as the product of the probability of a successful attack times the loss sustained by a successful attack. But the innovation in this model, compared to the qualitative ones, resides in the manner of calculating these values quantitatively. Efficiency and effectiveness metrics are introduced to measure how the implemented security mechanisms can protect against system failures and extend operational lifetimes [31]. These values are calculated through trials and samplings.

On the same tip of calculating risks of system failures and security investments, Keybl et al. define in [33] the preparedness metric. This metrics quantifies the preparedness of an organization on the strategic level in case of events that can compromise the security of a state or a region. The metric of preparedness can be applied on risks concerning information and communication systems that have a wide geographical extent.

In [29], Baker et al. define a new conception of threats and threat scenario by classifying them according to particular characteristics like source, channel or mode of attack, target, using always a chain of events. Metrics of probability and impact are assigned to the links of the threat scenarios. They are divided into sub-metrics allowing a better evaluation of their values in each stage of the threat chain. These sub-metrics are organization-specific, and collected directly from the organizations own data. They are divided into four categories: expected threat frequency; countermeasure effectiveness data; threat-to-impact transitions; and data concerning the financial loss from the impacts.

There are as many security metrics as quantitative risk methodologies. The choice of the metrics does not depend on security norms or standards, it varies with each framework.

4.2. Estimation Methods

In [30], the risk probability metric defined by the model, is calculated thanks to historical data that are used as input for a neural network. Since the model is focused on the impact of interaction between the system entities and the influence of such an interaction of the risk probabilities, historical data is collected and used to train the neural network and calculate the projected probability values when new entities are introduced. So log data is very important in this model, and in [30] a stress is put on the fact that not all historical data is relevant to the framework.

The Ebert et al. paper [2] details ten risks affecting the global software engineering projects. The metrics are the undertaken risk mitigation actions and the project deliveries. These metrics are easily assessed, and their correlation is calculated based of the family of predefined risks affecting these projects. Each risk is taken independently and risk mitigations actions are specified thanks to empirical and statistical data.

In [32], Gao et al. define the host security status metrics listed above. These multi-source metrics are directly collected from the hosts and the security equipment. A three-step method is used, and its first step is the evidence abstraction step during which four types of anomalies are defined, and evidence of these anomalies is collected directly from the sources. Before being used as quantitative security metrics, each data source is assigned a weight based on the entropy method (by calculating uncertainty). Once the evidence set is built, basic probabilities are assigned to pieces of evidence based on the opinion of the security expert. Then, the Dempster Shafer theory is used to calculate the probability of two combined pieces of evidence.

Ryan and Ryan developed in [31] a method of calculating expected loss through the probability of system failure and efficiency of security investments. Randomized controlled trials on sample groups and collection of failure time data are performed, in order to evaluate the efficiency of security investments and system failure probabilities. These steps of sampling and collecting data to use as metrics are repeated over time, and over independent groups to obtain estimated trends of the security state of the whole infrastructure.

Keybl et al. define in [33] the preparedness metric on a state strategic level to counter threats such as natural disasters and terrorism. They propose a method of measuring this metric by collecting data mainly from the available security and activity reports: Hazard mitigation plans, state accomplishment summaries and state preparedness reports. These documents provide information on the security mechanisms that are already in place. The metric values are assigned through quantifying the amount of funding associated to ensure the security and the preparedness of each activity to face incidents and failures. Decomposing the threat scenario chain, and affecting weight to the links is used by various quantitative methodologies [6, 14, 15]. The contribution of Baker *et al.* in [29] is to assign new metrics in a different understanding of the scenario chain thanks to the decomposition of the threat scenarios in threat scenarios events and threat scenarios results. Assigning metrics to the links, after identifying all the different outcomes of each scenario, becomes less complex. The metrics defined are threat frequency, threat impact, financial loss and countermeasure effectiveness. Measuring these metrics is based mainly on internal data collected from the company infrastructure. Measures of these metrics are collected from the analysis of internal logs (for frequency), public sources (threat statistics), countermeasure matrix for the effectiveness metric, independent testing of the infrastructure, internal testing and financial reports of bad outcomes. Percentages are assigned for the threat frequency, the countermeasure effectiveness and the impact metrics based on the analysis of these sources.

4.3. Contribution and Specificities

Each new methodology, defining new metrics, or enhancing existing ones, has its own distinctive contribution. In this section, an analytical survey of each contribution is given.

In [30], Chen et al. integrate the interaction factor between entities of the same infrastructure in calculating risk probabilities. A neural network is used to model the clustering and the interaction between the entities. The use of a neural network helps to predict the values of the probability by simulating all these interactions. Therefore, before calculating new values of risk after introducing a new input, training is done to predict the probability values change. This prediction framework using a neural network is the main contribution to the literature and can be integrated in other quantitative methodologies to improve the quality of the probability measures.

