



## CNAS REPORT

Printed January 2008

CNAS-2008-007  
Public

Supersedes CNAS-2006-002  
Dated March 2006

---

# NetRAM: A Framework for Information Security Risk Management

Mohamed Hamdi  
Jihène Krichène  
Mahmoud Tounsi  
Noureddine Boudriga

Prepared by  
CN&S Research Lab.

The Communication Network and Security (CN&S) research Laboratory,  
(Created in 1999, 02/UR/11-08) is located at the Communication School of Engineering  
(University of 7th of November at Carthage, Tunisia).

Approved for public release.

Copyright © 2007 by the Communication Networks and Security Research Lab. All rights reserved.

**NOTICE:** No part of this publication may be reproduced, stored in a retrieval system, or transmitted without written authorization from the CN&S research lab.

Available from

CN&S research lab.  
Engineering school of communications.  
Techno-parc El Ghazala, Route de Raoued.  
Ariana, 2083, Tunisia.

Telephone: (+216) 71857000 (ext. 2104)  
Facsimile: (+216) 71856829  
E-Mail: cnas@laposte.net

*Approved for public release*

Professor Nouredine Boudriga  
Head of CN&S research lab.

---

# NetRAM : A Novel Approach for Network Security Risk Management

Mohamed Hamdi, Jihène Krichène, Nouredine Boudriga, Mahmoud Tounsi

Higher School of Communications, Tunisia

This paper addresses the risk management in organizations networks and provides a 10-process approach to monitor security and prevent attacks. Our approach develops various formal techniques that are needed to guarantee the efficiency, correctness and generality of risk management.

**Key words** : Networked environment, risk management, quantitative risk assessment, theoretical design.

# NetRAM : A Novel Approach for Network Security Risk Management

## 1 Introduction

Over the last years, companies' dependence on information technology has grown tremendously. In many domains of activity, organizations rely totally on their networked environment and could not survive without it. However, the increasing occurrence of harmful attacks against networks and computing infrastructures has shown that security holes can lead to large damages. Therefore, security is becoming a crucial issue that has to be addressed seriously by network administrators and companies managers.

A statistical analysis of network attacks have revealed that most of the targets were protected by means of various security mechanisms and techniques, and that, in the presence of protection, the success of an attack is due to the misuse of the security resources by the administrators. In fact, many of the security administrators still rely on intuition to take strategic decisions related to their information system security.

Attempts to develop fundamental quantitative methods to avoid (or mitigate) network security risks arose recently ([1]). In addition, many governmental departments and organizations have published guides to assist companies in taking rational decisions to secure their systems security ([2, 3, 4]). Despite the increasing interest of many researchers in developing networks security technologies, and strengthening the existing approaches, security mechanisms are still non-sufficiently applied to the real world, because of many factors. In fact, quantitative risk analysis models present a high computational complexity, and their application in large environments, without the use of automated tools, is quasy unfeasible.

On the other hand, the available software tools do not permit to perform a complete risk management cycle as specified in the published methods. None of the available products automates all the steps of the risk management cycle. This makes risk management application hard for system administrators. Furthermore, most of the risk management products do not keep up with the evolution of risk analysis theoretical models.

To overcome these problems, we present an automated multi-process approach that assists information technology systems administrators and managers in their attempts to reduce security risks that threaten their assets. We also develop three major concepts: the composite data structure, which allows a better representation of the analyzed system, the optimization problem for risk analysis, and the security state monitoring of a network. We demonstrate that NetRAM covers the most important limits of the existing methods. From an architectural point of view, it introduces two extra processes that instil a continuity to the risk management process. The other differences reside mainly at the risk analysis level where a new formalism is proposed to avoid problems caused by asset-driven approaches. In addition, NetRAM relies on quantitative features to assess security risks unlike the most used methods that are based on qualitative criteria.

In the following sections, we give the key issues that characterize this approach. In Section 2, we present the main processes of our approach. In Section 3, we describe a set of theoretical tools that the proposed model uses to process specific data structures and we present a model for the decision making process. Furthermore, we address the problem of gathering and updating data necessary for conducting risk assessment. Section 4 addresses the definition and management of security network state. Section 5 concludes the paper.

