Sokratis Katsikas
Javier Lopez
Miguel Soriano (Eds.)

# Trust, Privacy and Security in Digital Business

LNCS 6264

7th International Conference, TrustBus 2010
Bilbao, Spain, August 2010
Proceedings

Springer

# Lecture Notes in Computer Science 6264

*Commenced Publication in 1973*
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

## Editorial Board

Sokratis Katsikas Javier Lopez
Miguel Soriano (Eds.)

# Trust, Privacy and Security in Digital Business

7th International Conference, TrustBus 2010
Bilbao, Spain, August 30-31, 2010
Proceedings

Springer

Volume Editors

Sokratis Katsikas
University of Piraeus
Digital Systems
Piraeus 18534, Greece
E-mail: ska@unipi.gr

Javier Lopez
University of Malaga
Computer Science Department
29071 Malaga, Spain
E-mail: jlm@lcc.uma.es

Miguel Soriano
Technical University of Catalonia
Department of Telematics Engineering
08034 Barcelona, Spain
E-mail: soriano@entel.upc.edu

Library of Congress Control Number: 2010932039

CR Subject Classification (1998): C.2, K.6.5, D.4.6, E.3, H.4, J.1

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-642-15151-5 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-15151-4 Springer Berlin Heidelberg New York



Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper 06/3180

# Preface

This book presents the proceedings of the 7th International Conference on Trust, Privacy and Security in Digital Business (TrustBus 2010), held in Bilbao, Spain during August 30–31, 2010. The conference continued from previous events held in Zaragoza (2004), Copenhagen (2005), Krakow (2006), Regensburg (2007), Turin (2008) and Linz (2009).

The recent advances in information and communication technologies (ICT) have raised new opportunities for the implementation of novel applications and the provision of high-quality services over global networks. The aim is to utilize this 'information society era' for improving the quality of life for all citizens, disseminating knowledge, strengthening social cohesion, generating earnings and finally ensuring that organizations and public bodies remain competitive in the global electronic marketplace. Unfortunately, such a rapid technological evolution cannot be problem-free. Concerns are raised regarding the 'lack of trust' in electronic procedures and the extent to which 'information security' and 'user privacy' can be ensured.

TrustBus 2010 brought together academic researchers and industry developers, who discussed the state of the art in technology for establishing trust, privacy and security in digital business. We thank the attendees for coming to Bilbao to participate and debate the new emerging advances in this area.

The conference program included one keynote presentation and six technical paper sessions. The keynote talk, "Trust, Risk and Usage Control," was delivered by Fabio Martinelli from CNR (Italy). The reviewed paper sessions covered a broad range of topics, from access control models to security and prevention systems, and from privacy to trust and security measurements. The conference attracted many high-quality submissions, each of which was assigned to at least three referees for review, and the final acceptance rate was 37%.

We would like to express our thanks to the various people who assisted us in organizing the event and formulating the program. We are very grateful to the Program Committee members and the external reviewers, for their timely and rigorous reviews of the papers. We would also like to thank our Publication Chair, Carmen Fernandez-Gago, and Publicity Chair, Isaac Agudo. Thanks are also due to the DEXA Organizing Committee for supporting our event, and in particular to Gabriela Wagner for her help with the administrative aspects.

Finally, we would like to thank all of the authors that submitted papers for the event, and contributed to an interesting set of conference proceedings.

August 2010

Sokratis Katsikas
Javier Lopez
Miguel Soriano

# Organization

## Program Committee Co-chairs

| | |
|---|---|
| Sokratis Katsikas | University of Piraeus (Greece) |
| Javier Lopez | University of Malaga (Spain) |

## General Chair

| | |
|---|---|
| Miguel Soriano | UPC (Spain) |

## Publication Chair

| | |
|---|---|
| Carmen Fernandez Gago | University of Malaga (Spain) |

## Publicity Chair

| | |
|---|---|
| Isaac Agudo | University of Malaga (Spain) |

## Program Committee Members

| | |
|---|---|
| Alessandro Acquisti | Carnegie Mellon University (USA) |
| Cristina Alcaraz | University of Malaga (Spain) |
| Vijay Atluri | Rutgers University (US) |
| Marco Casassa Mont | HP Labs Bristol (UK) |
| David Chadwick | University of Kent (UK) |
| Nathan Clarke | University of Plymouth (UK) |
| Frederic Cuppens | ENST Bretagne (France) |
| Ernesto Damiani | Università degli Studi di Milano (Italy) |
| Sabrina De Capitani di Vimercati | University of Milan (Italy) |
| Josep Domingo-Ferrer | University Rovira i Virgili (Spain) |
| Eduardo Fernandez | University of Castilla la Mancha (Spain) |
| Eduardo B. Fernandez | Florida Atlantic University (USA) |
| Josep L. Ferrer | University Islas Baleares (Spain) |
| Simone Fischer-Huebner | Karlstad University (Sweden) |
| Sara Foresti | University of Milan (Italy) |
| Jordi Forne | UPC (Spain) |
| Steven Furnell | University of Plymouth (UK) |
| Juergen Fuss | University of Applied Science in Hagenberg (Austria) |

