Lecture Notes in Computer Science 6426

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

Robert Meersman Tharam Dillon
Pilar Herrero (Eds.)

On the Move to Meaningful Internet Systems: OTM 2010

Confederated International Conferences:
CoopIS, IS, DOA and ODBASE
Hersonissos, Crete, Greece, October 25-29, 2010
Proceedings, Part I

Springer

Volume Editors

Robert Meersman
Vrije Universiteit Brussel (VUB), STAR Lab
Bldg G/10, Pleinlaan 2, 1050 Brussel, Belgium
E-mail: meersman@vub.ac.be

Tharam Dillon
Curtin University, Digital Ecosystems and Business Intelligence
Institute (DEBII), EU4, De Laeter Way, Bentley, 6102 Australia
E-mail: t.dillon@curtin.edu.au

Pilar Herrero
Universidad Politécnica de Madrid, Facultad de Informática
Campus de Montegancedo S/N
28660 Boadilla del Monte, Madrid, Spain
E-mail: pherrero@fi.upm.es

Library of Congress Control Number: 2010938246

CR Subject Classification (1998): C.2, D.2, H.4, I.2, H.3, K.6.5

LNCS Sublibrary: SL 3 – Information Systems and Application, incl. Internet/Web and HCI

ISSN 0302-9743
ISBN-10 3-642-16933-3 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-16933-5 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper 06/3180

General Co-chairs' Message for OnTheMove 2010

The OnTheMove 2010 event in Hersonissos, Crete, during October 24–29, further consolidated the growth of the conference series that was started in Irvine, California, in 2002, and held in Catania, Sicily, in 2003, in Cyprus in 2004 and 2005, in Montpellier in 2006, in Vilamoura in 2007 and 2009, and in Monterrey, Mexico, in 2008. The event continues to attract a diversified and representative selection of today's worldwide research on the scientific concepts underlying new computing paradigms, which, of necessity, must be distributed, heterogeneous and autonomous yet meaningfully collaborative. Indeed, as such large, complex and networked intelligent information systems become the focus and norm for computing, there continues to be an acute and ever increasing need to address and discuss face to face in an integrated forum the implied software, system and enterprise issues as well as methodological, semantic, theoretical and application issues. As we all realize, e-mail, the Internet and even video conferences are not by themselves sufficient for effective and efficient scientific exchange.

The OnTheMove (OTM) Federated Conferences series has been created to cover the scientific exchange needs of the community/ies that work in the broad yet closely connected fundamental technological spectrum of Web-based distributed computing. The OTM program every year covers data and Web semantics, distributed objects, Web services, databases, information systems, enterprise workflow and collaboration, ubiquity, interoperability, mobility, grid and high-performance computing.

OTM does not consider itself a so-called multi-conference but instead is proud to give meaning to the "federated" aspect in its full title: it aspires to be a primary scientific meeting place where all aspects of research and development of Internet- and intranet-based systems in organizations and for e-business are discussed in a scientifically motivated way, in a forum of (loosely) interconnected workshops and conferences. This ninth edition of the OTM Federated Conferences event therefore once more provided an opportunity for researchers and practitioners to understand and publish these developments within their individual as well as within their broader contexts. To further promote synergy and coherence, the main conferences of OTM 2010 were conceived against a background of three interlocking global themes, namely, "Cloud Computing Infrastructures," "The Internet of Things, or Cyberphysical Systems," "(Semantic) Web 2.0 and Social Computing for the Enterprise."

Originally the federative structure of OTM was formed by the co-location of three related, complementary and successful main conference series: DOA (Distributed Objects and Applications, since 1999), covering the relevant infrastructure-enabling technologies, ODBASE (Ontologies, DataBases and Applications of SEmantics, since 2002), covering Web semantics, XML databases

and ontologies, and CoopIS (Cooperative Information Systems, since 1993), covering the application of these technologies in an enterprise context through, for example, workflow systems and knowledge management. In 2007 the IS workshop (Information Security) was added to try cover also the specific issues of security in complex Internet-based information systems. Each of the main conferences specifically seeks high-quality contributions and encourages researchers to treat their respective topics within a framework that incorporates jointly (a) theory, (b) conceptual design and development, and (c) applications, in particular case studies and industrial solutions.