Ebert et al. define in [2] principles and practices for quantifying risks in global software engineering projects. Ten risks are used as the main ones and their quantification is based on the two metrics of mitigation actions and project delivery. These risks are mainly organizational. The main contribution of research on organizational risk measuring is summarizing them and simplifying the metrics of measuring such risks. Nevertheless, the metrics defined in [2] cannot be used in a context other than the software engineering domain. Thus, this contribution focuses on a particular type of business related to information and communication technologies.

Gao et al. establish metrics for host related security in [32]. These metrics are multi-source, and collected mainly from indicators of the hosts' activities. The entropy calculation allows us to give a weight to each of these sources and compute uncertainty of evidence, in addition to their combinations. Many methodologies [20, 34, 19] collect data

from multiple sources and aggregate them to calculate risk values. But the innovation of Gao et al. proposal is that the measured factors are all temporal. Therefore, an adaptive mechanism updating the hosts' profiles was introduced in the calculation of these metrics. This approach can then be used in an adaptive security cycle, thanks to its use of dynamic metrics and adaptation of hosts' profiles with changes occurring on these metrics.

Ryan and Ryan provide a new type of metrics in [31]. These metrics are used to measure how the existing security implementation can extend the lifetime of critical assets. These metrics are called efficiency and effectiveness metrics, and are measured through repeated calculations and sampling of groups inside the infrastructure. The specificity of these metrics is that they provide a decision making tool for managers to evaluate their security investments in a less complex and more efficient way than analyzing risk assessment reports. These metrics target directly the decision of whether managers need more or less security for their company.

Another approach defining metrics that are suitable to adaptive security is the Keybl et al. model in [33] for state wide risk management. The Adaptive Readiness Model (ARM), defined in [33], uses the preparedness metric to help the decision makers identify gaps between their preparedness activities and calibrate the investments accordingly. This model can be used in an adaptive risk management methodology during the first steps of assessing the already existing security mechanisms.

Baker et al. offered a new vision of the threat scenarios in [29]. By decomposing these scenarios into events and results, and defining the ways of collecting the metrics to affect for each link (probability, impact, countermeasure effectiveness and financial loss), a simpler view of quantitative threat scenarios is given. This view allows a simple measurement of each distinct link of the threat scenarios. Besides, measuring the metrics in Baker *et al*. approach can be performed on technical threats as well as organizational ones.

4.4. Summarizing table

Methodology	**Metrics**	**Estimation method**	**Certainty rate**	**Contribution**
Chen *et al*.	Risk probability	Historical data are the input for a neural network: average loss rate and similarity rate between unexpected vector and average	Not expressed	Prediction of risk probabilities can be calculated by simulating interactions
Ebert *et al*.	Risk mitigation action and project delivery dates		Not expressed	Correlation between risk mitigation actions and project deliveries

Gao *et al.*	Host security status (cpu, memory, os, etc.) and its probability	D-S Theory for evidence selection and entropy to decide the weight of each sub-variable	Not expressed, but the basic probability of each evidence is expressed by experts then it is calculated	Adaptive to dynamic host activity
Ryan and Ryan	Expected loss, efficiency of security investments, probability of system failure		Not expressed	Efficiency and effectiveness metrics
Keybl *et al.*	Preparedness (on a state level: natural disasters, terrorism, etc.)	-Data collected from: Hazard Mitigation Plans, State Accomplishment Summaries and State Preparedness Reports -Assignment of values is done through the amount of grant fundings associated to each activity	Not expressed	Very suitable to adaptive approaches
Baker *et al.*	-Expected threat frequency -Threat to asset impact -Impact and financial loss - Countermeasure effectiveness	-Threat scenario chains: internal logs analysis, public sources -Countermeasure matrix in [8] for effectiveness, independent testing, internal testing analysis -Cost of bad outcome: company data	Countermeasure effectiveness: Values are estimates	-A new view of the threat scenario -A more effective way of affecting values to the metrics -Applicable to a large risk spectrum

Table 3. Comparative Table of Security Metrics Estimation Methodologies

5. Adaptive Risk Management Approaches

In order to achieve accuracy while decreasing complexity, automating security managed has always been defended by experts [3]. Intelligent security systems have been developed in order to improve the operational security tasks, without being based on a threat or risk-based view of adaptive security [35, 36].