| | |
|---|---|
| Juan M. Gonzalez-Nieto | Queensland University of Technology (Australia) |
| Dimitris Gritzalis | Athens University of Economics and Business (Greece) |
| Stefanos Gritzalis | University of the Aegean (Greece) |
| Marit Hansen | Independent Center for Privacy Protection (Germany) |
| Jordi Herrera | UAB (Spain) |
| Audun Josang | Oslo University (Norway) |
| Yuecel Karabulut | SAP Labs (USA) |
| Dogan Kesdogan | University of Siegen (Germany) |
| Spyros Kokolakis | University of the Aegean (Greece) |
| Kostas Lambrinoudakis | University of the Aegean (Greece) |
| Antonio Lioy | Politecnico di Torino (Italy) |
| Olivier Markowitch | Université Libre de Bruxelles (Belgium) |
| Stephen Marsh | Communications Research Centre (Canada) |
| Fabio Martinelli | CNR (Italy) |
| Vashek Matyas | Masaryk University (Czech Republic) |
| Chris Mitchell | Royal Holloway, University of London (UK) |
| Haris Mouratidis | University of East London (UK) |
| Yuko Murayama | Iwate Prefectural Universty (Japan) |
| Pablo Najera | University of Malaga (Spain) |
| Eiji Okamoto | University of Tsukuba (Japan) |
| Martin S. Olivier | University of Pretoria (South Africa) |
| Rolf Oppliger | eSecurity Technologies (Switzerland) |
| Maria Papadaki | University of Plymouth (UK) |
| Ahmed Patel | Kingston University (UK)- Kebangsaan University (Malaysia) |
| Günther Pernul | University of Regensburg (Germany) |
| Andreas Pfitzmann | Dresden University of Technology (Germany) |
| Mario Piattini | University Castilla la Mancha (Spain) |
| Hartmut Pohl | FH Bonn-Rhein-Sieg (Germany) |
| Joachim Posegga | University of Passau (Germany) |
| Kai Rannenberg | Goethe University Frankfurt (Germany) |
| Arturo Ribagorda | University Carlos III Madrid (Spain) |
| Carsten Rudolph | Fraunhofer Institute for Secure Information Technology (Germany) |
| Christoph Ruland | University of Siegen (Germany) |
| Pierangela Samarati | University of Milan (Italy) |
| Ingrid Schaumueller-Bichl | University of Applied Science in Hagenberg (Austria) |
| Matthias Schunter | IBM Zurich Research Lab (Switzerland) |
| Antonio F. Skarmeta | University of Murcia (Spain) |
| Stephanie Teufel | University of Fribourg (Switzerland) |
| A Min Tjoa | Technical University of Vienna (Austria) |
| Allan Tomlinson | Royal Holloway, University of London (UK) |
| Edgar Weipl | SBA (Austria) |
| Christos Xenakis | University of Piraeus (Greece) |
| Jianying Zhou | I2R (Singapore) |



## External Reviewers

| | |
|---|---|
| Jorge Bernal Bernabé | Michael Netter |
| Katrin Borcea-Pfitzmann | Christoforos Ntantogian |
| Katja Böttcher | Vinh Pham |
| Mohamed Bourimi | Henrich C. Pöhls |
| Bastian Braun | Denis Royer |
| Christian Broser | Rainer Schick |
| Sebastian Clauß | Agusti Solanas |
| Rafael Deitos | Boyeon Song |
| Jaromir Dobias | Yannis Soupionis |
| Stelios Dritsas | Mark Stegelmann |
| Ludwig Fuchs | Andriy Stetsko |
| Manuel Gil Pérez | Petr Svenda |
| Andre Groll | Dionysia Triantafyllopoulou |
| Stephan Heim | Rolando Trujillo |
| Jan Holle | Bill Tsoumas |
| Benjamin Kellermann | Pavel Tucek |
| Stefan Köpsell | Alexandre Viejo |
| Tracy Ann Kosa | Benedikt Westermann |
| Ioannis Krontiris | Lei Zhang |
| Juan Manuel Marín Pérez | |

## Access Control



## Security and Trust Concepts



## Security for Dynamic Collaborations



# Usage Control, Risk and Trust*

Leanid Krautsevich[1,2], Aliaksandr Lazouski[1,2], Fabio Martinelli[2], Paolo Mori[2], and Artsiom Yautsiukhin[2]

[1] Department of Computer Science
University of Pisa
[2] Istituto di Informatica e Telematica
Consiglio Nazionale delle Ricerche

**Abstract.** In this paper we describe our general framework for usage control (UCON) enforcement on GRID systems. It allows both GRID services level enforcement of UCON as well as fine-grained one at the level of local GRID node resources. In addition, next to the classical checks for usage control: checks of conditions, authorizations, and obligations, the framework also includes trust and risk management functionalities. Indeed, we show how trust and risk issues naturally arise when considering usage control in GRID systems and services and how our architecture is flexible enough to accommodate both notions in a pretty uniform way.

## 1 Introduction

Usage control (UCON) is a conceptual model, developed by Park and Sandhu (e.g. see [25]), which is able to embody and encompass most of existing access control models. The main features are attribute mutability that allows a flexible management of policies and continuity of the usage decision process, i.e. the resource access has a duration and the specific authorization factors must continuously hold. This enhanced flexibility w.r.t. the usual access control frameworks, where, for instance, authorizations are checked once before the access, induces several opportunities as well as new challenges.

Usage control seems a particularly suitable model for managing resources in GRID systems. Those systems often consist of federations of resource providers and users, with many long-lived executions and several conditions and factors to be considered during the usage decision process. For instance, it is common to have GRID computations lasting for hours/days. During the access it is possible that conditions that were satisfied when the access to the computational resources was requested, change by demanding a revocation of access to the resource itself.

GRID systems allow for remote execution of code, where the user that submitted the code is often a priori unknown. This feature demands for both coarse grained usage control, managing the access to the GRID services (also taking

* This work has been partially supported by the EU FP7 project *Context-aware Data-centric Information Sharing* (CONSEQUENCE).