Following and expanding the model created in 2003, we again solicited and selected quality workshop proposals to complement the more "archival" nature of the main conferences with research results in a number of selected and more "avant-garde" areas related to the general topic of Web-based distributed computing. For instance, the so-called Semantic Web has given rise to several novel research areas combining linguistics, information systems technology and artificial intelligence, such as the modeling of (legal) regulatory systems and the ubiquitous nature of their usage. We were glad to see that seven of our successful earlier workshops (ADI, EI2N, SWWS, ORM, OnToContent, MONET, ISDE) re-appeared in 2010 with, in some cases, a fourth or even fifth edition, often in alliance with other older or newly emerging workshops, and that no fewer than four brand-new independent workshops could be selected from proposals and hosted: AVYTAT, DATAVIEW, P2PCDVE, SeDeS. Our OTM registration format ("one workshop buys all") actively intends to stimulate workshop audiences to productively mingle with each other and, optionally, with those of the main conferences.

We were also most happy to see that once more in 2010 the number of quality submissions for the OnTheMove Academy (OTMA, formerly called Doctoral Consortium Workshop), our "vision for the future" in research in the areas covered by OTM, took off again and with increasing success. We must thank the team of collaborators led by Peter Spyns and Anja Schanzenberger, and of course the OTMA Dean, Erich Neuhold, for their continued commitment and efforts in implementing our unique interactive formula to bring PhD students together. In OTMA, research proposals are submitted for evaluation; selected submissions and their approaches are (eventually) presented by the students in front of a wider audience at the conference, and are intended to be independently and are extensively analyzed and discussed in public by a panel of senior professors.

As said, all four main conferences and the associated workshops shared the distributed aspects of modern computing systems, and the resulting application pull created by the Internet and the so-called Semantic Web. For DOA 2010, the primary emphasis stayed on the distributed object infrastructure; for ODBASE 2010, it became the knowledge bases and methods required for enabling the use of formal semantics; for CoopIS 2010, the focus as usual was on the interaction of such technologies and methods with management issues, such as occur in networked organizations, and for IS 2010 the emphasis was on information security in the networked society. These subject areas overlap in a scientifically

natural fashion and many submissions in fact also treated an envisaged mutual impact among them. As for the earlier editions, the organizers wanted to stimulate this cross-pollination by a "shared" program of famous keynote speakers around the chosen themes: we were quite proud to announce Wil van der Aalst, T.U. Eindhoven, The Netherlands, Beng Chin Ooi, National University of Singapore, Michael Brodie, Chief Scientist, Verizon, USA, and Michael Sobolewski, Polish-Japanese Institute of IT, Poland.

We received a total of 223 submissions for the four main conferences and 127 submissions in total for the workshops. The numbers are about 5% lower than for 2009. Not only may we indeed again claim success in attracting an increasingly representative volume of scientific papers, many from the USA and Asia, but these numbers of course allow the Program Committees to compose a high-quality cross-section of current research in the areas covered by OTM. In fact, the Program Chairs of the CoopIS 2010 conferences decided to accept only approximately one paper from every five submissions, while ODBASE 2010 and DOA 2010 accepted about the same number of papers for presentation and publication as in 2008 and 2009 (i.e., average one paper out of three to four submitted, not counting posters). For the workshops and IS 2010 the acceptance rate varied but the aim was to stay consistently at about one accepted paper for two to three submitted, and subordinated of course to scientific quality assessment. As usual we have separated the proceedings into three volumes with their own titles, two for the main conferences and one for the workshops, and we are most grateful to the Springer LNCS team in Heidelberg for their professional suggestions and meticulous collaboration in producing the files for downloading on the USB sticks.