## 2 NetRAM: architecture and features

NetRAM (Network Risk Analysis Method) has been developed and designed at the National Digital Certification Agency<sup>1</sup> (NDCA, Tunisia) within the framework of the project "Risk Management in a Networked Environment". It consists of ten processes depicted in Figure 1 and discussed below.

---

<sup>1</sup>NetRAM was designed and developed with NDCA by the Communication Networks and Security Research Lab, University of Carthage, Tunisia.



**2. Asset analysis:** This process is designed to collect detailed information about the assets that make part of the analyzed system. Indeed, an inventory containing all the resources must be established including some parameters such as the criticality of each asset or the objects that are authorized to access it. Furthermore, knowing that the components of the analyzed system are - in most cases - interrelated, the interaction between the resources given in the inventory is a point of interest. For instance, issues as data or information flow between the different entities may be focused. Also, physical interaction has to be analyzed as the security of an asset can depend on the security of an other asset that contains it physically (e.g., the security of an equipment put in a room depends on the security level given by the walls, the doors and the windows of the room itself). Thus, dependency trees can be built to show the interrelation between the resources of the system to facilitate the risk analysis process. This will be discussed later.

It is worth to mention that the documents related to security (e.g., security strategy, security policy) should be considered as special assets.

**3. Vulnerability identification:** The purpose of this process is to identify the weaknesses of the system described in the former step. The recommended approach is to have a vulnerability library pre-built and to check, for every vulnerability, whether it is present or not in the studied case. Many types of vulnerabilities can be considered, including:

- **Bugs:** Most of the software used in networked environment contain security holes, which can be exploited by malicious entities.
- **Mis-configurations:** Lack of experience or insufficient training of the personnel opens many breaches in system security. For instance, a mistake in the security policy of a firewall can allow unauthorized users to gain access to a private network.
- **Physical vulnerabilities:** Computers, communication equipments and media must be located in a secure facility. For example, if an attacker has physical access to a router, he can break it (denial of service) or try to modify its configuration from the console port (information leakage) if he is more clever.
- **Conceptual vulnerabilities:** The theoretical specifications of widely used communication and security protocols contain vulnerabilities that have to be addressed when analyzing the target system. One of the most famous vulnerabilities of this class is related to Simple Mail Transfer Protocol (SMTP), which does not authenticate the source of an e-mail.
- **Procedural vulnerabilities:** Inadequate procedures or inappropriate security measures can be exploited to realize malicious acts. An example of this type of vulnerability could be the absence of a backup policy, which can result in an irrecoverable loss of data.

**4. Threat identification:** Threats are potential events that can affect the system under analysis. They can result from malicious actions, accidents, natural disasters, etc. Unlike vulnerabilities, threats are measurable as each of them can be represented by its frequency and severity. Obviously, threat rates and impacts depend on the environment in which the system is situated. Factors as geographical position, political stance, or activity domain have to be taken in consideration when allocating probabilities of occurrence to threats.

In our approach, the frequency and the severity of a threat are dynamically updated according to the values of several metrics measured during the monitoring process.

**5. Risk analysis:** We define an attack as a combination of a threat and a set of corresponding vulnerabilities. A risk can then be seen as a weighted attack. Many weights can be allocated to a single attack where each weight corresponds to a criterion. The probability of the attack, its technical difficulty or the amount of money needed to carry it out may constitute good criteria. Then, as an extension to this reasoning, we introduce the concept of attack scenarios which may be viewed as attack chains where the last link is called the main attack, the first link is an elementary attack while the other links are intermediate attacks. This approach expresses accurately the occurrence of real attacks where a malicious user performs a set of intermediate attacks in order to achieve his major goal : the main attack. Furthermore, as a weight can be assigned to each

attack, we can conclude that a global weight may be allocated to an attack scenario by combining the elementary weights corresponding to each attack of the scenario. Weighted attacks are then called risk scenarios.