An adaptive security model is a model that allows treating security event in an automatic real-time and proactive manner, by predicting the evolution of security indicators (or metrics) and adapting security mechanisms accordingly. Elements of

adaptive security were elaborated in parallel with quantitative security metrics. These two notions are linked because accurate security measures need to be performed in order to be able to measure changes in the security and react or adapt the protection level to these changes. Having a different judgment on the same scope cannot be tolerated.

Nevertheless, in the absence of norms and standards of quantitative risk management, adaptive capabilities were developed for risk management in information and communication systems and networks. In this section, adaptive risk management approaches are studied. Their mathematical models, risk spectrum and experimental results are presented.

These elements are necessary to comprehend the evolution of adaptive risk management in the literature on security, and how close we are today to an effective methodology that can be used in real life environments.

5.1. Model basis and Risk Coverage

In this section, each adaptive risk management approach is analyzed on the basis of its mathematical model. The main questions in this section are: How is the adaptive security implemented? Through which parameters? And what is the representation used? The methodologies overviewed herein, concern, to varying degrees, various fields of information and communication technologies. Some of these methodologies cover specific fields like applications security or project management. The remaining ones are more generic and cover a larger risk spectrum. In 2007, El Khodary and Whittle in [3] published a survey on adaptive application security approaches. The survey analyzed four adaptive application security approaches, and showed the absence in the literature of work on the design of effective adaptive models [3]. It also showed that incorporating best practice in application security cannot be the only feature of an adaptive approach on application security. Integrating the threat and risk view is necessary to achieve effectiveness in security management, even for a specific field as application security.

In [12], Deleris et al. expose an adaptive risk management model designed for project management. The model is named Adaptive Project Risk Management (APRM). Risks are modeled by two factors in the APRM which are: impact on relevant projects and resource flexibility on a project, which are organized into a Bayesian Belief Network (BBN). This representation allows learning and updating quantitative risk-activity relationships [12]. Probabilities of activities being on the critical path of a project are calculated with the critical Path Method. Estimated durations of activities are calculated with uncertainty level through Monte Carlo simulations. The BBN then combines the estimation of activities durations and probabilities of risk factors and updates the completion times of the project activities accordingly. The BBN allows a better calculation of cost-benefit analysis based on risk mitigation. The parameters and risks taken into consideration in the APRM model are quite simple to represent in an adaptive risk management model since it models only completion times through the estimated durations for each activity and their relationships with risk factors.

Evesti and Ovaska propose a specific adaptive risk management model in [37]. It concerns run-time adaptation for applications. Since the software environment can be subject to changes at run-time, the software security requirements need also to change and cannot be defined beforehand. Security ontology is used in this methodology (security mechanisms, objectives, measurements and connections between them). First, a start-up phase adaptation is required. Security requirements, levels and mechanisms are defined for the application. Based on the measurement collected during the control at run-time, the adaptation action is performed to reach the security level defined in this first step. Monitoring the changes in context and environment is a crucial task in Evesti and

Ovaskas methodology, so calibration techniques are the main focus to improve this methodology.

Hunt and Slay in [38] combine the use of security devices and forensics analysis to obtain an adaptive security model for forensically sound critical infrastructure. This model covers risks concerning computers and networks, which can be a large risk spectrum. But it reality, this model covers only technical risks that are linked to security incidents leaving traces for forensics analysis. In order to have an adaptive response to incidents, a combination of security devices and forensics data is performed in this model. Data is collected from the following sources: firewalls and IDP / IPS systems, honeypots and honeynets, Security Information Event Management (SIEM) systems, threat assessment, vulnerability scanning and surveillance, web notification system for real time notification delivery and a Data Loss Prevention system (DLP). Therefore, all the data collected from these sources is normalized in a forensically sound manner and analyzed by forensics tools. The only problem of this system is real-time reaction. Collecting the data and analyzing it by forensics software can be time and resource consuming even if the authors claim that this can be done at high speed parallel processing and cluster computing [38]. Adaptive risk management methodologies were also developed to meet organizational security requirements.

In [39], Mykkeltveit and Helvik present a model of management of connections to meet guarantees in service level agreements. This methodology concerns only a feature of organizational security, but the technique used here can be applied to other sorts of agreements or procedures for organizational risk management. Rules for priority orders are defined for recovery conditions. Thus, in order to trigger a reconfiguration, connections are checked to check if they meet these priority rules. Therefore, policies combining the four priority rules (allocation, class, budget and random) are defined for the concurrent connections. These policies are rule sequences defined for each reconfiguration trigger.

