SECRYPT 2006

Proceedings of the International Conference on
Security and Cryptography

Setúbal, Portugal

August 7 – 10, 2006

Organized by
INSTICC – Institute for Systems and Technologies of Information, Control and Communication

Sponsored by
Polytechnic Institute of Setúbal

Technically Co-Sponsored by
IEEE Systems, Man and Cybernetics (SMC) Society

In Cooperation with
International Association for Cryptologic Research

Hosted by
Setúbal College of Business Administration

Edited by Manu Malek, Eduardo Fernández-Medina and Javier Hernando

Printed in Portugal

ISBN: 972-8865-63-5

ISBN (13 digits): 978-972-8865-63-4

Depósito Legal: 245453/06

http://www.secrypt.org

secretariat@secrypt.org

SECRYPT is part of ICETE - The International Joint Conference on

e-Business and Telecommunications

BRIEF CONTENTS

KEYNOTE LECTURES

David Marca

University of Phoenix

U.S.A.

Manu Malek

Stevens Institute of Technology

U.S.A.

Les Barclay

Barclay Associates Ltd

U.K.

Fernando Pereira

Instituto Superior Técnico – Instituto de Telecomunicações

Portugal

Jan Jürjens

Technische Universität München

Germany

Anisse Taleb

Ericsson AB

Sweden

Tom Greene

M.I.T.

U.S.A.

TUTORIAL

David Marca

University of Phoenix

U.S.A.

ORGANIZING AND STEERING COMMITTEES

Conference Chair

Joaquim Filipe, INSTICC / Polytechnic Institute of Setúbal, Portugal

Honorary Chair

Mohammad S. Obaidat, Monmouth University, U.S.A.

Program co-Chairs

Manu Malek, Stevens Institute of Technology, U.S.A.

Eduardo Fernández-Medina, UCLM, Spain

Javier Hernando, Polytechnic University of Catalonia, Spain

Proceedings Production

Paulo Brito, INSTICC, Portugal

Helder Cide, INSTICC, Portugal

Bruno Encarnação, INSTICC, Portugal

Vitor Pedrosa, INSTICC, Portugal

Graphics Production

Marina Carvalho, INSTICC, Portugal

Secretariat and Webdesigner

Mónica Saramago, INSTICC, Portugal

PROGRAM COMMITTEE

Kamel Adi, University of Quebec in Outaouais (UQO), Canada

Gail-Joon Ahn, University of North Carolina at Charlotte, U.S.A

Ali Akhavi, LIAFA - CNRS, France

Jörn Altmann, School of Information Technology, Germany

Farooq Anjum, Telcordia Technologies, U.S.A.

Giuseppe Ateniese, The Johns Hopkins University, U.S.A.

Dan Bailey, RSA Laboratories, U.S.A.

Anthony Bedford, RMIT University, Australia

John Black, University of Colorado at Boulder, U.S.A.

Carlo Blundo, Università di Salerno, Italy

Xavier Boyen, Voltage Inc., U.S.A

Emmanuel Bresson, CELAR, France

Rahmat Budiarto, National Advanced IPv6 (NAv6) Center, Malaysia

Roy Campbell, University of Illinois, U.S.A

Rui Costa Cardoso, University of Beira Interior, Portugal

Eurico Carrapatoso, FEUP/INESC Porto, Portugal

Pascale Charpin, INRIA - Rocquencourt, France

Mathieu Ciet, Gemplus, France

Miguel Correia, LASIGE, Faculdade de Ciencias da Universidade de Lisboa, Portugal

Véronique Cortier, Loria, CNRS, France

Paolo D'Arco, D.I.A - University of Salerno, Italy

Sabrina De Capitani di Vimercati, DTI, Universita' degli Studi di Milano, Italy

Falko Dressler, University of Erlangen, Germany

Robert Erbacher, Utah State University, U.S.A.

Serge Fehr, CWI Amsterdam, The Netherlands

Eduardo B. Fernandez, Florida Atlantic University, U.S.A.

Marc Fischlin, Darmstadt University of Technology, Germany

Mário Freire, University of Beira Interior, Portugal

Mariagrazia Fugini, Politecnico di Milano, Italy

Steven Furnell, University of Plymouth, U.K.

