Proceedings

DEXA

ARES 2006

The First International Conference on Availability, Reliability and Security

20th-22nd April 2006 Vienna University of Technology, Austria

In Cooperation with

enisa European Network and Information Security Agency

TU WIEN Technische Universität Wien Vienna University of Technology

Oesterreichische Computer Gesellschaft Austrian Computer Society

Published by the IEEE Computer Society
10662 Los Vaqueros Circle
P.O. Box 3014
Los Alamitos, CA 90720-1314

IEEE Computer Society Order Number P2567
Library of Congress Number Pending
ISBN 0-7695-2567-9

Proceedings

The First International Conference on Availability, Reliability and Security

ARES 2006

IEEE Computer Society Order Number P2567
ISBN 0-7695-2567-9
ISBN 978-0-7695-2567-9
Library of Congress Number 2006923025

Additional copies may be ordered from:

IEEE Computer Society
Customer Service Center
10662 Los Vaqueros Circle
P.O. Box 3014
Los Alamitos, CA 90720-1314
Tel: + 1 800 272 6657
Fax: + 1 714 821 4641
http://computer.org/cspress
csbooks@computer.org

IEEE Service Center
445 Hoes Lane
P.O. Box 1331
Piscataway, NJ 08855-1331
Tel: + 1 732 981 0060
Fax: + 1 732 981 9667
http://shop.ieee.org/store/
customer-service@ieee.org

IEEE Computer Society
Asia/Pacific Office
Watanabe Bldg., 1-4-2
Minami-Aoyama
Minato-ku, Tokyo 107-0062
JAPAN
Tel: + 81 3 3408 3118
Fax: + 81 3 3408 3553
tokyo.ofc@computer.org

Individual paper REPRINTS may be ordered at: <reprints@computer.org>

Editorial production by Bob Werner
Cover art production by Joe Daigle/Studio Productions
Printed in the United States of America by The Printing House

IEEE Computer Society
Conference Publishing Services
http://www.computer.org/proceedings/

Table of Contents: ARES 2006

First International Conference on Availability, Reliability and Security

Session 4: Protocol and Communication

Session 5: Security as Quality of Service

Session 6: Networking and Fault Tolerance

Session 7: Identification and Authentication

Session 8: High Availability and Dependability

Session 9: Reliability and Availability

Session 10: Security and Privacy Issue

Session 11: Security Management

Session 12: Distributed Systems

Session 13: Software Security and Dependability

International Symposium on Frontiers in Availability, Reliability and Security (FARES)

Session 1: IP Network and Adhoc Network

Session 2: Wireless and Sensor Network

Session 3: Authentication and Authorization

Session 4: Trust Management and Recovery

Session 5: Secure Information System

Session 6: Availability

Session 7: Software Security 1

Session 8: Software Security 2

Session 9: Safety and Security

Session 10: E-commerce and E-Government

Workshop on Dependable and Sustainable Peer-to-Peer Systems (DAS-P2P 2006)

Session 1: Construction of Dependable Overlay Networks

Session 2: Security

Session 3: Social Front

Workshop on Bayesian Networks in Dependability (BND2006)

Workshop on Dependability in Large-scale Service-oriented Systems (DILSOS)

Workshop: Security in E-Learning (SEL)

Workshop "Dependability Aspects on Data WArehousing and Mining Applications (DAWAM 2006)

Workshop on Bioinformatics and Security (BIOS 06)

Workshop: Information Security Risk Management (ISRM)

Workshop "Dependability and Security in e-Government" (DeSeGov 2006)

Message from the Organizing Committee

The idea for this conference came from the colleagues of the various ARES 2006 committees; our goal being to build a bridge amongst the various aspects of system dependability as an integrated concept.

The idea to launch the conference in Austria in the first half of the year 2006 has also to do with Austria's Presidency of the European Union from January to June 2006.

The European Union and the Austrian Governmental Bodies are very keen to bridge the gap between the scientific work and applications in this area — especially in the areas of e-Government.

We are very pleased therefore to have this conference organised in cooperation with ENISA (The European Network and Information Security Agency). ENISA supports the idea of this conference due to the urgent need of research and dissemination of new techniques in this key area.

We hope that the conference will have a real benefit for innovative applications which have to consider the various dependability issues, and furthermore will build a platform for in-depth discussions between researchers in the different areas of Dependability such as Availability, Reliability, and Security.

We received 159 papers from 35 countries for ARES and the Program Committee eventually selected 58 papers, making an acceptance rate of 36.47 percent of submitted papers.

Eight workshops are organised on special topics of ARES, i.e.:

- Workshop on Dependable and Sustainable Peer-to-Peer Systems (DAS-P2P 2006)
- Workshop on Bayesian Networks in Dependability (BND2006)
- Workshop on Dependability in Large-scale Service-oriented Systems (DILSOS)
- Workshop: Security in E-Learning (SEL)
- Workshop "Dependability Aspects on Data WArehousing and Mining Applications" (DAWAM 2006)
- Workshop on Bioinformatics and Security (BIOS 06)
- Workshop: Information Security Risk Management (ISRM)
- Workshop "Dependability and Security in e-Government" (DeSeGov 2006)

As an additional feature of ARES we have invited distinguished scientists for the International Symposium on Frontiers in Availability, Reliability and Security (FARES) to present and discuss special aspects relevant for future applications and research.

We would like to express our gratitude to all program committee members, workshop organisers and committee members and all the external referees who reviewed the papers very thoroughly and in a timely manner.

Due to the high number of submissions and the quality of the submitted papers, the reviewing, and discussion process was an extraordinarily challenging task. In total they have dealt with 232 papers.

Special thanks must be given to Mr. Tho Manh Nguyen for all his support in the organization of the PC-tasks of ARES 2006 and workshop coordination. We would also like to thank all the authors who submitted their papers to ARES 2006.

Finally many thanks to Ms. Christine Tronigger for providing a great deal of support in administering the registrations.

