Research Journal of Engineering Sciences ___________________________________ ISSN 2278 – 9472
Vol. **1(5),** 51-54, November **(2012)** *Res. J. Engineering Sci.*

Cybernetics Security Requirements and Reuse for Improving Information Systems Security

Yadav Sunil Kumar[1] and Rizvi Syed Azhar Abbas[2]
[1]UP Beej Vikas Nigam Mahanager, Lucknow, UP, INDIA
[2] Emrald 9 Institute of Management Deva Road Barabanki, UP, INDIA

Available online at: www.isca.in
Received 12th October 2012, revised 17th October 2012, accepted 20th October 2012

Abstract

Information systems security issues have usually been considered only after the system has been developed completely, and rarely during its design, coding, testing or deployment. However, the advisability of considering security from the very beginning of the system development has recently begun to be appreciated, and in particular in the system requirements specification phase. We present a practical method to elicit and specify the system and software requirements, including a repository containing reusable requirements, a spiral process model, and a set of requirements documents templates. In this paper, this method is focused on the security of information systems and, thus, the reusable requirements repository contains all the requirements taken from MAGERIT, the Spanish public administration risk analysis and management method, which conforms to ISO 15408, Common Criteria Framework. Any information system including these security requirements must therefore pass a risk analysis and management study performed with MAGERIT. The requirements specification templates are hierarchically structured and are based on IEEE standards. Finally, we show a case study in a system of our regional administration aimed at managing state subsidies.

Keywords: Requirements engineering, requirements reuse, security, common criteria framework, risk analysis and management methods.

Introduction

There has recently been an increasing interest in information systems security issues. For instance, PITAC (President's Information Technology Advisory Committee)[1] has stated the need for a scalable information infrastructure, that is, for techniques which ensure that the United States information infrastructure -including communications systems, the Internet, large data repositories and other emerging systems- is reliable and secure and can grow smoothly to accommodate the massive numbers of new users and applications requiring high bandwidth which are anticipated over the next two decades.

Nowadays, information systems are vulnerable to many threats, such as new viruses (e.g. worm viruses) that propagate through Internet; the threats brought about by unacceptable employees use of the internet resources (such as non-business activities, accidental or deliberate disclosure of sensitive information, and hacking)[2], failure to observe the personal data privacy laws[3] (leading, in our country, to fines of up to $700,000 or to important administrative sanctions[4], even strikes or loss of key personnel are threats that information systems need to be able to cope with. In addition, the general acceptance of e-commerce and the digital signature to perform administrative and commercial transactions means that the security of information systems needs to be ever more reliable. A security breakdown can result in very serious problems for an organization: for example, a recent survey on 1,000 UK organizations[5] shows that the occurrence of a security failure in a business with no contingency plan leads to its shutdown in 80% of the cases, and 60% of UK businesses have suffered an important security breach in the last two years.

A large number of methods and regulations concerning the security of organizations have appeared in response to such a situation. Of particular importance are ISO 15408, Common Criteria Framework (CCF)[6] and the following national risk analysis and management methods: CRAMM in the UK (CCTA – Carmarthenshire College Of Technology and Art– Risk Analysis and Management Method)[7], MARION in France (Méthode d'Analyse de Risques Informatiques et d'Optimisation par Niveau)[8] and MAGERIT (Metodología de Análisis y GEstión de RIesgos del MinisTerio de Administraciones Públicas)[9], which is the Spanish Public Administration's adaptation of CCF.

In the information systems development field, requirements form the foundation for the rest of the software development process, since building a high-quality requirements specification is essential to ensure that the product satisfies the users' needs[10]. However, drawing up a specification of quality requirements is a difficult task. According to the IEEE 830-1998 standard, a requirement of quality is that it be correct, unambiguous, complete, consistent, ranked for importance and/or stability, verifiable, modifiable, and traceable. We agree with Mili et al. that "there exist few alternatives but software reuse as the (only) realistic approach to bring about the gains of productivity and quality that the software industry needs". It is the benefits of reuse are greater when the abstraction level is increased and not only code, but also designs and specifications, are reused. The usual practice during the early steps in information systems development has been to pay attention to such aspects as reliability, availability or integrity, while security issues have usually been considered only once the system has been deployed, or at best, during the system design, coding or testing[9].

