An Integrated use of ISO27005, Mehari and Multi-Agents System in order to Design a Comprehensive Information Security Risk Management Tool

Mohamed Ghazouani
ENSEM
Casablanca, MAROC

Hicham Medromi
ENSEM
Casablanca, MAROC

Adil Sayouti
ENSEM
Casablanca, MAROC

Siham Benhadou
ENSEM
Casablanca, MAROC

ABSTRACT

While there are many framework which help users in Security Risk Assessment, the authors of this paper know of none which actually try to automate the process by using multi agent system. This article presents a multi-agent expert system, a web-based solution where users create autonomous agents to perform an information security assessment. Users specify parameters to guide and constrain an agent's overall behavior. The key element that differentiates this research from the previous ones is that none of them are based on multi-agents system.

General Terms

Security risk assessment, risk management system, framework, audit, information system.

Keywords

ISO27001, ISO27005, MEHARI, Multi-agent system (MAS).

1. INTRODUCTION

Risk analysis is one of the first steps and is the main way to improve security. If to optimize means making big effort, it also means making it with the minimum of resources. With all interest in having adequate security and to minimize costs, the risk analysis is very important for all environments.

Risk management has long ago been incorporated businesses of all kinds. Now that computers came into the business, IT risk should be taken into consideration. Furthermore, the computer is now in charge of several critical operations, so the IT risk becomes one of the main risks of the company of today.

Risk assessment is the determination of value of risk related to a concrete situation and a recognized threat based on two factors, the probability and impact. The level of risk is the product of the two risk factors. IT risk assessment can be performed by a qualitative or quantitative approach. When the impact is assessed in dollars, this goes to quantitative analysis, otherwise it relates to qualitative analysis. The system addresses the qualitative risk.

This paper is presented as follows: in the section 2 it will give a survey of available information security risk management methods and tools, in the section 3 and 4 it will present a description of ISO27005 and Mehari, in the section 5 it will propose the approach, in the 6 and 7 it will introduce the multi agent system, in the section 8 it will propose the architecture for ISRMT Tool.

2. AVAILABLE RISK MANAGEMENT METHODS AND TOOLS

Risk management methods and tools enable the organization to plan and implement programs to maximize their opportunities and to control the impact of potential threats. This section provides an overview of available security risk analysis methods and tools.

2.1 Methods

Table 1. Risk Management Methods

Au IT Security Handbook	Cramm	A&K Analysis	Ebios
ISAMM	ISF Methods	SP800 30	ISO/IEC 2005
ISO/IEC 27001	IT Grundschutz	Magerit	Marion
Mehari	MIGRA	Octave	Risksafe Assesment

2.2 Tools

Table 2. Risk Management Tools

Countermea sures	Cramm	EAR/Pilar	Ebios
Gstool	GxSGSI	ISAMM	Mehari
Callio	Casis	CCS Risk Manager	Cobra
MIGRA Tool	Modulo Risk Manager	Proteus	Octave
Ra2	Real ISMS	Resolver*Ballot	Resolver*Risk
Risicare	Riskwatch	RM Studio	SISMS
TRICK light	Acuity Stream		

Most of these tools are Commercials.

None of the tools implement Multi agent system.

There is no tool developed in Morocco. Usability of the tools used by Moroccan organizations and contribute to help Moroccan organizations in the information security field are important for us.

There is very little research related to the applications of multi agent systems (MAS) in Audit Information System Security.

Absence of audit.

Do not provide recommendations or immediate solution to security problems.

Difficulty of use, it's requires a certain level of expertise.

Do not explain their calculation methods.

Require a lot of time to implement.

Based on the above methodologies, researches and others work described in [1] [2] [3] this work propose an integrated use of ISO27005, Mehari and multi-agents system to develop an Information Security Risk Management Tool (ISRMT).

3. ISO 27005

The purpose of ISO 27005 is to provide guidelines for information security risk management. It supports the general concepts specified in ISO 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach. It does not specify, recommend or even name any specific risk analysis method, although it does specify a structured, systematic and rigorous process from analyzing risks to creating the risk treatment plan [4].

Is a Standard that encompasses the code of practice for information security management describing a set of information security control objectives and a set of generally accepted best practice security controls [5].