Prof. Norman Revell, Prof. Roland Wagner (Honorary Co-chairs)
Prof. Günther Pernul, Prof. Makoto Takizawa (General Co-chairs)
Prof. Gerald Quirchmayr, Prof. A Min Tjoa (Program Co.-chairs)

ARES and Workshops Committees

Honorary Co-Chairs
Norman Revell, Middlesex University, United Kingdom
Roland Wagner, University of Linz, Austria

General Co-Chairs
Guenther Pernul, University of Regensburg, Germany
Makoto Takizawa, Tokyo Denki University, Japan

Program Co-Chairs
Gerald Quirchmayr, University of Southern Australia, Australia
A Min Tjoa, Vienna University of Technology, Austria

Workshops Co-Chairs
Nguyen Manh Tho, Vienna University of Technology, Austria
Abdelkader Hameurlain, University of Toulouse, France
Leonard Barolli, Fukuoka Institute of Technology (FIT), Japan

International Liaison Chair
Maria Wimmer, University of Koblenz-Landau, Germany
Charles Shoniregun, University of East London, United Kingdom

Publicity Chair
Vladimir Marik, Czech Technical University, Czech Republic

Publication Chair
Monika Lanzenberger, Norwegian University of Science and Technology, Trondheim, Norway

Local Organizing Co-Chairs
Maria Schweikert, Vienna University of Technology, Austria
Markus Klemen, Vienna University of Technology, Austria

Program Committee

Jemal Abawajy, Deakin University, Australia
Abiola Abimbola, Napier University, UK
Rafael Accorsi, University of Freiburg, Germany
Alessandro Acquisti, Carnegie Mellon University, USA
John Andrews, Loughborough, University, UK
Lisa Bartlett, Loughborough University, UK
Elisa Bertino, Purdue University, USA
Bharat Bhargava, Purdue University, USA
Stefan Biffl, Vienna University of Technology, Austria
Michael Burmester, Florida State University, USA
Jiannong Cao, Hong Kong Polytechnic University, Hongkong, China
Jordi Castellà-Roca, Rovira i Virgili University of Tarragona
Anirban Chakrabarti, Infosys Technologies, India
Guihai Chen, Nanjing University, China
John A. Clark, University of York, UK
George Davida, University of Wisconsinat Milwaukee, USA
Pierpaolo Degano, Università diPisa, Italia
Robert Deng, Singapore Management University, Singapore
Yvo Desmedt, University College London, UK

Zoran Despotovic, DoCoMo Euro-Labs, Germany
Roger Dingledine, The Free Haven Project, USA
Paolo Donzelli, Office of the Prime Minister, Italy
Jeroen Doumen, University of Twente, Neitherland
Schahram Dustdar, Vienna University of Technology, Austria
Gerhard Eschelbeck, Webroot Inc., USA
Yung-Chin Fang, Dell Corp., USA
Pascal Felber, Université de Neuchâtel, Switzerland
Elena Ferrari, Universita' dell' Insubria, Italy
Jordi Forné, Universitat Politècnica de Catalunya, Spain
Felix C. Freiling, RWTH Aachen University, Germany
Steven Furnell, University of Plymouth, UK
Stephan Groß, Technische Universität Dresden, Germany
Daniel Grosu, Wayne State University, USA
Yong Guan, Iowa State University, USA
Ibrahim Haddad, Concordia University, Canada
Abdelkader Hameurlain, Université Paul Sabatier, France
Marit Hansen, Independent Centre for Privacy Protection Schleswig-Holstein Kiel, Germany
Naohiro Hayashibara, Tokyo Denki University, Japan
Xubin (Ben) He, Tennessee Technological University, USA
Yanxiang He, Wuhan University, China
Rattikorn Hewett, Texas Tech University, USA
Jimmy Huang, York University, Canada
Jan Jürjens, Munich University of Technology, Germany
Erland Jonsson, Chalmers University of Technology, Sweden
Oliver Jorns, ftw. Forschungszentrum Telekommunikation Wien, Austria
Audun Josang, University of Queensland, Australia
Yukiko Kawai, National Institute of Information and Communications Technology, Japan
Dogan Kesdogan, RWTH Aachen Informatik IV, Germany
Hiroaki Kikuchi, Tokai University, Japan
Hong Ong Oak, Ridge National Laboratory, USA
Seungjoo Kim, Sungkyunkwan University, Korea
Christian Kirchsteiger, European Commission
Peter Küng, Credit Suisse, Switzerland
Sy-Yen Kuo, National Taiwan UniversityTaiwan, R.O.C
Marc Lacoste, France Télécom Division R&D., France
Kwok-Yan Lam, Tsinghua University, China
Monika Lanzenberger, Norwegian University of Science and Technology, Trondheim, Norway
Chokchai (Box) Leangsuksun, Louisiana Tech University,USA
Yih-Jiun Lee, Chienkuo Technology University,Taiwan, R.O.C
Chin-Laung Lei, National Taiwan University, R.O.C
Chae Hoon Lim, Sejong University, Korea
Ching Lin, Macquarie University, Australia
Tong Liu, Dell Corp., USA
Javier Lopez, University of Malaga, Spain
Sanlu Lu, Nanjing University, China
Burgazzi Luciano, ENEA, Italy
Jianhua Ma, Hosei University, Japan
Josef Makolm, Federal Ministry of Finance, Austria
Geyong Min, University of Bradford, UK
Yi Mu, University of Wollongong, Australia
Günter Müller, Telematik Universitaet Freiburg, Germany
Junghyun Nam, Sungkyunkwan University, Korea
Tho Manh Nguyen, Vienna University of Technology, Austria
Jesper Buus Nielsen, Aarhus University, Denmark
Flemming Nielson, Technical University of Denmark, Denmark

Juan Gonzalez Nieto, Queensland University of Technology, Australia
Thomas Nowey, University of Regensburg, Germany
Manish Parashar, Rutgers University, USA
Fernando Pedone, Universita della Svizzera Italiana, Switzerland
María S. Pérez-Hernández, Universidad Politécnica de Madrid,Spain
Mario Piattini, University of Castilla La Mancha, Spain
Makan Pourzandi, Ericsson Inc.
Christopher Price, University of Wales Aberystwyth, UK
Philipp Reisner, MD at LINBIT Information Technologies GmbH, Austria
Heiko Rossnagel, Johann Wolfgang Goethe University Frankfurt, Germany
Bimal Roy, Indian Statistical Institute, India
Rei Safavi-Naini, University of Wollongong, Australia
Kenji Saito, Keio University, Japan
Kouichi Sakurai, Kyushu University, Japan
Henrique Santos, Universidade do Minho, Portugal
Stephen L. Scott, Oak Ridge National Laboratory
Jean-Marc Seigneur, University of Geneva, Switzerland
Ahmed Serhrouchni, Telecom Paris, France
Ingrid Schaumüller-Bichl, ITSB Linz, Austria
Charles Shoniregun, University of East London, UK
Amund Skavhaug, Norwegian University of Science and Technology (NTNU), Norway
Neal. A. Snooke, University of Wales Aberystwyth, UK
Ketil Stølen, SINTEF and University of Oslo, Norway
Peter Struss, Technische Universitat and Occ'm Sofwtare, Germany
Tsuyoshi Takagi, FutureUniversity – Hakodate, Japan
Makoto Takizawa, Tokyo Denki University, Japan
A Min Tjoa, Vienna University of Technology, Austria
Jorge Villar, Universitat Politècnica de Catalunya, Spain
Roland Wagner, University of Linz, Austria
Edgar Weippl, Vienna University of Technology, Austria
Chuan-Kun Wu, Chinese Academy of Sciences, China
Cheng-Zhong Xu, Wayne State University, USA
Mariemma I. Yagüe, University of Malaga, Spain
Laurence T. Yang, St.Francis Xavier University, Canada
Alec Yasinsac, Florida State University, USA
George Yee, National Research Council, Canada
Sung-Ming Yen, National Central University, Taiwan, R.O.C
Bill Yurcik, National Center for Supercomputing Applications (NCSA)
Nicola Zannone, University of Trento, Italy
Jianhong Zhang, North China University of Technology, China
Jianying Zhou, Institute for Infocomm Research, Singapore
Huafei Zhu, Institute for Infocomm Research, Singapore

