Lecture Notes in Computer Science

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

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

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

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

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

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

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

Proposals for publication should be sent to
LNCS Editorial, Tiergartenstr. 17, 69121 Heidelberg, Germany
E-mail: lncs@springer.com

ISSN 0302-9743

Lecture Notes in Computer Science
LNCS LNAI LNBI

springer.com

Gavrilova et al. (Eds.)

LNCS 3982

ICCSA 2006

Marina Gavrilova et al. (Eds.)

Computational Science and Its Applications – ICCSA 2006

International Conference
Glasgow, UK, May 2006
Proceedings, Part III

3 Part III

Springer

Lecture Notes in Computer Science 3982

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

Marina Gavrilova Osvaldo Gervasi
Vipin Kumar C.J. Kenneth Tan
David Taniar Antonio Laganà
Youngsong Mun Hyunseung Choo (Eds.)

Computational Science and Its Applications – ICCSA 2006

International Conference
Glasgow, UK, May 8-11, 2006
Proceedings, Part III

Springer

Volume Editors

Marina Gavrilova
University of Calgary, Canada
E-mail: marina@cpsc.ucalgary.ca

Osvaldo Gervasi
University of Perugia, Italy
E-mail: ogervasi@computer.org

Vipin Kumar
University of Minnesota, Minneapolis, USA
E-mail: kumar@cs.umn.edu

C.J. Kenneth Tan
OptimaNumerics Ltd., Belfast, UK
E-mail: cjtan@optimanumerics.com

David Taniar
Monash University, Clayton, Autralia
E-mail: david.taniar@infotech.monash.edu.au

Antonio Laganà
University of Perugia, Italy
E-mail: lag@unipg.it

Youngsong Mun
SoongSil University, Seoul, Korea
E-mail: mun@computing.soongsil.ac.kr

Hyunseung Choo
Sungkyunkwan University, Suwon, Korea
E-mail: choo@ece.skku.ac.kr

Library of Congress Control Number: 2006925086

CR Subject Classification (1998): F, D, G, H, I, J, C.2-3

LNCS Sublibrary: SL 1 – Theoretical Computer Science and General Issues

ISSN 0302-9743
ISBN-10 3-540-34075-0 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-34075-1 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11751595 06/3142 5 4 3 2 1 0

Preface

This five-volume set was compiled following the 2006 International Conference on Computational Science and its Applications, ICCSA 2006, held in Glasgow, UK, during May 8–11, 2006. It represents the outstanding collection of almost 664 refereed papers selected from over 2,450 submissions to ICCSA 2006.

Computational science has firmly established itself as a vital part of many scientific investigations, affecting researchers and practitioners in areas ranging from applications such as aerospace and automotive, to emerging technologies such as bioinformatics and nanotechnologies, to core disciplines such as mathematics, physics, and chemistry. Due to the shear size of many challenges in computational science, the use of supercomputing, parallel processing, and sophisticated algorithms is inevitable and becomes a part of fundamental theoretical research as well as endeavors in emerging fields. Together, these far-reaching scientific areas contributed to shaping this conference in the realms of state-of-the-art computational science research and applications, encompassing the facilitating theoretical foundations and the innovative applications of such results in other areas.

The topics of the refereed papers span all the traditional as well as emerging computational science realms, and are structured according to the five major conference themes:

- Computational Methods, Algorithms and Applications
- High-Performance Technical Computing and Networks
- Advanced and Emerging Applications
- Geometric Modeling, Graphics and Visualization
- Information Systems and Information Technologies

Moreover, submissions from 31 workshops and technical sessions in areas such as information security, mobile communication, grid computing, modeling, optimization, computational geometry, virtual reality, symbolic computations, molecular structures, Web systems and intelligence, spatial analysis, bioinformatics and geocomputations, are included in this publication. The continuous support of computational science researchers has helped ICCSA to become a firmly established forum in the area of scientific computing.

We recognize the contribution of the International Steering Committee and sincerely thank the International Program Committee for their tremendous support in putting this conference together, the near 800 referees for their diligent work, and the IEE European Chapter for their generous assistance in hosting the event.

We also thank our sponsors for their continuous support without which this conference would not be possible.

Finally, we thank all authors for their submissions and all invited speakers and conference attendants for making the ICCSA Conference truly one of the premium events on the scientific community scene, facilitating exchange of ideas, fostering new collaborations, and shaping the future of computational science.

May 2006

Marina L. Gavrilova
Osvaldo Gervasi

on behalf of the co-editors
Vipin Kumar
Chih Jeng Kenneth Tan
David Taniar
Antonio Laganà
Youngsong Mun
Hyunseung Choo

Organization

ICCSA 2006 was organized by the Institute of Electrical Engineers (IEE)(UK), the University of Perugia (Italy), Calgary University (Canada) and Minnesota University (USA).