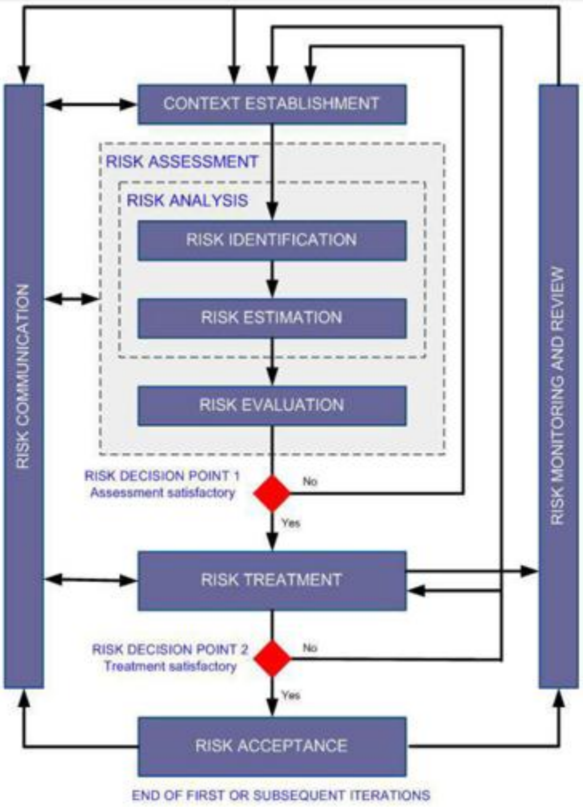


Fig 1 : Information security risk management

ISO 27005 is applicable to all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations) which intend to manage risks that could compromise the organization's information security."

Figure 1 gives an overview of the Information security risk management process in ISO 27005.

4. MEHARI

MEHARI is a risk analysis and management method developed by CLUSIF and supported by software managed by the company Risicare (http://www.risicare.fr). MEHARI, originally developed in 1996, aims at assisting the executives (operating managers, CISO, CIO, risk manager, auditor) in their efforts to manage the security of Information and IT resources and to reduce the associated risks. MEHARI is compliant to ISO 13335 risk management standard and is suitable for the ISMS process described by ISO 27001. It allows the stakeholder to develop security plans, based on a list of vulnerability control points and an accurate monitoring process to achieve a continual improvement cycle. MEHARI provides: [6]

- Knowledge bases of risk situations
- Rules for the consolidation of the risk analysis resulting in an optimal setting of action plans
- Analyze the major stakes
- Analyze the vulnerabilities
- Decrease and manage the risks
- Monitor the security of information
- Audit data base

5. PROPOSED APPROACH

ISRMT is a qualitative tool for assessing information security risks; it utilizes concepts defined in ISO27005 and Mehari. The tool provides an easy-to-apply information security risk analysis spanning the enterprise. With ISRMT

- The list of relevant assets can be established
- Threats can be identified
- vulnerabilities can be identified
- Probability that a threat will occur can be assessed
- The impact if the threat does occur can be assessed
- The risk levels can be established
- Mitigating controls and safeguards are identified
- Implementation action plan can be developed

This approach opts for a qualitative risk analysis for applications and databases. The quantitative method evaluate, based on judgment, experience, and situational awareness:

- The exposure of the asset and frequency of the threats to get the likelihood value.
- Control is the result from the audit questionnaires based on Mehari.

Probability = (exposure + frequency) / 2 * 1 / Control

- The confidentiality, integrity and availability of information to get the impact value. These three—the loss of confidentiality, integrity, and availability—are ranked as the top business liabilities by organizations. [7]

Impact = Max of (confidentiality, integrity, availability)

- Confidentiality concerns the protection of sensitive information from unauthorized disclosure.
- Integrity relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations.
- Availability relates to information being available when required by the business process now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities. [6]

Approaches that can be used for qualitative analysis include, but are not limited to, internal interviews, internal surveys, internal questionnaires, storyboarding and internal Focus groups. For this project the authors chose internal surveys and internal questionnaires, because surveys and questionnaires are usually the best mechanism to accomplish data collection when you have to query a large group of individuals. There will always be cases where the recipients will need additional clarification by conducting a focus group. [7]

6. MULTI AGENT SYSTEM

Multi-agents systems (MAS) are based on the idea that a cooperative working environment comprising synergistic software components can cope with problems which are hard to solve using the traditional centralized approach to computation. Smaller software entities – software agents – with special capabilities (autonomous, reactive, pro-active and social) are used instead to interact in a flexible and dynamic way to solve problems more efficiently. Agents model each other’s goals and actions; they may also interact directly (communicate) [8].

