Proceedings of the
5th International Workshop on
Security in Information Systems - WOSIS 2007
ISBN: 978-972-8865-96-2
http://www.iceis.org

Mariemma I. Yagüe and Eduardo Fernández-Medina (Eds.) WOSIS 2007 Security in Information Systems

WOSIS 2007

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

Security in Information Systems

Proceedings of the
5th International Workshop on
Security in Information Systems - WOSIS 2007
In conjunction with ICEIS 2007
Funchal, Portugal, June 2007

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

Security in Information Systems

**Proceedings of the
5th International Workshop on
Security in Information Systems
WOSIS 2007**

In conjunction with ICEIS 2007
Funchal, Madeira, Portugal, June 2007

INSTICC PRESS
Portugal

Volume Editors

Mariemma I. Yagüe
University of Málaga
Spain

and

Eduardo Fernández-Medina
University of Castilla-La Mancha
Spain

5th International Workshop on
Security in Information Systems
Funchal, Madeira, Portugal, June 2007
Mariemma I. Yagüe and
Eduardo Fernández-Medina (Eds.)

Printed in Portugal

ISBN: 978-972-8865-96-2
Depósito Legal: 258803/07

Foreword

The International Workshop on Security in Information Systems is an annual event organized in conjunction with ICEIS conferences. The workshop is primarily focussed on high quality and innovative research papers from different fields related to the most recent developments in Information Systems Security. Traditionally the best papers are published in a reputable journal dealing with WOSIS topics. This year, authors will have the opportunity to have their work selected for publication in an extended version in the well recognized ISI ranked Publication Computer Standards and Interfaces journal. We would like to thank Professor Bhavani Thuraisingham, editor in Chief of CS&I for giving her support to this project from the beginning.

The Computer Standards and Interfaces journal is concerned with the specification, development and application of standards and with high-level publications of developments and methods in the areas of Standards, Information Management, Formal Methods; Data Acquisition; Digital Instruments Standardization; Software Quality, Software Process; and Distributed Systems, Open Systems, and E-Topics. The last two areas are particularly close to WOSIS, including Information Systems, Distributed computing, Internet, Network security, Cryptology, E-services, E-business, E-commerce, and so on. As standards are always present in many security areas such as Cryptographic protocols, web services and biometric security, etc and there are many people working in the development of security standards, this union has proved to be very productive.

As a consequence, this year the review process has been particularly complex due to the excellent standard of the work submitted. Specifically, we have received a total of 35 submissions, a significant number of papers. All the submissions were reviewed by at least two program committee members or other experts in the field, although there were on average three reviewers for each paper. Finally, 16 papers have been accepted and 7 short papers will also have the chance to be presented during the sessions due to the excellent quality of the research. As usual, WOSIS 2007 will be held over two days in order for all the contributors to have time to hold talks and present their work. We would like to thank all the authors who took the time to submit papers to WOSIS, even though they were not finally accepted. Because of the high standard of the work submitted the review process was very difficult, and some good

We would also to express our gratitude for the excellent work done by the Program Committee and the external reviewers. Special thanks to Dr. Ruth Breu who will honour us by offering the Keynote Speech which we hope you find motivating.

The publication of the best papers in the prestigious Computer Standards and Interfaces Journal, along with the presence of a renowned Program Committee and Keynote Speaker, will contribute to the success of the 5th edition of WOSIS. We are indeed very happy that WOSIS has been well received and hope we can make progress in this direction in the future. Last but not least, on behalf of the Organizing and Program Committees we sincerely hope you enjoy the WOSIS technical program and the pleasant surroundings of Madeira during your free time.

Looking forward to see you in WOSIS 2008!

May 2007

Mariemma I. Yagüe, University of Málaga, Spain

Eduardo Fernández-Medina, Department of Information Technologies and Systems, University of Castilla-La Mancha, Spain

Mariemma I. Yagüe
University of Málaga
Spain

and

Eduardo Fernández-Medina
University of Castilla-La Mancha
Spain

Invited Speaker

Ruth Breu, University of Innsbruck, Austria

Program Committee

Sabrina De Capitani di Vimercati, Università degli Studi di Milano, Italy
Ernesto Damiani, Università degli Studi di Milano, Italy
Csilla Farkas, University of South Carolina, USA
Eduardo B. Fernández, Florida Atlantic University, U.S.A.
Steven Furnell, University of Plymouth, U.K.
Christian Geuer-Pollmann, European Microsoft Innovation Center, Germany
Paolo Giorgini, University of Trento, Italy
Ehud Gudes, Ben-Gurion Univerity, Israel
Carlos Gutierrez, Correos Telecom, Spain
Haralambos Mouratidis, University of East London, Dagenham, England
Jan Jürjens, TU Munich, Germany
Stamatis Karnouskos, SAP AG, Germany
Antonio Maña, University of Malaga, Spain
Martin Olivier, University of Pretoria, South Africa
Brajendra Panda, University of Arkansas, U.S.A.
Günther Pernul, University of Regensburg, Germany
Mario Piattini, University of Castilla-La Mancha, Spain
Joachim Posegga, University of Hamburg, Germany
Indrajit Ray, Colorado State University. U.S.A.