The aim of the risk analysis process is to define the main risks corresponding to each asset and to establish the risk scenarios leading to every main risk. Indeed, this process can be divided into the following steps :

- Identify the global (main) attacks corresponding to the asset;
- Build the attack scenarios for every main attack;
- Determine the risk coefficients (weights) for each scenario. A weight corresponding to a scenario is computed by combining the weights of the elementary attacks belonging to it.

New attack scenarios should be automatically appended to the existing ones whenever the occurrence of a new attack chain is detected during the monitoring step.

**6. Counter-measure proposal:** Possible risk scenarios issued from the former step can be ranked and prioritized. Then, for every scenario, a set of security rules are defined to minimize its priority. If the scenarios are ranked according to their probability of occurrence, the goal of the rule should be to minimize this probability. These rules must be general and must not include issues related to the effective implementation (e.g., practices to follow, products to acquire, technical standards to comply with, etc.).

The obtained set of rules constitutes the security strategy of the analyzed system.

**7. Counter-measure selection:** A set of candidate risk control techniques are proposed to implement the rules of the security strategy. Then, according to several criteria, the actions that would be taken to protect the system are selected and clearly described in a document that is called the security policy. These criteria may include: (1) the efficiency or the degree of protection given by the technique, (2) the cost of the technique, (3) the criticality of the asset concerned by the risk, and (4) the feasibility.

Moreover, a plan defining the prioritization of the retained actions with respect to the corresponding level of risk and to the allocated budget must be done during this process. Several counter-measures can even be omitted if the security level they allow to attain is not proportionate to their costs.

An incident response plan is also performed at this level. It defines the actions that might be taken when a security incident occurs. These actions should include procedures for the notification and the documentation of security incidents as well as a description of the recovery mechanisms.

**8. Implementation:** During this phase, the actions defined in the previous process are effectively implemented. The key operations of this process are:

- Acquiring the needed hardware and software specified in the security policy;
- Defining the teams that will be in charge of securing and monitoring the system;
- Promote security awareness;
- Enforce the application of the security practices;
- Implement the technical operations so that the system becomes compliant with the security strategy and with the security policy.

**9. Monitoring:** Monitoring is the central process of NetRAM. It can be seen as the detection of events that change several properties of the system under control. Events include security incidents, the addition of a new asset, or the appearance of a new vulnerability.

The monitoring module has two main features: it is continuous and retrospective. In fact, monitoring must be done, from the moment of the implementation of the first action of risk control, in a continuous way to ensure an efficient detection of the interesting events. In addition, it can be seen as a trigger that launches other processes which were already performed such as

vulnerability identification in the case of the appearance of a new vulnerability or counter-measure selection if a technological innovation allows the implementation of a solution that were impossible at the time of the initial application of the framework.

Moreover, several measurements are done at this level to compute the values of parameters used in the previous processes including the probability and the impact of an attack. This issue is discussed in more details in Section 3.

**10. Incident response:** This process is performed whenever an anomaly is detected at the “monitoring level”.

The incident response plan defines the constituency and the role of the incident response teams as well as the actions they have to take if an anomaly do occur. These actions cover essentially four topics:

- **Notification:** This includes the determination of who should be notified and which mean of communication should be used.
- **Impact attenuation:** This defines what should be done in order to reduce the impact of the incident and to stop its propagation through the analyzed system.
- **Recovery:** In case of damage, what should be done to ensure a recovery of the essential functions of the target system has to be clearly decided and achieved.
- **Documentation:** Part(s) of the information related to the incident has to be archived.

The two latter processes are not present in most of the existing methods such as OCTAVE, which has basically three phases consisting at building asset-based threat profiles, identifying infrastructure vulnerabilities and developing security strategy and plans. The main benefit of the addition of the monitoring and the incident response processes are to guarantee a continuous control of the system state and a better survivability meaning that the critical components can be recovered in an optimal time after the occurrence of an attack.