The reviewing process by the respective Program Committees was again performed very professionally, and each paper in the main conferences was reviewed by at least three referees, with arbitrated e-mail discussions in the case of strongly diverging evaluations. It may be worthwhile to emphasize that it is an explicit OTM policy that all conference Program Committees and Chairs make their selections completely autonomously from the OTM organization itself. Like last year, paper proceedings were on separate request and order this year, and incurred an extra charge.

The General Chairs are once more especially grateful to the many people directly or indirectly involved in the set-up of these federated conferences. Few people realize what a large number of individuals have to be involved, and what a huge amount of work, and in 2010 certainly also financial risk, the organization of an event like OTM entails. Apart from the persons in their roles mentioned above, we therefore wish to thank in particular our eight main conference PC Co-chairs: CoopIS 2010: Herve Panetto, Jorge Cardoso, M. Brian Blake; ODBASE 2010: Alejandro Buchmann, Panos Chrysanthis, York Sure; DOA 2010: Ernesto Damiani, Kai Hwang. And similarly the 2010 IS, OTMA and Workshops PC (Co-)chairs: Javier Cámara, Carlos E. Cuesta, Howard Foster, Miguel Angel Pérez-Toledano, Stefan Jablonski, Olivier Curé, David Thau, Sara Comai, Moira Norrie, Alessandro Bozzon, Giuseppe Berio, Qing Li, Kemafor Anyanwu,

Hervé Panetto (again), Alok Mishra, Jürgen Münch, Deepti Mishra, Patrizia Grifoni, Fernando Ferri, Irina Kondratova, Arianna D'Ulizia, Paolo Ceravolo, Majed Ayyad, Terry Halpin, Herman Balsters, Laura Ricci, Yan Tang, Jan Vanthienen, Yannis Charalabidis, Ernesto Damiani (again), Elizabeth Chang, Gritzalis Stefanos, Giles Hogben, Peter Spyns, Erich J. Neuhold and Anja Schanzenberger. Most of them, together with their many PC members, performed a superb and professional job in selecting the best papers from the harvest of submissions. We are all grateful to our supremely competent and experienced Conference Secretariat and technical support staff in Antwerp, Daniel Meersman, Ana-Cecilia, and Jan Demey, and last but certainly not least to our editorial team in Perth (DEBII-Curtin University) chaired by Houwayda El Fawal Mansour. The General Co-chairs acknowledge with gratitude the academic freedom, logistic support and facilities they enjoy from their respective institutions, Vrije Universiteit Brussel (VUB), Curtin University, Perth, Australia, and Universitad Politécnica de Madrid (UPM), without which such an enterprise would not be feasible. We do hope that the results of this federated scientific enterprise contribute to your research and your place in the scientific network... We look forward to seeing you again at next year's event!

August 2010

Robert Meersman
Tharam Dillon
Pilar Herrero

Organization

OTM (On The Move) is a federated event involving a series of major international conferences and workshops. These proceedings contain the papers presented at the OTM 2010 Federated conferences, consisting of four conferences, namely, CoopIS 2010 (Cooperative Information Systems), IS 2010 (Information Security), DOA 2010 (Distributed Objects and Applications) and ODBASE 2010 (Ontologies, Databases and Applications of Semantics).

Executive Commitee

General Co-chairs

Robert Meersman	VU Brussels, Belgium
Tharam Dillon	Curtin University of Technology, Australia
Pilar Herrero	Universidad Politécnica de Madrid, Spain

CoopIS 2010 PC Co-chairs

Hervé Panetto	Nancy University, France
Jorge Cardoso	Universidade de Coimbra, Portugal
Brian Blake	University of Notre Dame, USA

IS 2010 PC Co-chairs

Giles Hogben	European Network and Information Security Agency, Greece
Stefanos Gritzalis	University of the Aegean, Greece

DOA 2010 PC Co-chairs

Ernesto Damiani	Università degli Studi di Milano, Italy
Kai Hwang	University of Southern California, USA

ODBASE 2010 PC Co-chairs

Alejandro Buchmann	Technische Universität Darmstadt, Germany
Panos Chrysanthis	University of Pittsburgh, USA
York Sure	GESIS, Germany