Indrakshi Ray, Colorado State University, U.S.A.
Damian Sauveron, University of Limoges, France
Ambrosio Toval. University of Murcia, Spain
Rodolfo Villarroel, University Católica del Maule, Chile
Duminda Wijesekera, University George Mason, U.S.A.

Auxiliary Reviewers

Pierre-François Bonnefoi, XLIM, University of Limoges, France
Antonio Botella Galindo, University of Malaga, Spain.
Sudip Chakraborty, Colorado State University, U.S.A.
Serge Chaumette. LaBRI, University Bordeaux 1, France
Wolfgang Dobmeier, University of Regensburg, Germany
Nurit Gal-Oz. Ben-Gurion Univerity, Israel
Joaquin Lasheras, University of Murcia, Spain
Francisco Javier Lucas, University of Murcia, Spain
Miguel Angel Martinez, University of Murcia, Spain
Norbert Meckl, University of Regensburg, Germany
Fernando Molina, University of Murcia, Spain
Antonio Muñoz Gallego, University of Malaga, Spain
Nayot Poolsappasit, Colorado State University, U.S.A.
Boris Rozenberg, Ben-Gurion Univerity, Israel
Daniel Serrano Valero, University of Malaga, Spain

Table of Contents

Foreword iii

Workshop Chairs v

Invited Speaker v

Program Committee v

Invited Speaker

Model-Driven Approaches to Security 3
Ruth Breu

Security Services

Full Papers

A Key Management Method for Cryptographically Enforced Access Control 9
Anna Zych, Milan Petković and Willem Jonker

A Proposal for Extending the Eduroam Infrastructure with Authorization Mechanisms 23
Manuel Sánchez Cuenca, Gabriel López, Óscar Cánovas and Antonio F. Gómez-Skarmeta

A New Way to Think About Secure Computation: Language-based Secure Computation 33
Florian Kerschbaum

Administration 43
Marco Ramilli and Marco Prandini

A Reputation System for Electronic Negotiations 53
Omid Tafreschi, Dominique Maehler, Janina Fengel, Michael Rebstock and Claudia Eckert

A Fair Non-repudiation Service in a Web Services Peer-to-Peer Environment 63
Berthold Agreiter, Michael Hafner and Ruth Breu

Research on Counter Http DDoS Attacks based on Weighted Queue Random Early Drop 73
Guo Rui, Chang Guiran, Hou Ruidong, Baojing Sun, Liu An and Bencheng Zhang

Comparison of IPsec to TLS and SRTP for Securing VoIP 82
Barry Sweeney and Duminda Wijesekera

Short Papers

Security in TciNMP Systems 95
Katalin Anna Lázár and Csilla Farkas

Confining the Insider Threat in Mass Virtual Hosting Systems 105
Marco Prandini, Eugenio Faldella and Roberto Laschi

A General Approach to Securely Querying XML 115
Ernesto Damiani, Majirus Fansi, Alban Gabillon and Stefania Marrara

New Primitives to AOP Weaving Capabilities for Security Hardening Concerns 123
Azzam Mourad, Marc-André Laverdière and Mourad Debbabi

Full Papers

On the Relationship between Confidentiality Measures: Entropy and Guesswork 135
Reine Lundin, Thijs Holleboom and Stefan Lindskog

A Privacy Aware and Efficient Security Infrastructure for Vehicular Ad Hoc Networks 145
Klaus Plößl and Hannes Federrath

A Three Layered Model to Implement Data Privacy Policies 155
Gerardo Canfora and Corrado Aaron Visaggio

Implementing Mobile DRM with MPEG 21 and OMA 166
Silvia Llorente, Jaime Delgado and Xavier Maroñas

Short Papers

Inferring Secret Information in Relational Databases 179
Stefan Böttcher

A DRM Architecture for Securing User Privacy by Design 188
Daniel Kadenbach, Carsten Kleiner and Lukas Grittner

An Ontology for the Expression of Intellectual Property Entities and Relations 196
Víctor Rodríguez, Marc Gauvin and Jaime Delgado

Security Engineering

Full Papers

Obtaining Use Cases and Security Use Cases from Secure Business Process through the MDA Approach 209
Alfonso Rodríguez and Ignacio García-Rodríguez de Guzmán