Workshop on Dependable and Sustainable Peer-to-Peer Systems (DAS-P2P 2006)

Workshop Organizers
Yusuke Doi, Toshiba Corporation, Japan
Youki Kadobayashi, Nara Institute of Science and Technology, Japan
Kenji Saito, Graduate School of Media and Governance, Keio University, Japan

Program Committee
Stéphane Bressan, National University of Singapore, Singapore
Bernard Burg, Panasonic Research, USA
Ian Clarke, Freenet Project, UK
Roger Dingledine, The Free Haven Project, USA
Yusuke Doi, Toshiba Corporation, Japan (co-chair)
Claudiu Duma, Linköping University, Sweden
Debojyoti Dutta, University of Southern California, USA
Noria Foukia, University of Otago, New Zealand
Maria Gini, University of Minnesota, USA
Achmad Nizar Hidayanto, University of Indonesia, Indonesia
Sam Joseph, University of Hawaii, USA
Youki Kadobayashi, Nara Institute of Science and Technology, Japan (co-chair)
Anirban Mondal, University of Tokyo, Japan
Akiko Orita, Keio University, Japan
Omer F. Rana, Cardiff University, UK
Kenji Saito, Keio University, Japan (co-chair)
Claudio Sartori, University of Bologna, Italy
Nguyen Manh Tho, Vienna University of Technology, Austria
Sheng Zhong, State University of New York at Buffalo, USA

Workshop on Bayesian Networks in Dependability (BND2006)

Workshop Co-chairs
Stefania Montani, University of Piemonte Orientale
Hichem Boudali, University of Twente

Workshop Committee
Joanne Bechta Dugan, University of Virginia
Marc Bouissou, Electricite' de France
Helge Langseth, Sintef, Norway
Luigi Portinale, University of Piemonte Orientale
John L. Quigley, University of Strathclyde, Glasgow
Luis E. Sucar, Department of Computer Science, INAOE, Puebla, Mexico
Philippe Weber, Université Henri Poincaré, Nancy

Workshop on Dependability in Large-scale Service-oriented Systems (DILSOS 2006)

Program Chairs
Karl M. Göschka, Vienna University of Technology, Austria
Schahram Dustdar, Vienna University of Technology, Austria
Mehdi Jazayeri, University of Lugano, Switzerland

Organizational Chair
Martin Treiber, Vienna University of Technology, Austria

Program Committee
Marco Aiello, University of Trento, Italy
Mikio Aoyama, Nanzan University, Japan
Luciano Baresi, Politecnico di Milano, Italy
Boualem Benatallah, UNSW, Australia
Sara Bouchenak, University of Grenoble I, France
Sjaak Brinkkemper, Univ. of Utrecht, Netherlands
Tevfik Bultan, University of California, USA
Fabio Casati, HP, USA
Malu Castellanos, Hewlett-Packard, USA
Gianpaolo Cugola,, Italy
Harmke de Groot,, Netherlands
Asuman Dogac, METU, Turkey
Dieter Fensel, DERI, Ireland
Gianluigi Ferrari, University of Pisa, Italy
Jacqueline Floch, Sintef, Norway
Kary Fraemling, Helsinki University of Technology, Finland
Claude Godart, INRIA, France
Paul Grefen, Eindhoven Uni. of Technology, Netherlands
John Grundy, University of Auckland, New Zealand
Mohand-Said Hacid, Universite Claude Bernard Lyon, France
Manfred Hauswirth, EPFL, Switzerland
Alfons Kemper, TU Muenchen, Germany
Bernd Kraemer, University of Hagen, Germany
Frank Leymann, University of Stuttgart, Germany
Ozelin Lopez, ATOS Origin, Spain
Brahim Medjahed, University of Michigan, USA
Joachim Nern, Aspasia Systems, Germany
Beng Chin Ooi, National University of Singapore, Singapore
Maria Orlowska, UQ, Australia
Aris M. Ouksel, University of Illinois at Chicago, USA
Mike Papazoglou, Tilburg Univ., Netherlands
Jose Pereira, Universidade do Minho, Portugal
Barbara Pernici, Politecnico di Milano, Italy
Marco Pistore, Universita di Trento, Italy
Dimitris Plexousakis, FORTH, Greece
Alexander Romanovsky, University of Newcastle, UK
Anne-Marie Sassen, European Commission, EU
Vladimiro Sassone, University of Sussex, UK
Ian Sommerville, Lancaster University, UK
Jianwen Su, UCSB, USA
Katia Sycara, Carnegie Mellon University, USA
Stefan Tai, IBM Watson, USA
Paolo Traverso, ITC, Italy
Elena Troubitsyna, Aabo Akademi, Finland
Wil van der Aalst, Eindhoven University of Technology, Netherlands

Jos van Hillegersberg, Univ. of Twente, Netherlands
Steve Vinoski, IONA, USA
Martin Wirsing, Ludwig-Maximilians-University Munich, Germany
Jian Yang, Macuquarie University, Australia
Gianluigi Zavattaro, University of Bologna, Italy

Workshop: Security in E-Learning (SEL)

Program Chair
Edgar Weippl, Vienna University of Technology, Austria

Program Committee
Elke Franz, Dresden University of Technology, Germany
Gerald Quirchmayr, University of South Australia, Australia
Tomaz Klobucar, Jozef Stefan Institute, Slovenija
Günther Pernul, University of Regensburg, Germany

Workshop "Dependability Aspects on Data WArehousing and Mining Applications" (DAWAM 2006)

Organizer Co-chairs
Jimmy Huang, York University, Canada
Josef Schiefer, Senactive IT-Dienstleistungs GmbH, Austria
Nguyen Manh Tho, Vienna University of Technology, Austria

Program Committee
Jemal Abawajy, Deakin University, Australia
Aijun An, York University, Canada
Pawan Chowdhary, IBM T J Watson Research Center, USA
LiWu Chang, Naval Research Laboratory, USA
Josep Domingo-Ferrer, Rovira i Virgili University of Tarragona, Spain
Elena Ferrari, University of Insubria at Como, Italy
Ulrich Flegel, University of Dortmund, Germany
Tyrone Grandison, IBM Almaden Research, USA
Jimmy Huang, York University, Canada
Jun-Jang (JJ) Jeng, IBM T.J. Watson Research Center, USA
Hillol Kargupta, University of Maryland, Baltimore County, USA and Agnik, LLC
Zongwei Luo, University of Hong Kong, Hong Kong
Taneli Mielikäinen, University of Helsinki, Finland
Tho Manh Nguyen, Vienna University of Technology, Austria
Daniel E. O'Leary, University of Southern California, USA
Stanley Oliveira, Embrapa Information Technology, Brazil
Arnon Rosenthal, MITRE Corporation, USA
Josef Schiefer, Senactive IT-Dienstleistungs GmbH, Austria
Ben Soh, La Trobe University, Australia
David Taniar, Monash University, Australia
Juan Trujillo, University of Alicante, Spain
Vassilios S. Verykios, University of Thessaly, Greece
Justin Zhan, University of Ottawa, Canada
Sheng Zhong, State University of New York at Buffalo, USA