6.1 Agent

Agents are software entities that have a very specific task and that decide for themselves what they need to do in order to satisfy their design objectives. They perceive their environment through sensors and acts on that environment through effectors [9]:

A characteristic is an intrinsic or physical property of an agent. The following are some common agent characteristics (Morreale, 1998; Wooldridge & Jennings, 1995):

- Autonomy: An agent can act on another’s behalf without much guidance.
- Communication: An agent can communicate with other agents on a common topic of discourse by exchanging a sequence of messages in a speech-act-based language that others understand. The domain of discourse is described by its ontology.
- Mobility: An agent can migrate from one system to another in a pre-determined fashion or at its own discretion. Accordingly, agents can be static or mobile.
- Learning: An agent can have the ability to learn new information about the environment in which it is deployed and dynamically improve upon its own behavior.
- Cooperation: An agent can collaborate and cooperate with other agents or its user during its execution to minimize redundancy and to solve a common problem.

6.2 Potential of Multi-Agent Systems

The use of agent-orientation in the modeling, design, and implementation of an Information Security Risk Management provides at least the following benefits:

- **Flexible**. Agent architectures are more flexible, modular and robust than, for example, object-oriented ones. They tend to be open and dynamic as their components can be added, modified or removed at any time (Yu, 1997).
- **Pro-activeness**. [10] Intelegent agents are able to exhibit goal-directed behavior by taking the initiative in order to satisfy their design objectives :
    - **Goal-directed behavior**. [11] If agents are a level of abstraction between a user and a set of low-level tasks, an agent must be able to create a mapping between the high-level goal and the available tools such that it can use the tools effectively to achieve the goal. In other words, the agent must be able to plan. In this project, a RSSI may task an Audit agent to make an Information Systems Security Audit.

The ability of an agent to exhibit goal-directed behavior typically comes from incorporating AI planning techniques into the agent code.

- **Cognizant Failure**. An important (but often neglected) component of goal driven behavior is cognizant failure. Cognizant failure is the idea that once tasked, the agent either completes the task and returns, or recognizes that it cannot complete the task and reports a failure.

- **Reactivity**. Agents are crucial when operating in an unpredictable environment containing a large number of data sources scattered over multiples sources. If an agent queries an information source and finds no answers to its query, it would then try alternate sources of information until it could come up with a reasonable number of answers.
- **Learning**. Another important characteristic of autonomous behavior is the ability to enhance future performance as a result of past experiences. Machine learning techniques allow an agent to learn new methods or refine existing ones to meet specific needs.
- **Communication and cooperation**. Intelligent agents are capable of interacting with other agents (and humans) in order to o achieve a common goal.
- **Temporal continuity**. Persistence of identity and state over long periods of time.
- **Information gathering and filtering**. Is another useful example of using agents for user assistance. Using questionnaires and survey can be very time-consuming. But rather than do this work on our own, agents can do this work for us. In addition, automating data collection ensures that risk assessment is thorough and complete.

7. PROPOSED ARCHITECTURE

Figure 2 graphically illustrates the global view of the ISRMT Tool. This section discusses its components.