The major advantages of our method include the following four capabilities:

**NetRAM is a structured method.** The risk management task is organized among distributed collaborative processes. Any extension, addition, or modification within a process is transparent to the other processes,

**NetRAM is a general purpose method.** NetRAM is completely integrated to the activity of an enterprise in the sense that libraries, rules, metrics, and process localization take into consideration the enterprise specificity. Therefore, it can be applied in-house or outsourced without applying fundamental changes on its structure,

**NetRAM is adaptive.** Several processes are dynamic and adaptive in order to adapt cost estimation and security analysis to the evolution of the security technology,

**NetRAM is model based.** Theoretical developments support the process design in order to guarantee coherent representation of the enterprises’ systems and consistent formal validation when they are needed. This allows NetRAM to be automated to a high rate because of the theoretical tools it specifies and the multi-objective decision making it integrates,

## 3 NetRAM design

A variety of theoretical tools can be used in order to automate NetRAM’s steps and increase their efficiency. In this section we give a brief description of the activities associated with NetRAM most important processes.

### 3.1 Composite data structures

The basic ingredients of NetRAM design are four sets ( $R_b$ ,  $V_b$ ,  $A_b$  and  $D_b$ ) representing respectively assets, vulnerabilities, attacks and decisions (counter-measures). A key feature of these sets is that

they contain basic and composite elements. This allows an efficient modeling of the global situation of the system under analysis. Table 1 gives the meaning of basic and composite elements for each of the considered entities.

Table 1: Significance of basic and composite elements.

	Basic element	Composite element
Assets	Network node	Set of network nodes
Vulnerabilities	Single vulnerability	Set of vulnerabilities
Attacks	Simple attack	Attack scenario
Decisions	Single decision	Set of decisions

The reader would notice that composite assets, vulnerabilities and decisions have a different nature from composite network attacks. Indeed, by changing the order of the elements belonging to a composite attack, a different attack scenario is obtained. However, to represent a composite asset, vulnerability or decision, the order of the elements constituting it is not considered. For this reason, sets can be used to model the latter composite entities while uplets would represent attack scenarios. This means that, given the sets  $R_b$ ,  $V_b$ ,  $A_b$  and  $D_b$  that contain respectively the basic resources, vulnerabilities, attacks and decisions, the global sets representing these components have the following expressions:

- $R = R_b^*$ ,
- $V = V_b^*$ ,
- $A = \bigcup_{n \in \mathbb{N}} A_b^n$ ,
- $D = D_b^*$ ,

where  $(.)^*$  denotes the set of partitions of a given set.

Using this notation, the application of a set of security decisions to the analyzed system can be modeled by a counter-measure matrix, denoted  $C$ , having the size  $card(D) \times card(R)$  where each element can be equal to 0 or 1 according to the following rule:

$$\forall (i, j) \in \{1, \dots, card(D)\} \times \{1, \dots, card(R)\}$$

$$\begin{cases} C_{ij} = 1 & \text{if the decision } d_i \text{ is applied to the asset } r_j, \\ C_{ij} = 0 & \text{if not.} \end{cases}$$

Based on this notation, the objective of the risk analyst is to find the matrix  $C^*$  that is most appropriate to the system. This can be performed by allocating quantitative values to security attacks and decisions.

### 3.2 The risk analysis problem

Let  $\mathbf{I}$  and  $\mathbf{\Pi}$  be two  $card(A) \times card(R)$  matrices denoting the impact and the probability of the success of each attack against each asset. Similarly, consider two matrices  $\mathbf{I}_{\Pi}$  and  $\mathbf{\Pi}_{\mathbf{I}}$  where  $\mathbf{I}_{\mathbf{I}_{i,k}}$  (resp.  $\mathbf{\Pi}_{\mathbf{\Pi}_{i,k}}$ ) corresponds to the influence of the application of the decision  $d_i$  on the impact (resp. the probability) of the attack  $a_k$ , for every  $(i, k) \in \{1, \dots, card(D)\} \times \{1, \dots, card(A)\}$ . For instance,  $\mathbf{I}_{2,3} = 0.9$  means that if decision  $d_2$  is made, then the impact of the success of the attack  $a_3$  on any asset is reduced to a rate of 10% of the original impact.

In order to perform a balance between the efficiency of a set of counter-measures (modeled by the matrices defined above) and its cost, a  $card(D) \times card(R)$ -size matrix  $\Gamma$  should be introduced. For every  $(i, j) \in \{1, \dots, card(D)\} \times \{1, \dots, card(R)\}$ ,  $\Gamma_{ij}$  denotes the cost of the implementation of the decision  $d_i$  to protect the resource  $r_j$ .