SREPPLine: Towards a Security Requirements Engineering Process for Software Product Lines 220
Daniel Mellado, Eduardo Fernández-Medina and Mario Piattini

MMISS-SME Practical Development: Maturity Model for Information Systems Security Management in SMEs 233
Luis Enrique Sánchez, Daniel Villafranca and Mario Piattini

SECRDW: An Extension of the Relational Package from CWM for Representing Secure Data Warehouses at the Logical Level 245
Emilio Soler, Juan Trujillo, Eduardo Fernández-Medina and Mario Piattini

Author Index 257

INVITED SPEAKERS

MMISS-SME Practical Development: Maturity Model for Information Systems Security Management in SMEs

Luis Enrique Sánchez[1], Daniel Villafranca[1] and Mario Piattini[2]

[1] SICAMAN Nuevas Tecnologías. Departamento de I+D
Juan José Rodrigo, 4. Tomelloso, Ciudad Real, España
{lesanchez, dvillafranca}@sicaman-nt.com
[2] Castilla-La Mancha, ALARCOS Research Group
TSI Department, UCLM-Soluziona Research and Development Institute
University of Castilla-La Mancha, Paseo de la Universidad 4, Ciudad Real, Spain
{Mario.Piattini}@uclm.es

Abstract. For enterprises to be able to use information technologies and communications with guarantees, it is necessary to have an adequate security management system. However, this requires that enterprises know in every moment their security maturity level and to what extend their information security system must evolve. Moreover, this security management system must have very reduced costs for its implementation and maintenance in small and medium-size enterprises (from now on, SMEs) to be feasible. In this paper, we will put forward our proposal of a maturity model for security management in SMEs and we will briefly analyse other models that exist in the market. This approach is being directly applied to real cases, thus obtaining an improvement in its application.

1 Introduction

Information and processes supporting systems and nets are the most important assets for any organization [1] and they suppose the main differentiating factor in an enterprise evolution. These assets are exposed to a great variety of risks that can critically affect enterprises. There are many sources that provide us with figures that show the importance of the problems caused by the lack of adequate security measures [2-6].

At present, tackling the implementation of a security management system is very complex for a small or medium-size enterprise. The tendency in the field of enterprises security is that of migrating little by little their culture towards the creation of a security management system (ISMS) although this progression is very slow. Thus, studies such as that of René Sant-Germain [7] estimate that with the current models, in 2009, only 35% of the enterprises of the world with more than 2000 employees will have an ISMS implemented and the figures talking about SMEs will be much worse.

In this paper, we will describe a new proposal of a model of maturity and security management oriented to SMEs that is aimed at solving the problems detected in the

classical models that are showing not efficient at the time of their implementation into SMEs due to their complexity as well as other series of factors that will be analysed in detail in the following sections of the paper.

The paper continues with Section 2, very briefly describing existing maturity models, their current tendency and some of the new proposals that are arising. In Section 3, our proposal of a maturity model oriented to SMEs will be introduced. Finally, in Section 4, we will conclude by indicating our future work on this subject.

2 Related Work

Security Maturity Models [8-13] have the purpose of establishing a standardized valuation not only to determine the state of security information in an organization but also to allow us to plan the way to reach the desired security goals. These maturity levels will be progressive in a way that the implemented information security increases at the same time as maturity levels are risen.

Among the information security models [14] that are being more often applied to enterprises nowadays, we can highlight SSE-CMM (Systems Security Engineering Capability and Maturity Model), COBIT [9] and ISM3 [15], Besides, although there have been carried out researches to develop new models, none of them has been able to solve the current problems produced at the time of applying those models to SMEs. Among these new proposals, we can highlight CC_SSE-CCM developed by Jongsook Lee [13] that is based on the Common Criteria (CC) and SSE-CMM, the model by Eloff and Eloff [12] that defines four different classes of protection that allow us to progressively increase security levels.

Other proposals take risk analysis as ISMS main point, among them, we can highlight the proposal by Karen & Barrientes [11] and UE CORAS (IST-2000-25031) [16]. Karen & Barrientes [11]'s proposal is based on performing an analysis related to information security to identify the vulnerability degree to determine the improvement aspects to be carried out in the organization with the objective of reducing risk. On the other hand, UE CORAS (IST-2000-25031) [16] is developing a framework for security risk analysis that uses UML2, AS/NZS 4360, ISO/IEC 17799, RM-ODP6, UP7 y XML8.

The majority of the current models based on risks use the risk analysis Magerit v2 [17] as a methodology. The problem of this methodology is that being the most complete and efficient that exists in the market, it is not useful for SMEs since it requires an enormous complexity when collecting data and the direct involvement of users.