In [40], Savola et al. describe the GEMOM systems requirement in measurability to enhance practical monitoring for this adaptive security framework. The risk spectrum covered by this framework is very wide in terms of technical risks since the monitoring task uses data from multiple sources like security equipment, vulnerability scanners and sensors. Practical adaptive approaches require self-protection, resilience and self-healing features. They are implemented in the GEMOM framework through mechanisms that rely on credible data that can be measured, analyzed and that leads to reliable decisions. There are multiple mechanisms used to achieve this adaptive feature: Flexible Communication Mechanism: publish / subscribe, Security Measurement Mirroring and Data Redundancy, Multi-Point Monitoring, Auto-Recovery on Error. Security requirements are split and each component is associated with basic measurable metrics that can be combined and weighted. When attacks are detected, the threshold of security requirements affected by the attacks is increased, and stronger security mechanisms are activated (for example authentication with certificate instead of user / password authentication). The GEMOM framework is based on security measurability features in order to integrate adaptive mechanisms.

Tapiador and Clark in [41] present another approach to implement adaptive security in a quantitative risk management. It consists of learning dynamic security policies that change with the context and the evolution of the whole infrastructure. This methodology has the advantage of covering a wide risk spectrum and is applicable to various information and communication networks that function with security policies. Tapiador and Clark argue that security policies should not be specified, and imposed, they should rather be learnt in order to be more efficient and adapt to changes in their environment and still be usable (not impacting performances). Genetic Programming is used to model this adaptive security technique. It consists of reproducing in a tree structure, mechanisms

of selection, crossover, mutation and reproduction of the infrastructures assets with internal operators depending on the risk exposure. The contribution of this model is not about adapting the policies dealt with in the past [42], but are about characterizing the usability of the reconfigured security policies in such a model thanks to the Genetic Programming approach.

Li presents in [43] a similar approach, taking into account the system performance parameter, while adapting the security level of communication. This model covers risks and threats affecting the communication medium. A state machine of security level is represented as a one dimension Markov chain. It models the migration of security states. Each security state has a set of security mechanisms, called security strategy, related to it. The adaptive side of this model is named comprehensive evaluation which consists of constantly getting inputs from servers and adjusting the security strategy accordingly by using a knowledge base. This knowledge base is the abstraction of the security expert knowledge into data that can be used by a computer. It is built as a qualitative matching between security strategies and inputs from the servers. Li admits that such a base cannot cover all the possibilities, and this explains why their work limited its scope to cloud computing. Cloud-Trust model, as developed by Li and Du in [44] to cover service level agreements guarantees, is another model for cloud computing adaptive security. Various cloud trust models are found in the literature, but Cloud-Trust model provides an adaptive capability integrating real-time trust assessment according to the SLA. This model defines trust attributes for security objectives. For example, and as shown in the figure below, trust attributes of security are the number of illegal connections and the number of denial of services.

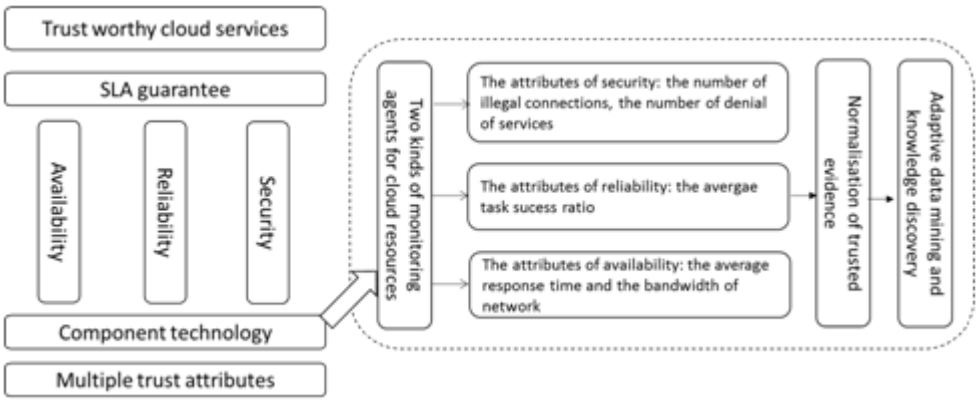

Figure 2. Trust Attributes of Trust Worthy Cloud Service in the Cloud-Trust Model

Evidence is collected dynamically from the monitoring agents and compared to the service level agreement signed by the user and the cloud manager. The Cloud-Trust model presented in this paper is an adaptive model, in the sense that it conducts knowledge discovery with the rough set method, which in this case is better than classical weight attribution methods. This adaptive character is also due to the use of the Induced Ordered Weighting Averaging (IOWA) operators, which are used to calculate global trust degree in real-time. This model offers a better visibility in an adaptive manner for users to choose a trust worthy cloud provider based on the SLA guarantee. Risk control methodologies are often developed to respond to security needs. So there are some methodologies that are specifically designed for environments that have a specific need for adaptive risk management models. Ma et al. in [ma] present an adaptive risk control and security management model for embedded real-time systems. The adaptive side

resides in the fact of considering the inherent characteristics of the embedded system, and measuring the energy efficiency of different cryptographic algorithms, and design a new indicator to quantify the security performance. System administrators just need to specify the expected performance and the system is capable of dynamically adjusting security levels of tasks in the waiting queue.