Luciano Gaspary, Universidade Federal do Rio Grande do Sul, Brazil

Paolo Giorgini, University of Trento, Italy

Dieter Gollmann, TU Hamburg-Harburg, Germany

Carlos Goulart, Federal University of Vicosa, Brazil

Lisandro Granville, Federal University of Rio Grande do Sul, Brazil

Stefanos Gritzalis, University of the Aegean, Greece

Vic Grout, University of Wales, U.K.

Cynthia Irvine, Naval Postgraduate School, U.S.A.

Hamid Jahankhani, University Of East London, U.K.

Nigel Jefferies, Vodafone Group R&D, U.K.

Willem Jonker, Philips Research / Twente University, The Netherlands

Elias P. Duarte Jr., Federal University of Parana, Brazil

Agggelos Kiayias, University of Connecticut, U.S.A

Seungjoo Kim, Sungkyunkwan Universit and Twente University, Korea

Paris Kitsos, Hellenic Open University (HOU), Greece

Lars Knudsen, Technical University of Denmark, Denmark

Cetin Koc, Istanbul Commerce University, Turkey

Christopher Kruegel, Technical University Vienna, Austria

Kaoru Kurosawa, Ibaraki University, Japan

Tanja Lange, Technical University of Denmark, Denmark

Victor Peral Lecha, France Telecom R&D, U.K.

Albert Levi, Sabanci University, Turkey

Chae Hoon Lim, Sejong University, Korea

Javier Lopez, University of Malaga, Spain

Olivier Markowitch, Université Libre de Bruxelles, Belgium

Alexander May, TU Darmstadt, Germany

Madjid Merabti, Liverpool John Moores University, U.K.

Ali Miri, University of Ottawa, Canada

PROGRAM COMMITTEE (CONT.)

Atsuko Miyaji, Japan Advaned Institute of Science and Technology, Japan

Edmundo Monteiro, University of Coimbra, Portugal

Haralambos Mouratidis, University of East London, U.K.

Yi Mu, University of Wollongong, Australia

Volker Müller, University of Luxembourg, Luxembourg

Juan Gonzalez Nieto, Queensland University of Technology, Australia

Kaisa Nyberg, Helsinki University of Technology and Nokia, Finland

Tatsuaki Okamoto, NTT, Japan

José Luis Oliveira, University of Aveiro, Portugal

Martin Olivier, University of Pretoria, South Africa

Rolf Oppliger, eSECURITY Technologies, Switzerland

Elisabeth Oswald, Graz University of Technology, Austria

Guenther Pernul, University of Regensburg, Germany

George Polyzos, AUEB, Greece

Atul Prakash, University of Michigan, Greece

Jean-Jacques Quisquater, UCL, Louvain, Belgium

Indrakshi Ray, Colorado State University, U.S.A

Indrajit Ray, Colorado State University, U.S.A

David Samyde, FemtoNano, France

Susana Sargento, Instituto de Telecomunicações - Universidade de Aveiro, Portugal

Damien Sauveron, University of Limoges, France

Erkay Savas, Sabanci University, Turkey

Berry Schoenmakers, Technical University of Eindhoven, The Netherlands

Bruno Schulze, LNCC, Brazil

Alice Silverberg, University of California, Irvine, U.S.A.

Nicolas Sklavos, University of Patras, Greece

Jose Neuman de Souza, Federal University of Ceará, Brazil

Mark Stamp, San Jose State University, U.S.A.

Lily Sun, The University of Reading, U.K.

Berk Sunar, Worcester Polytechnic Institute, U.S.A.

Willy Susilo, University of Wollongong, Australia

Tsuyoshi Takagi, Future University-Hakodate, Japan

Robert Tolksdorf, Freie Universität Berlin, Germany

Ambrosio Toval, University of Murcia, Spain

Wade Trappe, WINLAB, Rutgers University, U.S.A.

Wen-Guey Tzeng, National Chiao Tung University, Taiwan

Ulrich Ultes-Nitsche, University of Fribourg, Switzerland

Guillaume Urvoy-Keller, Institut Eurecom, France

Huaxiong Wang, Macquarie University, Australia

Yongge Wang, University of North Carolina, U.S.A.