Publication Chair

Houwayda Elfawal Mansour	DEBII, Australia

Publicity-Sponsorship Chair

Ana-Cecilia Martinez Barbosa	DOA Institute, Belgium

Logistics Team

Daniel Meersman	Head of Operations
Ana-Cecilia Martinez Barbosa	
Jan Demey	

CoopIS 2010 Program Committee

Marco Aiello
Antonia Albani
Antonio Ruiz Cortés
Kemafor Anyanwu
Joonsoo Bae
Zohra Bellahsene
Salima Benbernou
M. Brian Blake
Nacer Boudjlida
Christoph Bussler
James Caverlee
Francisco Curbera
Vincenzo D'Andrea
Xiaoyong Du
Schahram Dustdar
Johann Eder
Rik Eshuis
Opher Etzion
Renato Fileto
Ted Goranson
Paul Grefen
Michael Grossniklaus
Amarnath Gupta
Mohand-Said Hacid
Geert-Jan Houben
Zhixing Huang
Stefan Jablonski
Paul Johannesson
Epaminondas Kapetanios
Dimka Karastoyanova
Rania Khalaf
Hiroyuki Kitagawa
Akhil Kumar
Frank Leymann
ZongWei Luo
Sanjay K. Madria
Tiziana Margaria
Leo Mark
Maristella Matera
Massimo Mecella
Ingo Melzer
Jan Mendling
John Miller
Arturo Molina
Jörg Müller
Nirmal Mukhi
Miyuki Nakano
Moira C. Norrie
Werner Nutt
Andreas Oberweis
Gerald Oster
Jin Woo Park
Cesare Pautasso
Barbara Pernici
Li Qing
Lakshmish Ramaswamy
Manfred Reichert
Stefanie Rinderle-Ma
Duncan Ruiz
Paulo Rupino
Kai-Uwe Sattler
Ralf Schenkel
Jialie Shen
Aameek Singh
Michael W. Sobolewski
Xiaoping Sun
Susan Urban
Willem-Jan Van den Heuvel
Irene Vanderfeesten
François B. Vernadat
Maria Esther Vidal
Mathias Weske
Jian Yang
Aoying Zhou

IS 2010 Program Committee

Alessandro Acquisti
Vijay Atluri
Daniele Catteddu
Bruno Crispo
Gwenael Doerr
Josep Domingo Ferrer
Simone Fischer-Huebner
Clemente Galdi
Janusz Gorski
Jiankun Hu
Hai Jin
Maria Karyda
Stefan Katzenbeisser
Spyros Kokolakis
Wei-Shinn Ku
Evangelos Markatos
Sjouke Mauw
Chris Mitchell
Yi Mu
Nuno Ferreira Neves
Siani Pearson
Milan Petkovic
Andreas Pfitzmann
Frank Piessens
Norbert Pohlmann
Rodrigo Roman
Pierangela Samarati
Biplab K. Sarker
Aggeliki Tsochou
Luis Javier Garcia Villalba
Roman Yampolskiy
Alec Yasinsac
Andre Zuquete

DOA 2010 Program Committee

Subbu Allamaraju
Mark Baker
Boualem Benatallah
Elisa Bertino
Lionel Brunie
Athman Bouguettaya
Judith Bishop
Gordon Blair
Harold Carr
Geoffrey Coulson
Schahram Dustdar
Frank Eliassen
Pascal Felber
Benoit Garbinato
Niels Gruschka
Medhi Jazayeri
Eric Jul
Nick Kavantzas
Deyi Li
Ling Liu
Joe Loyall
Frank Manola
Gero Mühl
Nikola Milanovic
Graham Morgan
Lionel Ni
Rui Oliveira
Francois Pacull
Arno Puder
Michel Riveill
Luis Rodrigues
George Spanoudakis
Joerg Schwenk
Cyrus Shahabi
Azzel Taleb-Bendiab
Gaogang Xie
Kokou Yentongon
Albert Zomaya