These matrices are particularly useful to quantify security counter-measures. In fact, using the operators  $*$  and  $.$  denoting the term-by-term and classical multiplication, the functions that the risk analysis process aims at optimizing are represented as follows:

$$\begin{aligned} f_1(C) &= \|C * (\mathbf{I}_I \cdot (\mathbf{I} * \mathbf{M}))\|, \\ f_2(C) &= \|C * (\mathbf{I}_\Pi \cdot (\Pi * \mathbf{M}))\|, \\ f_3(C) &= \|C * \Gamma\|, \end{aligned} \quad (1)$$

where

- the operators  $*$  and  $.$  are respectively the term-by-term and the classical product of matrices,
- $\mathbf{M}$  is a  $\text{card}(A) \times \text{card}(R)$ -size matrix such that

$$\begin{aligned} &\forall (k, j) \in \{1, \dots, \text{card}(A)\} \times \{1, \dots, \text{card}(R)\} \\ &\begin{cases} \mathbf{M}_{kj} = 1 & \text{if the attack } a_k \text{ is possible to carry out against the asset } r_j, \\ \mathbf{M}_{kj} = 0 & \text{if not.} \end{cases} \end{aligned}$$

- $\|\cdot\|$  is a norm on the  $\text{card}(A) \times \text{card}(R)$ -size matrices vector space.

The matrix  $\mathbf{M}$  ensures that only possible attacks are taken into consideration when evaluating the efficiency of a set of counter-measures. In fact, even if a decision mitigates the effect of a given attack, it has not a positive impact on the system if there is not an asset such that this attack is possible to perform against it.

The functions  $f_1$  and  $f_2$  allow to evaluate the efficiency of a matrix  $C$  while  $f_3$  represents the cost of the decisions enclosed within this matrix. In practice, the objective is to minimize these former functions which can not be directly achieved due to the lack of natural order on the set of vectors. We propose heuristic-based evolutionary algorithms to address this multi-objective decision problem as they have been widely used in this context since several years.

### 3.3 Data collection

In the above analysis, we assumed that the basic components, sets and matrices, are known. In practical situations, gathering this data requires specific procedures and equipments which are described in this subsection.

- The set  $R_b$  consists in an inventory of the assets and can be determined by doing on-site visits or surveys,
- The set  $V_b$  is the vulnerability library that can be built through the use of databases provided with known vulnerability scanners (e.g., Nessus, etc.). Expert opinion can also be used, particularly for human behavior vulnerabilities,
- The sets of attacks  $A_b$  are obtained from Intrusion Detection Systems (IDSs). Furthermore, attack scenarios are deduced by the mean of attack trees that were first introduced by B. Schneier in [6] and then discussed in [7]. Our purpose is to determine and assess the possible sequences of events that would lead to the occurrence of main attacks.

The root of a tree represents the main objective of an attacker while the subordinate nodes are elementary attacks that are necessary to perform for achieving the global goal. A *qualitative analysis* yields to a logical representation of the tree by reducing it to the form:

$$t_0 = S_1 \vee S_2 \vee \dots \vee S_N, \quad (2)$$

where  $t_0$  is the root of the tree and  $S_i$ , for  $i \in \{1, \dots, N\}$ , is the  $i^{\text{th}}$  attack scenario corresponding to  $t_0$  and having the following structure:

$$S_i = t_1^{S_i} \wedge t_2^{S_i} \wedge \dots \wedge t_{N_{S_i}}^{S_i}, \quad (3)$$

where  $(t_j^{S_i})_{j \in \{1, \dots, N_{S_i}\}}$  are the elementary threats belonging to  $S_i$ .

For instance, the tree shown in figure 2 can be reduced to the following expression:

$$a = (b \wedge e \wedge f) \vee c \vee (d \wedge g) \vee (d \wedge h). \quad (4)$$

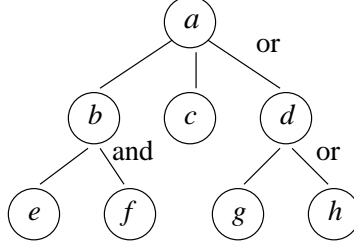


Figure 2: Typical attack-tree.