We describe in this section the variety of adaptive security and risk management understandings in the literature. Many attempts to design adaptive risk management frameworks were tested in experimental evaluations with various simulation parameters. These models are compared to existing ones based on their experimental results, performances and contributions.

5.2. Experimental Results

In this section, the presence or the absence of experimental results backing up the claims of the designers of the adaptive models is detailed. Most adaptive models perform simulations with various risk scenarios and compare the results. The maturity of a model can also be assessed by the results it has when confronted to a real ICT environments.

Deleris et al. designed simulation scenarios where they provide risk factors to a BBN and run various batches of tests with different risk scenarios against various resource scenarios [12]. This simulation shows results confirming that the APRM (Adaptive Project Risk Management) model allows gains in cost of the project and time for the project completion compared to base line plans. The BBN was updated with the occurrence of each new risk, which was not predefined. During the project, the APRM model can predict remaining cost and time after calculating risk factors, impact and changes in the resource allocation. The project manager receives important data helping in risk mitigation actions during the implementation of the project.

Evesti and Ovaska in [37] made a demonstration of their ontology based adaptive security model for reducing risk levels at run-time for applications. The case study was performed on a mobile device application. Security mechanisms were adapted at run-time to fulfill the security requirement for various situations. The validation was carried out, and measurements were made to monitor the current security level at run-time and select the optimal security mechanisms. The experimental results showed that the adaptation has taken place without the users' intervention.

The methodology presented by Hunt and Slay in [38] is inspired by the existing techniques, but adds the integration of forensically sound data collected and analyzed at run-time for adaptation purposes. There are no experimental results for this model. Therefore, it is not possible to assess the efficiency of this adaptive model linking operational security with forensics analysis at run-time.

Mykkeltveit and Helvik present in [39] a model for adaptive management of connections to meet availability guarantees in SLAs. A simulation was carried out on three di
erent scenarios: partially protected connections, fully protected connections and two classes of customers with different requirements. Different models of failure and repair processes were also simulated. The results of these simulations indicate that in many cases, the use of adaptive management reduces significantly the risk of violating requirements.

Savola et al. introduce in [40] security-measurability enhancement mechanisms for adaptive security in the GEMOM framework. The GEMOM framework has proved an efficient framework for adaptive security, but the measurability mechanisms ensuring the adaptability of the model presented in [40] were not tested in simulations or in real-life scenarios.

Tapiador and Clark use in [41] a simulation environment to evaluate the performance of their autonomic security reconfiguration policies. The simulation scenario is about a

MANET network with various services like email, http and ftp. Redundant servers are distributed in the network. The risk scenario is a geographical risk consisting of eavesdropping, capture, physical attack, etc. A hypothetical risk map is used instead of real life risk data. When a server is in a risk zone it should consider migrating to another node. This is the basic reconfiguration action in the simulation. The policies of reconfiguration exclusively determine what, where and when to move. Five different experiments were carried out in the simulation: minimizing risk, maximizing performance, minimizing the number of reconfigurations, combined objectives and finally a multi-objective optimization. The final experiment shows that it is possible to allocate weights to the objectives and respect thresholds that once reached trigger the adaptive side of the model through the reconfiguration policies.

The Adaptive Security Model for Communication on Cloud (ASMCC) developed by Li in [43] is a model based on securing communications by adjusting the security strategies according to the system state and performance. Experiments were carried out on the ASMCC model and the results were compared to similar models (static security, dynamic security and no security models). The ASMCC method proposed by Li is a tradeoff between security performance and computing cost when compared with the other models applied to the same environment.

The other model of adaptive and attribute-based trust model for service level agreement guarantee in cloud computing developed by Li and Du in [44] is designed to integrate adaptability in weight assignment for attributes. The experiments performed with this model are used to evaluate efficiency and accuracy of the model with different inputs. The data collected from the experiments shows that Cloud-Trust is a solid model for cloud users to compare providers. The Cloud-Trust model provides highly reliable results in many typical cases when compared to other trust models that do not integrate the adaptive side.

Ma et al. present in [45] an adaptive risk control and security management approach for embedded real-time systems. The experiments carried out on this model aim at showing that this technique can be risk-adaptive in real-time systems. So performances are evaluated with various input workloads and with significant drops in processing capacity. The results indicate that the proposed mechanism adapts to fluctuations in input, and resources while maintaining low risk levels. And once compared to another control system, Ma et al.'s model has given better results in terms of performance.