Conference Chairs

Vipin Kumar (University of Minnesota, Minneapolis, USA), Honorary Chair
Marina L. Gavrilova (University of Calgary, Calgary, Canada), Conference Co-chair, Scientific
Osvaldo Gervasi (University of Perugia, Perugia, Italy), Conference Co-chair, Program

Steering Committee

Vipin Kumar (University of Minnesota, USA)
Marina L. Gavrilova (University of Calgary, Canada)
Osvaldo Gervasi (University of Perugia, Perugia, Italy)
C. J. Kenneth Tan (OptimaNumerics, UK)
Alexander V. Bogdanov (Institute for High Performance Computing and Data Bases, Russia)
Hyunseung Choo (Sungkyunkwan University, Korea)
Andres Iglesias (University of Cantabria, Spain)
Antonio Laganà (University of Perugia, Italy)
Heow-Pueh Lee (Institute of High Performance Computing, Singapore)
Youngsong Mun (Soongsil University, Korea)
David Taniar (Monash University, Australia)

Workshop Organizers

Applied Cryptography and Information Security (ACIS 2006)

Sherman S.M. Chow (New York University, USA)
Joseph K. Liu (University of Bristol, UK)
Patrick Tsang (Dartmouth College, USA)
Duncan S Wong (City University of Hong Kong, Hong Kong)

Approaches or Methods of Security Engineering (AMSE 2006)

Haeng Kon Kim (Catholic University of Daegu, Korea)
Tai-hoon Kim (Korea Information Security Agency, Korea)

Authentication, Authorization and Accounting (AAA 2006)
Haeng Kon Kim (Catholic University of Daegu, Korea)

Computational Geometry and Applications (CGA 2006)
Marina Gavrilova (University of Calgary, Calgary, Canada)

Data Storage Devices and Systems (DSDS 2006)
Yeonseung Ryu (Myongji University, Korea)
Junho Shim (Sookmyong Womens University, Korea)
Youjip Won (Hanyang University, Korea)
Yongik Eom (Seongkyunkwan University, Korea)

Embedded System for Ubiquitous Computing (ESUC 2006)
Tei-Wei Kuo (National Taiwan University, Taiwan)
Jiman Hong (Kwangwoon University, Korea)

4th Technical Session on Computer Graphics (TSCG 2006)
Andres Iglesias (University of Cantabria, Spain)
Deok-Soo Kim (Hanyang University, Korea)

GeoComputation (GC 2006)
Yong Xue (London Metropolitan University, UK)

Image Processing and Computer Vision (IPCV 2006)
Jiawan Zhang (Tianjin University, China)

Intelligent Services and the Synchronization in Mobile Multimedia Networks (ISS 2006)
Dong Chun Lee (Howon University, Korea)
Kuinam J Kim (Kyonggi University, Korea)

Integrated Analysis and Intelligent Design Technology (IAIDT 2006)
Jae-Woo Lee (Konkuk University, Korea)

Information Systems Information Technologies (ISIT 2006)
Youngsong Mun (Soongsil University, Korea)

Information Engineering and Applications in Ubiquitous Computing Environments (IEAUCE 2006)
Sangkyun Kim (Yonsei University, Korea)
Hong Joo Lee (Dankook University, Korea)

Internet Communications Security (WICS 2006)
Sierra-Camara Josè Maria (University Carlos III of Madrid, Spain)

Mobile Communications (MC 2006)
Hyunseung Choo (Sungkyunkwan University, Korea)

Modelling Complex Systems (MCS 2006)
John Burns (Dublin University, Ireland)
Ruili Wang (Massey University, New Zealand)

Modelling of Location Management in Mobile Information Systems (MLM 2006)
Dong Chun Lee (Howon University, Korea)

Numerical Integration and Applications (NIA 2006)
Elise de Doncker (Western Michigan University, USA)

Specific Aspects of Computational Physics and Wavelet Analysis for Modelling Suddenly-Emerging Phenomena in Nonlinear Physics, and Nonlinear Applied Mathematics (PULSES 2006)
Carlo Cattani (University of Salerno, Italy)
Cristian Toma (Titu Maiorescu University, Romania)

Structures and Molecular Processes (SMP 2006)
Antonio Laganà (University of Perugia, Perugia, Italy)

Optimization: Theories and Applications (OTA 2006)
Dong-Ho Lee (Hanyang University, Korea)
Deok-Soo Kim (Hanyang University, Korea)
Ertugrul Karsak (Galatasaray University, Turkey)

Parallel and Distributed Computing (PDC 2006)
Jiawan Zhang (Tianjin University, China)

Pattern Recognition and Ubiquitous Computing (PRUC 2006)
Jinok Kim (Daegu Haany University, Korea)

Security Issues on Grid/Distributed Computing Systems (SIGDCS 2006)
Tai-Hoon Kim (Korea Information Security Agency, Korea)

Technologies and Techniques for Distributed Data Mining (TTDDM 2006)
Mark Baker (Portsmouth University, UK)
Bob Nichol (Portsmouth University, UK)

Ubiquitous Web Systems and Intelligence (UWSI 2006)
David Taniar (Monash University, Australia)
Eric Pardede (La Trobe University, Australia)

Ubiquitous Application and Security Service (UASS 2006)
Yeong-Deok Kim (Woosong University, Korea)

Visual Computing and Multimedia (VCM 2006)
Abel J. P. Gomes (University Beira Interior, Portugal)

Virtual Reality in Scientific Applications and Learning (VRSAL 2006)
Osvaldo Gervasi (University of Perugia, Italy)
Antonio Riganelli (University of Perugia, Italy)