ODBASE 2010 Program Committee

Karl Aberer
Harith Alani
María Auxilio Medina
Sonia Bergamaschi
Leopoldo Bertossi
Alex Borgida
Christof Bornhoevd
Mohand Boughanem
Paolo Bouquet
Silvana Castano
Tiziana Catarci
Paolo Ceravolo
Catherine Chronaki
Oscar Corcho
Ernesto Damiani
Irini Fundulaki
Aldo Gangemi
Benjamin Habegger
Mounira Harzallah
Manfred Hauswirth
Bin He
Prateek Jain
Vana Kalogeraki
Uladzimir Kharkevich
Manolis Koubarakis
Werner Kuhn
Maurizio Lenzerini
Li Ma
Vincenzo Maltese
Riichiro Mizoguchi
Peter Mork
Anne Ngu
Olga Papaemmanouil
Adrian Paschke
Ilia Petrov
Peter R. Pietzuch
Evaggelia Pitoura
Demetris Plexousakis
Wenny Rahayu
Rajugan Rajagopalapillai
Satya Sahoo
Pavel Shvaiko
Sergej Sizov
Veda C. Storey
Umberto Straccia
Heiner Stuckenschmidt
York Sure
Robert Tolksdorf
Susan Urban
Guido Vetere
Kevin Wilkinson
Baoshi Yan
Benjamin Zapilko
Demetris Zeinalipour

Supporting and Sponsoring Institutions

OTM 2010 was proudly supported or sponsored by Vrije Universiteit Brussel in Belgium, Curtin University of Technology in Australia, Universidad Politecnica de Madrid in Spain, Object Management Group, and Collibra.

Table of Contents – Part I

On the Move 2010 Keynotes

Cooperative Information Systems (CoopIS) International Conference 2010

Coopis Keynote Paper

Process Models and Management

Modeling of Cooperation

Services Computing

Information Processing and Management

Human-Based Cooperative Systems

Ontology and Workflow Challenges

International Symposium on Information Security (IS) International Conference 2010

Access Control, Authentication and Policies

Secure Architectures

Cryptography

Applicability of Security Patterns

Roberto Ortiz[1], Santiago Moral-García[2], Santiago Moral-Rubio[3], Belén Vela[2], Javier Garzás[2,4], and Eduardo Fernández-Medina[5]

[1] S21SecLabs-SOC. Group S21Sec Gestión S.A., Valgrande, 10, 28108, Madrid, Spain
r.ortizpl@gmail.com
[2] Kybele Group. Dep. of Computer Languages and Systems II, University Rey Juan Carlos, Tulipán, s/n, 28933, Madrid, Spain
{santiago.moral,belen.vela,javier.garzas}@urjc.es
[3] Dep. Logical Security, BBVA, Batanes 3, 28760, Madrid, Spain
santiago.moral@grupobbva.es
[4] Kybele Consulting, Oliva, Las Rozas, Madrid
javier.garzas@kybeleconsulting.com
[5] GSyA Research Group, Dep. of Information Technologies and Systems, University of Castilla-La Mancha, Paseo de la Universidad, 4, Ciudad Real, Spain
Eduardo.FdezMedina@uclm.es

Abstract. Information Security has become one of the fundamental mainstays in organizations owing to the ever-increasing cyber attacks against them in recent years. Both the designers of security mechanisms and the security engineers therefore need reliable security solutions to minimize the impact of the attacks on an organization's systems. Good mechanisms for solving these deficiencies are security patterns, which present a reliable and tested scheme to deal with recurring security problems. In this paper, we perform an analysis of some of the most important works that describe security patterns. Our main objective is to verify their applicability for the analysis and design of secure architectures in real and complex environments. Finally, and after presenting the detected shortcomings of the existing security patterns, we show which features should be incorporated into the patterns to be applicable in the field of information security engineering related to the development of secure architectures.

Keywords: Security patterns, information security engineering, real environments.

