WOSIS 2009

Alfonso Rodríguez, Mariemma I. Yagüe and
Eduardo Fernández-Medina (Eds.)

Security in Information Systems

Proceedings of the
7th International Workshop on
Security in Information Systems – WOSIS 2009
In conjunction with ICEIS 2009
Milan, Italy - May, 2009

INSTICC
Press

Alfonso Rodríguez
Mariemma I. Yagüe and
Eduardo Fernández-Medina (Eds.)

Security in Information Systems

**Proceedings of the
7th International Workshop on
Security in Information Systems
WOSIS 2009**

In conjunction with ICEIS 2009
Milan, Italy, May 2009

INSTICC PRESS
Portugal

Volume Editors

Alfonso Rodríguez
University of Bio-Bio
Chile

Mariemma I. Yagüe
University of Málaga
Spain

and

Eduardo Fernández-Medina
University of Castilla-La Mancha
Spain

7th International Workshop on
Security in Information Systems
Milan, Italy, May 2009

Printed in Portugal

ISBN: 978-989-8111-91-3
Depósito Legal: 292365/09

Foreword

The Seventh International Workshop on Security in Information Systems was held in conjunction with ICEIS 2009 in Milan, Italy. As in previous years, this workshop served as a meeting point, bringing together researchers from academia and commercial developers from industry to review the current state of the art in Security in Information Systems.

Papers presenting the most recent theoretical, and practical works in security for Information Systems were received, a total of 19 submissions. This year the number of submitted papers has decreased, maybe due to the high number of new security conferences held recently. All submissions were reviewed by at least three program committee members. Finally, we accepted 8 full papers, and 5 short papers. Unfortunately, some good papers had to be rejected because they did not correspond to WOSIS'09 criteria.

As is tradition in WOSIS as part of the works selection, the best papers are included in an extended and revised version in the prestigious Journal of Universal Computer Science.

It is our pleasure to thank the members of both the program committee and the members of the organisation committee for all their hard work, dedication and commitment to the success of the project.

Finally, we gratefully acknowledge all the authors who submitted papers, accepted or not, to WOSIS 2009 for their efforts, and we hope to receive new contributions for WOSIS 2010. Also the participants who together made this workshop an intellectually successful event through their active contributions.

May 2009,

Alfonso Rodríguez
University of Bio-Bio, Chile

Mariemma I. Yagüe
University of Málaga, Spain

Eduardo Fernández-Medina
University of Castilla-La Mancha, Spain

Workshop Chairs

Alfonso Rodríguez
University of Bio-Bio
Chile

Mariemma I. Yagüe
University of Málaga
Spain

and

Eduardo Fernández-Medina
University of Castilla-La Mancha
Spain

Program Committee

Ernesto Damiani, University of Milan, Italy
Jaime Delgado, Universitat Politècnica de Catalunya, Spain
Csilla Farkas, University of South Carolina, U.S.A.
Eduardo B. Fernandez, Florida Atlantic University, U.S.A.
Simon Foley, University College Cork, Ireland
Steven Furnell, University of Plymouth, U.K.
Christian Geuer-pollmann, European Microsoft Innovation Center, Germany
Paolo Giorgini, University of Trento, Italy
Carlos Gutiérrez, Correos Telecom, Spain
Michael Hafner, University of Innsbruck, Austria
Renato Iannella, NICTA, Australia
Jan Jurjens, Open University, U.K.
Stamatis Karnouskos, SAP Research, Germany
Martin Olivier, University of Pretoria, South Africa
Brajendra Panda, University of Arkansas, U.S.A.
Günther Pernul, University of Regensburg, Germany
Mario Piattini, Escuela Superior de Informatica, Spain
Joachim Posegga, Institute of IT Security and Security Law, Germany
Torsten Priebe, Capgemini, Austria
Indrajit Ray, Colorado State University, U.S.A.

Indrakshi Ray, Colorado State University, U.S.A.
Damien Sauveron, Xlim – University of Limoges, France
Ambrosio Toval, University of Murcia, Spain
Rodolfo Villarroel, Universidad Católica del Maule, Chile
Sabrina De Capitani Di Vimercati, University of Milan, Italy

Table of Contents

Foreword iii

Workshop Chairs v

Program Committee v

Full Papers

Unconditionally Secure Authenticated Encryption with Shorter Keys 3
Basel Alomair and Radha Poovendran

Deterministic Cryptanalysis of some Stream Ciphers 16
P. Caballero-Gil, A. Fúster-Sabater and C. Hernández-Goya