Web-Based Learning (WBL 2006)
Woochun Jun Seoul (National University of Education, Korea)

Program Committee

Jemal Abawajy (Deakin University, Australia)
Kenny Adamson (EZ-DSP, UK)
Srinivas Aluru (Iowa State University, USA)
Mir Atiqullah (Saint Louis University, USA)
Frank Baetke (Hewlett Packard, USA)
Mark Baker (Portsmouth University, UK)
Young-Cheol Bang (Korea Polytechnic University, Korea)
David Bell (Queen's University of Belfast, UK)
Stefania Bertazzon (University of Calgary, Canada)
Sergei Bespamyatnikh (Duke University, USA)
J. A. Rod Blais (University of Calgary, Canada)
Alexander V. Bogdanov (Institute for High Performance Computing and Data Bases, Russia)
Peter Brezany (University of Vienna, Austria)
Herve Bronnimann (Polytechnic University, NY, USA)
John Brooke (University of Manchester, UK)
Martin Buecker (Aachen University, Germany)
Rajkumar Buyya (University of Melbourne, Australia)
Jose Sierra-Camara (University Carlos III of Madrid, Spain)
Shyi-Ming Chen (National Taiwan University of Science and Technology, Taiwan)
YoungSik Choi (University of Missouri, USA)
Hyunseung Choo (Sungkyunkwan University, Korea)
Bastien Chopard (University of Geneva, Switzerland)
Min Young Chung (Sungkyunkwan University, Korea)
Yiannis Cotronis (University of Athens, Greece)
Danny Crookes (Queen's University of Belfast, UK)
Jose C. Cunha (New University of Lisbon, Portugal)
Brian J. d'Auriol (University of Texas at El Paso, USA)
Alexander Degtyarev (Institute for High Performance Computing and Data Bases, Russia)
Frederic Desprez (INRIA, France)
Tom Dhaene (University of Antwerp, Belgium)
Beniamino Di Martino (Second University of Naples, Italy)
Hassan Diab (American University of Beirut, Lebanon)
Ivan Dimov (Bulgarian Academy of Sciences, Bulgaria)
Iain Duff (Rutherford Appleton Laboratory, UK and CERFACS, France)
Thom Dunning (NCSA and University of Illinois, USA)
Fabrizio Gagliardi (Microsoft, USA)
Marina L. Gavrilova (University of Calgary, Canada)
Michael Gerndt (Technical University of Munich, Germany)
Osvaldo Gervasi (University of Perugia, Italy)
Bob Gingold (Australian National University, Australia)
James Glimm (SUNY Stony Brook, USA)

Christopher Gold (Hong Kong Polytechnic University, Hong Kong)
Yuriy Gorbachev (Institute of High Performance Computing and Information Systems, Russia)
Andrzej Goscinski (Deakin University, Australia)
Jin Hai (Huazhong University of Science and Technology, China)
Ladislav Hluchy (Slovak Academy of Science, Slovakia)
Xiaohua Hu (Drexel University, USA)
Eui-Nam John Huh (Seoul Women's University, Korea)
Shen Hong (Japan Advanced Institute of Science and Technology, Japan)
Paul Hovland (Argonne National Laboratory, USA)
Andres Iglesias (University of Cantabria, Spain)
Peter K. Jimack (University of Leeds, UK)
In-Jae Jeong (Hanyang University, Korea)
Chris Johnson (University of Utah, USA)
Benjoe A. Juliano (California State University at Chico, USA)
Peter Kacsuk (MTA SZTAKI Researc Institute, Hungary)
Kyung Wo Kang (KAIST, Korea)
Carl Kesselman (USC/ Information Sciences Institute, USA)
Daniel Kidger (Quadrics , UK)
Haeng Kon Kim (Catholic University of Daegu, Korea)
Jin Suk Kim (KAIST, Korea)
Tai-Hoon Kim (Korea Information Security Agency, Korea)
Yoonhee Kim (Syracuse University, USA)
Mike Kirby (University of Utah, USA)
Dieter Kranzlmueller (Johannes Kepler University Linz, Austria)
Deok-Soo Kim (Hanyang University, Korea)
Vipin Kumar (University of Minnesota, USA)
Domenico Laforenza (Italian National Research Council, Italy)
Antonio Laganà (University of Perugia, Italy)
Joseph Landman (Scalable Informatics LLC, USA)
Francis Lau (The University of Hong Kong, Hong Kong)
Bong Hwan Lee (Texas A&M University, USA)
Dong Chun Lee (Howon University, Korea)
Dong-Ho Lee (Institute of High Performance Computing, Singapore)
Sang Yoon Lee (Georgia Institute of Technology, USA)
Tae-Jin Lee (Sungkyunkwan University, Korea)
Bogdan Lesyng (ICM Warszawa, Poland)
Zhongze Li (Chinese Academy of Sciences, China)
Laurence Liew (Scalable Systems Pte, Singapore)
David Lombard (Intel Corporation, USA)
Emilio Luque (University Autonoma of Barcelona, Spain)
Michael Mascagni (Florida State University, USA)
Graham Megson (University of Reading, UK)
John G. Michopoulos (US Naval Research Laboratory, USA)
Edward Moreno (Euripides Foundation of Marilia, Brazil)