- The impact of performing an attack on a given resource is assessed by the risk analysis team members. This task is among the hardest in the risk analysis process as different kinds of potential effects should be translated to monetary values (e.g. loss of popularity, etc.),
- Determining the probability of an attack is a crucial issue that has an important influence on the performance of the risk analysis method. In NetRAM, probabilities are determined on the basis of expert opinions. Statistics provided by renowned institutes can be helpful in this context,
- Similarly, the evaluation of the influence of counter-measures on attacks, represented by the matrices  $\mathbf{I}_I$  and  $\mathbf{I}_{II}$ , relies on human intervention.

The three latest points show that even NetRAM processes can be automated to high rate, the human factor remains a basic component of the risk management cycle. To this end, the risk analysis team members should be chosen appropriately to guarantee the efficiency of the method. For example, technical skills should be a good selection factor.

Concerning the matrix  $\mathbf{M}$ , it can be seen as the product of two matrices  $\mathbf{E}$  ( $card(A) \times card(V)$ -size) and  $\mathbf{P}$  ( $card(V) \times card(R)$ -size) containing binary elements according on the following rules.

$$\forall (k, l) \in \{1, \dots, card(A)\} \times \{1, \dots, card(V)\}$$

$$\begin{cases} \mathbf{E}_{kl} = 1 & \text{if the attack } a_k \text{ exploits the vulnerability } v_l, \\ \mathbf{E}_{kl} = 0 & \text{if not.} \end{cases} \quad (5)$$

$$\forall (l, j) \in \{1, \dots, card(V)\} \times \{1, \dots, card(R)\}$$

$$\begin{cases} \mathbf{P}_{lj} = 1 & \text{if the vulnerability } v_l \text{ is present in the asset } r_j, \\ \mathbf{P}_{lj} = 0 & \text{if not.} \end{cases} \quad (6)$$

$\mathbf{E}$  can be built using public attack databases such as Mitre's CVE [10] (Common Vulnerabilities and Exposures) or the NIST I-cat project [11].  $\mathbf{P}$  can be filled using various vulnerability detection mechanisms. In our case, automated scanners and questionnaires are used.

### 3.4 Data update

Since NetRAM is a continuous process that involves a periodical re-assessment of security risks, its quantitative parameters must be updated depending on the changes that occur in the studied environment. For instance, the probability of an attack can be assimilated to its frequency of

occurrence. Indeed, supposing two occurrences of an attack are independent events, it can be stated, according to the central limit theorem, that is a good estimation of the probability of the attack.

Moreover, attack and vulnerability databases ( $A$  and  $V$ ) should be maintained in order to take into consideration the appearance of new threats and exploits. This is addressed by implementing a learning system based on neural networks [12]. Discussing this mechanism is beyond the scope of this paper and will be addressed in a future work.

This shows that putting and implementing an efficient update policy assumes the use of a set of sensors as well as several event collectors and analyzers. A distributed hybrid (host-based and network-based) IDS presents a good alternative to achieve this objective, if enriched with an appropriate learning mechanism.

## 4 Network state definition and management

Several metrics that help expressing the state of the analyzed network should be measured in a continuous way to permit an efficient detection of various anomaly. [13] offers a good list of such metrics. In particular, a warning system has to be implemented to generate alerts if a metric (input signal) exceeds a given threshold value.

Define  $X$  to be a random variable that represents the actual percentage of use of a resource (e.g., CPU, memory, and disk space) and  $Y$  a random variable that represents the estimated percentage of use of the same resource. Let  $p(x)$  be the probability density function (pdf) of  $X$  and  $p(y|x)$  the conditional pdf of  $Y$ , given  $X$ . Then, the posterior pdf  $p(x|y)$  can be expressed as:

$$p(x|y) = \frac{p(y|x)p(x)}{k(y)}, \quad (7)$$

where  $k(y) = \int_0^\infty p(y|x)p(x)dx$ , according to Bayes rule.