Enhancing Rights Management Systems Through the Development of Trusted Value Networks 26
Víctor Torres, Jaime Delgado, Xavier Maroñas, Silvia Llorente and Marc Gauvin

An Enhanced Approach to using Virtual Directories for Protecting Sensitive Information 36
Dongwan Shin and William Claycomb

Risk-Aware Secure Supply Chain Master Planning 46
Axel Schröpfer, Florian Kerschbaum, Dagmar Sadkowiak and Richard Pibernik

SLSB: Improving the Steganographic Algorithm LSB 57
Juan Jose Roque

MMSM-SME: Methodology for the Management of Security and its Maturity in SME 67
Luís Enrique Sánchez, Antonio Santos-Olmo Parra, Eduardo Fernández-Medina and Mario Piattini

Security as a Service - A Reference Architecture for SOA Security 79
Mukhtiar Memon, Michael Hafner and Ruth Breu

Short Papers

Detecting Malicious Insider Threats using a Null Affinity Temporal Three Dimensional Matrix Relation 93
Jonathan White, Brajendra Panda, Quassai Yassen, Khanh Nguyen and Weihan Li

Rethinking Self-organized Public-key Management for Mobile Ad-Hoc Networks 103
Candelaria Hernández-Goya, Pino Caballero-Gil and Amparo Fúster-Sabater

DL$\delta\epsilon$ - OrBAC: Context based Access Control 111
Narhimene Boustia and Aicha Mokhtari

A Model Driven Approach for Generating Code from Security Requirements 119
Óscar Sánchez, Fernando Molina, Jesús García Molina and Ambrosio Toval

Managing Security Knowledge through Case based Reasoning 127
Corrado Aaron Visaggio and Francesca De Rosa

Author Index 137

MMSM-SME: Methodology for the Management of Security and its Maturity in SME

Luís Enrique Sánchez[1], Antonio Santos-Olmo Parra[1]
Eduardo Fernández-Medina[2] and Mario Piattini[2]

[1]SICAMAN NT. Dep. of R+D, Juan José Rodrigo, 4. Tomelloso, Ciudad Real, Spain
{lesanchez,asolmo}@sicaman-nt.com
[2]ALARCOS Research Group, TSI Department, UCLM-Indra R+D Institute
University of Castilla-La Mancha, Paseo de la Universidad, 4 – 13071 Ciudad Real, Spain
{eduardo.fdezmedina,mario.piattini}@uclm.es

Abstract. Due to the growing dependence of information society on Information and Communication Technologies (ICTs), the need to protect information is getting more and more important for enterprises. In this context, Information Security Management Systems (ISMSs), that are very important for the stability of the information systems of enterprises, have arisen. The fact of having these systems available has become more and more vital for the evolution of Small and Medium-Sized Enterprises (SMEs). In this article, we show the methodology that we have developed for the development, implementation and maintenance of a security management system, adapted for the needs and resources available for SMEs. This approach is being directly applied to real case studies and thus, we are obtaining a constant improvement in its application.

1 Introduction

In a global and competitive business environment as the one existing today, enterprises depend more and more on their information systems because it has been proved that they have an enormous influence on improving the level of competitiveness of enterprises. Nevertheless, without an adequate security management, these information systems lack real value since they cannot provide enterprises with enough guarantees of business continuity. For that reason, enterprises start being conscious of the huge importance of having adequate information systems as well as a correct management of them. In this way, in spite of the fact that there are still many enterprises assuming the risk of lacking adequate protection measures; there are many others that have understood that information systems are not useful without security management systems and the protection measures associated with them.

A great part of this mentality change in enterprises has its origin in the social change produced by the Internet along with the speed of information interchange that has caused that enterprises become conscious of the value of information for their organizations and worry about protecting their data. This way, enterprises are already conscious of the fact that information and the processes that support systems and nets are their most important assets [5]. These assets are submitted to a great variety of risks that can critically affect the enterprise. So, the importance of security in information systems is supported by many works [16, 33], just to mention some of them.

In the past, the enterprises that decided to protect their information systems faced these projects from the perspective of considering that security was individual, in other words, that only affected an object and not the whole set to which the object belonged. That is to say, they were based on the implementation of security measures but without carrying out an adequate management of such measures [9]. As time went by, as enterprises did not have an adequate management, the implemented controls were not maintained and were converted into passive controls that instead of helping improve security, contributed to misinforming, offering erroneous information in many cases. Thus, in [29], authors highlight the fact that technological aspects are not enough for the construction of a security system but management as well as legal and ethical aspects are necessary too.