Youngsong Mun (Soongsil University, Korea)
Jiri Nedoma (Academy of Sciences of the Czech Republic, Czech Republic)
Genri Norman (Russian Academy of Sciences, Russia)
Stephan Olariu (Old Dominion University, USA)
Salvatore Orlando (University of Venice, Italy)
Robert Panoff (Shodor Education Foundation, USA)
Marcin Paprzycki (Oklahoma State University, USA)
Gyung-Leen Park (University of Texas, USA)
Ron Perrott (Queen's University of Belfast, UK)
Dimitri Plemenos (University of Limoges, France)
Richard Ramaroson (ONERA, France)
Rosemary Renaut (Arizona State University, USA)
Reneé S. Renner (California State University at Chico, USA)
Paul Roe (Queensland University of Technology, Australia)
Alexey S. Rodionov (Russian Academy of Sciences, Russia)
Heather J. Ruskin (Dublin City University, Ireland)
Ole Saastad (Scali, Norway)
Muhammad Sarfraz (King Fahd University of Petroleum and Minerals, Saudi Arabia)
Edward Seidel (Louisiana State University, USA and Albert-Einstein-Institut, Potsdam, Germany)
Jie Shen (University of Michigan, USA)
Dale Shires (US Army Research Laboratory, USA)
Vaclav Skala (University of West Bohemia, Czech Republic)
Burton Smith (Cray, USA)
Masha Sosonkina (Ames Laboratory, USA)
Alexei Sourin (Nanyang Technological University, Singapore)
Elena Stankova (Institute for High Performance Computing and Data Bases, Russia)
Gunther Stuer (University of Antwerp, Belgium)
Kokichi Sugihara (University of Tokyo, Japan)
Boleslaw Szymanski (Rensselaer Polytechnic Institute, USA)
Ryszard Tadeusiewicz (AGH University of Science and Technology, Poland)
C.J. Kenneth Tan (OptimaNumerics, UK and Queen's University of Belfast, UK)
David Taniar (Monash University, Australia)
John Taylor (Streamline Computing, UK)
Ruppa K. Thulasiram (University of Manitoba, Canada)
Pavel Tvrdik (Czech Technical University, Czech Republic)
Putchong Uthayopas (Kasetsart University, Thailand)
Mario Valle (Swiss National Supercomputing Centre, Switzerland)
Marco Vanneschi (University of Pisa, Italy)
Piero Giorgio Verdini (University of Pisa and Istituto Nazionale di Fisica Nucleare, Italy)
Jesus Vigo-Aguiar (University of Salamanca, Spain)

Jens Volkert (University of Linz, Austria)
Koichi Wada (University of Tsukuba, Japan)
Stephen Wismath (University of Lethbridge, Canada)
Kevin Wadleigh (Hewlett Packard, USA)
Jerzy Wasniewski (Technical University of Denmark, Denmark)
Paul Watson (University of Newcastle Upon Tyne, UK)
Jan Weglarz (Poznan University of Technology, Poland)
Tim Wilkens (Advanced Micro Devices, USA)
Roman Wyrzykowski (Technical University of Czestochowa, Poland)
Jinchao Xu (Pennsylvania State University, USA)
Chee Yap (New York University, USA)
Osman Yasar (SUNY at Brockport, USA)
George Yee (National Research Council and Carleton University, Canada)
Yong Xue (Chinese Academy of Sciences, China)
Igor Zacharov (SGI Europe, Switzerland)
Xiaodong Zhang (College of William and Mary, USA)
Aledander Zhmakin (SoftImpact, Russia)
Krzysztof Zielinski (ICS UST / CYFRONET, Poland)
Albert Zomaya (University of Sydney, Australia)

Sponsoring Organizations

Institute of Electrical Engineers (IEE), UK
University of Perugia, Italy
University of Calgary, Canada
University of Minnesota, USA
Queen's University of Belfast, UK
The European Research Consortium for Informatics and Mathematics (ERCIM)
The 6th European Framework Project "Distributed European Infrastructure for Supercomputing Applications" (DEISA)
OptimaNumerics, UK
INTEL
AMD

Table of Contents – Part III

Workshop on Approaches or Methods of Security Engineering (AMSE 2006, Sess. A)

General Tracks

A Comparative Study of Proposals for Establishing Security Requirements for the Development of Secure Information Systems

Daniel Mellado[1], Eduardo Fernández-Medina[2], and Mario Piattini[2]

[1] Ministry of Labour and Social Affairs, Management Organism of Information Technologies of the Social Security, Quality, Auditing and Security Institute, Madrid, Spain
Daniel.Mellado@alu.uclm.es
[2] 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, Mario.Piattini)@uclm.es

Abstract. Nowadays, security solutions are focused mainly on providing security defences, instead of solving one of the main reasons for security problems that refers to an appropriate Information Systems (IS) design. In this paper a comparative analysis of eight different relevant technical proposals, which place great importance on the establishing of security requirements in the development of IS, is carried out. And they provide some significant contributions in aspects related to security. These can serve as a basis for new methodologies or as extensions to existing ones. Nevertheless, they only satisfy partly the necessary criteria for the establishment of security requirements, with guarantees and integration in the development of IS. Thus we conclude that they are not specific enough for dealing with security requirements in the first stages of software development in a systematic and intuitive way, though parts of the proposals, if taken as complementary measures, can be used in that manner.