# Building ISMS through the Reuse of Knowledge

Luis Enrique Sánchez[1], Antonio Santos-Olmo[1],
Eduardo Fernández-Medina[2], and Mario Piattini[3]

[1] Departament R&D, Sicaman Nuevas Tecnologias, Juan José Rodrigo 4,
13700 Tomelloso, Spain
[2] Rearch GSyA Group, University of Castilla-La Mancha, Paseo de la Universidad 4,
13071 Ciudad Real, Spain
[3] Rearch Alarcos Group, University of Castilla-La Mancha, Paseo de la Universidad 4,
13071 Ciudad Real, Spain
{Lesanchez,Asolmo}@sicaman-nt.com,
Eduardo.FdezMedina@uclm.es,
Mario.Piattini@uclm.es

**Abstract.** The information society is increasingly more dependent upon Information Security Management Systems (ISMSs), and the availability of these systems has become crucial to the evolution of Small and Medium-size Enterprises (SMEs). However, this type of companies requires ISMSs which have been adapted to their specific characteristics. In this paper we show the strategy that we have designed for the management and reuse of security information in the information system security management process. This strategy is set within the framework of a methodology that we have designed for the integral management of information system security and maturity, denominated as "Methodology for Security Management and Maturity in Small and Medium-sized Enterprises (MSM2-SME)". This model is currently being applied in real cases, and is thus constantly improving.

**Keywords:** ISMS, ISO27001, Security Knowledge Reuse, Pattern, SME.

## 1 Introduction

It is extremely important for enterprises to introduce security controls which will allow them to discover and to control the risks that they may be confronted with [1-3]. However, the introduction of these controls is not sufficient, and systems which manage security in the long term, thus permitting a swift reaction to new risks, vulnerabilities and threats are also necessary [4, 5]. Unfortunately, the current companies often do not have security management systems, or those which do exist have been created without the appropriate guidelines or documentation, and with insufficient resources [6, 7].

Therefore, in spite of the fact that real-life has shown that for a business to be able to use information technology and communication with guarantees it needs to have at its disposal guidelines, measures and tools which will allow it to know at all times both the level of its security and those vulnerabilities which have not been covered



[8], the level of successful deployment of these systems is, in reality, very low. This problem is particularly accentuated in the case of SMEs, which have the additional limitation of not having sufficient human and economic resources to be able to carry out an appropriate management [7].

Therefore, and taking into consideration the fact that SMEs represent the vast majority of enterprises, both at a national and at an international level, and are extremely important to business as a whole, we believe that advances in knowledge reuse oriented research to improve security management for this type of enterprises, may make important contributions in this area, and may contribute not only towards improving the security in SMEs, but also towards improving their level of competitiveness. In recent years we have, therefore, created a methodology (MSM2-SME) for security management and for the establishment of a security maturity level in SMEs' information systems [9-12]. We have also developed a tool that completely automates this methodology [13], which has been applied in real cases [14], and which has allowed us to evaluate the methodology, the tool, and the improvement effects produced by knowledge reuse provided by this tool.

We have paid particular attention to the methodology's capacity for knowledge reuse through the definition of reusable patterns, which are a complete parametrizable configuration that permit the immediate implantation of ISMSs in businesses, taking advantage of the knowledge obtained in the previous implantation of other ISMSs in companies that share similar structural characteristics (business sector and size). In order to validate this methodology we have recently created a single pattern denominated as "Root Pattern" with the intention of it being as generic as possible in order for it to serve as a basis from which to create new more specific patterns. Our objective is to create a pattern for each business sector, which will be obtained from the NACE code (The European standard of industry classification), and the experience of applying this methodology will, therefore, increase with each pattern. This signifies that the implementation of the ISMSs (in each business sector) will be progressively more precise, more economic and faster. We can therefore conclude that the principal contribution of this paper centres on presenting the elements of which the GSMP (Generation of Security Management Patterns) process in the MSM2-SME methodology is composed [14-16]. This process is entrusted with the generation of patterns, and a first pattern, denominated as the "Root Pattern", will serve as a basis for the generation of other patterns.

The paper continues in Section 2, which briefly describes the existing security management methodologies and models and their current tendencies. In Section 3 a brief introduction to our proposal for a security management methodology oriented towards SMEs is provided. In Section 4 we concentrate on knowledge reuse patterns and the activities which permit them to be generated. Finally, in Section 5 we present our conclusions and future work.

## 2 Related Work

Attempts to reduce the lacks that ISMSs have been shown to have in businesses, and the losses that they cause, have led to the appearance of a large number of processes [17] and information security frameworks and methods [18], whose need for implantation is

being increasingly recognised and considered by organizations but, as has been shown, are inefficient in the case of SMEs [19] and do not take into consideration aspects which are, from our point of view, fundamental, such as knowledge reuse.

With regard to the most prominent standards, it is possible to state that the majority of security management models have taken the ISO/IEC17799 and ISO/IEC27002 international standards as their basis, and that the security management models which are most successful in large companies are ISO/IEC27001, COBIT and ISM3, but that they are very difficult to implement and require too high an investment for the majority of SMEs [20]. This is owing to the fact that they are oriented towards large companies, and aspects such as knowledge reuse, which are fundamental to SMEs in that they reduce the cost of instalment and maintenance in these types of systems, take second place.

Numerous bibliographic sources detect and highlight the difficulty that SMEs confront with the use of traditional security management methodologies and maturity models which were conceived for use in large enterprises [21-24]. It is repeatedly justified that the application of this type of methodology and maturity models to SMEs is difficult and costly. Moreover, organisations, including those which are large, have a greater tendency towards adopting groups of processes which are related as a set rather than dealing with processes independently [25].