Against these models that take risk analysis as ISMS main point, in our case, despite we consider it very important, it is only taken as one more piece of the system. Siegel [18] points out that computer security models that are exclusively centred in risk elimination models are not enough. On the other hand, Garigue [19] highlights that nowadays managers want to know not only what has been performed to mitigate risks but also that this task has been effectively carried out and if the performance of it has made the company save money.

We must take into account that risk analysis is an expensive process that cannot be repeated any time that a modification is performed. Hence, it is important to develop specific methodologies that allow the maintenance of risk analysis results. UE Coras [16] project makes this risk analysis maintenance the main point of their model.

The main problem of all mentioned maturity models is that they are not being successful at the time of being implemented into SMEs, mainly due to the fact that they were developed thinking of great organizations and the associative structures associated with them; their structures are strict, complex and costly. That's the reason why they are inadequate for a SME environment.

The vision of how to face these maturity levels differs according to the authors taken as a reference. Thus, some authors insist on using ISO/IEC 17799 international regulation in security management models but always in an incremental way, taking into consideration the particular security needs [11, 12, 15, 20]. He proposal presented in this paper is also based on the ISO/IEC 17799 international regulation but it has been oriented to be applied to SMEs and avoiding the problems detected in the current models.

3 MMISS-SME: Maturity Model for Security Management in SMEs

The Information Security Maturity Model that we propose allows any organization to evaluate the state of its security but it is mainly oriented to SMEs since it develops simple, cheap, rapid, automated, progressive and maintainable security management models that are the main requirements that these enterprises have at the time of implementing these models. The most outstanding characteristics of our model are the following: i) it has three security levels (1 to 3) instead of the 5-6 levels proposed by the classical models, ii) we propose that each level is certifiable instead of the total certification existing so far, and finally, iii) the maturity level is associated with the characteristics of the enterprise.

One of the objectives pursued during the whole process that we have developed is that of obtaining the highest possible automation level with the minimum information collected in a much reduced period of time. In our system, we have prioritized speed and cost saving, sacrificing to do so, the precision offered by other models, in other words, our model will look for one of the best security configurations but not the optimal one and always prioritizing times and cost saving.

Other of the main contributions presented by the model that we have developed is a set of matrixes that let us relate the ISMS different components (controls, assets, threats, vulnerabilities, risk, procedures, registers, templates, technical instructions, regulations and metrics) and that the system uses to automatically generate a big amount of the necessary information, remarkably reducing the necessary period of time for ISMS development and implementation. This set of interrelations between all ISMS components allows that if there is any change of these components in any of those objects, the measurement value of the rest of system objects is altered in a way that we can have at all times an updated valuation of how the security system of the company evolves.

The security management model is formed by three phases and the results of each

same time, there is an information feedback from Phase III to phases I and II that allows the system to modify its parameters if necessary and to adapt itself to the new circumstances.

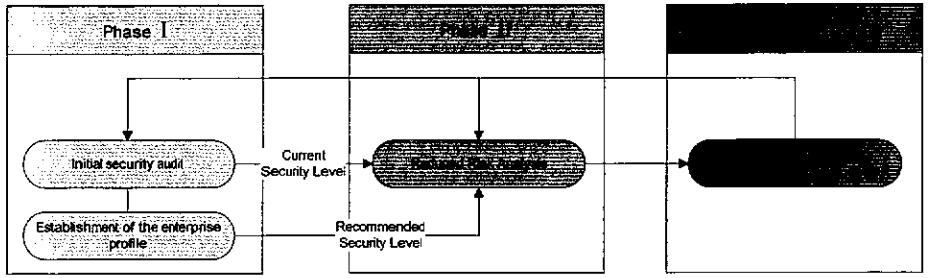

Fig. 1. Simplified Diagram of the spiral model phases.

From now on, we will analyse in a summarised way the functioning of each phase of the model by reviewing and analysing the algorithms that the system uses to generate adequate information for the enterprise with minimum effort. At the end of the section, we will briefly present the tool used to automate the model.

3.1 Phase I: Establishment of the Current and Desired Maturity Level

The main objective of this phase is the establishment of the security level desirable for the enterprise and later, we will obtain the current security level through the audit. Moreover, vital information for Phases II and III will be achieved. This section is composed of two sub-phases.

- **Establishment of the enterprise profile:** The model that we propose uses a set of characteristics intrinsic to the enterprise in order to define the maximum maturity level to which the enterprise must evolve taking into account the current situation. Each one of these parameters are translated into a value and the normalized sum of these values determines the maximum maturity level that the system considers appropriate for the enterprise.