Nowadays, experts consider that security in information systems has a bidimensional character [26]. Today, security in information systems is not dealt with as an exclusively technical aspect where the correct use of certain security mechanisms (e.g. security protocols, cipher schemas, etc.) guarantees the security of a system in absolute terms. Besides, and given the social integration of software systems, there is a new dimension that becomes very relevant and must be carefully analyzed. This new dimension has mainly a social and organizational character and is linked to the fact that the interaction between mankind and secure information systems is becoming higher. There are research results that have shown that the human factor has a significant impact on security [25].

The problem of information security is characterized by its complexity and interdependence. Security management contains an important number of factors and elements that are interrelated between them. SMEs in developed countries normally have a weak comprehension of information security, security technologies and control measures and so, they tend to forget about risk analysis or the development of security policies [7]. This can be due to the fact that SMEs lack the resources, time and specialized knowledge necessary for coordinating information security or offering adequate information about security, training and education. However, the literature suggests a very different explanation. Authors in [13] state that SMEs do not want to pay for security and they prefer to maintain a physical security they are familiarized with. Authors in [7] point out that SMEs lacking of a specialized knowledge in security technologies, tend to maintain security using the technologies they are already familiarized with. Additionally, SMEs do not consider that security is linked to the enterprise strategy and this fact directly impacts on its fulfilment [20]. In fact, a recent research puts forward the need to link information security to strategic planning information systems and therefore, to the enterprise objectives [6].

Despite that there are many security standards in ICT such as the code of good practice [11], methodologies for security management such as COBIT [4], or for risk management such as MAGERIT [15], or even maturity models for information security management such as SSE–CMM [28], they are normally designed for big corporations, are very rigid and their practical application in SMEs requires plenty of time and is very expensive. These are the reasons why many enterprises offer resistance to integrate adequate security management techniques, thus assuming security risks and so, the loss of competitiveness that are not acceptable in the modern enterprise.

In many bibliographic sources, the difficulty of using methodologies and maturity models for traditional security management that have been created for big enterprises in SMEs [2, 3, 8, 30] is detected and highlighted. The fact that the application of this kind of methodologies and maturity models in SMEs is difficult and expensive is justified many times.

In this paper, we will describe the methodology that we have developed for security management in SMEs with the aim of solving the problems detected in the classical methodologies that have shown not to be efficient at the time of their implementation into SMEs due to their complexity and other series of factors that will be analyzed in detail in the following sections of the paper.

The remainder of the paper is structured as follows. In section 2, we will briefly describe the existing methodologies and models for security management and their current tendency. In section 3, we will introduce our proposal of methodology for security management oriented to SMEs. In section 4, we will show the tool developed to support the methodology and finally in Section 5, we will conclude indicating the work that we will develop in the future.

2 Related Work

In the last years, a great number of processes, frameworks and methods for information security management whose need to be implemented is being more and more known and considered by organizations have appeared. However, they have proved to be inefficient for SMEs.

Among them, we can highlight the model presented in ISO/IEC27001 [12], that of COBIT [4] and the information security management maturity model [10]. [32] and [22] study the coexistence and complementary use of COBIT and ISO/IEC17799 through the development of a mapping for the synchronization of both frameworks. Some of the detractors of ISO/IEC17799 present, as a disadvantage, the fact that it is a support guide but it does not reach the necessary framework for the government of information technologies. Its main advantage against COBIT is that it is more detailed and has more guides oriented to how things must be done. A recent report of the ITGI (Information Technology Government Institute) solves the problem of synchronization by developing a mapping between.

Following this "philosophy", many other more specific maturity models have been proposed: for project management [17], requirements engineering [27], distributed development [23], maintenance [1], outsourcing [14], architectures [19, 24, 21, 31], security [28], e–Government services [34], etc.

In many bibliographic sources, the difficulty of using methodologies and maturity models for traditional security management that have been created for big enterprises in SMEs [30] is detected and highlighted. The fact that the application of this kind of methodologies and maturity models in SMEs is difficult and expensive is justified many times. Moreover, organizations, even the big ones, tend more to adopt groups of processes related as a set than to deal with processes independently [18].

The main problem of all the presented management models of security and its maturity is that they are not being successful when being implemented into SMES, mainly due to the following reasons: i) Some of them were developed thinking of big organizations (ISO/IEC27001, COBIT) and the organizational structures associated with them, and ii) others (ISM3, etc.) have tried to centre in the problems of SMEs but they are incomplete models that only face part of the problem or try to provide us with basic guides of the steps to follow but without dealing with the problem of how to really manage the ISMS. Furthermore, the majority of models are theoretical and they are still under development.