In this paper, we present a proposal to consider information systems security beginning with the Requirements Engineering (RE) process. The approach is based on the reuse of security requirements which are compatible with MAGERIT (and, therefore, also with a CCF subset) and which are collected in a reusable requirements repository. This approach complements SIREN (simple reuse of software requirements), a general purpose RE method based on requirements reuse that we are currently defining. As this paper explains, the inclusion of requirements from the repository controls risk levels within the information system to be built, so that the information system will fulfill the demands of risk analysis performed with MAGERIT. How this approach has been applied to a real case study concerning an information system in our regional government is shown in this paper.

Objectives: This research is based on the lessons learned during a risk analysis and management project developed with MAGERIT in our regional government. Our research offers a combination of RE, reuse, and information systems security in order to improve information systems quality and productivity.

RE and Security

The essential reason behind this proposal is the need to include security explicitly in information systems development, as of the RE process, and thus improve several information systems quality attributes, namely security, safety, reliability, and robustness. Sommerville[10] claims that a high percentage of system malfunctions are the result of errors in specification rather than design. For example, the specification may be incomplete in that it does not describe the behavior of the system required in some critical situations. In a study of errors in embedded systems, Lutz[11] concludes that difficulties with requirements are the key root cause of the safety-related software errors which have persisted until integration and system testing".

RE process improvement: Our proposal also addresses the improvement of information systems quality through the improvement of the quality of the RE process. In this section we deal with the improvement of the quality of the RE process by means of the main processes life cycle standards and quality standards. To this extent, neither life cycle processes standards (such as ISO 12207) nor quality standards (such as ISO 9000) provide precise guidelines for identifying problems and planning improvements in the life cycle processes of systems and software (in particular, ISO 9000 does not include any section specifically devoted to RE.

In contrast, capability maturity models, such as CMM and ISO 15504/SPICE (Software Process Improvement and Capability dEtermination), do provide guidelines to improve the quality of the life cycle processes. However, once again, they do not cover the RE process.

Magerit

Magerit[9] is the information systems risk analysis and management method of the Spanish public administration, which is compatible with ISO 15408, Common Criteria Framework. In this paper we show how we have translated the security measures stated in Magerit into reusable security requirements. Magerit is, therefore, the source of our reusable security requirements repository. Magerit, moreover, specifies how risk analysis has to be performed before selecting the required security requirements. This section summarizes the basic elements of Magerit beginning with a brief description of the evolution of the risk analysis and management methods. Baskerville studies the evolution of information systems security design methods.

The risk analysis and management model of MAGERIT includes: i. the submodel of elements, providing the basic entities related to the information system risk analysis: assets, threats, vulnerabilities, effects, risks, and countermeasures; ii. the submodel of processes, describing the stages in the security project that is to be developed: planning, risk analysis, risk management, and recommendation of countermeasures.

Risk analysis with MAGERIT involves the following major steps: i. identification of the assets of the organization, which are the resources of the information system, and which may either directly belong to the information system or just to the information system environment; ii. study of the vulnerabilities of these assets and the threats to them; iii. estimation of the risk related to these assets, based on the threats and vulnerabilities associated (threats are qualified by the likelihood of their occurring); iv. proposal of the countermeasures managing the risk. Therefore, countermeasures manage threats and are transitively linked to assets.

Magerit organizes assets in five layers: i. The information system environment layer includes the facilities containing the information system, such as furniture and supplies. ii. The information system layer includes the information related to the software, hardware, and personnel, which make up the information system. iii. The information layer includes the information managed by the information system: applications data and metadata (such as data structures and data dictionaries). iv. The organization's functions layer justifies the usefulness of the information system, by providing it with a purpose; it describes the assets and services produced by the information system, and the users of the information system services. v. Finally, the other assets layer describes assets that are usually intangible, and do not fit into the lower layers, as, for instance, the organization credibility or an individual's privacy.

Each layer can be refined into blocks of homogeneous assets. Besides, each block can be further divided into sub-blocks.

