Automated Security Metrics in ISMSs to Discover the Level of Security of OSs and DBMSs

Angel Gallego[1], Antonio Santos-Olmo[2], Luís Enrique Sánchez[2] and Eduardo Fernández-Medina[3]

[1]EZENTIS. Departamento de I+D
Federico Mompou, 5., Madrid, Spain

[2]SICAMAN Nuevas Tecnologías. Departament R&D
Ave Maria, 5. Tomelloso, Ciudad Real, Spain

[3] Grupo de Investigación GSyA. Universidad de Castilla-La Mancha
Paseo de la Universidad, 4 – 13071, Ciudad Real, Spain

Abstract. The information society is ever-increasingly dependent upon Information Security Management Systems (ISMSs), and the availability of these systems has come to be vital to the evolution of SMEs. However, this type of companies requires ISMSs which have been adapted to their particular characteristics, and which are optimised from the point of view of the resources that are necessary to install and maintain them. This paper concentrates on the development of a process for ISMSs that will allow the level of security of critical applications installed in these sytems, i.e., Operative Systems and Data Base Management Systems, to be measured. This process is currently being directly applied in real cases, thus leading to an improvement in its application.

1 Introduction

It is extremely important for businesses to install security controls which will allow them to know and control the risks to which they may be subjected [1, 2], since the installation of these controls supposes important improvements for these companies [3]. However, the mere installation of these controls is not sufficient, since long-term security management systems are also necessary if companies are to react to new risks, vulnerabilities, threats etc. in an agile manner [4, 5]. Nevertheless, companies frequently do not have security management systems, or if they do, the systems have been created without appropriate guidelines and documentation, and with insufficient resources [6].

Although it has been shown that for a business to be able to use information technologies and communications with guarentees it must have guidelines, metrics and tools at its disposal that will provide it with constant knowledge of its level of security and any vulnerabilities that have not yet been covered [7], the level of successfully installed systems is extremely low. This problem is particularly accentuated in the

Gallego A., Santos-Olmo A., Enrique Sánchez L. and Fernández-Medina E..
Automated Security Metrics in ISMSs to Discover the Level of Security of OSs and DBMSs.
DOI: 10.5220/0003593901590166
In *Proceedings of the 8th International Workshop on Security in Information Systems* (WOSIS-2011), pages 159-166
ISBN: 978-989-8425-61-4

case of small and medium-sized enterprises, which face the additional limitation of not having sufficient human and economic resources to be able to carry out appropriate management [6].

In this paper we concentrate upon analysing a method which is oriented towards fulfilling the seventh of these factors – *"defining a measurement system with which to evaluate the security management's output and suggest improvements",* and this will be adapted to the case of SMEs in order to ensure that maintenance costs are greatly reduced, thus offering those resposible for security the maximum possible value, and allowing them to know the short-term fulfillment level of the various controls.

The paper continues in Section 2 in which the objectives pursued during this research are described. Section 3 describes the measurement process used. Section 4 analyses the control objectives created for the research phase it self. Section 5 presents the tool that supports the process defined and shows some of the results obtained. Finally, in Section 6 we show our concusions and future work.

2 Objectives Pursued by this Research

The aforementioned view of the current market situation and its security needs has been used as a starting point upon which to centre the objective of this research: the creation of a process that will permit the simple yet efficient measurement of the level of security in those applications that can be considered to be critical to the correct functioning of a company's Information System. This process will allow us to obtain a guarantee of the risk that is assumed with a business' Information System, with the lowest cost in both time and money, which will be extremely useful for SMEs.

This metric was created by bearing in mind the latest research concerning the most important standards related to security metrics [8, 9]. The mechanism created is not intended to substitute these regulations, but to complement them and to assist in their fulfilment.

We can therefore state that the principal objective of this research has been to create a process that will permit the definition of a series of measurable and evaluable aspects with regard to critical applications, along with a tool to support it which will allow us to provide an objective evaluation and an updated risk report of the Operative Systems and of the Data Base Management Systems (key elements in any company) with which they will be integrated and upon which the company's remaining applications are sustained. This process will be integrated into the other processes forming part of an ISMS.

Four clearly defined phases were followed to attain the objective proposed in this research:

- During the 1st phase we analysed how to define a simple system that would allow us to evaluate the critical applications' current level of security.
- During the 2nd phase we extracted the tools selected for the research, which would be the principal factors evaluated in order to define the level of security. We then carried out an in-depth study of the Windows O.S., along with the two DBMS most frequently used at present (Oracle and SQL Server) in order to define the control objectives that would later allow us to carry out

an evaluation of both the level of security and the evaluation system that would be used for the securitization of the environment.

- During the 3rd phase we created an application that would allow us to support the analysis of the process defined in the 1st phase. We were consequently able to provide an evaluation of of the security level in the systems analysed, according to their current configuration. Certain recommendations associated with the actions that should be taken to raise the Information Systems' security level were also obtained.
- Finally, in the 4th phase, the process and the tool that supports the various systems that function in the Sicaman Company were applied. The process allowed us to obtain a set of results with which to determine the current security level in this company's systems, and enabled us to provide recommendations on how to improve them.