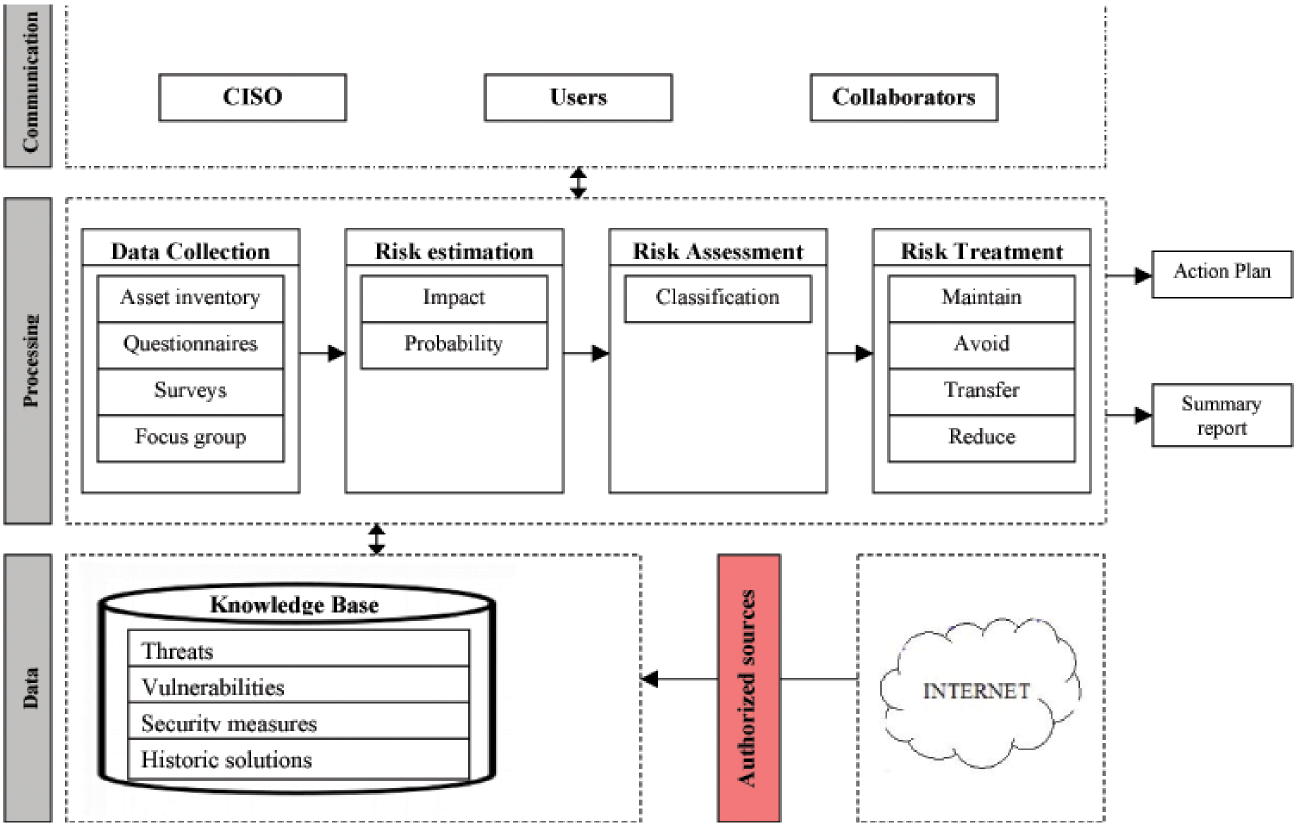


Fig 2 : Global view of the ISRMT Tool

The system is totally interactive and based on multi agent system which is composed of the following agents: Risk Agent, Collect agent, Estimation agent, Evaluation agent, Treatment agent, Historian agent, Service agent and Listening agent. The proposed SMA architecture is depicted in figure 3.

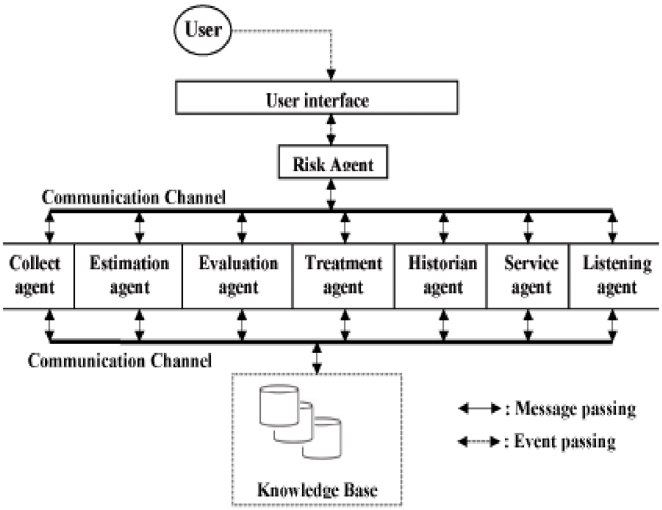


Fig 3 : Multi agent architecture

Risk agent is in charge of creating Goal-directed behavior to solve the problems it receives from the human interface agent. It handles all communication with the users and communicates with the Collect agent, Estimation agent, Assessment agent, Treatment agent, Historian agent in order to manage the planning and execution.

Collect agent is in charge of sending audit questionnaires and survey to users or collaborators and ensure respect duration, retransmit, make a first consolidation and detect anomalies in respondents' answers. It’s also in charge of Assessment of level of compliance for a given level and derives a control score that was described in section 5.

Estimation agent handles the execution of the impact and the probability calculation.