The equation to calculate the maturity level associated with the company is as follows:

$$\Sigma(Weight*(ValorationFactor/MaximumValueFactor)/NumberOfFactors$$

According to that expression and our practical experience with our customers, we have considered three maturity levels:

- 1: If the result is between 0-0.25.
- 2: If the result is between 0.25–0.75.
- 3: If the result is between 0.75–1.

The different elements of this expression are exposed below:

- ***Factors:*** Factors represent a set of parameters that we have selected and that affect at the time of determining the security dimensioning adequate for the enterprise. In the current version, the following
  - Number of employees.
  - Annual turnover.
  - Dependency on I+D Department.
  - Number of employees using the Information System.
  - Number of people directly associated with the Systems Department.
  - Level of enterprise dependency on I.S. outsourcing.

  These factors have values ranges associated that are determined depending on the characteristics of the enterprise.
- ***WeightFactor:*** It is a correct parameter extracted from a matrix that assigns values to the factor—sector pair. This parameter of the equation allows us to control the deviations that the special characteristics of enterprises belonging to certain sectors can produce. For instance, in the case of technological enterprises, it allows us to increase the weight of the factor "number of people associated with I.S.".

Table 1. Controls associated with maturity levels.

Maturity Level	Dominions	Objectives Control	Controls	Subcontrols
1	10	14	29	153
2	9	19	47	277
3	7	20	51	305
	TOTAL:	53	127	735

- ***Initial Security Audit:*** This subphase, included in Phase I, consists of performing a detailed check-list that helps us position the current state of the company with regard to its maturity level. The 735 subcontrols (Table 1) can belong to different maturity levels, although in the initial configuration that we recommend all subcontrols belong to a same level. In Table 1, we can see how at Level2 we must fulfil 47 controls additional to the 29 ones that we have had to fulfil at Level1. To go from a Level to the following one, first of all we must fulfil- at least 75% of the subcontrols of the previous level. This margin between 75% - 100% lets a security range due to the degradation that controls will be suffering as time goes by.

3.2 Phase II: Risk Analysis

Once we have carried out the first phase to position the enterprise at a Maturity Level as well as to decide to what extend the ISMS implementation must be developed, we must perform a risk analysis of the enterprise assets.

This phase is extremely delicate due to the important cost that it can suppose and the importance of its results for the ISMS success.

The risk analysis model that we have developed is based on the models proposed by Stephenson [21] that are centered in the synergy between the technical testing and

methodology Magerit v2 [17]. These models have not shown to be adequate for SMEs due to the following reasons: First of all, their enormous complexity, in the second place, the fact that they require an enormous effort of involvement by the members of the enterprise and finally the costs associated with them are not acceptable by this type of enterprises.

For that reason, in our model, we have tried at all times to simplify the previous models to adequate them to SMEs. The main base on our methodology is defined are: Flexibility, Simplicity and Efficiency on costs (human and temporal). It is, then, a methodology aimed at identifying with the lowest possible costs the enterprises assets and their associated risks, using to do so, the results generated in Phase I and some simple algorithms.

This risk analysis will be formed by different objects (Assets, Threats, Vulnerabilities, Impacts and Risks) that interact between themselves.

One of the most important aspects of the risk analysis that we have developed is that of **Association Matrixes** that let us minimize the risk analysis cost and produce the maximum result and information for the enterprise with minimum effort. There have been performed a series of matrixes that allow us to associate the different components of the risk analysis (assets-threats-vulnerabilities) and at the same time, these components with the results produced in Phase I (controls). These matrixes are of great importance due to the fact that they help us both simplify risk analysis and obtain a valoration of the level of coverage of an asset with respect to ISO/IEC 17999 controls. These matrixes are ***static*** although the consultant can decide to modify them to adequate them to the company:

- ***Assets vs vulnerabilities Matrix:*** It lets us associate assets with the vulnerabilities that can affect them.
- ***Threats vs vulnerabilities Matrix:*** It lets us associate vulnerabilities to each type of threat. With this matrix, we can also associate threats and assets through the assets-vulnerabilities matrix.
- ***ISO17799 threats vs controls Matrix:*** It allows us to associate threats with the ISO17799 controls that affect them and thanks to the previous matrixes, it also lets us establish a security level over an asset from the controls associated with it.

Other of the aspects that we provide in our risk model is the **Level of fulfilment of a control subjected to an unacceptable risk**. The level of fulfilment of a control has a vital importance at the time of prioritizing the system improvement plan because it lets us determine the level of current coverage of a particular asset. In the case of an asset whose risk is high because of the impact that a security mistake could have on the organization and that, at the same time, has a low control coverage, we must prioritize the increasing of such coverage in order to rise its level of protection.

The level of current coverage of a control over an asset and for a given threat is calculated in the following way:

$$NCCAA = \Sigma(VACAM)/NCAM$$

Being:

- ***VACAM:*** Current value of the control affected by the threat measured in Phase I for each one of the maturity levels.

system for an X asset against a Y threat with respect to a maturity level Z.