Workshop on Bioinformatics and Security (BIOS 06)

Workshop Chairs
Küng Josef, University of Linz, FAW Austria
Mazuran Petra, FAW, Austria
Wagner Roland, University of Linz, FAW Austria

Program Committee
Eisenacher Martin, University of Münster, Germany
Hochreiter Sepp, TU Berlin, Germany
Hof Sonja, (DWS) AG,Switzerland
Kramer Stefan, TUM, Germany
Marik Vladimir, Technical University Prag, Czech
Mazuran Petra, FAW, Austria
Palkoska Jürgen, FAW Austria
Retschitzegger Werner, University of Linz, Austria
Revell Norman, Middlesex University, UK
Tjoa A Min, Technical University of Vienna, Austria

Workshop: Information Security Risk Management (ISRM)

Workshop Chairs
Professor Dr. D. Karagiannis, University of Vienna, Austria
Dr. L. Marinos, ENISA, Greece

Program Committee
M. Dietrich, BSG Unternehmensberatung, Switzerland
M. Hoevers, ECP-NL, Platform voor eNetherland, The Netherland
K. Kalmelid, Swedish Emergency Management Agency, Sweden
S. Lebel, Dir. Centrale de la Sécurité des Systèmes d'information, France
Prof. Dr. G. Müller, Telematik, Univ. of Feiburg, Germany
M. Rohde, European Commission, DG Information Society and Media, Belgium
Dr. I. Schaumüller-Bichl, IT Security Consultant, Austria

Workshop "Dependability and Security in e-Government" (DeSeGov 2006)

Workshop Chairs
A Min Tjoa, Vienna University of Technology, Austria
Erich Schweighofer, University of Vienna, Austria

Program Committee
Peggy Agouris, University of Maine, USA
Yigal Arens, USC/Columbia University Digital Government Research Center, USA
Jon Bing, University of Oslo, Norway
Fernando Galindo, University of Zaragoza, Spain
Dieter Klumpp, Alcatel SEL Foundation, Germany
Robert Krimmer, Vienna University of Economics and Business Administration, Austria
Scott F. Midkiff, Virginia Polytechnic Institute and State University,USA
Enrico Nardelli, University of Rome TorVergata, Italy
Tho Manh Nguyen, Vienna University of Technology, Austria
Erich Schweighofer, University of Vienna, Austria
Efthimios Tambouris, CERTH/ITI, Greece
A Min Tjoa, Vienna University of Technology, Austria
Greg B. White, The University of Texas at San Antonio, USA
Maria A. Wimmer, University of Koblenz, Germany

Practical Approach of a Secure Management System based on ISO/IEC 17799

Luís Enrique Sánchez, Daniel Villafranca
SICAMAN NT. Departamento de I+D,
JuanJosé Rodrigo, 4. Tomelloso, Ciudad Real, Spain
{lesanchez, dvillafranca} @sicaman-nt.com

Eduardo Fernández-Medina, Mario Piattini
ALARCOS Research Group. TSI Department.
UCLM-Soluziona Research and Development Institute. University of Castilla-La Mancha
Paseo de la Universidad, 4 – 13071 Ciudad Real, Spain.
{Eduardo.FdezMedina, Mario.Piattini}@uclm.es

Abstract

For enterprises to be able to properly use information and communications technologies, it is necessary to have guides, metrics and tools that allow us to always know the level of our security and the points in which we are not covering it. In small and medium-size enterprises, the application of security standards has an additional problem, that is, the fact that they do not have enough resources to perform an appropriate management. In this article we will analyze some of the existing maturity models and we will compare them to the maturity model we are applying in practice. Finally we will introduce a first approach to a scoreboard which is being developed as part of a security management tool for IT systems

This approach is being directly applied to real cases and it is obtaining a constant improvement in its application.

1. Introduction

Information and processes supporting systems and nets are the most important assets for any organization [1]. These assets can be object of very varied risks that can critically affect the enterprise. The social change produced by the Internet and the fast information interchange has generated that enterprises begin to be conscious of the value of information for their organizations and to be worried about protecting their data.

The new enterprise model that began to be use at the beginning of the century and was based on the implementation of information systems has shown us to have enormous advantages to increase the competitiveness level of enterprises. Moreover, this model has become the most valuable asset for enterprises and so, the most important asset from the point of view of security. To protect these information systems that meant the main differentiation factor regarding their competence, some enterprises carried out security information implementation projects based on the setting up of punctual controls. These projects solved punctual security aspects but they did not include either the management of those controls or a framework of global management of security, that allowed their short and long term stability. As the time went by, those controls stopped to be maintained due to the fact that they did not have an adequate management and became passive controls that, instead of helping to improve security, helped to create a false sensation of security. In fact, for the construction of a security system, it is not enough to consider the technological aspects, but also it is necessary to take into account management aspects as well as legal and ethical aspects [2].

Considering this new security approach in which security is managed, the security policies are crucial and they contain the set of rules and regulations that are necessary to protect the organizations against security problems [3, 4].

Once enterprises have started to be a bit conscious in the field of security, they find that they do not know how to keep their information systems secure. The vast majority of enterprises have chaotic information systems created without following appropriate guides, without documentation and without enough resources. The classic controls are shown to be not enough by themselves to supply minimum security guarantees; the security tools existing in the market help to solve part of the security problems, but never face the problem in a global and integrated way; at last, the great diversity of these tools and their lack of integration mean an enormous cost on resources to be able to manage them.

Some indicators that show the importance of the problems caused by the lack of adequate security measures are stated, for example, in [5], in which it is

0-7695-2567-9/06 $20.00 © 2006 IEEE

indicated that from a study carried out over 257 enterprises, 90% of them had security failures, 70% of these failures were serious (laptop computers stolen, stolen information, financial fraud, intruders' access to the systems, data or net sabotages) and 74% of the studied enterprises admitted financial losses due to security failures.

Today, the market demands that enterprises are able to guarantee that technologies for computer assets and information are secure, fast and easy to interact. However, to fulfill these requirements, the systems administrators have found two problems without a satisfactory solution: the lack of tools that allow us to face the management of information systems security in a centralized, simple and according to the size of the enterprises way and the lack of information security.