3 MMSM-SME: Methodology for ISMSs in SMES

The methodology for the management of security and its maturity in SMEs that has been developed allows any organization to manage, evaluate and measure the security of its information systems but it is mainly oriented to SMEs because they are the enterprises with a higher rate of failure in the implementation of the existing security management methodologies.

One of the objectives pursued by the MMSM–SME methodology is to be easy to apply and that the model developed with it, allows us to obtain the highest possible level of automation with minimum information, collected in a very short period of time. In the methodology, we have prioritized speed and cost saving and to do so; we have sacrificed the precision offered by other methodologies. That is to say, the developed methodology has the purpose of developing one of the best security configurations but not the optimum one, prioritizing time and cost saving against precision although guaranteeing that the obtained results have enough quality.

Other of the main contributions of the methodology is that a matrix set allowing us to relate the different components of the ISMS (controls, assets, threats, vulnerabilities, risk criteria, procedures, registers, templates, technical instructions, regulations and metrics) has been developed. The model will use it to automatically generate a great part of the necessary information, reducing in a notorious way the necessary time for ISMS development and implementation. This set of interrelations between all the ISMS components allow that the change of any of these objects alters the measurement value of the rest of objects composing the model in a way that, at any time, we can have an updated valuation of how the security system of the enterprise evolves.

In this way and starting from the information obtained through the implementation into different enterprises, we have developed a methodology of management and maturity of information system security and a model associated with it. This methodology is composed of three main sequential subprocesses: i) GEGS – Generation of Security Management Schemas, ii) GSGS – Generation of Security Management Systems, and iii) MSGS – Maintenance of the Security Management System.

3.1 GEGS – Generation of Security Management Schemas

Generation of Security Management Schemas (GEGS), is the first subprocess of the MMSM–SME methodology and its main objective is to produce a schema containing all the structures necessary for generating an ISMS and those relations that could be established between them for a determined type of enterprises (same sector and size) with the aim of saving time and resources at the time of generating an ISMS for an enterprise that has the same characteristics as those for which the schema was created. In Fig. 1, we can see in detail the different objects composing the schema.

GECS subprocess for schemas generation is basically composed of the following activities:

- A1.1 – Generation of master tables: The initial configuration tables are established and they will contain: i) the roles of the information system users that will be able to participate in the system; ii) the different business sectors to which the enterprise can belong; and iii) the maturity levels over which the ISMS could evolve throughout its lifecycle.

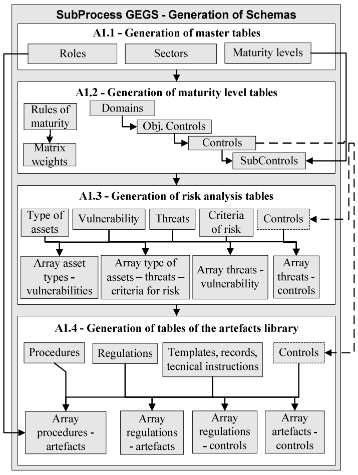
SubProcess GEGS - Generation of Schemas
A1.1 - Generation of master tables
Roles
Sectors
Maturity levels
A1.2 - Generation of maturity level tables
Rules of maturity
Matrix weights
Domains
Obj. Controls
Controls
SubControls
A1.3 - Generation of risk analysis tables
Type of assets
Vulnerability
Threats
Criteria of risk
Controls
Array asset types - vulnerabilities
Array type of assets – threats – criteria for risk
Array threats - vulnerability
Array threats - controls
A1.4 - Generation of tables of the artefacts library
Procedures
Regulations
Templates, records, tecnical instructions
Controls
Array procedures - artefacts
Array regulations - artefacts
Array regulations - controls
Array artefacts - controls

Fig. 1. Elements of GECS subprocess GEGS.

- A1.2 – Generation of maturity level tables: We will select maturity rules that will allow us to determine the current maturity level of the ISMS of the enterprise and the list of controls that could be established. These controls will be divided into subcontrols to be able to find out the approximate level at which they are currently fulfilled with higher precision. Also, these subcontrols will be associated with the maturity levels defined in the previous activity.
- A1.3 – Generation of risk analysis tables: We select the list of elements of the artefacts associated with risk analysis as well as the relations existing between them.
- A1.4 – Generation of tables of the artefacts library: We select the list of elements of the artefacts associated with the ISMS generation along with the relations existing between them.