At last, risk analysis will be based on two algorithms:

- ***Risk Level Algorithm:*** The definition of risk level (RN) will be given by the combination of the probability (P) of occurrence (vulnerabilities) with the threat level (TL):

$$RN = P * TL$$

- ***Improvement Plan Generation Algorithm.*** For the current phase of the project, the improvement plan generation algorithm that has been developed is very basic and it is only generated taking as a reference the assets that have obtained a high risk and ordering them from highest to lowest according to the control coverage. With the obtained results, the system achieves the controls and issues a report indicating the control that must be improved and those factors that will improve.

Table 2. Example of application of risks models.

Asset	Threat	Vulnerabilidades	Impact	Vulner	Risk	Control
Equipment	Non-authorized use	Controls of inadequate or inexisting physical access to facilities.	*High*	*High*	*High*	**15,24**
Paper document	Floods	Situation in areas possible to be flooded.	*High*	*Medium*	*High*	**15,24**

In **Table 2**, we can see a simplified example of how to apply all matrixes and equations to determine the level of coverage of a control with respect to an asset.

3.3 Phase III: ISMS Generation

In this phase, we have tried to make ISMS manageable, oriented to dominions of the most interesting regulation for the organization and with a reduced number of metrics, obtaining rapid results and feeding back the process in each cycle with the purpose of achieving the initially indicated maturity level.

In the previous phases, we have obtained the enterprise profile, its current maturity level, its maximum advisable maturity level, the state of its controls, its assets, the risks associated with it and the improvement plan. Now, with all this information, the system is ready to automatically prepare an information system management plan for the enterprise, using to do so, a series of matrixes associated with the previous results.

This set of matrixes that together with those shown in Phase I and II are the main contributions of our model will be internally used by the system to determine what procedures, technical instructions, registers, etc must activate for the enterprise.

The objects library composing the ISMS application will be growing as time goes by. That's the reason why we have preferred to generate the first version of the model with a single library that is composed of the following set of objects (Table 3):

Table 3. Composition of the ISMS objects library.

Type	Description	Number of Objects
ITxx	Technical instruction.	4
Nxx	Regulation	25
Pxx	Pattern	65
PRxx	Procedure	50
Rxx	Register	35

In this phase of ISMS generation, one of the most important aspects is that of the **Association Matrixes** that allow us to associate all objects of these libraries. These matrixes are internally used by the system to recommend an ISMS initial plan for the SME according to the information obtained in previous phases. There are four types of matrixes:

- ***Relationship between regulation and documents:*** The regulation defines rules that must be fulfilled in an ISMS concrete subject. The violation of a rule of this regulation is normally associated with the unfulfilment of other objects (procedures, patterns, registers and so on). When a violation of a rule of the regulation is identified, we must add 1 to the unfulfilment of the documents associated with this regulation in a way that the subsequent metrics show that the control is not being efficiently fulfilled.
- ***Relationship between regulation and ISO17779: This matrix allows us to associate the rules of the regulation with*** ISO17799 controls in a way that we can measure unfulfilment of ISO17799 controls. The importance of this matrix is that it allows us to feedback the initial report and in the future, it will allow us to dynamically evolve the security Level showing it on a Score-Board. As a regulation is associated with a procedure, this matrix also defines the set of procedures that must or must not activate regarding the data collected in the previous phases.

  Furthermore, the level defined in Phase I can invalidate points of the regulation if it considers that the Maturity Level that must be reached by the enterprise does not require the fulfilment of those points of the regulation.
- ***Relationship between documents and ISO17799 controls:*** It is the most important matrix since it lets us associate the documents composing our model with ISO17799 controls. This matrix is used by the ISMS generation algorithm in order to generate the enterprise ISMS from the information generated in Phase I and II.
- ***Relationship between procedures and their associated documents:*** This matrix is used today as a reference to determine what documents are input/output and those that are only input or only output.

Matrixes associated with ISO17799 are vitally important for the design of our system since they are used by the algorithm for the selection of documents and procedures considered vitally important not only for the ISMS design but also for its subsequent follow-up.

To finish this phase, an **ISMS generation Algorithm** is used. Given the enormous scope of the research, the ISMS generation Algorithm has been developed looking for

the simplicity principle. This algorithm is composed of the following steps:

1°.-**ISMS objects Selection:** From the set of defined matrixes and the current maturity level, the system determines the set of objects and flow diagrams that will form the ISMS current version.

2°.- **Application of colour codes:** From the improvement plan generated in phase II, we will apply a colour code to the different objects composing the ISMS to make it visually more intuitive for users.