Susanne Wetzel, Stevens Institute of Technology, U.S.A.

Duminda Wijesekera, George Mason University, U.S.A.

Chaoping Xing, National University of Singapore, Singapore

Shouhuai Xu, University of Texas at San Antonio, U.S.A.

Mariemma Yagüe, University of Malaga, Spain

Jeff Yan, University of Newcastle, U.K.

Alec Yasinsac, SAIT Laboratory, FSU, U.S.A.

Sung-Ming Yen, National Central University, Taiwan

Meng Yu, Monmouth University, U.S.A.

Moti Yung, RSA Labs and Columbia University, U.S.A.

Yuliang Zheng, UNC Charlotte, U.S.A.

André Zúquete, University of Aveiro, Portugal

AUXILIARY REVIEWERS

Jun Furukawa, NEC Corporation, Japan

Goichiro Hanaoka, Research Center for Information Security, AIST, Japan

Chien-Ning Chen, National Central University, Taiwan

Kuo-Zhe Chiou, National Central University, Taiwan

Chao-Chih Hsu, National Central University, Taiwan

Fu-Hau Hsu, National Central University, Taiwan

Hsi-Chung Lin, National Central University, Taiwan

Rachel Akimana, Universite Libre de Bruxelles, Belgium

Daniel J. Bernstein, University of Illinois at Chicago, U.S.A.

Marc Joye, Gemplus, Card Security Group, France

Claude Barral, Gemalto, France

Christophe Clavier, Gemalto, France

Damien Giry, UCL CryptoGroup, Belgium

Guerric Meurice de Dormale, UCL CryptoGroup, Belgium

Steve Kremer, LSV ENS Cachan, France

Ozgur Gurleyen, Vodafone, UK

Wolfgang Dobmeier, University of Regensburg, Germany

Rolf Schillinger, University of Regensburg, Germany

Christian Schläger, University of Regensburg, Germany

Francisco Javier Lucas Martínez, Universidad de Murcia, Spain

Fernando Molina Molina, Universidad de Murcia, Spain

Miguel Ángel Martínez Aguilar, Universidad de Murcia, Spain

Celalettin Emre Sayin, Sabanci University, Turkey

Abdulhakim Unlu, Sabanci University, Turkey

Fabien Laguillaumie, INRIA Futurs, France

Didier Alquie, CELAR, France

Johann Barbier, CELAR, France

Lutz Suhrbier, FU Berlin, Germany

Franck Landelle, CELAR, France

Xiaofeng Gong, University of Newcastle upon Tyne, U.K.

Toshihiro Tabata, Okayama University, Japan

Masakazu Soshi, JAIST, Japan

Takeshi Okamoto, Tsukuba University, Japan

Sotiris Ioannidis, Stevens Institute of Technology, U.S.A.

C. Lambrinoudakis, University of the Aegean, Greece

SELECTED PAPERS BOOK

A number of selected papers presented at SECRYPT 2006 will be published by Springer, in a book entitled e-Business and Telecommunication Networks. This selection will be done by the conference and program co-chairs, among the papers actually presented at the conference, based on a rigorous review by the SECRYPT 2006 program committee members.

FOREWORD

We warmly welcome you to SECRYPT 2006 - the *International Conference on Security and Cryptography*, which is held, this year, in Portugal. This conference reflects a continuing effort to increase the dissemination of recent research among professionals who work on the fields of security and cryptography, especially for telecommunications. SECRYPT is integrated as one of the modules of the ICETE joint conference.

The major goal of ICETE is to bring together researchers, engineers and practitioners interested in information and communication technologies, including e-business, wireless networks and information systems, security and cryptography, signal processing and multimedia applications. These are the main knowledge areas that define the four component conferences, namely: ICE-B, WINSYS, SECRYPT and SIGMAP, which together form the ICETE joint conference.