There is a dependency in activity A1.2 because it requires an input of activity A1.1. In the same way, activities A1.3 and A1.4 require an input element generated during activity A1.2 but they have not any dependency between them.

This subprocess will receive as inputs:

- The knowledge of the experts that has been acquired during other ISMS implementations (for example, relations between elements, procedures, etc.).

- Lists of elements coming from other regulations, guides of good practice (such as ISO/IEC27002) or methodologies (such as MAGERIT v2).

And it will generate as output a schema that will be used by the following subprocesses that are basically composed of the following elements:

- A subset of elements selected from the input lists.
- A matrix series that relate the main elements (controls, types of assets, vulnerabilities, threats and risk criteria) necessary for the elaboration of a risk analysis between them.
- A matrix series that relate the main elements (controls, procedures, regulations, templates, registers, technical instructions) necessary for the ISMS generation between them.

All this set of artefacts necessary for generating the management system of the enterprise information system are included in the repository of schemas for ISMS that is constantly updated with the new knowledge obtained in each new implementation.

Due to the complexity of the development of a schema and as part of the research, we have developed an initial schema called base schema (EB), obtained from the knowledge acquired during the research process, with the purpose of making it possible the creation of new schemas through a cloning process (generate a new schema from an existing schema) of the base schema and after that, performing the necessary adjustments in the new schema to adequate it to the desired type of enterprises.

3.2 GSGS – Generation of the Security Management System

The Generation of the Security Management System (GSGS) is the second subprocess and its main objectives are on the one hand, the ISMS generation through the selection of the most adequate schema for the type of enterprise and on the other hand, the request of business and technical information of the enterprise performed by a speaker (Int) designed by the enterprise. In Fig. 2, we can see the different objects composing this subprocess.

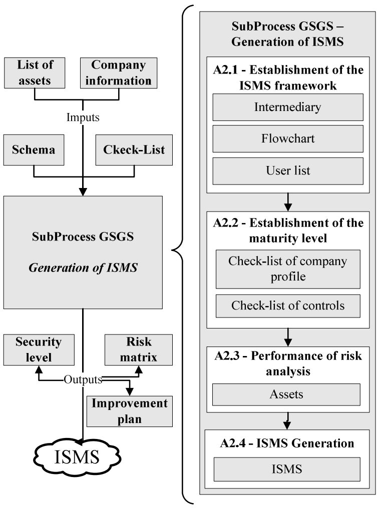

Fig. 2. Elements of GSGS subprocess.

The GSGS subprocess for ISMS generation is composed of these activities:

- A2.1 – Establishment of the ISMS framework: We will establish the relations with the enterprise, defining a valid speaker and requesting information from the enterprise: i) enterprise organization chart; ii) users with access to the information system and roles represented by them.
- A2.2 – Establishment of the maturity level:
  - Through a business meeting, we request information related to the enterprise (number of employees, turnover, etc.) with the objective of determining the most adequate schema for this type of enterprise among those existing in the repository of schemas.
  - A second meeting, this one of a technical character, is carried out to determine in detail the current situation of the enterprise with respect to the security management of its information system.
- A2.3 – Performance of risk analysis: A set of basic assets of thick grain, will be identified determining the cost (qualitative and quantitative) that their loss would mean for the organization. From the set of assets, we will determine the security risks to which they are submitted and a plan to mitigate them in an efficient way will be generated.
- A2.4 – ISMS Generation: From the obtained information and the selected schema, the elements that will form the ISMS for the enterprise will be generated and we will proceed to implement it into the enterprise.

This subprocess will receive the following inputs:

- Information of the enterprise in which we want to carry out the ISMS: i) business information; ii) valid speaker for the development of the ISMS; iii) enterprise organization chart; and iv) list of users and the roles that they perform within the information system of the enterprise.
- The most adequate schema to generate the ISMS from the business profile of the enterprise and from the repository of schemas.
- Two lists of verification: i) a list of verification with business information; ii) a list of verification with information about the level of security management.
- A list of assets associated with the information system of the enterprise, trying to group them into the lowest possible number of assets (thick grain) to reduce the cost of the generation and management of the information system.

And it will generate the these outputs that contain a description of the ISMS:

- The current maturity level of the enterprise with respect to its information security management system and to what maturity level it should progress.
- A matrix with the risks to which the assets of the enterprise are submitted.
- An ordered improvement plan that indicates which controls should be reinforced for the security level of the enterprise to evolve as fast as possible.
- A set of elements that compose the ISMS of the enterprise including: i) a control board that indicates the security level for each control related to security management; ii) a set of regulations, templates and technical instructions valid for this enterprise in the current moment; iii) a set of metrics; iv) a set of users, associated with roles that will allow us to execute a series of procedures to interact with the information system; and v) a set of regulations that must be fulfilled for the ISMS functioning.