5.3. Summarizing Table

Methodology	**Model basis**	**Risk coverage**	**Experimental results**
Deleris et al.	Statistical estimation techniques to predict project time and cost, and to drive replanning Bayesian Belief Network (BBN) to organize risk factors	Project management: project duration and cost	Yes: simulation with different risk and resource scenarios
Elkhodary and Whit- tle (survey)	-Extensible Security Infrastructure: access control policies changed at run-time by privileged	Application security	-The scale defined in the survey to assess the adaptive approaches was not fully fulfilled by anyone of the approaches

	programs -Strata Security API: monitor binary instructions and execute listeners depending on specified policies -The Willow Architecture: run with reduced functionalities when under attack to determine survivability –The Adaptive Trust Negotiation Framework (ATNAC): adaptive authorization through changing access control policies according to a system threat level		-Such methodologies should incorporate not only best practices in software engineering but also best practices in security engineering, such as threat modeling.
Evesti and Ovaska	Security ontologies, measurements (from risk management approaches), context information, assets values taken into account	Run-time adaptation for applications	A demonstration shows that it is possible to adapt an application running on a mobile device both at the start-up and run-time phases ensuring the selection of optimal security mechanisms
Hunt and Slay	Reactive firewalls and IDS/IPS, honeypots and honeynets, SIEM and log, threat assessment, vulnerability scanning, web notication system, DLP	Computer security and network forensics	No
Mykkeltveit and Helvik	Taking the history of outages into account and let outages affect connections which are expected to tolerate them	Availability guarantees for SLAs	Yes: A simulation study shows that the risk of violating the requirements may in many cases be significantly reduced by using adaptive management
Savola et al.	GEMOM	Security monitoring, telecommunications and	Yes for GEMOM, but the new measurement mechanisms for adaptive security are not

		software-intensive systems	tested
Tapiador and Clark	Security policies can be learnt rather than specified. A server under too much risk should consider migrating to a different node with lower risk. A reconfiguration policy should establish what, when and where to move.	Used for risk reduction	Yes with MANET
Li	Environmental parameters of servers are analyzed and then a security communication strategy is picked from the library (mapping states and strategies) and applied on the communication	Adaptive security of the communications	Yes: the ASMCC is a tradeoff between security performance and computing cost
Li and Du	Cloud-Trust defines, collects and analyses multiple key trust attributes of cloud services. Then, it uses the rough set the-ory to adaptively conduct knowledge discovery of multiple trust attribute values (evidences)	SLAs in cloud computing	Yes: very good results when comparedto other trust models
Y. Ma et al.	Considering the in-herent characteristics of the embedded system, the energy efficiency of different cryptographic algorithms is measured and a new indicator to quantify the security performance is designed	Security-critical real-time applications running on uniprocessor server system	Yes

Table 4. Comparative Table of Adaptive Security Methodologies

6. Conclusion

In this survey we discussed the positive, as well as negative aspects of quantitative and adaptive security and risk management in the literature. A comparative study was carried out in order to identify the main issues regarding quantitative risk management in the IT fields. These issues revolve around the absence of a simple core framework to be used on a daily basis, or even occasionally, capable of providing results that could be easily interpreted by decision makers.

The following conclusions were made after studying the quantitative and adaptive security and risk management approaches. While there are many methodologies that are specific to certain environments or activities, the literature lacks methodologies with a wide risk spectrum, like the ISO standard but in a quantitative model. The quantitative parameters are usually defined through a scale, and not through objective measured and treated data. We may note that quantitative risk management methodologies, and security metrics only have minor crossing areas. On the one hand, the quantitative risk management frameworks usually define their own metrics which contain a subjective assessment at some point during the process. On the other hand, the quantitative security models have specific application fields which limit their use by the quantitative methodologies that tend to build frameworks capable of covering the largest possible risk spectrum. While surveying the literature, one can notice the dissociation between the risk management notion and the adaptive security paradigm. In this survey, we discussed how quantitative risk management and adaptive security can be merged in one framework. This framework can still integrate the risk vision, while proposing adaptive means of treating the risks.