The aforementioned methodologies and security management models have not proved to be valid in SMEs for three reasons:

- They tackle only part of the security management system and almost none of them tackle the deployment of these systems from a global perspective, which thus obliges companies to acquire, implement, manage and maintain various methodologies, models and tools to manage their security.
- We can conclude that although various standards, regulations, guides to good practices, methodologies, and security management and risk analysis models exist, they are not integrated into a global model which can be applied to small and medium-sized enterprises with a guarantee of success.
- And what is most important, none of them centre on knowledge reuse which, according to our research, is fundamental if viability is to be guaranteed not only during the ISMS installation phase but also during its lifecycle.

Therefore, and to conclude this sub-section, it could be said that it is pertinent and opportune to tackle the problem of developing a new methodology for the management of security and its maturity for information systems in SMEs. This methodology must be capable of reusing the knowledge acquired in previous instalments, and have the objective of making large reductions in costs which would make the installation of ISMSs in SMEs viable.

## 3 MSM2-SME Overview

The methodology for the management of security and its maturity in SMEs that we have developed will allow any organisation to manage, evaluate and measure the security of its information systems, but is oriented mainly towards SMEs, since it is these organisations which have the highest level of failure in the deployment of existing security management methodologies.



One of the desired objectives of the MSM2-SME methodology was that it will be easy to apply, and that the model developed on it will permit the greatest possible level of automation and reusability to be obtained with a minimum amount of information collected in a greatly reduced time. To do this, during the development of this methodology priority has been given to the search for solutions that will permit a high resolution of the reuse of knowledge acquired in previous installations, with the objective of making significant reductions in costs and obtaining better results in general, at the expense of a slight reduction in the precision obtained, but always ensuring that the results will be of a sufficiently high quality.

Knowledge reuse is achieved through a structure of matrices which allow us to relate the various ISMS components (controls, actives, threats, vulnerabilities and risk criteria) that the model will use to generate a considerable part of the necessary information, thus notably reducing the time needed to deploy and develop the ISMS.

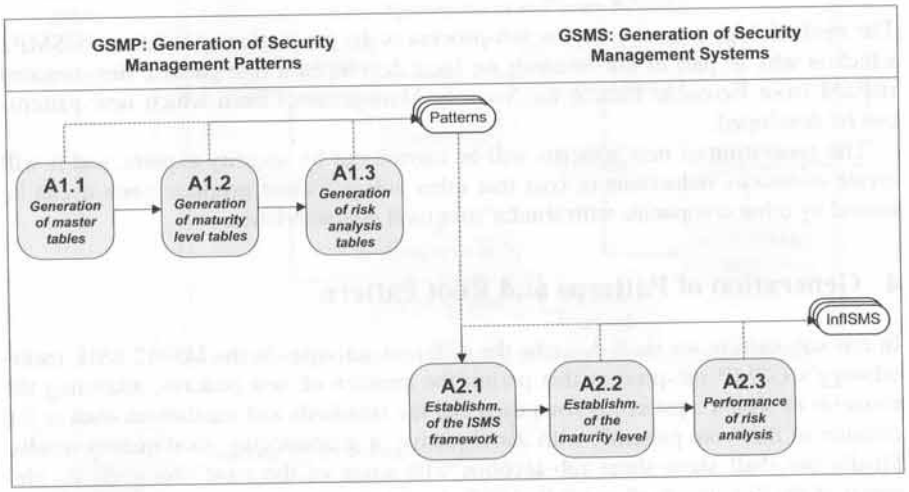



**Fig. 1.** The sub-processes of the methodology

The entire weight of the knowledge reuse process falls on the first of the two sub-processes of which the MSM2-SME methodology is composed. Figure 1 shows details of these sub-processes and the activities of which they are composed. Each of these sub-processes will be briefly analysed below:

- GSMP – Generation of Security Management Patterns: The principal objective of this sub-process is to create the structures that are necessary to store the knowledge obtained from different instalments with the objective of being able to reuse it in future instalments, thus obtaining great advantages. These structures will contain reusable patterns, and will permit both the time needed to create the ISMS and the maintenance costs to be reduced, signifying that they are suitable for the dimensions of an SME. The use of patterns is of special interest in the case of SMEs since their special characteristics tend to mean that they have simple information systems which are very similar to each other.

Each pattern will contain the knowledge obtained during the installation of an ISMS in a company, and will be suitable for reuse by companies with similar structural characteristics.

When tackling the construction of an ISMS, the company must determine whether it can reuse any of its existing patterns. If the situation arises that it is not possible to totally adapt a pattern to another company because it has certain specific characteristics, this pattern can be reused and later refined to adapt it to its special casuistry. And if a pattern exists which can be totally adapted to its characteristics it will not be necessary to use this methodology process, which will suppose an enormous reduction in costs for the SME when generating the ISMS.

- GSMS – Generation of Security Management Systems: The main objective of this sub-process is to create a suitable ISMS for a company by using an already existing pattern.

The methodology's most complex sub-process is the generation of a pattern (GSMP), which is why as part of our research we have developed a first pattern, denominated rRPSM (root Reusable Pattern for Security Management) from which new patterns can be developed.

The generation of new patterns will be carried out by security experts, and it will create enormous reductions in cost that other sub-processes produce since it can be reused by other companies with similar structural characteristics.

## 4 Generation of Patterns and Root Pattern

In this sub-section we shall describe the different activities in the MSM2-SME methodology's GSMP sub-process that permit the creation of new patterns, analysing the elements of which a pattern is composed and the standards and regulations used in the creation of the "root pattern", with the objective of guaranteeing good quality results. Finally we shall show three sub-sections with some of the most characteristic elements of the "root pattern" in relation to their maturity levels, procedures and profiles.