All this set of objects that compose the ISMS are included in the ISMS repository and will be used by the enterprise to be able to correctly manage the security of the information system.

3.3 MSGS – Maintenance of the Security Management System

The maintenance of the Security Management System (MSGS) is the third subprocess defined in MMSM–SME and its main purpose is to allow the performance of the set of tasks necessary for being able to work with the ISMS, to measure its evolution and to facilitate the collection of knowledge for the continuous improvement of the generated schemas and ISMSs. In Fig. 3, we can see the different objects composing this subprocess.

The MSGS subprocess for ISMS maintenance is basically composed of the following activities:

- A3.1 – Obtain or renew the certificate of security culture: We will establish a system that allows creating in a progressive way a security conscience among the users of the information system that guarantees its quality.
- A3.2 – Execute ISMS procedures: General and specific (for example, complaint procedure) that will allow the ISMS of the enterprise to be updated will be executed.
- A3.3 – Follow-up of the ISMS fulfilment. We will have a set of metrics to keep the control board of the security of the enterprise updated in a dynamic way and in real time for the responsible for security to be able to make decisions without waiting for the performance of an external audit.

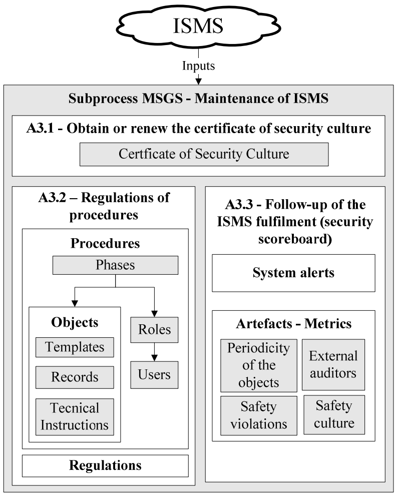
ISMS
Inputs
Subprocess MSGS - Maintenance of ISMS
A3.1 - Obtain or renew the certificate of security culture
Certficate of Security Culture
A3.2 – Regulations of procedures
Procedures
Phases
Objects
Templates
Records
Tecnical Instructions
Roles
Users
Regulations
A3.3 - Follow-up of the ISMS fulfilment (security scoreboard)
System alerts
Artefacts - Metrics
Periodicity of the objects
External auditors
Safety violations
Safety culture

Fig. 3. Elements of MSGS subprocess.

This subprocess will receive these inputs coming from the previous subprocess: i) A set of users and the roles that they will develop within the information system; these roles will determine which procedures they have access to, ii) A set of regulations that must be fulfilled for the good functioning of the ISMS, iii) A set of security procedures and elements (templates, registers, technical instructions) associated with them, and iv) A control board that will indicate the security level for each control related to the security management of the enterprise.

And it will generate the following outputs: i)Some instances of the existing procedures that will be executed as time goes by and that will allow us to manage and maintain the ISMS of the enterprise, ii) A set of metrics that will allow us to maintain the control board associated with the security level of the ISMS updated: i) a set of general metrics; ii) specific metrics: regular recurrence of objects, security violations, security conscience and external audits, and iii) Statistics extracted from the daily use of the ISMS carried out by the users of the information system that will be converted into knowledge for experts in security to be able to elaborate new schemas and refine those already existing.

All output information generated during the useful lifecycle of the ISMS will be included in the repository of information of the ISMS and will be used by the enterprise to be able to correctly manage information system security as well as by the group of experts in security to improve the schemas of GECS subprocess.

4 Applicability of MMSM-SME

To validate the MMSM-SME methodology, a tool called MMSM-TOOL has been developed. This tool allows us to develop simple, inexpensive, fast, automated, progressive and sustainable security management models. These are the main requirements that this type of enterprises have at the time of implementing these models.

From the viewpoint of the user, this tool presents two clear advantages: i) Simplicity: All ISMS activities are oriented to reduce the complexity of the process of construction and maintenance of ISMSs, thinking of organizations (SMEs) whose organizational structures are very simple, and ii) Automation: The whole system uses a concept called schemas to be able to automate the necessary steps to build and maintain the ISMS of the enterprise.