The first problem is still unsolved but we think that we could solve it when we solve the second one. Concerning the second problem, not only national organizations but also international ones have worried themselves to elaborate a set of rules and specifications related to security of information and communication technologies. These rules are above all focused on the definition of security controls through codes of good practices, rules defining security management systems and rules with criteria to certify security. Nevertheless, the situation is complex and for a small or medium-size enterprise, it is a very difficult task to implement a security management system, with the possibility of several levels of exigency and with limited resources. In addition, almost always, the process finishes with the fact that the enterprise must take the risk of not having a security management system because it is not able to implement it.

In this paper, we will present an approach to the implementation of security management systems, based on ISO/IEC 17799 that we are developing and continuously improving thanks to the feedback directly received from SICAMAN customers, which mainly are Spanish, but some others are from the rest of Europe.

Our paper continues with Section 2, in which the concept of security management system is described. Then, in Section 3, we will introduce the management systems implementation scheme including the news we are applying, at the methodological and software levels. Finally, in section 4, we will put forward our conclusions and future work.

2. Information Security Management Systems

An Information Security Management System (ISMS) can be defined as a management system used to establish and maintain a secure environment for information. This system must deal with the starting out and maintenance of processes and procedures to manage information technology security [6]. These actions include the identification of the needs of information security, the starting out of the strategies to satisfy these needs, the measurements of the results and the improvement of the protection strategies.

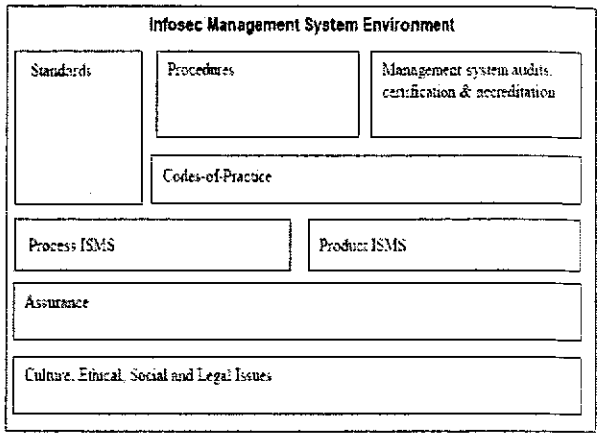

Figure 1. Component of ISMS (Eloff y Eloff, 2003)

This secure environment should take into consideration a set of elements that, in an integrated way, would take part in the information management system (see Figure 1). The standards can include technical aspects such as net security, digital signature, non repudiation, password management and so on. The procedures can be operational, technical and related to management. Audit, certification and accreditation of the management system are important to make the security environment credible. Obviously, a code of good practice, such as ISO/IEC 17799, is necessary to supply the security controls to be both implemented and managed.

The management system will be formed by a set of processes that will generate a set of products. These products will help us have an adequate security level that will depend on the particular security needs.

One of the most relevant aspects of ISO/IEC 17799 has been its help to control the outsourcing mechanisms of the services of the enterprises' information systems [7] since this externalization process is starting to be commonly used for all enterprises to minimize costs without taking into account that it can imply new security risks because normally the security levels of the enterprises with which other enterprises externalize their services are unknown.

3. Security Management Implementation Scheme

In spite of the international relevance of ISO/IEC 17799, we cannot state that it provides an information security management system but a set of controls that can be used as a guide to carry out a detailed review of the situation of our systems regarding security. However and although not all controls that can be found in it are applicable to all enterprises, it is advisable that organizations get ready to comply with this rule, at least as a starting point [8]. Thus, for example, Pittsburgh University is beginning to develop and put into practice a comprehensible security standard based on the guides provided by the ISO/IEC 17799 security standard [9]. Although, as indicated by Eloff and Eloff (2003), it is suggested to perform a progressive implementation of controls that allows the enterprise to adapt itself to the evolution of security in a non-traumatic way. Other studies consider the rule important but they complement it with other aspects such as [10] that incorporates American HIPPA requirements into a security program complementing ISO/IEC 17799; [11] that considers to apply COBIT and the rule together in a complementary way; or even Masacci [12] that considers it necessary to use controls related to the Italian legislation in the field of data protecting and privacy together with the rule. Others insist on using the ISO/IEC 17799 in security management models but always in an increasing way, taking into consideration the security particular needs [13].

Therefore, although the norm is not a security management system itself, there are many authors who show their interest in developing security management systems based on it.

The information security Management can be implemented from several perspectives: a strategic perspective, approaching it from the corporate government and policies; or from the "human" viewpoint, trying to implement a culture of security, training, ethical aspects, etc. [6].

Before initiating a project of information security management system (ISMS) in a company, it is necessary to determine the level of the Information Security Government of the company, since its absence, guarantees the failure of the security management. For that reason, it is fundamental to initially detect the level of commitment of key positions of the company, and the state of definition of roles associated to the information security systems. It is not viable to start the implantation of an information security management system in absence of a Information Security Government stable and defined [14].

Another essential aspects before initiating the implantation of ISMS is to create a suitable atmosphere between the personnel of the company, that allows to guarantee its support to the security plan. In order to create this support, it is required to establish days of awareness in which to show the benefits that the security project will have for the company. These days of formation must have three levels of application: high direction, average positions and personnel of the company.

Moreover, one of the aspects that more importance has acquired in the SGSI projects has been the metrics of security, which have become fundamental and indispensable part of the last development methodologies of the SGSI. At the moment, metric management systems are being developed, having an enormous impact in the development of the short term SGSI and in the form to perceive them on the part of the companies [15].

Some authors insist on using the ISO/IEC 17799 in models of security management, but always doing it of incremental way, considering the particular security necessities [13]. Within these models, the ISM3 is obtaining a great importance [16]. The cause of it is that it is a model created to adapt to any type of company, and have a lot of companies in which they make tests for its evolution and continuous improvement.

The most efficient model considered by SICAMAN customers has been that one based on the creation of improvement cycles through the spiral model shown in Figure 2. This model facilitates the realization of fast and cheap cycles that allow us to create a culture of security within the organization in a constant and progressive way. Instead of beginning with an analysis of risks like the classic SGSI, our model proposes to initially make an estimation of the level of maturity of the company. In such a way, with a low cost, and a short time, we can determine the existing generic risks in the society, before starting the project.

By means of our model, we can estimate fastly the level of maturity of the SGSI of the company and to identify the regulation that better adapts to it, fixing a landmark that can be reached in short term of time of the evolution waited for in the company for each cycle of the spiral (see Figure 2).

This model is based on three levels of security that we will apply according to the level of maturity and the size of the company. A company that, according to the parameters of employees and invoicing, is only considered small would have to apply the version of

Iso17799-1 norm (see Figure 3). This would entail an increase of the risk level, that the implanted controls are not sustainable and would produce a continuous degradation of the controls and the level of maturity.