In the program for this joint conference, we have included keynote lectures, tutorials, papers, and posters to present the widest possible view on these technical areas. With these tracks, we expect to appeal to a global audience of engineers, scientists, business practitioners and policy experts, interested in the research topics of ICETE. All tracks focus on real world applications and rely on contributions from the industry, with different solutions for end-user applications and enabling technologies, in a diversity of communication environments. The proceedings demonstrate a number of new and innovative solutions for e-business and telecommunication, and demonstrate the vitality of these research areas.

We have received 326 papers in total, with contributions from 53 different countries, from all continents, which really shows the success and global dimension of ICETE 2006. To evaluate each submission, a double blind paper evaluation method was used: each paper was reviewed by at least two internationally known experts from our Program Committee, and more than 95% of the papers had 3 reviews or more. In the end, 98 papers were selected to be published and presented as full papers, 30' oral presentations, corresponding to a 30% full paper acceptance ratio; 105 additional papers were published and presented, including short papers and posters, corresponding to a 62% total acceptance ratio. Furthermore, a short list of about thirty top-quality papers will be selected to appear in a book that will be published by Springer.

We would like to emphasize the fact that ICETE 2006 includes one tutorial and seven outstanding keynote lectures in areas which are very relevant, nowadays. These talks are presented by distinguished researchers who are internationally recognized experts in all ICETE areas, and contribute to heighten the overall interest of the Conference.

ICETE 2006 is a joint conference that has achieved a high quality level, which we hope and strive not only to maintain but even increase in next year's conference, ICETE 2007, which is already planned to be held in Barcelona/Spain.

But life is more than technology, so a Conference Banquet was planned for the evening of August 9 (Wednesday) in order to facilitate social networking. We hope that you enjoy this exciting conference and we wish you an unforgettable stay in the beautiful city of Setúbal.

We would like to express our thanks, first of all, to the authors of the technical papers presented at the conference, whose work made possible to put together a high quality program. Next, we would like to thank all the members of the program committee and reviewers, who helped us with their expertise, dedication and time. We would also like to thank the invited speakers for their invaluable contribution, sharing their vision and knowledge. Naturally, a word of appreciation for the work of the secretariat and all other members of the organization, whose diligence in dealing with all organizational issues were essential and required a collaborative effort of a dedicated and highly capable team.

We hope that you will find these proceedings interesting and a helpful reference in the future for all those who need to address the areas of security and cryptography.

Manu Malek

Stevens Institute of Technology, U.S.A.

Eduardo Fernández-Medina

UCLM, Spain

Javier Hernando

Polytechnic University of Catalonia, Spain

Joaquim Filipe

Polytechnic Institute of Setúbal / INSTICC, Portugal

Mohammad Obaidat

Monmouth University, U.S.A.

CONTENTS

ACCESS CONTROL AND INTRUSION DETECTION

FULL PAPERS

SHORT PAPERS

POSTERS

NETWORK SECURITY AND PROTOCOLS

FULL PAPERS

SHORT PAPERS

POSTERS

CRYPTOGRAPHIC TECHNIQUES AND KEY MANAGEMENT

FULL PAPERS

SHORT PAPERS

POSTERS

INFORMATION ASSURANCE

FULL PAPERS

SHORT PAPERS

POSTERS

SECURITY IN INFORMATION SYSTEMS

FULL PAPERS

SHORT PAPERS

POSTERS

SECURE INFORMATION SYSTEMS DEVELOPMENT
Based on a Security Requirements Engineering Process

Daniel Mellado
Ministry of Labour and Social Affairs, Information Technology Center of the National Social Security Institute, Madrid, Spain
Daniel.Mellado@alu.uclm.es

Eduardo Fernández-Medina, Mario Piattini
Alarcos Research Group, Information Systems and Technologies Department, UCLM-Soluziona Research and Development Institute, University of Castilla-La Mancha
Paseo de la Universidad 4, 13071 Ciudad Real, Spain.
Eduardo.FdezMedina@uclm.es, Mario.Piattini@uclm.es

Keywords: Security Requirements, Security Requirements Engineering, Common Criteria.