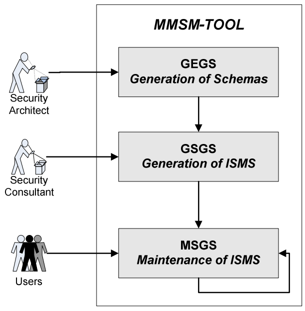

Fig. 4. Zones of application of MMSM-TOOL.

The tool is composed of three clearly differentiated parts that can be seen in Fig. 4 and that correspond to the subprocesses of the methodology: i) Schemas Generator (GEGS): This zone of the tool can only be accessed by the security management architect (AGS) and the group of experts in the dominion (GED) and from this zone, we can carry out three basic operations: i) create new schemas; ii) clone schemas from an existing schema; and iii) modify schemas to improve the ISMS generation, ii)

ISMS Generator (GSGS): This zone of the tool can only be accessed by the security consultant (CoS) and the objective here is that of generating the ISMS for the enterprise, and iii) ISMS Support (MSGS): This zone of the tool can be accessed by the users of the information system. The most relevant profile within this zone is the responsible for security (RS). From this zone, we can carry out three basic operations: i) management of the certificates of security culture; ii) procedure management; and iii) control board management.

Schemas are the nucleus over which the tool is developed because they allow the ISMS automation. These schemas are formed by a set of elements and associations between them, defined from the knowledge acquired by the customers.

The tool has allowed us to reduce the implementation costs of the systems and implies a higher percentage of success in implementations into SMEs. For these reasons, we consider that the results of this research can be very positive for SMEs because this tool allows them to access to the use of security management with a cost of resources reasonable for their size. Also, through the use of this methodology and the tool supporting it, we can obtain short-term results and reduce the costs that the use of other models and tools implies, thus obtaining a higher degree of satisfaction and efficiency in the enterprise.

Additionally, the tool allows us to maintain repositories containing not only information about the specifications of the necessary schemas for the construction of ISMSs but also information about the results obtained in the different use cases, thus allowing the constant improvement of the methodology along with the models.

5 Conclusions and Future Work

In this paper, we have presented the proposal of a new methodology for the management of security and its maturity in SMEs. This methodology lets SMEs develop and maintain an ISMS with a cost of resources acceptable for this type of enterprises. With the purpose of showing the validity of the methodology, we have defined a model (base schema) that allows supporting the results generated through the research and that fulfils the pursued objectives.

We have defined how this methodology must be used and the improvements that it offers with respect to other methodologies that face the problem partially or in an excessively expensive way for SMEs.

The characteristics offered by the new methodology and its orientation to SMEs has been very well received and its application is showing to be very positive because it allows this kind of enterprises to access to the use of information security management systems and so far, this had only been possible for big enterprises. In addition, with this methodology, we obtain short-term results and we reduce the costs that the use of other methodologies implies, obtaining a higher degree of satisfaction of the enterprise.

At last, we consider that the work done must be widened with new specifications, new schemas, increasing the set of artefacts of the library and deeping into the model with new example cases.

Among the improvements of the model on which we are working as future research lines we can highlight: i) improvements associated with GEGS subprocess: Adaptation of the predefined schemas for SMES to the new rules and standards that arise associated with security management, ii) improvements associated with GSGS subprocess: Review aspects related to ISMS generation, and iii) improvements associated with MSGS subprocess: Improve and increase the mechanisms of security measurement and auto-evaluation through the introduction of new metrics in the model that allow us to know the security level at any time; thus minimizing the number of auto adjustment audits necessary for maintaining such security level updated.

All these future improvements of the methodology as well as the model are being oriented to improve the precision of the model but always respecting the principle of cost of resources; in other words, we are aimed at improving the model without generating ISMS generation costs and maintenance costs.

Acknowledgements

This research is part ESFINGE (TIN2006-15175-C05-05), granted by the “Ministerio de Educación y Ciencia” (Spain), and QUASIMODO (PAC08-0157-0668) project from the Castilla-La Mancha Ministry of Education and Science (Spain).