When a procedure has to be only partially fulfilled, this will imply that only the parts affected by ISO17799 controls will be compulsory to be fulfilled for the current maturity level. In subsequent versions, objects will become more automated in a way that procedures will dynamically change according to the initial selection of controls and maturity levels. In the current version, users have the option of filling out or not those documents.

The system will mark in red those documents affecting both controls that have a low security level (Phase I) and high risk assets (Phase II) so that users are conscious of their importance and it will mark in blue those objects (patterns, registers, etc) that are currently optional and therefore, they will not notably affect the evolution of the security level and so, the objectives achievement.

The final result of this phase will be a set of regulations and procedures that must be fulfilled to improve the security level of the enterprise. They will have a colour code visually and rapidly indicating to users where a greater effort must be applied. ISMS will be dynamic, adapting it self to the changes in the controls coverage levels as well as in the security levels depending on how the system evolves. The evolution of the system will be measured through a set of metrics defined over the ISMS set of objects.

3.4 Model Automation

The whole model explained in previous sections has been integrated into a tool (Fig.2) that allows us to automate all the maturity cycle. Thanks to this tool, the model can be managed and maintained with reduced and affordable costs for this type of enterprises.

This tool includes a scoreboard that allows those in charge of the enterprise know in every moment the state of its security. This helps them make the best decisions in the security field with minimum effort.

In spite of the fact that the current version of the tool is still very basic, we hope to improve the automation level and the complexity of the algorithms and plans generated in next versions. Anyway, the results obtained so far let us be very optimistic regarding the success of the model.

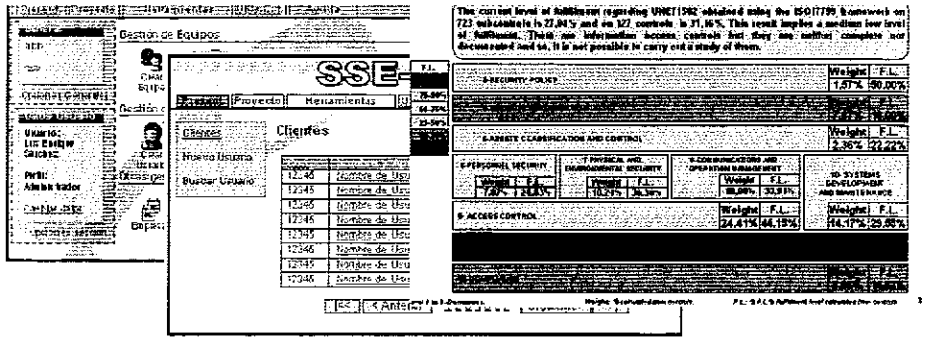

Fig. 2. Tool for maturity model automation.

4 Conclusions and Future Work

Despite the enormous efforts that are being made to create adequate maturity models to manage security in SMEs, these do not fit properly yet with the environment where they must be implemented. The most possible reason for that is the lack of maturity of enterprises as well as the fact of having tried to carry out too general and ambitious models. This causes that firstly, very often enterprises do not know the reach they must fulfil or from which part they should start restructuring their systems from or secondly, that the proposed goals are too far away and enterprises management becomes discouraged. One of the documents generated by international standardization groups that has had more importance is the ISO/IEC 17799 code of good practices that defines a very wide set of security controls and that is being used in some of the most innovating maturity models in the market. Nevertheless, this code of good practices does not offer a global solution and must be complemented with other adequate rules and mechanisms although it is a very good starting point for the development of new maturity models.

In this paper, we have presented the proposal of a new maturity and security management model oriented to SMEs that allows us to reconfigure and adapt them to guarantee their security and the stability of their management system with respect to the dimension of each enterprise. To do so, we have defined a methodology and a tool able to support the results that have been generated during the research (in this paper, due to space restrictions, we have not described this tool). We have clearly defined how this new maturity model must be used and the improvements that it offers with respect to the classical models.

Some of the main and most valuable conclusions obtained from the feedback of the participant enterprises in which several models have been analysed are exposed below:

- If we overdimension the security level of an enterprise with respect to its size, a degradation of the controls that we have overdimensioned will be produced until they reach their natural balance. The direct consequence is incurred and expense from which it will not obtain an investment return. It has been determined that security systems have a natural tendency to find their balance and that tendency is directly linked to several factors (size, sector, etc). In other words, the overdimensioning of the applied security measures becomes an economic loss for the enterprise since its own business structure finishes rejecting this security over-effort.

Enterprises are shown to be more receptive to very short-term implementation plans than to long- term ones. The certification by levels offers a guarantee for the valuation of the short-term evolution of the project.