Abstract: Integration of security into the early stages of the system development is necessary to build secure systems. However, in the majority of software projects security is dealt with when the system has already been designed and put into operation. This paper will propose an approach called SREP (Security Requirements Engineering Process) for the development of secure software. We will present an iterative and incremental micro-process for the security requirements analysis that is repeatedly performed at each phase. It integrates the Common Criteria into the software lifecycle model as well as it is based on the reuse of security requirements, by providing a security resources repository. In brief, we will present an approach which deals with the security requirements at the early stages of software development in a systematic and intuitive way, and which also conforms to ISO/IEC 17799:2005.

1 INTRODUCTION

In the last years we have observed more and more organizations becoming heavily dependent on Information Systems (IS). However, software applications are increasingly ubiquitous, heterogeneous, mission-critical and vulnerable to unintentional or intentional security incidents (CERT; Kemmerer 2003), so that it is absolutely vital that IS are properly ensured from the very beginning (Baskeville 1992; McDermott and Fox 1999), due to the potential losses faced by organizations that put their trust in all these IS.

A very important part in the software development process for the achievement of secure software systems is that known as Security Requirements Engineering. Which provides techniques, methods and norms for tackling this task in the IS development cycle. It should involve the use of repeatable and systematic procedures in an effort to ensure that the set of requirements obtained is complete, consistent and easy to understand and analyzable by the different actors involved in the development of the system (Kotonya and Sommerville 1998).

After having performed a comparative analysis of several relevant proposals of IS security requirements, as those of (Toval, Nicolás et al. 2001), (Popp, Jürjens et al. 2003), (Firesmith 2003), (Breu, Burger et al. 2004), etc., in (Mellado, Fernández-Medina et al. 2006), we concluded that those proposals did not reach the desired level of integration into the development of IS, nor are specific enough for a systematic and intuitive treatment of IS security requirements at the first stages of software development. Therefore, in this poster we will present the Security Requirements Engineering Process (SREP), which describes how to integrate security requirements into the software engineering process in a systematic and intuitive way. In order to achieve this goal, our approach is based on the integration of the Common Criteria (CC) into the software lifecycle model, because the CC helps us deal with the security requirements along all the IS development lifecycle, together with

the reuse of security requirements which are compatible with the CC Framework subset. In addition, in order to support this method and make it easy the treatment and specification of the security requirements, assets, security objectives and threats, we will propose the use of several concepts and techniques: a security resources repository (with assets, threats, requirements, etc), the use of UMLSec (Popp, Jürjens et al. 2003), misuse cases (Sindre, Firesmith et al. 2003), threat/attack trees, and security uses cases (Firesmith 2003). These latter techniques will be used following the criteria of effectiveness, and they allow us to integrate security aspects from the beginning into an IS development process, for example by expressing security-related information within the diagrams in a UML system specification, thanks to UMLSec.

The remainder of the paper is set out as follows: in section 2, we will outline an overview of our Security Requirements Engineering Process. Lastly, our conclusions and further research are set out in section 3.

2 A GENERAL OVERVIEW OF SREP

The Security Requirements Engineering Process (SREP) is an asset-based and risk-driven method for the establishment of security requirements in the development of secure Information Systems. Basically, this process describes how to integrate the CC into the software lifecycle model together with the use of a security resources repository to support reuse of security requirements (modelled with UMLSec, or expressed as security use cases or as plain text with formal specification), assets, threats (which can be expressed as misuse cases, threat/attack trees, UMLSec diagrams) and countermeasures. The focus of this methodology seeks to build security concepts at the early phases of the development lifecycle.

As it is described in Figure 1, the Unified Process (UP) (Booch, Rumbaugh et al. 1999) lifecycle is divided into a sequence of phases, and each phase may include many iterations. Each iteration is like a mini-project and it may contain all the core workflows (requirements, analysis, design, implementation, and test), but with different emphasis depending on where the iteration is in the lifecycle. Moreover, the core of SREP is a micro-process, made up of nine activities which are repeatedly performed at each iteration throughout the iterative and incremental development, but also with different emphasis depending on what phase of the lifecycle the iteration is in. Thus, the model chosen for SREP is iterative and incremental, and the security requirements evolve along the lifecycle. At the same time, the CC Components are introduced into the software lifecycle, so that SREP uses different CC Components according to the phase, although the Software Quality Assurance (SQA) activities are performed along all the phases of the software development lifecycle. And it is in these SQA activities where the CC Assurance Requirements might be incorporated into, according to (Kam 2005).