Acknowledgement

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

References

[1] M. Ouedraogo, R. M. Savola, H. Mouratidis, D. Preston, D. Khadraoui and E. Dubois, Software Quality Journal, vol. 21, no. 1, **(2013)**.
[2] C. Ebert, B. K. Murthy and N. N. Jha, "Managing Risks in Global Software Engineering: Principles and Practices", Proceedings of the IEEE International Conference on Global Software Engineering, **(2008)**; Bangalore, India.
[3] A. Elkhodary and J. Whittle, "A Survey of Approaches to Adaptive Application Security", Proceedings of the 2nd International Workshop on Software Engineering for Adaptive and Self-Managing Systems, **(2007)**; Minneapolis, USA.
[4] T. Aven, Risk Analysis, vol. 32, no. 10, **(2012)**.
[5] R. Fredriksen, M. Kristiansen, B.A. Gran, K. Stlen, T. A. Opperud and T. A. Dimitrakos, "Lecture Notes in Computer Science", Springer, Heidelberg, vol. 2434, **(2002)**, pp. 94--105.
[6] The Communication Networks and Security (CN&S) research Laboratory, www.cnas.org.tn/selected-papers/netram_paper.pdf.
[7] I. Felani and A. Dwiputra, "Developing Objective-Quantitative Risk Management Information System", Proceedings of the World Congress on Engineering, **(2012)**; London, U. K.
[8] W. Liu, Y. Zhu and Y. Wang, "Organizational Vulnerability: New Perspective in Risk Management Research", Proceedings of the International Conference on Business Management and Electronic Information (BMEI), **(2011)**; Guangzhou, China.
[9] A. A. Odejide and T. Iyamu, "Structuration Analysis of Factors Influencing Risk Management System deployment", Proceedings of the IEEE 6th International Conference on Management of Innovation & Technology, **(2012)**; Sanur Bali, Singapore
[10] K. J. Hole, Computer, vol. 46, no. 1, **(2013)**.
[11] A. Rajavat and V. Tokekar, "A Quantitative Model for the Evaluation of Reengineering Risk in Infrastructure Perspective of Legacy System", Proceedings of CSI Sixth International Conference on Software Engineering (CONSEG), **(2012)**; Indore, India.

[12] L. A. Deleris, K. Katircioglu, S. Kapoor, R. Lam and S. Bagchi, "Adaptive Project Risk Management", Proceedings of IEEE International Conference on Service Operations and Logistics, and Informatics, **(2007)**; Philadelphia, USA.
[13] X. Tan, Y. Zhang, X. Cui and H. Xi, "Using hidden markov models to evaluate the real-time risks of network", Proceedings of IEEE International Symposium on Knowledge Acquisition and Modeling Workshop, **(2008)**; Wuhan, China.
[14] M. Keramati and A. Akbari, "An Attack Graph Based Metric for Security Evaluation of Computer Networks", Proceedings of the 6th International Symposium on Telecommunications, **(2012)**; Tehran, Iran.
[15] M. Sahinoglu, IEEE Security & Privacy, vol. 3, no. 3, **(2005)**.
[16] O. H. Alhazmi and Y. K. Malaiya, "Modeling the Vulnerability Discovery Process", Proceedings of the 16th IEEE International Symposium on Software Reliability Engineering, **(2005)**; Chicago, USA.
[17] W. M. Abdelmoez, K. G. Popstojanova and H. H. Ammar, "Methodology for Maintainability-Based Risk Assessment", Proceedings of the Annual Reliability and Maintainability Symposium, **(2006)**; Newport Beach, USA.
[18] E. Bagheri and A.A. Ghorbani, "Risk Analysis in Critical Infrastructure Systems based on the Astrolabe Methodology", Proceedings of the Fifth Annual Conference on Communication Networks and Services Research, **(2007)**; Fredericton, Canada.
[19] R. Falcon, A. Nayak and R. Abielmona, "An Evolving Risk Management Framework for Wireless Sensor Networks", Proceedings of IEEE International Conference on Computational Intelligence for Measurement Systems and Applications, **(2011)**; Ottawa, Canada.
[20] F. Sun and Z. Wu, "A New Risk Assessment Model for E-Government Network Security Based on Antibody Concentration", Proceedings of the International Conference on E-Learning, E-Business, Enterprise Information Systems, and E-Government, **(2009)**; Hong Kong, Hong Kong.
[21] W. Han, Q. Ni and H. Chen, "Apply Measurable Risk to Strengthen Security of a Role-Based Delegation Supporting Workflow System", Proceedings of IEEE International Symposium on Policies for Distributed Systems and Networks, **(2009)**; London, U.K.
[22] E. Bagheri and A.A. Ghorbani, IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans, vol. 39, no. 1, **(2008)**.
[23] Y. G. Kim and S. Cha, "Security and Communication Networks, vol. 5, no. 3, **(2012)**.
[24] D. Raptis, T. Dimitrakos, B. A. Gran and K. Stlen, "The coras approach for model-based risk management applied to e-commerce domain", Proceedings of the Sixth Joint Working Conference on Communications and Multimedia Security: Advanced Communications and Multimedia Security, **(2002)**; Portoroz, Slovenia.
[25] J. Aubert, T. Schaberreiter, C. Incoul, D. Khadraoui and B. Gateau, "Risk-Based Methodology for Real-Time Security Monitoring of Interdependent Services in Critical Infrastructures", Proceedings of the 10th International Conference on Availability, Reliability and Security, **(2010)**; Krakow, Poland.
[26] B. Bates, K. M. Goertzel and T. Winograd, "Measuring Cyber Security and Information Assurance: A State-of-the Art Report", Information Assurance Technology Analysis Center (IATAC), **(2009)**.
[27] I. Eusgeld, F.C. Freiling and R. Reussner, Lecture Notes in Computer, Springer, Heidelberg vol. 4909, **(2008)**, pp. 1-4
[28] ISO/IEC 27004, Information technology - Security techniques - Information security management - Measurement, http://www.iso.org/iso/catalogue_detail?csnumber=42106, **(2009)**.
[29] W. H. Baker, L. P. Rees and P. S. Tippett, Communications of the ACM, vol. 50, no. 10, **(2007)**.
[30] Y. Chen, C. D. Jensen, E. Gray and J. M. Seigneur, "Risk probability estimating based on clustering", Proceedings of the IEEE Systems, Man and Cybernetics Society Information Assurance Workshop, **(2003)**; New York, USA.
[31] J. J. C. Ryan and D. J. Ryan, IEEE Security & Privacy, vol. 6, no. 5, **(2008)**.
[32] C. Gao, Z. Li and L. Chen, "Host Risk Evaluation Framework Based on Multi-Source Information", Proceedings of ISECS International Colloquium on Computing, Communication, Control, and Management, **(2009)**; Sanya, China.
[33] M. Keybl, J. Fandozzi, R. Graves, M. Taylor and B. Yost, "Harmonizing risk and quantifying preparedness", Proceedings of the IEEE Conference on Technologies for Homeland Security, **(2012)**; Waltham, USA
[34] T. Li, Science in China Series F: Information Sciences, vol. 48, no. 5, **(2005)**.
[35] E. Hooper, "Intelligent Network Infrastructure Systems Architecture and Integration", Risk Management and Validation. Proceedings of the 1st Annual IEEE Systems Conference, **(2007)**; Honolulu, Hawaii.
[36] D. Kostopoulos, G. Leventakis, V. Tsoulkas and N. Nikitakos, "An Intelligent Fault Monitoring and Risk Management Tool for Complex Critical Infrastructures: The SERSCIS Approach in Air-Traffic Surface Control", Proceedings of the UKSim 14th International Conference on Computer Modelling and Simulation, **(2012)**; Cambridge, U.K.