During our research, in which we used the research in action method [26, 27], we obtained a first pattern by using the knowledge acquired in various installations. In this first pattern, denominated rRPSM, we introduced the common characteristics detected principally in SMEs in which we had made installations using our methodology. We therefore consider that rRPSM contains a first valid pattern from which new refined patterns can be derived, with the objective of applying them in groups of companies with common structural characteristics, in order to successively obtain more precision without incrementing the cost of process generation and installation of the ISMS. The rRPSM was obtained by using the knowledge of a group of domain experts. It was later refined through the application of the methodology with various clients from the SNT2[1] company.

As Figure 2 shows, a pattern contains all the elements that are necessary to generate an ISMS and the relationships that can be established between them. One fundamental aspect for which the results of the methodology are suitable is that the root

[1] SNT is a technology company specializing in security consulting for ICT.



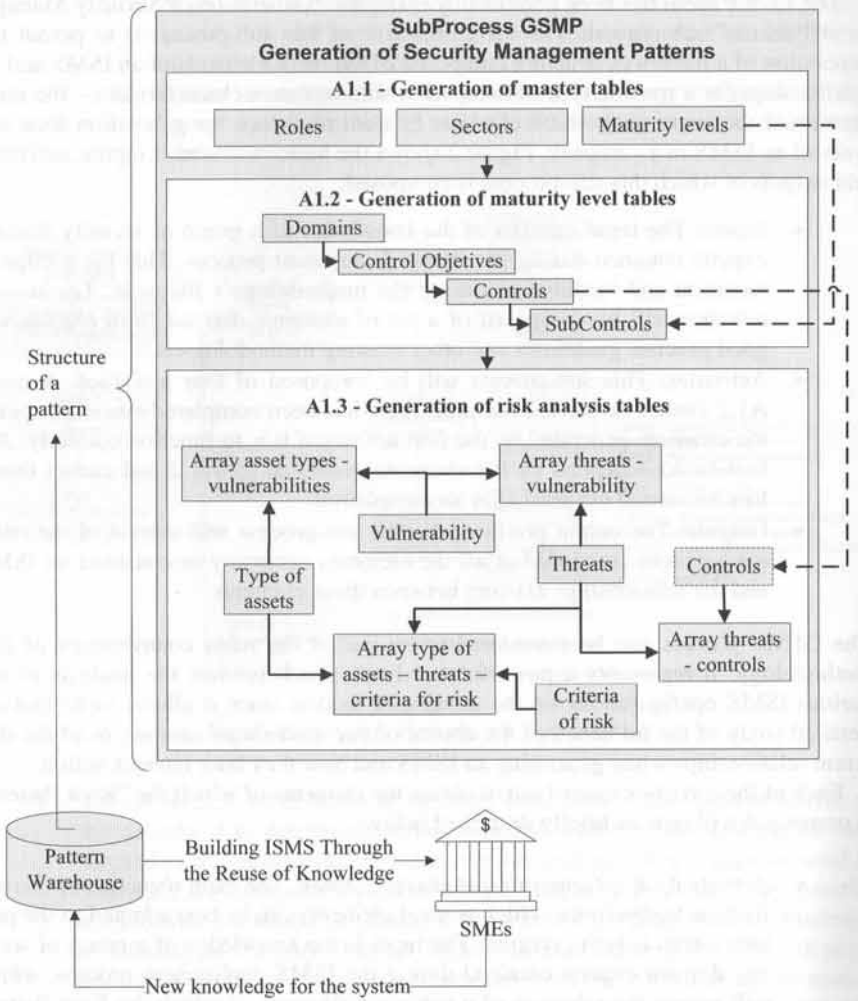



**Fig. 2.** Principal elements of which a pattern is composed and the relationships among them

pattern or origin pattern from which the remaining patterns are derived has been created from a solid base. To do this, the creation of the root pattern in the MSM2-SME methodology has always been based on internationally recognized standards and regulations which will guarantee its validity.

The main objective of this pattern is that it will serve as a starting point to create new more specific patterns (for concrete sectors and company-sizes) in such a way that the generation of new patterns can be carried out by taking the Root Pattern as a reference, cloning it (copying the structure of pattern A onto pattern B) and then carrying out the appropriate modifications to adapt it to a specific type of company.

The Root Pattern has been obtained by using the "Generation of Security Management Patterns" sub-process. The main objective of this sub-process is to permit the generation of a pattern (a structure composed of the main elements of an ISMS and its relationships for a specific type of companies with common characteristics – the same sector and the same size) which can later be used to reduce the generation time and costs of an ISMS in a company. Figure 2 shows the basic structure of inputs, activities and outputs of which this sub-process is composed:

- Inputs: The input consists of the knowledge of a group of security domain experts obtained during the ISMS deployment process. This knowledge is recurrent and incremental during the methodology's lifecycle. The second entrance will be composed of a set of elements derived from regulations, good practice guidelines and other existing methodologies.
- Activities: This sub-process will be composed of four activities. Activity A1.2 cannot be carried out until A1.1 has been completed since it requires the elements generated by the first activity if it is to function correctly. Activities A1.3 depend on the elements generated by A1.2 and cannot therefore be carried out until after its completion.
- Outputs: The output produced by this sub-process will consist of the complete pattern composed of all the elements necessary to construct an ISMS and the relationships existing between those elements.

The GSMP process can be considered to be one of the main contributions of this methodology. It represents a powerful test bank which permits the analysis of the various ISMS configurations on the developed models since it allows us to make a detailed study of the influence of the choice of one element or another, or of the different relationships when generating an ISMS and how they later interact with it.