In addition, it facilitates the requirements reusability. 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 (Cybulsky and Reed 2000). Moreover, reusing security requirements helps us increase their quality: inconsistency, errors, ambiguity and other problems can be detected and corrected for an improved use in subsequent projects (Toval, Nicolás et al. 2001). Thereby, it will guarantee us the fastest possible development cycles based on proven solutions.

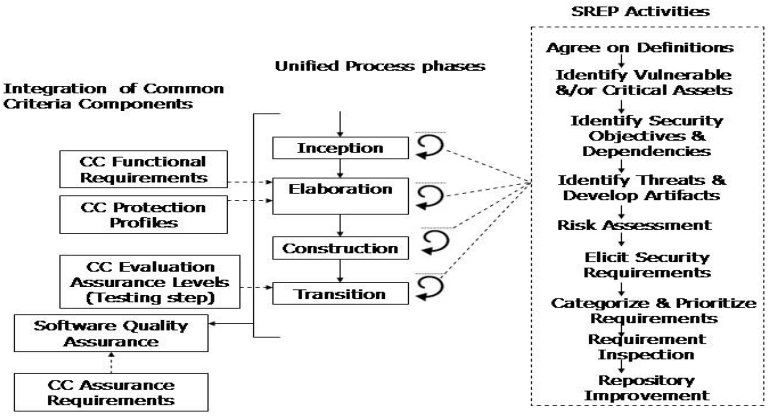

Figure 1: SREP overview.

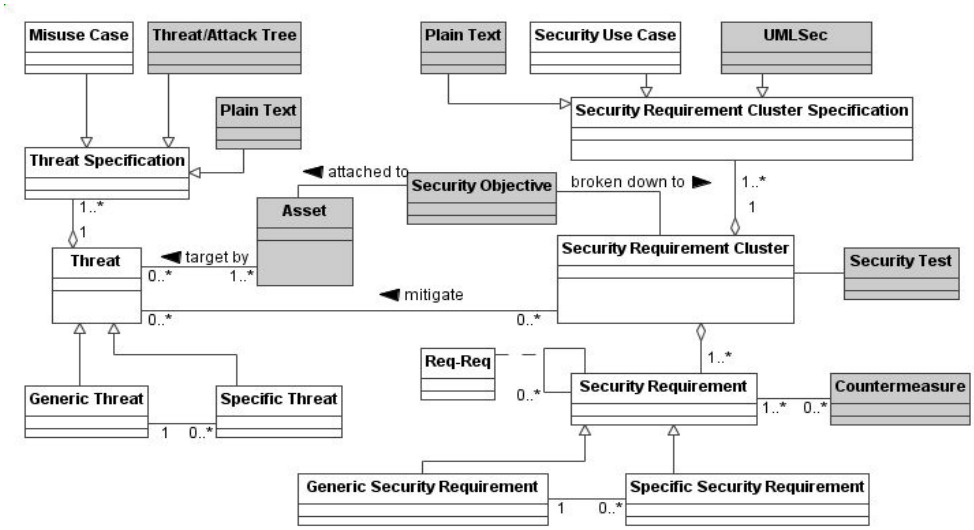

Figure 2: Meta-model for security resources repository.

2.1 The Security Resources Repository

We propose a *Security Resources Repository* (SRR), which stores all the reusable elements. The repository, as SIREN (Toval, Nicolás et al. 2001) approach, supports the concepts of domains and profiles. We propose to implement the domains and profiles by taking advantage of the CC concepts of packages and Protection Profiles (PP). Thus, the requirements are stored as standardized subsets of specific security requirements together with its related elements of the SRR (threats, etc.). In brief, each domain or profile is a view of the global SRR.

A meta-model, which is an extension of the meta-model for repository proposed by (Sindre, Firesmith et al. 2003), showing the organization of the SRR is exposed below in Fig. 2. The dark background in the objects represents our contribution to the meta-model.