1 Introduction

Present-day information systems are vulnerable to a host of threats. What is more, with increasing complexity of applications and services, there is a correspondingly greater chance of suffering from breaches in security [25]. In our contemporary Information Society, depending as it does on a huge number of software systems which have a critical role, it is absolutely vital that IS are ensured as being safe right from the very beginning [2, 18]. That is so, is obvious from the potential losses faced by organizations that put their trust in all these IS.

As we know, the principle which establishes that the building of security into the early stages of the development process is cost-effective and also brings about more robust designs is widely-accepted [15]. The biggest problem, however, is that in the majority of software projects security is dealt with when the system has already been designed and put into operation. On many occasions, this is thanks to an inappropriate management of the specification of the security requirements of the new system, since the stage known as the requirement specification phase is often carried out with the

M. Gavrilova et al. (Eds.): ICCSA 2006, LNCS 3982, pp. 1044 – 1053, 2006.

aid of just a few descriptions, or the specification of objectives that are put down on a few sheets of paper. Added to this, the actual security requirements themselves are often not well understood. This being so, even when there is an attempt to define security requirements, many developers tend to describe design solutions in terms of protection mechanisms, instead of making declarative propositions regarding the level of protection required [8].

A very important part of the achieving of secure software systems in the software development process is that known as Security Requirements Engineering .This 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 [16]. A good requirement specification document should include both functional requirements (related to the services which the software or system should provide), and non-functional (related to what are known as features of quality, performance, portability, security, etc). As far as security is concerned, it should be a consideration throughout the whole development process, and it ought to be defined in conjunction with the requirements specification [19].

In this paper eight relevant technical proposals are studied. They are ones which place importance on eliciting security requirements in the development of IS. These proposals will be presented briefly and then compared in this paper. This should serve as an introduction to the current state of the art of security requirements in the development of IS. The remainder of the paper is set out as follows: in section 2, we will describe each one of the technical proposals. We will present the comparative study performed on these proposals in section 3. Lastly, our conclusions are set out in section 4.

2 Technical Proposals Which Support Security Requirements

The proposals which will be analyzed in this comparative study are as follows:

- Breu, et al. 2004 & Breu & Innerhofer–Oberperfler, 2005: "Towards a systematic development of secure systems" [5] and "Model based business driven IT security analysis" [6].
- Firesmith, 2003 & 2004: "Security Use Cases" [9] and "Security Requirements in Open Process Framework" [10].
- Jennex 2005: "Modeling security requirements for information system development" [13].
- Myagmar, Lee, & Yurcik, 2005: "Threat modeling as a basis for security requirements" [20].
- Toval et al. 2001: "Security requirements in SIREN" [24] and Gutiérrez, et al. 2005: "Security Requirements for Web Services based on SIREN" [11].
- Peeters 2005: "Agile security requirements engineering" [21].
- Popp et al. 2003: "Security-Critical system development with extended use cases" [22].
- Yu 1997: "Security requirements based on the i* framework" [26].

We have chosen these proposals because the majority of them try to solve the problem of security in the different phases of IS development. They also place an

emphasis on security requirements in the development of secure Information Systems. We give a brief outline of each of these approaches below.

2.1 Towards a Systematic Development of Secure Systems, and Model Based Business Driven IT Security Analysis (Proposed by Breu et al. 2004 [5] and Breu & Innerhofer–Oberperfler, 2005 [6])

The authors propose a new process model for security engineering, which extends object oriented, use case driven software development by the systematic treatment of security related issues. They also introduce the notion of security aspects, describing the most relevant security requirements and the countermeasures at a certain level of abstraction. Starting from the concept of iterative software construction, they present a micro-process for the security analysis, made up of five steps, which are performed repeatedly at each level of abstraction throughout the incremental development: elicitation of security requirements, threats and risks analysis, taking measures and the correctness check relating measures and requirements. Finally, the authors conclude that security of information is a business issue, and for this reason its management should be business driven.

2.2 Security Use Cases, and Security Requirements in Open Process Framework (Proposed by Firesmith, 2003 [9] & 2004 [10])

Firesmith in [10] offers some steps which allow security requirements to be defined from reusable templates. His analysis of security requirements is founded on two basic principles obtained from OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) [1] based on resources and risk-driven. The steps in his process for the identification and analysis of security requirements are: identification of assets; identifying the most likely attackers types; identification of the possible threats to these assets; determining the negative impacts for each vulnerable resource; estimating and prioritizing security risks with respect to vulnerable resources and according to the most relevant threats and their potentially negative impact; choosing security subfactors, to limit the risk to an acceptable level; choosing the relevant templates for each subfactor and security risk; identify the relevant functional requirements; determine the security criteria; define the security metric, along with the minimum level that is acceptable; specify the requirement.

Moreover, the author proposes security use cases as a technique that should be used to specify the security requirements that the application shall successfully protect itself from its relevant security threats [9].

The final suggestions from this author are that, given that systems usually have similar security requirements, templates should be employed to specify the security requirements in such a way that they can easily be re-used from one system to another.