Each of the activities carried out to obtain the elements of which the "Root Pattern" is composed will now be briefly described below:

- *Activity A1.1. – Generation of Master Tables:* The main objective of this activity is to determine which general elements can be best adapted to the pattern which is being created. The input is the knowledge of a group of security domain experts obtained during the ISMS deployment process, which will permit the selection of a subset of elements of which the Root Pattern will be composed. Figure 3 shows the structure created to store the knowledge from this activity and the values load in the root pattern. Thus, for example, we have initially introduced six profiles and some subprofiles for the element created to contain the roles and profiles. The principal sources from which the elements that fill the different components in this zone of the root pattern have been extracted are analysed below:
  - Roles: The Root Pattern is composed of the roles proposed by the ISACA[2] Company for the members of its systems department, and it has been completed with the principal profiles defined in the methodology.

[2] ISACA: Information Systems Audit and Control Association.



  - Maturity Levels: The Root Pattern is a variation of the Eloff proposal [28] and has 3 maturity levels, although other models with 5 maturity levels were also studied.
  - Business sectors: This Root Pattern has been composed of the proposals of the NACE code (The European standard of industry classification).

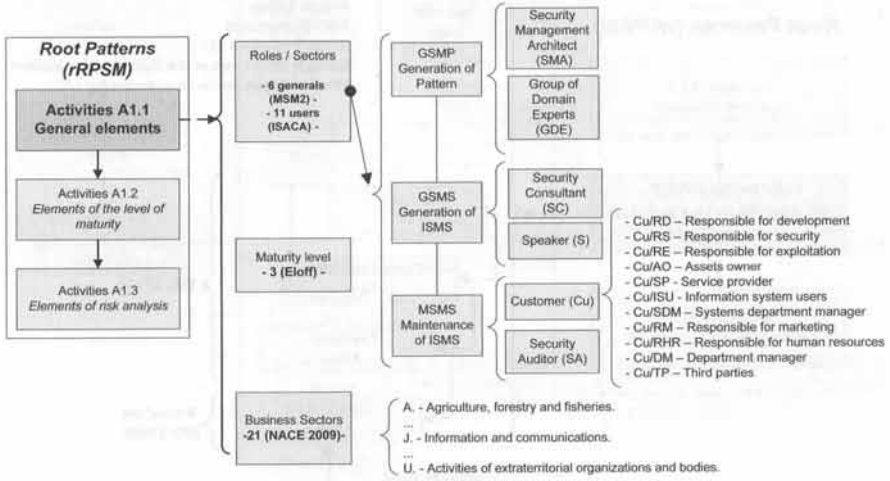



**Fig. 3.** Root Pattern elements for Activity A1.1

- *Activity A1.2. – Generation of maturity level tables:* The main objective of this activity is to determine the controls and maturity rules that can be best adapted to the pattern that is being created, and which will later be used to determine the company's present security maturity level, and the maturity level to which it would be advisable to evolve. The inputs are the knowledge of a Group of Security Domain Experts obtained during the ISMS deployment process, the maturity levels obtained from the "Establishing the maturity levels" task and a set of elements from which the final elements that will form this part of the Root Pattern will be selected. Figure 4 shows the structure created to store the knowledge from this activity and the values load in the root pattern. Thus, for example, we have introduced 133 controls for the element created to contain the controls, initially taking ISO/IEC27002 as our basis since it is an internationally recognized standard. One of the principal advantages of this pattern structure is that it can easily be adapted to other international regulations. The principal sources from which the elements with which the different components in this zone of the root pattern have been extracted are analysed below:
  - Maturity rules: These are used to define the level of security that it is desirable for the company to attain, i.e., the maximum maturity level that it should be able to attain based on its structural characteristics.

- Security controls: The ISO/IEC27002 [29] proposals for good practice guidelines have been used in the Root Pattern, and the controls have been decomposed into a set of sub-controls, which has allowed the company's current security management level to be obtained with greater precision.

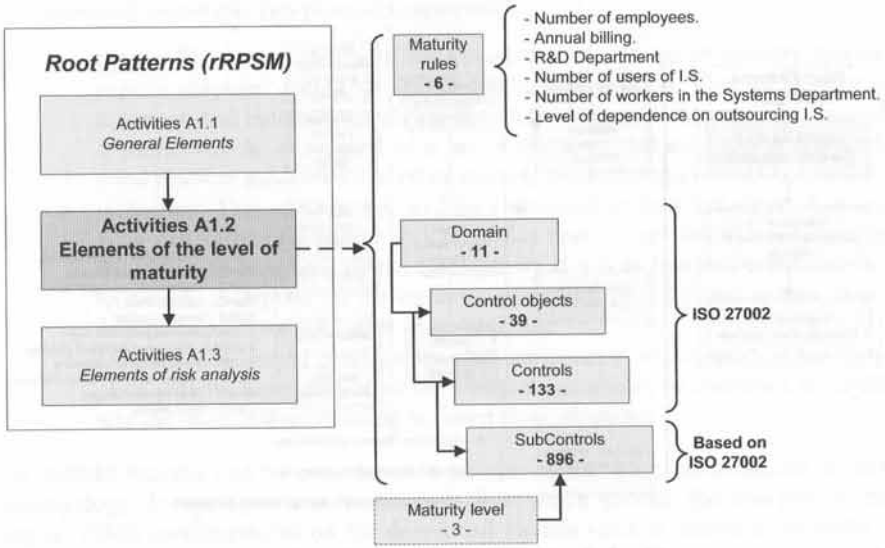



**Fig. 4.** Root Pattern elements for Activity A1.2

- *Activity A1.3. – Generation of risk analysis tables:* The main objective of this activity is to select those elements which are necessary to be able to carry out a low cost basic risk analysis of the activities of which the company's information system is composed which can be adapted to the requirements of SMEs, in activities subsequent to the methodology. The inputs are the knowledge of the group of security domain experts which was obtained during the ISMS deployment process, the controls selected in the Establishing Controls task, which are stored in the patterns repository, and a set of elements (types of activities, threats, vulnerabilities and risk criteria) which are necessary for the creation of the risk analysis.