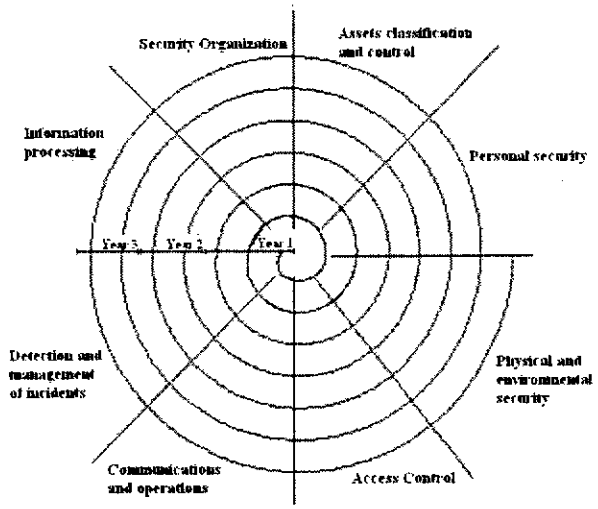

Figure 2. Spiral model for ISMS maturity

Maturity level (According pre-audit performed about ISO17799)		Enterprise Type (according to number of employees and turnover)			
Security Evaluation	Maturity Level		Small	Medium	Big
		Employees	0 – 25	25 – 250	>250
		Million €	0 – 1	1 – 100	>100
0 - 30%	Low		ISO17799-1 [100]	ISO17799-1 [100]	ISO17799-1 [100]
30% - 70%	Medium		ISO17799-1 [100]	ISO17799-2 [300]	ISO17799-2 [300]
70 - 100%	High		ISO17799-1 [100]	ISO17799-2 [300]	ISO17799-3 [500]

Figure 3. Models proposed according to the type of enterprise and its maturity level

One of the main and most valuable conclusions obtained from the feedback of SICAMAN customers in which these models have been analyzed is the following one: The over-dimensioning of the security level of an enterprise with respect to its size finishes generating a degradation of the over-dimensioned controls until they reach their natural balance. The final consequence of this fact is that the enterprise invests more resources than the strictly necessary ones that will not provide any value. In Figure 4, we can see a simulation of how, according to the enterprise size, there is a natural tendency of security systems to find their balance. We are currently developing other models that include new factors that can have influence at the time of deciding about the level of fulfillment that must be applied: the type of activity of the enterprise, the dependency on departments (such as Research and Development Department), and so on.

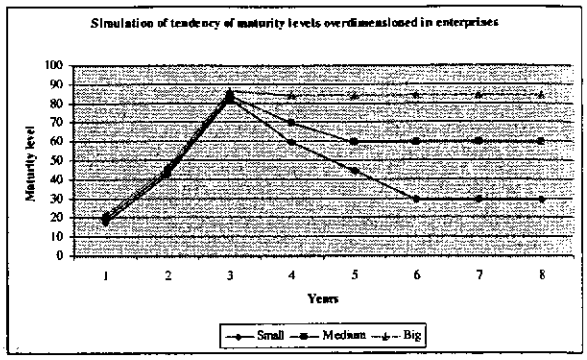

Figure 4. Simulation of tendency of maturity levels over-dimensioned in enterprises

Eloff and Eloff [6] prefer to define four different classes of protection, that allow us to implement the security levels in a progressive way, instead of the three classes selected by us:

- Class 1: Inadequate protection. It does not cover any section of ISO17799.
- Class 2: Minimal protection. It covers legal aspects and aspects regarding the business continuity.
- Class 3: Reasonable Protection. To the previous covered aspects, organizational aspects, assets control and access management are added.
- Class 4: Adequate Protection: All sections of ISO17799 are covered.

A representation of the model proposed by this simulation is shown in Figure 5. We have used grey colour to highlight the sections of the rule that are not fulfilled for each protection level.

On the contrary, our model does not associate protection levels with sections of the rule but divides each section into three levels and we can evolve the rule over those levels.

ISO17799 Section Name	Protection Classes			
	Class 1: Inadequate Protection	Class 2: Minimal Protection	Class 3: Reasonable Protection	Class 4: Adequate Protection
Security Policy				
Security Organization				
Assets Classification and Control				
Personnel security				
Physical security				
Communications and operations				
Access Control				
Systems development and maintenance				
Business continuity planning				
Compliance				

Figure 5. Example of association between ISO17799 sections and protection classes

Another alternative at the maturity levels is ISM3 [16], which establish five maturity levels of the company security:

- Level ISM3 0: Although this level can produce a short-term improvement, it is unlikely that it

causes a significant reduction of the risk of and internal threats in a medium-long-term, without unpredictable investments.

- Level ISM 1: This should cause a significant reduction of the risk of technical threats, with a minimum investment in ISM essential processes. This level is recommended for organizations with low security goals in low risk environments.
- Level ISM3 2: This level should cause a greater reduction of the risk of technical treats with as reasonable investment in ISM processes. This level is recommended for organizations with ordinary security goals in ordinary risk environments.
- Level ISM3 3: This level should cause a great reduction of the risk of technical threats, with a serious investment in ISM processes. This level is recommended for organizations with high security goals in high risk environments.
- Level ISM3 4: This level should cause the greatest reduction of the risk threats, both technical and internal, with a serious investment in ISM processes. This level is recommended for organizations with specific requirements (such as energy and water suppliers, financial institutions and organizations which share o store important information) with high security goals in high risk environments.

Proceso	ISM3 0	ISM3 1	ISM3 2	ISM3 3	ISM3 4
GP-1		X	X	X	X
SSP-1,2,3,6		X	X	X	X
SSP-4,5					X
TSP-1,2,3,12		X	X	X	X
TSP-5,6,10,11			X	X	X
TSP-4,9				X	X
TSP-7,8					X
OSP-1,5,10,16,17		X	X	X	X
OSP-2,4,6,7,9,11,12,14,19,22			X	X	X
OSP-3,8,13,15,20,24				X	X
OSP-18,21,23,25					X

Figure 6. Application of ISM3 processes .

These levels must be associated with processes and according to the maturity level, the company will be obligated to comply with a series of processes. In that way, a 0 level involves to comply with no process. In Figure 6, we can see the table of application of ISM3 levels related with processes.

In opposition to these maturity levels technologies, SICAMAN base its investigations in make a new approach to the maturity levels, developing a method that allow to evolve protection to a similar level as the sections of ISO/IEC 17799. It would be perfect that the proposed improvement plan could be adapted to the unification of the different sections before performing a second level of evolution of the rule, in case it was necessary.