Assessment agent has the role of classifying the risk based on the ISO 27005 risk assessment matrix. An agent who has done multiple assessments within an organization would probably already have some expectations on what the results will be and could easily identify inconsistencies in the results based on these expectations.

Treatment agent is in charge of, according to the user choice, risk treatment. It suggests administrative controls, technical or physical to be applied within the information system and propose solutions that were applied to similar problems by consulting knowledge base or communicate with the historian agent.

Historian agent is used to identify plans that where applied in similar problems. The historian agent is in charge of archiving data and making it available for agents. It receives problems from many agents and stores them in a database. Storing these problems is important because they contain information about previous task executions, information that is important for agents to make decisions.

Service agent handles the relation between the users and the system. It sends periodic updates to the user interface so they can relay task progress to the user.

In case of execution problems for all these above agents, they will ask a risk agent to find alternatives/suggest a solution for it.

Listening agent has the role of store the threats and vulnerabilities that it receive from internet.

The system consists of three layers.

7.1 Communication

This layer is composed of:

- Chief Information Security Officer (CISO). The CISO develops and maintains enterprise security and risk policies, oversees vendor and technology risk management, and influences user behavior.
- Users. The asset owners, prior to the focus group, they all received an electronic questionnaire or survey about the asset they use.
- Collaborators. All employees involved in the process of risk assessment.

7.2 Processing

The processing layer consists of the following steps:

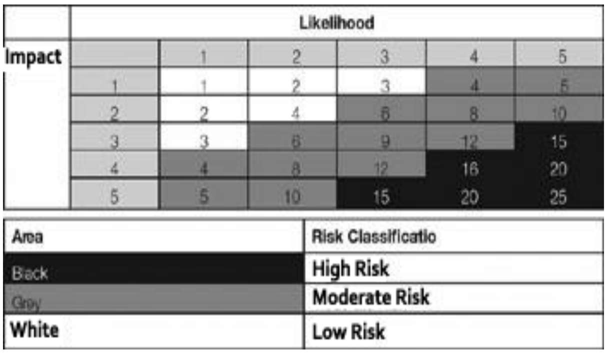
- **Data collection**. This phase does not actually take a lot of manpower in terms of the security office but it does take a long time because the activity mainly relies on collecting data from different parts of the organization. [7]. Depending on how many assets are being analyzed and the turnover time for collection from other departments, this phase could last from a few weeks to several months. Its why this phase should be done through a questionnaire and survey send to those concerned. The main output for this phase is a matrix containing all the application, databases, asset owners, technical contacts, description of the asset and the results of control score.
- **Risk estimation**. Once all the necessary information has been collected the next step is to start risk estimation activities. The main activities in this phase are the calculation of the impact and probability for each threat. Using this formula RISK= IMPACT x PROBABILITY by a simple multiply the impact and likelihood scores to obtain the final risk score as shown in Table 3. The main output for this phase is the score risk.

Table 3. Sample Risk Score

E-mail system			
Threat	**Impact**	**Probability**	**Risk score**
Disclosure of confidential data	5	1	5

- **Risk assessment**. The first thing to do is make sense of the risk scores. Based on the results of the previous activity all we really have are a bunch of numbers. The challenge is to take these numbers, and transform them into something that is of a more "human readable" format by using a risk threshold chart based on the ISO 27005 as illustrated below in Figure 4. This allowed us to categorize each risk into buckets of HIGH, MEDIUM, and LOW.

By utilizing this technique, it's easy to prioritize the high risk items for remediation. This does not mean that only HIGH risk items should be remediated. The system use this risk classification method as more of a prioritization technique and what would subsequently be targeted for remediation based on this analysis is based on the organization's risk acceptance process. Some organizations may only ever address high risk items while others may choose to address all risks to some extent.



	Likelihood					
Impact		1	2	3	4	5
	1	1	2	3	4	5
	2	2	4	6	8	10
	3	3	6	9	12	15
	4	4	8	12	16	20
	5	5	10	15	20	25

Area	Risk Classificatio
Black	High Risk
Grey	Moderate Risk
White	Low Risk

Fig 4 : Risk threshold chart

- **Risk treatment**. Once risks have been identified and assessed, all techniques to manage the risk fall into one or more of these four major categories :
  - **Avoidance**. Risk avoidance involves eliminating the risk-producing activity entirely (or never beginning it).
  - **Transferring (sharing).** Risk transfer strategies turn over or share the responsibility of performing a risky activity to another party. Examples of risk transfer are transferring the liability for losses to an insurance carrier, or outsourcing an activity to a contractor with the stipulation that the contractor assume the risk.
  - **Acceptance.** After all reasonable and cost effective risk responses have been taken, an organization is left with risk acceptance.
  - **Reduction**. If the user chose to reduce the risk the system propose a list of safeguards measures and controls to be implemented. Controls are mechanisms that detect or prevent threats sources from leveraging vulnerabilities and thus are closely tied to likelihood as it affects the probability of a risk [7].