1 Introduction

Technological advances are currently improving many aspects related to the development and design of information systems, thus entailing an increase in the complexity of systems, which in turn augments the number of computer attacks, since attackers have more possibilities of finding new vulnerabilities in systems, such as susceptibility to Cross Site Scripting, injection flaws, malicious file execution, man-in-the-middle, etc. [1].

Information Security is therefore one of the main concerns that organizations have had to deal with in recent years. On the one hand, companies wish to prevent their

R. Meersman et al. (Eds.): OTM 2010, Part I, LNCS 6426, pp. 672–684, 2010.

information from becoming endangered, and on the other hand, there is a growing number of attacks as a result of the great benefits that attackers may obtain with the information plundered from organizations. All this signifies that information systems engineers must include security requirements in their systems, i.e., they must ensure the confidentiality, integrity and availability of data, besides auditing, privacy/anonymity, authentication/authorization, non-repudiation, usability, etc., while safeguarding the organization's information assets. The importance of system security is growing, since most attacks on software systems are based on vulnerabilities caused by software that has been poorly designed and developed [2]. That's the reason why information systems engineers need reliable solutions to problems related to security in order to be able to reduce the number of successful attacks against these systems.

Patterns are a good means of satisfying this need, since they describe a problem which occurs time and again in our environment, thus providing a trustworthy solution that can be used on multiple occasions [3]. One of the main advantages of patterns is that they combine experience and good practices in the development of models [4], thus increasing efficiency in the design of systems. Therefore, information security engineers can use security patterns to obtain reliable solutions related to this field, since patterns are a good mechanism through which to systematize the process of solving a recurring security problem. Another advantage of security patterns is that they include extensive accumulated and structured knowledge about security, thus providing guidelines for the construction and evaluation of secure systems [5]. The use of security patterns as a guide for developing a secure system is an extremely widespread practice [6, 7]. In fact, the number of published security patterns has increased considerably in recent years [8, 9, 10, 11, 12, 13, 14, 15], and there is a great heterogeneity between the descriptions of each of the proposals [16, 17, 18, 19, 20]. Different patterns have even been defined to provide an answer to the same set of security problems or requirements [21, 22]. For this reason, in some works [23, 5, 24], authors affirm that security patterns do not satisfy their needs when applying them to real problems, since it is more difficult to select the most suitable patterns with which to solve a specific problem from among the great variety of patterns that exist to solve the same problem.

Numerous patterns currently exist for the construction of security mechanisms. Security mechanisms are artifacts that are designed to detect problems, prevent risks or perform immediate corrections and avoid undesirable events that jeopardize security. Examples of such mechanisms are a secure access system [25] or a secure authentication system [10]. These types of patterns are very useful for the security engineers who perform this work. After these mechanisms have been created, they are used by organizations' security engineers to analyze and design the security architectures of real systems.

The main goal of this paper is, therefore, to verify whether the security patterns that have been proposed to build security mechanisms are applicable to the analysis and design of security architectures in real and complex information systems. We understand a real and complex environment or an information system to be all the elements involved in an organization, i.e., human resources, business processes, systems and technologies. Moreover, the concept of security architecture can be defined as the practice of applying a structured, coordinated, and rigorous method with the intention of discovering an organization's structure, bearing in mind human resources, business processes and technologies, i.e., all the elements that are involved in the organization to provide its systems with security and thus ensure the safety of its assets. Ensuring the safety of assets implies the necessity to establish a set of

technological infrastructure controls with which to identify the security mechanisms that are needed to define the system's security.

For this purpose, we have performed a systematic review [26] in the context of existing security patterns in the literature at an earlier date, up to March 2010, which is in period of validation for its publication. For this work, we have used digital libraries (Springer Link, Science@Direct, ACM digital library, IEEE digital library, etc.), book chapters and conferences (Pattern Languages of Programs (PLOP), Software Patterns and Quality (SPAQu), etc.) as sources. We will only focus on the works analyzed in this systematic review that describe security patterns, trying to cover the most important areas and aspects of information systems security. After synthesizing these works, a study on the applicability of the selected patterns will be carried out to find out to what extent these patterns can be applied to a particular environment, i.e., information security engineering that is focused on the analysis and design of security architectures.