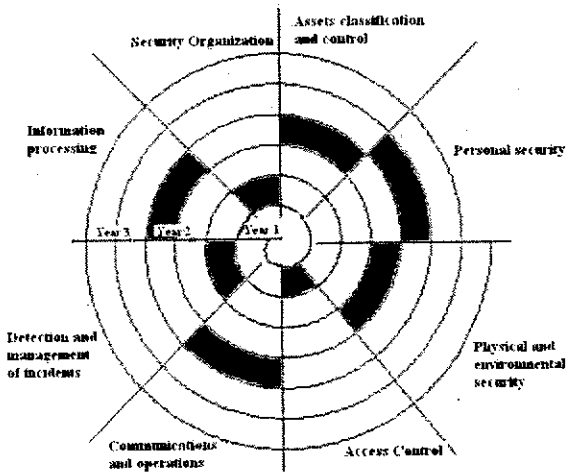

Figure 7. Example of maturity levels by sections in the spiral model.

In Figure 7, we can see a maturity level represented through our "spiral model". Even when the different sections could improve independently, it is more logical that we plan improving those aspects that have less security. In our example, we should improve the "access control" section before improving any other section.

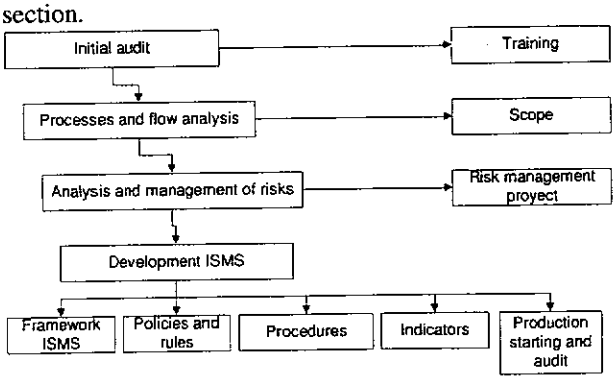

Figure 8. Stages of an ISMS implementation

Once the protection level that we aim at using has been established, we have decided to carry out a systematic approach to study the implementation of information security management systems. We have considered as main core 17799 rule but without declining to use other kind of standards and recommendations in the field of security and

management security. The main processes are shown in Figure 8.

A brief description of these stages is exposed as follows:

- Initial audit: In an ISMS, the first thing to do is to know the current situation of the enterprise concerning security as well as to know the enterprise as organization. This stage implies the establishment of the current maturity level of the ISMS of the enterprise (see Figure 3).
- Processes and flows analysis. From the previous analysis of the security level, we could carry out an analysis of the necessary processes and flows to reach the objectives.
- Analysis and Management of Risk. It is one of the most important stages and the majority of studies performed have dealt with it. In spite of this fact, an approach based on analysis and management of risks is not enough [17]. It is also necessary to identify and eliminate risks, activity that must be carried out efficiently, saving money as a direct consequence of a correct security management [18].
- Development ISMS. Once the real current situation regarding information security is known, the information security management system is elaborated by defining a set of security controls obtained from ISO/IEC 17799 and taking into account the particularities of the enterprise and systems.

	ISO/IEC 17799-1	ISO/IEC 17799-2	ISO/IEC 17799-3
Security Policy	1	2	4
Security Organization	3	10	19
Assets Classification and Control	1	3	8
Personnel security	3	10	25
Physical security	3	13	90
Communications and operations	3	24	172
Access control	8	31	168
Systems development and maintenance	5	18	100
Business continuity planning	1	5	58
Compliance	3	11	79

Figure 9. Controls to identify according the level of the company maturity

To confront the first phase and fix the initial point of our maturity spiral, we'll set which level of rules we must apply according to company (see Fig.3). Once we identify the suitable level, we should make the checklist according this level (see Fig.9).

In the figure 7 we can see the level application at the spiral model. In this way, all the company will go from 0%-100% of security (see fig.11), for each one of the three levels of maturity predicted, and inside of this level we'll keep six sub-levels.

	0-10%	10-25%	25-50%	50-75%	75-90%	90-100%
ISO/IEC 17799-1						
ISO/IEC 17799-2						
ISO/IEC 17799-3						

Figure 10. Evolution of maturity's model.

The highest maturity's level this related by the type of company. We must avoid that a company who tries to reach a maturity level the over sizing of the security level, causing the problems showed in the fig.5. Every control we'll use (see figure 10) will be valued this way: Yes (value 2), partially (value 1), No (value 0), N/A (No Apply). The final value for every section will be the result to divide the sum of the value retrieved between the greatest possible values, to obtain the percentage of actual fulfilment. From this percentage we'll know the level of every section, which we'll apply taking as base the fig.11. The colour's code will allow a fast recognition of the conflictive controls when we'll apply in the security scoreboard.

In addition, one of the market tendencies during ISMS implementation is the development of a SCOREBOARD that allows the enterprise management board to know immediately the failures and improvements produced in the enterprise systems. To do so, we have developed a prototype oriented to associate sections, control objectives and ISO/IEC 17779 controls with a scoreboard that indicates to the enterprise management board through a colour code what security aspects must be improved. A small sample of this prototype can be seen in Figure 11a that shows the scoreboard at the section level and in Figure 11b, that shows it at the control objective level. Moreover, it is possible to show the scoreboard at the individual security control level.

The idea of this prototype is to be able to integrate all information coming from the different security tools existing in enterprises into an only tool that, through the development of security metrics, allows us to update (with the minimum human interaction) the scoreboard proposed in Figure 11. This will make possible that enterprises know in every moment the state of their security, investing the minimum possible resources. To obtain this, our prototype will face the challenge of making decisions based on the incidences communicated by the staff, detected alerts and so on.