An action plan and a summary report are derived at the end of these steps. The action plan suggests administrative controls, technical or physical to be applied within the information system.

7.3 Data

The Data tier contains the central knowledge base for the whole system. Its may be populate automatically (by Agents or Internet) or manually (uploading CSV files). Because the first version of system restricted the risk assessment to software assets, the threat catalog is based on Microsoft Threat Model—A list of 36 threats focusing on application security risks. This is freely available from the Microsoft website [13].

8. CONCLUSION AND FUTURE WORK

In general, the safety of SI has several objectives. Safety, then, must protect information such as company assets against data loss, disclosure or alteration to ensure continuity of business operations. This research document could form the basis for a technical project to develop an actual web-based Information Security Risk Management Tool to achieve theses objectives. In the future, this project could then also include the COBIT standard to assist organizations in exactly on 'what' must be done.

9. ACKNOWLEDGMENTS

I would like to thank to my advisor Ms. H. Medromi, PhD. Sayouti Adil, PhD. amd Benhadou Siham for their invaluable guidance and many useful suggestions during my work on this paper. I would also like to express my gratitude to all those who gave me the possibility to complete this paper.

10. REFERENCES

[1] SAPA: Software Agents for Prevention and Auditing of Security Faults in Networked Systems. Information Networking. Convergence in Broadband and Mobile Networking. Lecture Notes in Computer Science Volume 3391, 2005, pp 80-88.

[2] Approach to Solving Security Problems Using Meta-Agents in Multi Agent System. Agent and Multi-Agent Systems: Technologies and Applications. Lecture Notes in Computer Science Volume 4953, 2008, pp 122-131.

[3] A Multi-agent System for Computer Network Security Monitoring. Agent and Multi-Agent Systems: Technologies and Applications. Lecture Notes in Computer Science Volume 4953, 2008, pp 842-849.

[4] Information technology—Security techniques—Information security risk management. INTERNATIONAL STANDARD ISO/IEC 27005 First edition 2008-06-15.

[5] Jake Kouns and Daniel MinoliInformation. 2010. ISBN:9780471762546 Technology Risk Management in Enterprise Environments: A Review of Industry Practices and a Practical Guide to Risk Management Teams.

[6] by Jake Kouns and Daniel Minoli 2010. ISBN:9780471762546. Information Technology Risk Management in Enterprise Environments: A Review of Industry Practices and a Practical Guide to Risk Management Teams

[7] Mark Ryan M. Talabis and Jason L. Martin 2013. ISBN:9781597497350. Information Security Risk Assessment Toolkit: Practical Assessments Through Data Collection and Data Analysis

[8] InTech, April 4, 2011. "Multi-Agent Systems - Modeling, Control, Programming, Simulations and Applications", ISBN 978-953-307-174-9

[9] Prentice Hall; 3 edition, 2009. Stuart J. Russell and Peter Norvig, "Artificial Intelligence: a Modern Approach".

[10] M. Wooldridge and N.R Jennings. Intelligent agents : Theory and practice. The Knowledge Engineering Review, 10(2) : 115-152, 1995.

[11] Roxanne E. Burkey and Charles V. Breakfield (eds.) 2001. Designing a Total Data Solution: Technology, Implementation, and Deployment. ISBN:9780849308932

[12] Automating System Security Audits. *ISACA Journal*, volume 1, 2004.

[13] http://msdn.microsoft.com/en-us/library/ff648641.aspx Improving Web Application Security: Threats and Countermeasures. J.D. Meier, Alex Mackman, Michael Dunner, Srinath Vasireddy, Ray Escamilla and Anandha Murukan. Microsoft Corporation.

[14] "Autonomous and Intelligent Mobile Systems based on Multi-Agent Systems" Auteurs: A. Sayouti and H. Medromi. Book Chapter in the book "Multi-Agent Systems - Modeling, Control, Programming, Simulations and Applications", ISBN 978-953-307-174-9, InTech, April 4, 2011.