2.3 Modeling Security Requirements for Information System Development (Proposed by Jennex, 2005) [13]

Jennex puts forward the idea of using barrier analysis and the concept of defence in-depth to modify Siponen and Baskervilles's integrated design paradigm [23] into a more graphical and easier to understand and use methodology.

The methodology suggested by the author, then, proposes using barrier analysis diagrams as a graphical method of identifying and documenting security requirements. Furthermore, this approach used meta-notation to add security details to existing system development diagrams. The process follows the approach of integrating security design into the software development life-cycle. The objective of using barrier diagrams in the requirement phase, therefore, is that the security requirements should be appropriately identified.

2.4 Threat Modeling as a Basis for Security Requirements (Proposed by Myagmar, Lee, & Yurcik, 2005) [20]

The authors take as starting point for their proposal the following question, one that is important to ask in every IS- "Are the system's security features really necessary, and do they really meet the system's security needs?

The writers offer a viewpoint on the process of requirement engineering in which, with an appropriate identification of threats and a proper choice of countermeasures, the ability of attackers to misuse or abuse the system is lessened.

The threat-modelling process set out by these authors is made up of three high-level steps: Characterizing the system; Identifying assets and access points; Identifying threats.

As far as the specification of security requirements is concerned, the greater part of the information needed for the elicitation of requirements and for composing an initial set of security requirements is provided by means of threat modelling. This is done by changing a declaration of threat into a requirement by including "must not" in the declaration.

Lastly, with the final goal being to achieve 100% risk acceptance, the risk management the writers propose consists of: risk assessment (to do this risks should be prioritized according to the damage they might cause and to the likelihood of their occurring), risk reduction, and risk acceptance.

2.5 Security Requirements in SIREN and Security Requirements for Web Services Based on SIREN (Proposed by Toval, et al. 2001 [24] and Gutierrez, et al. 2005 [11])

In [24] Toval et al. define a Requirement Engineering process, based on the re-use of security requirements, which is also compatible with MAGERIT (the Spanish public administration risk analysis and management method), which conforms to CCF (Common Criteria Framework) defined by the ISO 15408 (ISO/IEC, 1999). The re-use of security requirements is carried out at different specification level: at a documentation level through the defining of a hierarchical structure of security requirement specifications, and at the level of security requirement by means of its being stored in the repository of re-usable requirements. SIREN (SImple REuse of software requiremeNts) describes a process model, some basic guidelines, techniques and tools. The guidelines consist of a hierarchy of requirement specification documents, together with the template for each document. It is a spiral model process, and includes the phases of requirements elicitation, requirements analysis and negotiation, requirements specification and validation. A repository of requirements classified by domains and profiles is also defined.

Moreover, in [11] Gutiérrez et al. present a catalogue of security requirement templates for Web Services (WS) based on the SIREN method of requirement engineering. They focus their efforts on the security requirement templates for the following subfactors: authentification, authorization, confidentiality, integrity and privacy.

2.6 Agile Security Requirements Engineering (Proposed by Peeters, 2005) [21]

Peeters proposes to extend agile practices to deal with security in an informal, communicative and assurance-driven spirit. To increase the agility of requirement engineering, Peeters puts forward the idea of using "abuser stories". These identify how the attackers may abuse the system and jeopardize stakeholders' assets. Thus, throughout the abuser stories, the establishing of security requirements is made easier. As with "user stories", "abuser stories" are short and informal and they are scored and ranked according to the perceived threat they pose to customers' assets. Correct planning will consequently mean considering the "user stories" and the "abuser stories" together. This will ensure an explicit, rational trade-off between functionality and security.

2.7 Security-Critical System Development with Extended Use Cases (Proposed by Popp, et al. 2003) [22]

What these authors provide is an extension to the conventional process of developing use-case-oriented processes [7, 12]. This process normally consists of three activities as far as requirement engineering is concerned.

1. They deal with the static concepts of the domain of an application in a class model known as Application Core. In this point they extend the domain by modelling access policies and security properties based on UMLSec [14].
2. Identification of the use cases and their manifestation in a Use Case Model. These are completed by the textual description coming from characteristics which measure the threats and vulnerability of input and output. They also outline the security policies which are a response to previous threats. The outcome is a model known as Model of Security Use Cases.
3. Integration of the previous two viewpoints in a single oriented object model, mainly through the description of use cases in terms of message flows between objects. The extension consists of the integration of the Security Use Case Model, and the Application Core refines the security policy in terms of the message flows between objects.

2.8 Security Requirements Based on the i* Framework (Proposed by Yu, 1997) [26]

The *i** framework provides a framework which allows the easy integration of different techniques and concepts for dealing with Systems Security. The structural representation defined in *i** shows the dependence relationships between the actors, and is what makes security aspects appear.

In (Fig. 1. Requirement elicitation process with i*) we see the process of functional requirements elicitation and analysis defined by *i**, and how it is integrated into the process of elicitation and analysis of security requirements [17].