The warning threshold  $y^*$  is defined by the fact that the domain for issuing an alert is  $\{y \geq y^*\}$ . If  $c$  denotes the capacity of the considered resource available in the system under analysis (CPU speed, amount of memory, etc.), the probability that this capacity will be crossed, conditioned by the estimation  $y$  is  $P(x \geq c|y)$ . The decision system is represented by four cost functions:

- $D_{00}(y, c)$ : no exceed, no alert,
- $D_{10}(y, c)$ : alert present, no exceeds,
- $D_{01}(y, c)$ : no alert, exceeding noticed,
- $D_{11}(y, c)$ : alert and exceeding noticed.

Thus, the expected property loss without a warning system is

$$R_1(c) = \int_0^\infty q(y, c)D_{01}(y, c)k(y)dy, \quad (8)$$

$q(y, c)$  is the exceeding probability  $P(x > c|y)$ .

The expected property loss with a warning system is equal to

$$R_2(c) = \int_0^{y^*} (q(y, c)D_{01}(y, c) + (1 - q(y, c))D_{10}(y, c))k(y)dy \\ + \int_{y^*}^\infty (q(y, c)D_{11}(y, c) + (1 - q(y, c))D_{10}(y, c))k(y)dy.$$

The warning threshold is then determined by solving the problem

$$\mathbf{max}(R_1(c) - R_2(c)).$$

## 5 Conclusion and Perspectives

In this paper, we have exposed a risk management method, called NetRAM. We began by defining the main processes of this method and detailing the constituency of each of them. We attempted to palliate the theoretical lacks of the commonly used methods. Therefore, a substantial portion of the paper was devoted to outlining the theoretical developments related to the proposed method. In our future work, we plan to extend the formalisms introduced in this paper in order to obtain a global mathematical framework that represents NetRAM's risk management cycle.

## References

- [1] Christopher J. Alberts, Audrey J. Dorofee, "*Managing Information Security Risks: The OCTAVE Approach*," Addison Wesley Professional, ISBN: 0321118863, July 2002.
- [2] G. Stonebumer, A. Grogen, A. Fering, "*Risk Management Guide for Information Technology Systems*," National Institute for Standards and Technology, special publication 800-30.
- [3] "*A Guide to Risk Management and Safeguard Selection for IT Systems*," Government of Canada, Communications Security Establishment, January 1996.
- [4] "*Information Security Risk Assessment: Practices of Leading Organizations*," United States General Accounting Office, GAO/AIMD-00-33, November 1999.
- [5] J. Kontio, G. Getto, D. Landes, "*Experiences in Improving Risk Management Processes Using the Concepts of the Riskit Method*," SIGSOFT98, Sixth Symposium of the Foundations of Software Engineering, November 98.
- [6] Bruce Schneier, "*Secrets and Lies: Digital Security in a Networked World*," John Wiley & Sons, ISBN: 0471253111, 2001.
- [7] A. P. Moore, R. J. Ellison, R. C. Linger, "*Attack Modeling for Information Security and Survivability*", Carnegie Mellon University, Technical Note, CMU/SEI-2001-TN-001.
- [8] R. E. Rosenthal, "*Concepts, Theory, and Techniques: Principles of Multi-objective Optimization*", Decision Sciences, vol. 16, pp. 133-152, 1985.
- [9] K. Deb, "Evolutionary Algorithms in Engineering and Computer Design," John Wiley & Sons, pp. 135-161, 1999.
- [10] FedCIRC, U.S. General Services Administration, "Common Vulnerabilities and Exposures," <http://www.cve.mitre.org>.
- [11] National Institute for Standards and Technology, Computer Security Division "The ICAT Project," <http://icat.nist.gov>.
- [12] C. M. Bishop, "Neural Networks for Pattern Recognition," Oxford University Press, Oxford, 1995.
- [13] "*Detecting signs of intrusions*", Carnegie Mellon University/Software Engineering Institute, Security Improvement Modules (m-09), December 2000.
- [14] D. J. Marchette, "Computer intrusion Detection and Network Monitoring: A Statistical Viewpoint," Springer-Verlag, ISBN: 0387952810, 2001.