3 Development of Measurement Process

The development of this phase involved making a prior selection of those tools and applications which, in the event of a security failure, would make most impact on the company's computer services. The results of this study showed that the company's greatest risk concerned the loss or undesired leaking of its data.

The following step in this phase was to determine what the control objectives were for each of the applications, along with determining tests and levels that would allow us to evaluate the system's current risk level.

These control objectives were developed by using the technical security documentation provided by the company's manufacturers, in addition to the personal experience of the human team which participated. This knowledge enabled us to select those points in each application that supposed the greatest risk. Each of these points was then dicretized to enable its quantification.

The quantification or evaluation mechanism of the control objectives is based solely upon the experts' knowledge of these applications, which implies that later versions of the application may experience variations.

The structure followed to define the control objectives was:

- ***Id:*** A unique code which allows the control objective and the application to which it belongs to be identified.
- ***Level:*** To what level the control objective is affected within the global environment.
- ***Question:*** The control objective pursued.
- ***Responsibility:*** The person responsible for applying this control objective.
- ***Instant:*** Determine at what instant the control objective should be tested.
- ***Action:*** Determine how the control objective should be verified.
- ***Correct configuration:*** What the control objective should be like if it is to be considered secure.
- ***Evaluation:*** Criteria to decide whether or not the control objective is fulfilled, thus establishing it as being safe or unsafe.

The execution of the process defined led us to obtain the application's security level, which can be calculated as:

Table 1. Equiation with which to calculate the fulfillment level of a control.

RL = (([TGVF]*100)/[TGPV]) ***SL = 100 – RL***
• **RL:** Risk level. • **SL:** Security level. • **TGVF:** Total grading of vulnerabilities found. • **TGPV:** Total grading of possible vulnerabilities.

The associated risk is obtained according to the value obtained, and is discretized in the following table:

Table 2. Risk measurement levels.

Risk	Interval (according to security level)	Description
No risk	90% - 100%	No serious faults have been detected.
Potential risk	60% - 90%	Medium-level faults have been detected.
High risk	0% - 60%	High-level faults have been detected.

4 Definition of Controls

In this research phase a detailed analysis has been made of the critical applications with the objective of extracting the set of control objectives for each of the applications forming part of the research. The following applications were analysed:

- **Windows Server:** A set of 25 controls were extracted for evaluation. The total number of points that will define the application's security varies between 0 (maximum security level) and 37 (minimum security level). The aspects to be evaluated are divided into 5 typologies: access level, service level, level of applications, management level and network level.
- **Oracle:** A set of 26 controls were extracted whose level of security coverage was evaluated. The total number of points that will define the application's level of security varies between 0 (maximum security level) and 44 (minimum security level). The aspects to be evaluated are divided into 4 typologies: general level, server level, DBMS level and DB level.
- **SQL Server:** A set of 37 controls were extracted whose security coverage was evaluated. Of these, 26 can be automated to reduce costs and 13 currently require manual analysis. The total number of points defining the security level of the application varies between 0 (maximum security level) and 53

(minimum security level). Table 3 shows an example of the controls defined for this type of applications. The aspects to be evaluated are divided into 4 typologies: general level, server level, DBMS level and DB level.

Table 3. Control manual/automatic for SQL Server**.**

Id: [SQL.4.2]

Question: Are views used to minimize the dependencies between DBs?

Level: Data Base.

Responsibility: Programmer.

Instant: General.

Action: Code control.

Correct configuration: Protect against access via SQL through the development of a structured programme.

Evaluation:

- ***Unsafe:*** Dependencies exist between DBs which are not contained in views.
- ***Safe:*** Views are used to minimize the dependencies between DBs.

Test requested: Analyse the dependencies with linked servers and verify the type of objects that they contain. Use the sysservers, sysobjects and syscomments tables for this.

Script for automation:

```
select srvname collate SQL_Latin1_General_CP1_CI_AS from mas-
ter.dbo.sysservers
declare @servidor varchar(128)
select @servidor = ''
select total, servidor_novista, servidor_vista,
    case when total=0 then 0 else
100*convert(decimal(9,2),servidor_novista)/convert(decimal(9,2),total) end as
porc_servidor_novista,
    case when total=0 then 0 else
100*convert(decimal(9,2),servidor_vista)/convert(decimal(9,2),total) end as
porc_servidor_vista
from (select    count(*) as total,
                isnull(sum(case when xtype='V' then 1 else 0 end),0) servidor_vista,
                isnull(sum(case when xtype='V' then 0 else 1 end),0) servi-
dor_novista
    from sysobjects a, syscomments b
    where text like '%'+@servidor+'%') a
```

5 Practical Results

A tool has been created to provide the development process with automated support. The system tests have been carried out on the installations in the Sycman Company (SNT) on the development and production servers, the Windows Server and Oracle Data Base Management Systems and the SLQ Server operative systems. Table 4 shows some of the conclusions reached after applying the process defined to real applications.

Table 4. Results of application of metrics in real cases.