  Figure 5 shows the structure created to store the knowledge from this activity and the values load in the root pattern. The selection of elements for this zone of the root pattern is based on the contents of Magerit's risk analysis methodology [30] and on the ISO/IEC27005 standard [31], from which a set of elements is obtained. For example, in the case of threat types we have considered the six most important threat types derived from Magerit and have established 1040 relationships between these and the controls selected in the previous activity.



The patterns are under constant evaluation and are up-dated with the knowledge obtained from the Group of Domain Experts in each new deployment.

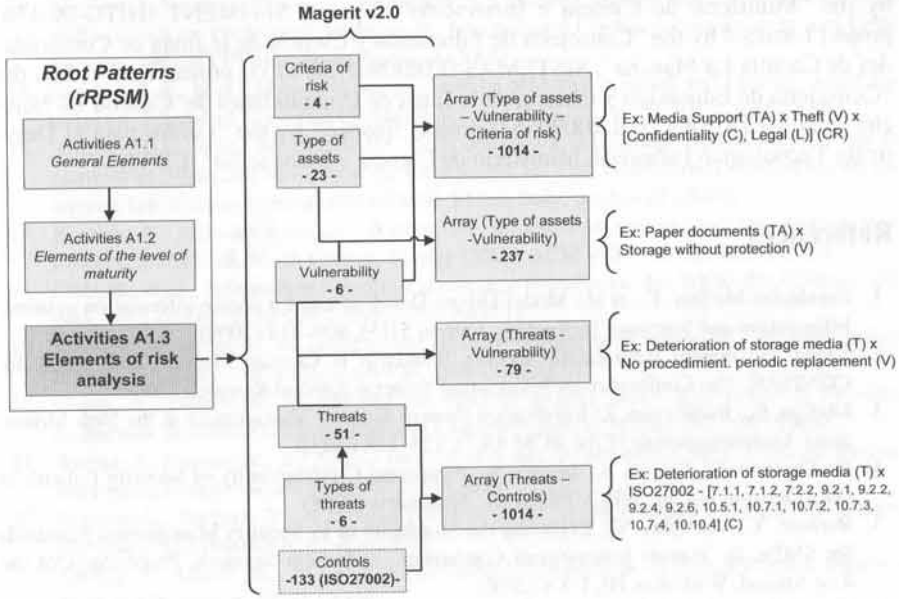



**Fig. 5.** Root Pattern elements for Activity A1.3

## 5 Conclusions

This paper shows the mechanisms defined in the MSM2-SME methodology that make it possible to reuse knowledge acquired in different instalments, thus obtaining enormous benefits (cost reductions, robust results, etc.). We have also analysed the root pattern, which was developed from the starting point of all the knowledge obtained in order to create new more refined patterns for other companies.

We have shown how the root pattern has been developed from internationally renowned standards to guarantee a high quality in the results obtained when implementing ISMSs, and how the structure of the patterns allows them to be adapted to any type of regulation. This will even make it possible to take only parts of the patterns, which supposes an enormous potential when applying our methodology.

We have defined how this model can be used and the improvements that it offers in comparison to other models which tackle the problem only partially or in a manner which is too costly for SMES.

All future improvements to the methodology and the model are oriented towards improving its precision, whilst always respecting the principal of the cost of resources, i.e., we seek to improve the model without incurring higher generation and maintenance costs of the ISMS.

## Acknowledgments

This research is part of the following projects: BUSINESS (PET2008-0136) granted by the "Ministerio de Ciencia e Innovación" (Spain), SEGMENT (HITO-09-138) project financed by the "Consejería de Educación y Ciencia de la Junta de Comunidades de Castilla-La Mancha", SISTEMAS (PII2I09-0150-3135) project financed by the "Consejería de Educación y Ciencia de la Junta de Comunidades de Castilla-La Mancha" and MEDUSAS (IDI-20090557) project financed by the "Centro para el Desarrollo Tecnológico Industrial. Ministerio de Ciencia e Innovación" (CDTI).

## References

1. Fernández-Medina, E., et al.: Model-Driven Development for secure information systems. Information and Software Technology Journal 51(5), 809–814 (2009)
2. Kluge, D.: Formal Information Security Standards in German Medium Enterprises. In: CONISAR: The Conference on Information Systems Applied Research (2008)
3. Dhillon, G., Backhouse, J.: Information System Security Management in the New Millennium. Communications of the ACM 43(7), 125–128 (2000)
4. De Capitani, S., Foresti, S., Jajodia, S.: Preserving Confidentiality of Security Policies in Data Outsourcing. In: WPES'08. ACM, Alexandria (2008)
5. Barlette, Y., Vladislav, V.: Exploring the Suitability of IS Security Management Standards for SMEs. In: Hawaii International Conference on System Sciences, Proceedings of the 41st Annual, Waikoloa, HI, USA (2008)
6. Vries, H., et al.: SME access to European standardization. Enabling small and medium-sized enterprises to achieve greater benefit from standards and from involvement in standardization. In: E.U. Rotterdam School of Management (ed.) Rotterdam, the Netherlands, pp. 1–95 (2009)
7. Wiander, T., Holappa, J.: Theoretical Framework of ISO 17799 Compliant. Information Security Management System Using Novel ASD Method in Technical Report, V.T.R.C.o. Finland, Editor (2006)
8. Wiander, T.: Implementing the ISO/IEC 17799 standard in practice – experiences on audit phases. In: AISC '08: Proceedings of the Sixth Australasian Conference on Information Security, Wollongong, Australia (2008)
9. Sánchez, L.E., et al.: Security Management in corporative IT systems using maturity models, taking as base ISO/IEC 17799. In: International Symposium on Frontiers in Availability, Reliability and Security (FARES'06) in Conjunction with ARES, Viena, Austria (2006)
10. Sánchez, L.E., et al.: MMISS-SME Practical Development: Maturity Model for Information Systems Security Management in SMEs. In: 9th International Conference on Enterprise Information Systems (WOSIS'07), Funchal, Madeira (Portugal) (June 2007b)
11. Sánchez, L.E., et al.: Developing a model and a tool to manage the information security in Small and Medium Enterprises. In: International Conference on Security and Cryptography (SECRYPT'07), Barcelona, Junio, Spain (2007a)
12. Sánchez, L.E., et al.: Developing a maturity model for information system security management within small and medium size enterprises. In: 8th International Conference on Enterprise Information Systems (WOSIS'06), Paphos, Chipre (March 2006)