The Siren Approach to Requirements Reuse

Our proposal, called siren (simple reuse of software requirements), is a method for RE based on requirements reuse. The purpose of development with requirements reuse is to identify descriptions of systems that could be used (either totally or partially) with a minimal number of modifications, thus reducing the total effort of development. SIREN also conforms to the most well-known Software Engineering standards for requirements specification. Requirements have a textual format, but can include any kind of objects as complementary information - for instance, tables or schemas of any type. SIREN encompasses a process model, some guidelines, techniques and tools. The guidelines that SIREN provides consist of a hierarchy of requirements specification documents together with the templates for each document. These serve to structure a reusable requirements repository. Finally, we will present the SIREN process model and a discussion on the tools used to support the process.

Requirements Documents Hierarchy

The SIREN requirements documents hierarchy. In accordance with Gabb, we consider that each document correspond to a different specification level and, therefore, it has different objectives and users.

SRS (Software Specification Requirements)

In the SRS, the functions and performance allocated to software as part of system engineering are refined by establishing a complete information description, a detailed functional description, a representation of system behavior, an indication of performance requirements and design constraints.

The SRS includes requirements on the software functionality, external interfaces, performance, design constraints, and software attributes (portability, maintenance, security, availability, and reliability). Most software requirements are directly derived from the system requirements; hence the hierarchical vision presented. The SIREN SRS template is based on the IEEE Std 830-1998 and on the VOLERE template proposed by Robertson and Robertson[11].

System and Software Testing Specifications

Any requirement in the SRS must be quantifiable in order to be subsequently validated. Each requirement in the SRS and SRS needs to have been linked to a testing criterion (called fit criteria in[11]) in the STS and STS documents, respectively. These testing criteria specify how to check that the system or software implemented fulfills the requirements defined. We believe that STS can be very useful in the security field because the security plan of the organization can be specified directly from the STS. This plan will include a list of security questions (related to personnel, organization, and functions) which may be then easily checked.

Interface Requirements Specification

The requirements related to the interfaces between the software elements and between software and users can be included in the SRS. Nevertheless, in order not to produce overlong documents, it is sometimes useful to collect all this information in a separate document, called IRS. Therefore, traceability relationships need to be established between the SyRS, the SRS modules and the interfaces described. The IRS template has the same structure as the SRS section for specifying interfaces.

Conclusion

Magerit- location, whose values are the initials that specify the position of the security requirement within the Magerit asset hierarchy. For example, the initials IS.SW.IS.S.F (Firewall sub-block in the information system layer, which are the value of this attribute for the requirements. In this way, the security profile in the requirements repository may be sorted following two criteria: the structure of the requirements specification documents and the structure of the Magerit asset hierarchy.

Obligement level, providing the analyst with information about the requirements that have to be included. The possible values for this attribute in the security profile are: compulsory, recommendable and optional.

The traceability relationships between the requirements of the repository also have to be collected. In the current SIREN model, a trace can be established between requirements belonging to the same or different documents.

References

1. Constitutional Law 15/1999 of December 13, on Protection of private data of individuals in Spain. (Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal en España), (In Spanish) **(2012)**

2. Real Decreto 994/1999, of June 11, in which the Ruling on security measures of automated files containing private data on individuals is passed. (Real Decreto 994/1999, de

11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal), (In Spanish), 24241 **(1999)**

3. Infosec. Information Security Breaches Survey, http://www.infosec.co.uk **(2000)**

4. ISO/IEC Std. 15408, Evaluation Criteria for Information Technology Security **(2009)**

5. CCTA, SSADM-CRAMM Subject Guide for SSADM Version 3 and CRAMM Version 2, Central Computer and Telecommunications Agency, IT Security and Privacy Group, Her Majesty's Government, London, **(2011)**

6. CLUSIF, MARION version 98, La Commission Méthodes du CLUSIF (Club de la Securité des Systèmes d'Information Français) **(2008)**

7. MAP, Metodología de Análisis y Gestión de Riesgos del Ministerio de Administraciones Públicas Español, MAGERIT v.1.0. (In Spanish) **(2006)**

8. Kotonya G. and Sommerville I., Requirements Engineering. Processes and Techniques, John Wiley and Sons, **(2004)**

9. Robertson S. and Robertson J., Mastering the requirement process, Addison-Wesley, **(2005)**

10. Sommerville I., Software Engineering (6th edition), Pearson Education Limited **(2001)**

11. IEEE Std 830-1998, Guide to Software Requirements Specifications (ANSI), The Institute of Electrical and Electronics Engineers, *Inc. IEEE Software Engineering Standards Collection*, **(2001)**