The remainder of the paper is organized as follows: in Section 2, we shall present a synthesis of the analyzed proposals. In Section 3, we shall study the applicability of security patterns to specific environments, that is, in the field of information security engineering related to the development of security architectures. In section 4, we shall perform an analysis of the works that describe security patterns, presenting the results, and then discussing them. Finally, in Section 5 we shall set out our main conclusions and future work.

2 Synthesis of the Proposals

In this section, we shall sum up some of the proposals for the definition of new security patterns. In this set of works, extracted from a systematic review previously conducted in the field of security patterns, different means of creating security patterns are presented. Here, we have grouped these proposals according to the problem area for which they provide solutions: communications, privacy, access control, etc.

2.1 Description of Security Patterns for Secure Communications

This group includes those proposals related to security solutions for communication between several systems and for their sending and receiving of messages. Fernandez et al. [27] present four security patterns that could be used to design secure VoIP systems, describing mechanisms that can control many of the possible attacks. This approach also provides a framework for applying security. Chavhan and Chhabria [28] propose three design patterns for VoIP implementations related to specific security problems. The IPsec module for VoIP is deployed in the Client/Server environment. Fernandez and Ortega-Arjona [29] present the secure pipes and filters pattern, which is a secure version of the original pattern. The secure pipes and filters pattern may help us to add security controls during the processing stage, thus ensuring that only predefined operations are applied to data streams.

2.2 Description of Security Patterns for Secure Access Control and Identity

This group comprises the proposals regarding security patterns for building secure systems, focusing on building effective authorization, authentication and access control mechanisms. Delessy et al. [30] propose a pattern language for an identity

management system based on trust relationships between different security domains. Cuevas et al. [31] describe a solution that ensures end-to-end access control for data generated by wireless sensors. They use security patterns for the definition of an abstract model for encryption-based access control to sensor data. Fernandez et al. [32] propose a security pattern for use in distributed systems. This pattern describes the identification of information which provides authentication and access control elements. Fernandez et al. [33] also describe several patterns for showing the effect of sessions on an access control model.

2.3 Description of Security Patterns for Securing Privacy

This group includes the proposals related to those security patterns defined to solve problems related to privacy. They consider this concept to be highly relevant in the exchange of personal information between users and systems. These works show several security solutions that reinforce the security policies of web sites, e-mails, web applications, and other systems, to preserve the user's identity. Lobato et al. [34] present a set of patterns for the standardization of the development of privacy policies for use on websites. These patterns mostly consider aspects related to security, integrity, and privacy, since in order to access these sites users need to provide personal information and expect that these issues will be born in mind. Schumacher [16] shows two security patterns for protecting the identity of users when they access a website or wish to use a mail service without revealing their identity. Romanosky et al. [35] describe patterns for web-based activity. These new patterns may help those security engineers associated with the development of information systems to solve the problem of maintaining privacy.

2.4 Description of Attack/ Misuse Patterns

This group includes the proposals for describing a new concept of security patterns. Fernandez et al. denominate them as attack patterns or misuse patterns. In this kind of patterns, authors put themselves on the side of the attacker, and describe all the elements of the attack step by step. Then, they set out the security patterns which neutralize this attack, and provide a description of how to trace the attack once it has occurred. In [19] a misuse pattern is proposed. A model that characterizes the structure of this type of pattern is also presented. Similarly, in [36] an attack pattern which provides a specific description of the attack objectives and the steps that the attack follows as it proceeds is presented. In addition, an attack of Denial-of-Service on VoIP networks is presented to demonstrate the value of the pattern.

2.5 Description of Security Patterns to Build Trust Relationships

This group includes those proposals for security patterns which are used to secure the trust relationships between user and systems or between two users when attempting to enforce security requirements such as integrity, confidentiality, and availability. Fischer et al. [37] present a security pattern, denominated as the secure GUI system. This pattern may help us to ensure the security of graphical user interface systems and evaluate their use in different systems. Sorniotti et al. [38] describe an untraceable secret handshake, a protocol that allows two users to mutually verify the other's properties without disclosing their identity.