13. Sánchez, L.E., et al.: SCMM-TOOL: Tool for computer automation of the Information Security Management Systems. In: 2nd International Conference on Software and Data Technologies (ICSOFT'07), Barcelona-España Septiembre (2007c)
14. Sánchez, L.E., et al.: Practical Application of a Security Management Maturity Model for SMEs Based on Predefined Schemas. In: International Conference on Security and Cryptography (SECRYPT'08), Porto–Portugal (2008)
15. Sánchez, L.E., et al.: Managing Security and its Maturity in Small and Medium-Sized Enterprises. Journal of Universal Computer Science (J.UCS) 15(15), 3038–3058 (2009)
16. Sánchez, L.E., et al.: MMSM-SME: Methodology for the management of security and its maturity in Small and Medium-sized Enterprises. In: 11th International Conference on Enterprise Information Systems (WOSIS09), Milan, Italy, pp. 67–78 (2009)
17. Kostina, A., Miloslavskaya, N., Tolstoy, A.: Information Security Incident Management Process. In: SIN'09, North Cyprus, Turkey (2009) ACM 978-1-60558-412-6/09/10
18. Ohki, E., et al.: Information Security Governance Framework. In: WISG'09, Chicago, Illinois, USA (2009) ACM 978-1-60558-787-5/09/11
19. Siponen, M., Willison, R.: Information security management standards: Problems and solutions. Information & Management 46, 267–270 (2009)
20. Gupta, A., Hammond, R.: Information systems security issues and decisions for small businesses. Information Management & Computer Security 13(4), 297–310 (2005)
21. Batista, J., Figueiredo, A.: SPI in very small team: a case with CMM. Software Process Improvement and Practice 5(4), 243–250 (2000)
22. Hareton, L., Terence, Y.: A Process Framework for Small Projects. Software Process Improvement and Practice 6, 67–83 (2001)
23. Tuffley, A., Grove, B.,, M.: SPICE For Small Organisations. Software Process Improvement and Practice 9, 23–31 (2004)
24. Calvo-Manzano, J.A., et al.: Experiences in the Application of Software Process Improvement in SMES. Software Quality Journal 10(3), 261–273 (2004)
25. Mekelburg, D.: Sustaining Best Practices: How Real-World Software Organizations Improve Quality Processes. Software Quality Professional 7(3), 4–13 (2005)
26. Dick, B.: Applications. Sessions of Areol. Action research and evaluation (2000)
27. Kock, N.: The threee threats of action research: a discussion of methodological antidotes in the context of an information systems study. Decision Support Systems, 265–286 (2004)
28. Eloff, J., Eloff, M.: 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, pp. 130–136 (2003)
29. ISO/IEC27002, ISO/IEC 27002, Information Technology - Security Techniques - The international standard Code of Practice for Information Security Management (2007)
30. MageritV2, Methodology for Information Systems Risk Analysis and Management (MAGERIT version 2), Ministerio de Administraciones Públicas, Spain (2006)
31. ISO/IEC27005, ISO/IEC 27005, Information Technology - Security Techniques - Information Security Risk Management Standard (under development) (2008)

# Author Index

Printing: Mercedes-Druck, Berlin
Binding: Stein+Lehmann, Berlin

## Lecture Notes in Computer Science

The LNCS series reports state-of-the-art results in computer science research, development, and education, at a high level and in both printed and electronic form. Enjoying tight cooperation with the R&D community, with numerous individuals, as well as with prestigious organizations and societies, LNCS has grown into the most comprehensive computer science research forum available.

The scope of LNCS, including its subseries LNAI and LNBI, spans the whole range of computer science and information technology including interdisciplinary topics in a variety of application fields. The type of material published traditionally includes

- proceedings (published in time for the respective conference)
- post-proceedings (consisting of thoroughly revised final full papers)
- research monographs (which may be based on outstanding PhD work, research projects, technical reports, etc.)

More recently, several color-cover sublines have been added featuring, beyond a collection of papers, various added-value components; these sublines include

- tutorials (textbook-like monographs or collections of lectures given at advanced courses)
- state-of-the-art surveys (offering complete and mediated coverage of a topic)
- hot topics (introducing emergent topics to the broader community)

In parallel to the printed book, each new volume is published electronically in LNCS Online.

Detailed information on LNCS can be found at
**www.springer.com/lncs**

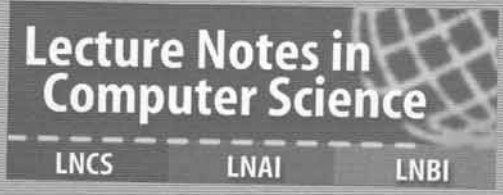
Proposals for publication should be sent to

LNCS Editorial, Tiergartenstr. 17, 69121 Heidelberg, Germany

E-mail: lncs@springer.com

ISSN 0302-9743

ISBN 978-3-642-15151-4


springer.com