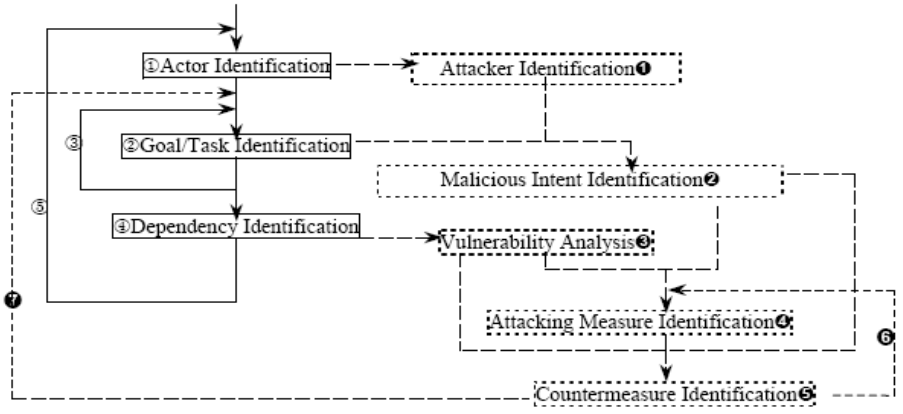

Fig. 1. Requirement elicitation process with i*

3 Comparison

To get a general overview of the different proposals which we have discussed above, a comparative study of these will be carried out in this section. To this end, we propose an analytical framework based on the following criteria:

- Degree of Agility. This refers to the degree of agility of the methodology of development, as compared with traditional, planned methodologies. To see this we will take as our basis the observations carried out Boehm and Turner [3, 4]. These authors propose a method based on risks, by means of which they try to keep both kinds of methodologies (those which are agile and those driven by planning- traditional ones) in balance, taking advantage of the positive points of the two types and taking steps to make up for their disadvantages. Each proposal will be given a rating using the following scale: high, medium-high, medium, medium-low, low.
- Support. This refers to aspects such as tools, procedures, guides, standards and study cases which help make the proposal easier to use. Each proposal will be given a rating using the following scale: high, medium-high, medium, medium-low, low.
- Degree of integration with other software requirements. This is all about how the establishing of security requirements fits in with the establishing of other software requirements (with the other non-functional requirements, as well as with the functional ones) in the development of an IS. To do this it will take into account aspects such as the use of similar and already-existing techniques for the determining of other requirements, such as, for instance, UML diagrams. It also bears in mind the degree of parallelization and co-ordination with the elicitation of other requirements, etc. Each proposal will be given a rating using the following scale: high, medium-high, medium, medium-low, low.

- User friendliness. Here the reference is to the ease with which the technique could be used without any previous knowledge or special training. In this case characteristics such as the help support and the use of techniques which already exist for other requirements will be taken into account, as well as widely-used standards, etc. Each proposal will be given a rating using the following scale: high, medium-high, medium, medium-low, low.
- Contributions of the proposal as regards security. New perspectives which the proposal brings to the improvement of the establishing of security requirements.

In the following table (Table 1. Comparison of proposals) the comparison between the proposals from different authors, within the analysis framework we propose, is set out.

Table 1. Comparison of proposals

Criteria / Proposals	Degree of Agility	Help Support	Degree of integration with other software requirements	User friendliness	Contributions of the proposal as regards security
Breu, et al. 2004 [5] and Breu & Innerhofer–Oberperfler, 2005 [6]	Low	Medium	Medium	Medium-High	▪ A micro-process for the security analysis
Firesmith, 2003 and 2004 [9, 10]	Medium	Medium-High	Medium	Medium-High	▪ Security use cases. ▪ Re-usable templates
Jennex, 2005[13]	High	Medium-Low	Medium-High	High	▪ Diagrams of barriers
Myagmar, Lee, & Yurcik 2005 [20]	Medium-Low	Medium	Medium	Medium-High	▪ Threat modeling as a basis for security requirements
Peeters, 2005[21]	High	Medium-Low	High	Medium-High	▪ Abuser stories
Popp, et al. 2003 [22]	Medium-Low	High	Medium-High	Medium-High	▪ UMLSec
Toval,, et al. 2001 [24] & Gutierrez, et al.2005 [11]	Low	Medium-High	Medium	Medium-High	▪ Re-use of security requirements compatible with MAGERIT ▪A catalogue of security requirements templates for WS
Yu, 1997 [26]	Low	Medium-Low	Medium-High	Medium-High	▪ Integration of functional and security requirements

As can be seen in the table, after our analysis we reach the conclusion that the proposals discussed above present some weaknesses. These include the difficulty of integrating them into the software development; the lack of an overall/complete support of security modelling at an organizational, conceptual and technical level. There is also an increasing distance between the development of the IS and the implementation of the necessary security. Moreover, these proposals are not specific enough for a systematic and intuitive treatment of IS security requirements in the first stages of software development. In short, the proposals we have analyzed partially satisfy the criteria that are necessary for the establishing of security requirements with some degree of guarantee. They do not reach the desired level of integration in the development of IS. At the same time, having said all that, each one of these methodologies contributes highly important aspects to do with security. These are features that can be used as the basis for new methodologies, or as extensions of those that already exist.

4 Conclusions

In our present so-called Information Society the increasingly crucial nature of IS with corresponding levels of new legal and governmental requirements is obvious. So the development of more and more sophisticated approaches to ensuring the security of information is becoming a necessity. 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 establishing of security requirements, since these form the basis for the achieving of a robust IS. Various interesting methodological proposals which have to do with this issue exist some of them have been described and compared in this paper, although they all present some weak points, as we have said above. In a similar vein, it must be said that these approaches are not specific enough for a treatment of IS security requirements in the first stages of the IS development process.