[37] A. Evesti and E. Ovaska, "Ontology-based Security Adaptation at Run-time", Proceedings of the 4th IEEE International Conference on Self-Adaptive and Self-Organizing Systems, **(2010)**; Budapest, Hungary.
[38] R. Hunt and J. Slay, "The Design of Real-time Adaptive Forensically Sound Secure Critical Infrastructure", Proceedings of the 4th International Conference on Network and System Security, **(2010)**; Melbourne, Australia.
[39] A. Mykkeltveit and B. E. Helvik, "Adaptive management of connections to meet availability guarantees in SLAs", Proceedings of the IFIP/IEEE International Symposium on Integrated Network Management, **(2009)**; Long Island, USA.
[40] R. M. Savola and P. Heinonen, "Security-Measurability-Enhancing Mechanisms for a Distributed Adaptive Security Monitoring System", Proceedings of the 4th International Conference on Emerging Security Information, Systems and Technologies, **(2010)**; Venice, Italy.
[41] J. E. Tapiador and J. A. Clark, "Learning Autonomic Security Reconfiguration Policies", Proceedings of the 10th IEEE International Conference on Computer and Information Technology, **(2010)**; Bradford, U.K.
[42] R. M. Venkatesan and S. Bhattacharya, "Threat-adaptive security policy", Proceedings of IEEE International Performance, Computing, and Communications Conference, **(1997)**; Phoenix, USA.
[43] W. Li, "An Adaptive Security Model for Communication On Cloud", Proceedings of the International Conference on Computer Science and Network Technology, **(2011)**; Harbin, China.
[44] X. Li and J. Du, IET Information Security, vol. 7, no. 1, **(2013)**.
[45] Y. Ma, W. Jiang, N. Sang and Z. Zhong, "An Adaptive Risk Control and Security Management for Embedded Real-Time System", Proceedings of the 7th International Conference on Availability, Reliability and Security, **(2012)**; Prague, Czech Republic.