References

1. April, A., J. Huffman, et al. (2005). "Software Maintenance Maturity Model: the software maintenance process model. Journal of Software Maintenance and Evolution." Research and Practice 17: 197-223.
2. Batista, J. and A. Figueiredo (2000). "SPI in very small team: a case with CMM." Software Process Improvement and Practice 5(4): 243-250.
3. Calvo-Manzano, J. A. (2000). Método de Mejora del Proceso de desarrollo de sistemas de información en la pequeña y mediana empresa (Tesis Doctoral). Universidad de Vigo.
4. COBITv4.0 (2006). Cobit Guidelines, Information Security Audit and Control Association.
5. Dhillon, G. and J. Backhouse (2000). "Information System Security Management in the New Millennium." Communications of the ACM 43(7): 125-128.
6. Doherty, N. F. and H. Fulford (2006). "Aligning the Information Security Policy with the Strategic Information Systems Plan." Computers & Security 25(2): 55-63.
7. Gupta, A. and R. Hammond (2005). "Information systems security issues and decisions for small businesses." Information Management & Computer Security 13(4): 297-310.
8. Hareton, L. and Y. Terence (2001). "A Process Framework for Small Projects." Software Process Improvement and Practice 6: 67-83.
9. Humphrey, E. (2008). Information security management standards: Compliance, governance and risk management. Information Security Tech. Report.
10. ISM3 (2007). Information security management matury model (ISM3 v.2.0), ISM3 Consortium.
11. ISO/IEC17799 (2005). ISO/IEC 17799, Information Technology - Security Techniques - Code of practice for information security management.
12. ISO/IEC27001 (2005). ISO/IEC 27001, Information Technology - Security Techniques Information security management systemys - Requirements.

13. Johnson, D. W. and H. Koch (2006). Computer Security Risks in the Internet Era: Are Small Business Owners Aware and Proactive? 39th Annual Hawaii International Conference on System Sciences (HICSS'06).
14. KcKinney, C. (2005). "Capability Maturity Model and Outsourcing: A Case for Sourcing Risk Management." Information Systems Control 5.
15. MageritV2 (2005). Metodología de Análisis y Gestión de Riesgos para las Tecnologías de la Información, V2, Ministerio de Administraciones Públicas.
16. Masacci, F., M. Prest, et al. (2005). "Using a security requirements engineering methodology in practice: The compílanse with the Italian data protection legislation." Computer Standards & Interfaces 27: 445-455.
17. McBride, T., B. Henderson-Sellers, et al. (2004). Project Management Capability Levels: An Empirical Study. 11th Asia-Pacific Software Engineering Conference (APSEC´04), IEEE Computer Society.
18. Mekelburg, D. (2005). "Sustaining Best Practices: How Real-World Software Organizations Improve Quality Processes." Software Quality Professional 7(3): 4-13.
19. NASCIO (2003). National Association of State Chief Financial Officers. Enterprise Architecture Maturity Model, Version 1.3. National Association of State Chief Financial Officers. Lexington KY.
20. O'Halloran, J. (2003). "ICT business management for SMEs." Computer Weekly December 11.
21. OMB (2004). OMB Enterprise Architecture Assessment v 1.0. The Office of Management and Budget, The Executive Office of the President.
22. Pertier, T. R. (2003). "Preparing for ISO 17799." Security Management Practices jan/feb: 21-28.
23. Ramasubbu, N., M. S. Krihsnan, et al. (2005). "Leveraging Global Resources: A Process Maturity Framework for Managing Distributed Development." IEEE Software: 80-86.
24. Schekkerman, J. (2003). Extended Enterprise Architecture Maturity Model. Institute for Enterprise Architecture Developments (IFEAD). Amersfoort, The Netherlands.
25. Schumacher, M. (2003). Security Engineering with Patterns, Springer-Verlag.
26. Siponen, M. T. (2006). Information Security Standards Focus on the Existence of Process, Not Its Content? C. o. t. ACM. 49: 97-100.
27. Sommerville, I. and J. Ransom (2005). "An Empirical Study of Industrial Requirements Engineering Process Assessment and Improvement." ACM Transactions on Software Engieering and Methodology 14(1): 85-117.
28. SSE-CMM (2003). Systems Security Engineering Capability Maturity Model (SSE-CMM), Version 3.0. Department of Defense. Arlington VA. 326.
29. Tsujii, S. (2004). Paradigm of Information Security as Interdisciplinary Comprehensive Science. International Conference on Cyberworlds (CW'04), IEEE Computer Society.
30. Tuffley, A., B. Grove, et al. (2004). "SPICE For Small Organisations." Software Process Improvement and Practice 9: 23-31.
31. Van der Raadt, B., J. F. Hoorn, et al. (2005). Alignment and Maturity are siblings in architecture assesment. Caise 2005.
32. Von Solms, B. (2005). "Information Security governance: COBIT or ISO 17799 or both?" Computers & Security . 24: 99-104.
33. Walker, E. (2005). "Software Development Security: A Risk Management Perspective." The DoD Software Tech. Secure Software Engineering 8(2): 15-18.
34. Widdows, C. and F. Duijnhouwer (2003). Open Source Maturity Model. Cap Gemini Ernst & Young. New York NY.