Finally, according to ISO/IEC 17799:2005, we propose to include legal, statutory, regulatory, and contractual requirements that the organization, its trading partners, contractors, and service providers have to satisfy, and their socio-cultural environment. After converting these requirements into software and system requirements format, these requirements along with the CC security functional requirements would be the initial subset of security requirements of the SRR.

3 CONCLUSIONS

In our present so-called Information Society the Information Security is usually only tackled from a technical viewpoint at the implementation stage, even though it is an important aspect. We believe it is fundamental to deal with security at all stages of IS development, especially in the establishment of security requirements, since these form the basis for the achievement of a robust IS.

Consequently, we present an approach that deals with the security requirements at the first stages of software development in a systematic and intuitive way, which is based on the reuse of security requirements, by providing a Security Resources Repository (SRR), together with the integration of the Common Criteria into software lifecycle model. Moreover, it conforms to ISO/IEC 15408 and ISO/IEC 17799:2005. Starting from the concept of iterative software construction, we propose a micro-process for the security requirements analysis, made up of nine activities, which are repeatedly performed at each iteration throughout the iterative and incremental development, but with different emphasis depending on where the iteration is in the lifecycle. Finally, one of the most relevant aspects is the fact that this proposal integrates other approaches, such as UMLSec (Popp, Jürjens et al. 2003), security use cases (Firesmith 2003) or misuse cases (Sindre, Firesmith et al. 2003).

Further work is also needed to provide a CARE (Computer-Aided Requirements Engineering) tool which supports the process, as well as a refinement of the theoretical approach by proving it with a real

case study in order to complete and detail more SREP.

ACKNOWLEDGEMENTS

This paper has been produced in the context of the DIMENSIONS (PBC-05-012-2) Project of the Consejería de Ciencia y Tecnología de la Junta de Comunidades de Castilla- La Mancha along with FEDER and the CALIPO (TIC2003-07804-CO5-03) and RETISTIC (TIC2002-12487-E) projects of the Dirección General de Investigación del Ministerio de Ciencia y Tecnología.

REFERENCES

Baskeville, R. (1992). "The development duality of information systems security." *Journal of Management Systems* **4**(1): 1-12.

Booch, G., J. Rumbaugh and I. Jacobson (1999). *The Unified Software Development Process*, Addison-Wesley.

Breu, R., K. Burger, M. Hafner and G. Popp (2004). "Towards a Systematic Development of Secure Systems." *Proceedings WOSIS 2004*: 1-12.

CERT http://www.cert.org.

Cybulsky, J. and K. Reed (2000). "Requirements Classification and Reuse: Crossing Domains Boundaries." *ICSR'2000*: 190-210.

Firesmith, D. G. (2003). "Security Use Cases." *Journal of Object Technology*: 53-64.

Kam, S. H. (2005). "Integrating the Common Criteria Into the Software Engineering Lifecycle." *IDEAS'05*: 267-273.

Kemmerer, R. (2003). "Cybersecurity." *Proc. ICSE'03-25th Intl. Conf. on Software engineering*: 705-715.

Kotonya, G. and I. Sommerville (1998). *Requirements Engineering Process and Techniques*,

McDermott, J. and C. Fox (1999). Using Abuse Case Models for Security Requirements Analysis. *Annual Computer Security Applications Conference*, Phoenix, Arizona.

Mellado, D., E. Fernández-Medina and M. Piattini (2006). "A Comparative Study of Proposals for Establishing Security Requirements for the Development of Secure Information Systems." *The 2006 International Conference on Computational Science and its Applications (ICCSA 2006), Springer LNCS 3982* **3**: 1044-1053.

Popp, G., J. Jürjens, G. Wimmel and R. Breu (2003). Security-Critical System Development with Extended Use Cases. *10th Asia-Pacific Software Engineering Conference***:** 478-487.

Sindre, G., D. G. Firesmith and A. L. Opdahl (2003). A Reuse-Based Approach to Determining Security Requirements. *Proc. 9th International Workshop on Requirements Engineering: Foundation for Software Quality (REFSQ'03)*, Austria.

Toval, A., J. Nicolás, B. Moros and F. García (2001). Requirements Reuse for Improving Information Systems Security: A Practitioner's Approach. *Requirements Engineering Journal*. **6:** 205-219.