Consequently, we consider that it would be interesting to obtain some systematic and intuitive way of eliciting and defining security requirements with some guarantee. Such a technique should allow integration of security requirements into the IS development as far and as much as is possible. It will also permit the re-use of requirements from some projects to others. Added to these considerations is the fact that it will have to be valid for the new Internet-based IS and especially for those based on SOA architecture, supported by the technology of Web Services. To this end it would be good if it provided support tools. Positive it would also be if it were based on standards of normalization for the definition of requirements. Some examples of this might be XML or the use of templates; modeling standards like UML can be used to similar advantage. It would also be desirable for it to conform to security management standards such as ISO/IEC 17799 or COBIT.

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

1. Alberts, C.J., Behrens, S.G., Pethia, R.D., and Wilson, W.R., *OCTAVE Framework, Version 1.0*. 1999: Networked Systems Survivability Program. p. 84.
2. Baskeville, R., *The development duality of information systems security.* Journal of Management Systems, 1992. **4**(1): p. 1-12.
3. Boehm, B. and Turner, R., *Observations on Balancing Discipline and Agility*. 2003: Agile Development Conference (ADC '03). p. 32.
4. Boehm, B. and Turner, R., *Balancing Agility and Discipline: Evaluating and Integrating Agile and Plan-Driven Methods*. 2004: ICSE'04. p. 718-719.
5. Breu, R., Burger, K., Hafner, M., and Popp, G., *Towards a Systematic Development of Secure Systems*. 2004: WOSIS 2004.
6. Breu, R. and Innerhofer–Oberperfler, F., *Model based business driven IT security analysis*. 2005: SREIS 2005.
7. D'Souza, D.F. and Wills, A.C., *Objects, Components & Frameworks with UML: The Catalysis Approach*. 1998: Addison-Wesley Publishing Company.
8. Firesmith, D.G., *Engineering Security Requirements.* Journal of Object Technology, 2003. **2**(1): p. 53-68.
9. Firesmith, D.G., *Security Use Cases*. 2003: Journal of Object Technology. p. 53-64.
10. Firesmith, D.G., *Specifying Reusable Security Requirements*. 2004: Journal of Object Technology. p. 61-75.
11. Gutiérrez, C., Moros, B., Toval, A., Fernández-Medina, E., and Piattini, M., *Security Requirements for Web Services based on SIREN.* Symposium on Requirements Engineering for Information Security (SREIS-2005), together with the 13th IEEE International Requirements Engineering Conference – RE'05, 2005.
12. Jacobson, I., Booch, G., and Rumbaugh, J., *The Unified Software Development Process*. 1999: Addison-Wesley Longman Inc.
13. Jennex, M.E., *Modeling security requirements for information systems development*. 2005: SREIS 2005.
14. Jürjens, J., *Secure Systems Development with UML*. 2005: Springer. 309.
15. Kim., H.-K., *Automatic Translation Form Requirements Model into Use Cases Modeling on UML*, C. Youn-Ky, Editor. 2005: ICCSA 2005.
16. Kotonya, G. and Sommerville, I., *Requirements Engineering Process and Techniques*. 1998.
17. Liu, L., Yu, E., and Mylopoulus, J., *Security and Privacy Requirements Analysis within Social Setting*. 2003: 11th IEEE International Requirements Engineering Conference.
18. McDermott, J. and Fox, C. *Using Abuse Case Models for Security Requirements Analysis*. in *Annual Computer Security Applications Conference*. 1999. Phoenix, Arizona.
19. Mouratidis, H., Giorgini, P., Manson, G., and Philp, I. *A Natural Extension of Tropos Methodology for Modelling Security*. in *Workshop on Agent-oriented methodologies, at OOPSLA 2002*. 2003. Seattle, WA, USA.
20. Myagmar, S., J. Lee, A., and Yurcik, W., *Threat Modeling as a Basis for Security Requirements*. 2005: SREIS 2005.
21. Peeters, J., *Agile Security Requirements Engineering*. 2005: SREIS 2005.

22. Popp, G., Jürjens, J., Wimmel, G., and Breu, R., *Security-Critical System Development with Extended Use Cases*. 2003: 10th Asia-Pacific Software Engineering Conference. p. 478-487.
23. Siponen, M. and Baskerville, R., *A new paradigm for adding security into IS development methods,*. 2001: 8th Annual Working Conference on Information Security Management andSmall Systems Security.
24. Toval, A., Nicolás, J., Moros, B., and García, F., *Requirements Reuse for Improving Information Systems Security: A Practitioner's Approach*. 2001: Requirements Engineering Journal. p. 205-219.
25. Walton, J.P., *Developing a Enterprise Information Security Policy*. 2002, ACM Press: Proceedings of the 30th annual ACM SIGUCCS conference on User services.
26. Yu, E., *Towards Modelling and Reasoning Support for Early-Phase Requirements Engineering*. 1997: 3rd IEEE International Symposium on Requirements Engineering (RE'97). p. 226-235.