- The presented maturity model reduces the systems implementation costs as well as improves the success percentage of its implementation into SMEs. For these reasons, as the majority of our customers are SMEs, our proposal is being well received and its application is being very positive because it allows this type of enterprises to access to the use of security maturity models that so far, it has only been possible for big enterprises. In addition, with this model, we can obtain short-term results and reduce the costs supposed by the use of other models, thus achieving a higher degree of satisfaction of the enterprise.

As this proposal is under constant development, our short and long term objective is that of deepening into maturity models to refine our model as well as the tool that is being developed at the same time as the model. Through the research method "action research", with the help of the feedback directly obtained from our customers, we hope to achieve a continuous improvement of these implementations.

Acknowledgements

This research is part of the following projects: DIMENSIONS (PBC-05-012-1) and MISTICO (PBC-06-0082), both supported by the FEDER and the "Consejería de Ciencia y Tecnología de la Junta de Comunidades de Castilla-La Mancha", RETISTRUST (TIN2006-26885-E) granted by the "Ministerio de Educación y Ciencia" (Spain), and Proyect SCMM-SME (FIT-360000-2006-73) supported by the PROFIT granted by the "Ministerio de Industria, Turismo y Comercio).

References

1. Dhillon, G. and J. Backhouse, *Information System Security Management in the New Millennium.* Communications of the ACM, 2000. 43(7): p. 125-128.
2. CSI, *Computer Security Institute.* 2002: Computer Crime and Security Survey.
3. Wood, C.C. *Researchers Must Disclose All Sponsors And Potential Conflicts.* in *Computer Security Alert.* 2000. San Francisco, CA: Computer Security Institute.
4. Biever, C., *Revealed: the true cost of computer crime.* Computer Crime Research Center, 2005.

5. Goldfarb, A., *The medium-term effects of unavailability* Journal Quantitative Marketing and Economics 2006. 4(2): p. 143-171
6. Telang, R. and S. Wattal. *Impact of Vulnerability Disclosure on Market Value of Software Vendors: An Empirical Analysis.* in *4h Workshop on Economics and Information Security.* 2005. Boston.
7. Sant-Germain, R., *Information Security Management Best Practice Based on ISO/IEC 17799.* Setting Standars, The information Management JournaL, 2005. 39(4): p. 60-62, 64-66.
8. Areiza, K.A., A.M. Barrientos, R. Rincón, and J.G. Lalinde-Pulido. *Hacia un modelo de madurez para la seguridad de la información.* in *IV Congreso Internacional de Auditoría y Seguridad de la Información.* 2005.
9. COBIT, *Cobit Guidelines, Information Security Audit and Control Association.* 2000.
10. Aceituno, V., *Ism3 1.0: Information security management matury model.* 2005.
11. Barrientos, A.M. and K.A. Areiza, *Integración de un sistema de gestión de seguridad de la información conun sistema de gestión de calidad.*, in *Master's thesis.* 2005, Universidad EAFIT.
12. Eloff, J. and M. Eloff. *Information Security Management - A New Paradigm.* in *Annual research conference of the South African institute of computer scientists and information technologists on Enablement through technology SAICSIT'03.* 2003.
13. Lee, J., J. Lee, S. Lee, and B. Choi. *A CC-based Security Engineering Process Evaluation Model.* in *Proceedings of the 27th Annual International Computer Software and Applications Conference (COMPSAC).* 2003.
14. Areiza, K.A., A.M. Barrientos, R. Rincón, and J.G. Lalinde-Pulido. *Hacia un modelo de madurez para la seguridad de la información.* in *3er Congreso Iberoamericano de seguridad Informática.* 2005.
15. Walton, J.P. *Developing an Enterprise Information Security Policy.* in *30th annual ACM SIGUCCS conference on User services.* 2002.
16. Lund, M.S., F.d. Braber, and K. Stolen, *Proceedings of the Seventh European Conference On Software Maintenance And Reengineering (CSMR'03).* IEEE, 2003.
17. MageritV2, *Metodología de Análisis y Gestión de Riesgos para las Tecnologías de la Información, V2.* 2005.
18. Siegel, C.A., T.R. Sagalow, and P. Serritella, *Cyber-Risk Management: Technical and Insurance Controls for Enterprise-Level Security.* Security Management Practices, 2002. sept/oct: p. 33-49.
19. Garigue, R. and M. Stefaniu, *Information Security Governance Reporting.* Information Systems Security, 2003. sept/oct: p. 36-40.
20. Von Solms, B. and R. Von Solms, *Incremental Information Security Certification.* Computers & Security, 2001. 20: p. 308-310.
21. Stephenson, P., *Forensic Análisis of Risks in Enterprise Systems.* Law, Investigation and Ethics, 2004. sep/oct: p. 20-21.