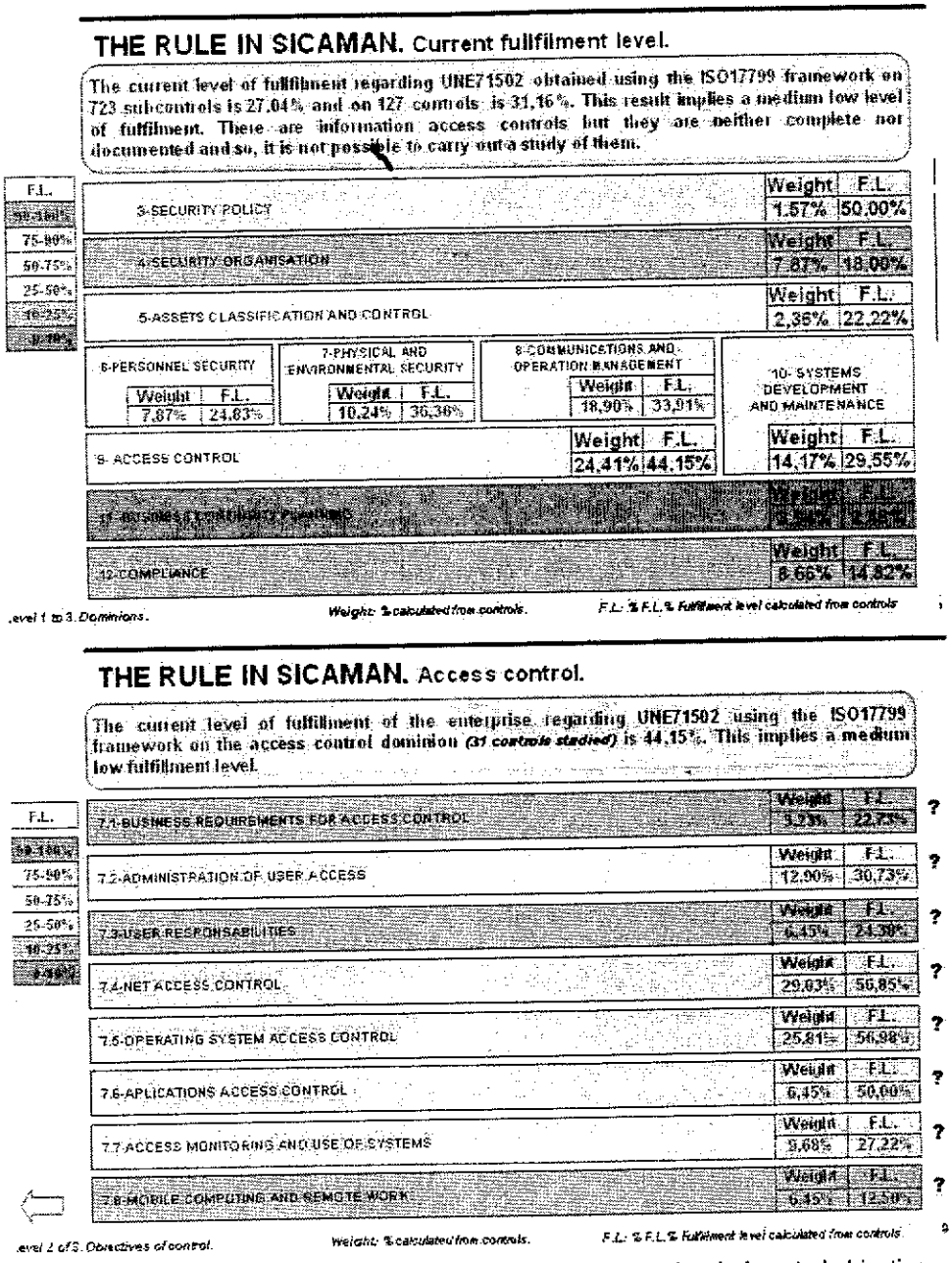

Figure 11. Scoreboard at the section level and Scoreboard at level of control objective

4. Conclusions and Future Work

In spite of the enormous efforts being made to create security regulations and adequate metrics to manage security within enterprises, these regulations do not properly fit with the environment where they must be implemented. The most possible reason is the enterprises lack of maturity and the fact that they have tried to implement too general regulations. For this reason, many times, enterprises do not know what objective they must fulfill or how to begin to restructure their systems. One of the documents generated by standardization international groups that have had more influence all over the world is ISO/IEC 17799 Code of Good Practice that defines a very vast set of security controls. Nevertheless, this code of good practice does not offer a global solution to the security problem since it does not include management mechanisms.

In this paper, we have presented, from the viewpoint of our practical experience, a first approximation to the implementation of security

management systems in small and medium-size enterprises, taking as a basis or framework ISO/IEC 17799 and adapting it to both the size and the maturity level of the enterprise in which it will be implemented.

Given that this proposal is very preliminary, our medium and long term purpose is to perform a research on the complete development of a methodology to implement security management systems that allow an adequate adaptation depending on the security needs and the enterprises characteristics, mainly oriented to small and medium-size enterprises. This methodology will be based on the main security and security management standards and it will be adapted to the social conditions, and above all, to the legal conditions of the environment in which we develop our professional activity. We hope to obtain a continuous improvement of these implementations through the 'in action' research method as well as the feedback directly obtained from our customers.

This methodology will be complemented with a security systems management tool, mainly oriented to the enterprise management board, to facilitate decision making when planning security systems.

Acknowledgments

This research is part of the following projects: DIMENSIONS, partially financed by FEDER and the Consejería de Educación y Ciencia de la Junta de Comunidades de Castilla-La Mancha (PBC-05-012-1), CALIPO (TIC2003-07804-C05-03) and RETISTIC (TIC2002-12487-E) financed by "Dirección General de Investigación del Ministerio de Ciencia y Tecnología" (España)

5. References

[1] Dhillon, G. y Backhouse, J. Information System Security Management in the New Millennium, Communications of the ACM, (2000) 43(7).

[2] Tsujii, S. Paradigm of Information Security as Interdisciplinary Comprehensive Science. Proc. of the 2004 International Conference on Cyberworlds (CW'04), IEEE Computer Society, (2004) 1-12.

[3] Rodriguez, Luis Ángel. Seguridad de la Información en Sistemas de Computo. Ventura Ediciones, México, (1995).

[4] Cabrera Martin, Álvaro. Políticas de Seguridad. Boletín del Criptonomicón #71.Madrid, (2000).

[5] Computer Security Institute – CSI. Computer Crime and Security Survey. (2002)

[6] Eloff, J. y Eloff, M. Information Security Management – A New Paradigm. Proc. of the 2003 annual research conference of the South African institute of computer scientists and information technologists on Enablement through technology SAICSIT'03, (2003) 130-136.

[7] Power, E.M. y Trope, R.L. Adverting Security Missteps in Outsourcing. IEEE Security & Privacy, marzo/abril, (2005) 70-73.

[8] Peltier, T.R. Preparing for ISO 17799. Security Management Practices, jan/feb, (2003) 21-28.

[9] Walton, J.P. Developing an Enterprise Information Security Policy. Proc. of the 30th annual ACM SIGUCCS conference on User services, (2002) 153-156.

[10] Endorf, C. Outsourcing Security: The Nedd, the Risks, the Providers, and the Process. Information Security Management, (2004) 17-23.

[11] Von Solms, B. Information Security governance: COBIT or ISO 17799 or both? Computers & Security 24, (2005) 99-104.

[12] Masacci, F., Prest, M., Zannone, N. Using a security requirements engineering methodology in practice: The compílanse with the Italian data protection legislation. Computer Standards & Interfaces 27, (2005) 445-455.

[13] Von Solms, B. y Von Solms, R. Incremental Information Security Certification. Computers & Security 20, (2001) 308-310.

[14] Isg, Information Security Governance a call to action, Abril 2004.

[15] NIST, SP 800-55 Security Metrics Guide for Information Tecnology Systems, July 2003.

[16] Vicente Aceituno Canal, ISM3 1.0. - Information Security Management Maturity Model.

[17] Siegel, C.A., Sagalow, T.R. y Serritella, P. Cyber-Risk Management: Technical and Insurance Controls for Enterprise-Level Security. Security Management Practices, sept/oct, (2002) 33- 49.

[18] Garigue, R. y Stefaniu, M. Information Security Governance Reporting. Information Systems Security, sept/oct, (2003) 36-40.