System Data	Results Obtained
Name of computer: Sicaman\Pc18 **IP Address: Dirección IP:** 192.168.2.8 **Name of Auditing Team:** SNT DB Server Servidor BD de SNT **Date of Audit:** 20/11/2010 9:46 **Scanned with SEM version:** 1.0 **Security Level:** 14/53 → 73.58% **Risk Level:** 26.42% (Potential risk).	The negative grading was 14 out of 53, which implies that the auditing platform's current security level is 73.58% with an associated risk of 26.42%. If the securitiy level is to be raised then the following points must be reviewed: ***Very high risk:*** [SQL.3.2], [SQL.3.10], [SQL.3.25] ***High risk:*** [SQL.1.3], [SQL.1.4], [SQL.3.3], [SQL.3.7], [SQL.3.9], [SQL.3.22], [SQL.3.24], [SQL.4.4]

The application of the method defined to the SNT development and production environments led to the following results:

- The production server for the SQL Server 2005 environment obtained an evaluation for the "SQL Server 2005" application of 14 out of 53, which implies a potential risk of 26.42% and a security level of 73.58%.

The risk level obtained in the reviews is shown in Table 5:

Table 5. Risk level for applications analysed.

	Windows 2003	**SQL Server 2005**	**Oracle 11i**	**Average risk**
Production server [SQL]	27,03	26,42	-	26,67

The final conclusions obtained are:

- The SNT production environment has an average security level, both at the server level and at the level of individual applications. It would be advisable to follow the recommendations obtained during the execution of the process in order to obtain secure processes, particularly if we bear in mind that this is a production environment.
- The SNT development environment has a low security level at the server level and at the level of individual applications in both the SQL Server and Oracle environments. In a development environment it is advisable for the risk to be at a medium level, and we therefore advise the company to follow the recommendations made in the audit report.

6 Conclusions and Future Work

This paper presents a proposal for a process which is oriented towards measuring the level of security in critical applications that form part of an information system.

We have defined how this process can be used and how it could assist SMEs to discover the risks that they may confront without the need to assume large costs.

The characteristics of this process and its orientation towards SMEs have been very well received, and its application is proving to be very positive since it allows this type of businesses to better understand the risks to which their information assets are subjected. This process allows allows companies to obtain short-term results, thus reducing the costs supposed by other analysis mechanisms and leading to greater company satisfaction.

We are currently analysing the possibility of integrating this process into the Security Management methodology for SMEs denominated as MMSM-SME [10-13], and into the tool that supports this methodology [14].

Thanks to the development of this research project, the companies in which the results obtained have been tested have been able to identify security risks and improvable aspects in their systems.

In later versions of this application we shall continue the automation process of control objectives that commenced here.

Finally, we believe that the work carried out must be extended with new applications, new controls, and mechanisms that will permit the inclusion of an increasing amount of automated controls.

All future improvements to the process and the model will be oriented towards improving their levels of automation and precision, whilst always respecting the principle of the cost of resources. In other words, we seek to improve the process without incurring generation and maintenance costs.

Acknowledgements

This research is part of the following projects: MEDUSAS (IDI-20090557), financed by the Centre for Industrial Technological Development (CDTI), ORIGIN (IDI-2010043(1-5)) financed by the CDTI and the FEDER, BUSINESS (PET2008-0136) awarded by the Spanish Ministry for Science and Technology and MARISMA (HITO-2010-28), SISTEMAS (PII2I09-0150-3135) and SERENIDAD (PII11-0327-7035) financed by the Council of Education and Science of the Castilla-La Mancha Regional Government.

References

1. Kluge, D. *Formal Information Security Standards in German Medium Enterprises.* in *CONISAR: The Conference on Information Systems Applied Research.* 2008.
2. Dhillon, G. and J. Backhouse, *Information System Security Management in the New*

Millennium. Communications of the ACM, 2000. 43(7): p. 125-128.
3. Park, C.-S., S.-S. Jang, and Y.-T. Park, *A Study of Effect of Information Security Management System[ISMS] Certification on Organization Performance.* IJCSNS International Journal of Computer Science and Network Security., 2010. 10(3): p. 10-21.
4. Barlette, Y. and V. Vladislav. *Exploring the Suitability of IS Security Management Standards for SMEs*. in *Hawaii International Conference on System Sciences, Proceedings of the 41st Annual*. 2008. Waikoloa, HI, USA.
5. Fal, A.M., *Standardization in information security management* Cybernetics and Systems Analysis 2010. 46(3): p. 181-184.
6. Wiander, T. and J. Holappa, *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.
7. 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.* 2008. Wollongong, Australia.
8. Yao, L., *Discussion on Effectiveness Measurement in ISMS: Based on Analysis of ISMS Effectiveness Measurement in ISO/IEC 27004:2009.* Electronic Product Reliability and Environmental, 2010.
9. ISO/IEC27004, *ISO/IEC FCD 27004, Information Technology - Security Techniques - Information Security Metrics and Measurement (under development).* 2009.
10. 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.* 2006. Viena (Austria).
11. 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).* 2007b. Funchal, Madeira (Portugal). June.
12. 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).* 2007a. Barcelona. Spain.: Junio.
13. 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)*. 2006. Paphos (Chipre). March.
14. 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).* . 2007c. Barcelona-España Septiembre.