2.6 Other Description of Security Patterns to Build Secure Systems

This group includes the proposals for security patterns which are used to build secure systems using patterns from both architectural security and security design. Fernandez et al. [39] propose the Secure Three-Tier Architecture pattern, which extends the Three-Tier Architecture pattern. Its authors have reviewed this pattern in order to separate and analyze its security aspects. Fernandez et al. [40] also describe security patterns for the representation of processes and threads of Operating Systems. Spanoudakis et al. [41] introduce patterns with which to express basic Security Monitoring Properties that can be checked during runtime using a general runtime requirements monitoring framework.

An analysis of the applicability of security patterns to support analysis and design of secure architectures in real and complex environments will be shown in the following section.

3 Analysis of the Applicability of Security Patterns to the Development of Security Architectures

According to the pattern definitions [10], their contribution is to provide a proven and documented solution for similar context problems. In order to identify whether security patterns can be applied to the analysis and design of security architectures in real and complex environments, it is essential to find out whether the existing security patterns satisfy these requirements.

On the basis of certain security experts' experience in the field of security patterns [42, 25, 43], security patterns should serve to attain at least the following goals:

- Simplification of the analysis process for information security engineers who have to design the security of a new information system, in order to reduce the time needed to complete the analysis;
- Reliable identification of good and bad practices to reduce the time and cost required in security analysis; and finally;
- Provision of a uniform security guide to allow different information security engineers to develop equivalent solutions.

Similarly, in some cases, security patterns should not be implemented in the development of a secure system if their use would cause the situations stated below and, in addition, a negative report of the analysis of risks of the system opposite to business requirements has been obtained:

a. The impact that the deployment of the solution will have on the rest of the components in the system will cause a decrease in performance;
b. The business processes, the architecture, and the number of physical and logical elements of which the information system is composed are not compatible with security patterns;
c. They do not consider the complexity and difficulties that a security engineer may encounter when implementing the solution;

d. They do not consider the complexity of use that the solution will have for the final user;
e. They do not consider how the management and maintenance tasks are performed.

In the following section, the proposals synthesized in Section 2 will be analyzed in an effort to verify whether the security patterns currently available in the literature can be applied to the development of security architectures. The results of this analysis will then be presented and discussed. Finally, the features that should be incorporated into the security patterns to help security engineers to develop security architecture will be shown.

4 Results and Discussion

Having carried out the synthesis of the proposals that describe security patterns and after analyzing the applicability of security patterns to the development of security architectures, in this section we shall conduct an analysis to verify whether these proposed patterns are really useful for those security engineers who have to analyze or design secure architectures in the field of systems engineering. Once this has been completed, we shall present a discussion of the obtained results

In order to analyze the applicability of the security patterns defined in the proposals synthesized in section 2, we shall now present the features (*Considerations*) (partially based on the considerations exposed in [44, 45, 46], which should be incorporated into the security patterns template to achieve more usable, robust and complete patterns) that have been considered to carry out our applicability study of security patterns. These features are the considerations (following items) that a security engineer should take into account when applying a security pattern within a real and complex system, because they reflect questions related to parameters as important as cost, performance, usability and manageability.

- *Impact on the other components* of the system (Performance, Cost): it should be checked whether the deployment of the proposed solution is compatible with other components of the system.
- *Complexity in the deployment* of a security pattern (Performance, Cost): it should be checked whether the deployment of the solution has a complexity that the organization may assume.
- *Complexity of use* of a security pattern (Usability): it should be checked whether the use of the solution for final user is the desired one.
- *Complexity of the maintenance* of the solution (Manageability): it should be checked whether the maintenance of the solution may be realizable by security engineers of the organization.

When a security engineer has to design a secure architecture, it is virtually impossible that he has not considered some of the features listed previously. In the case of not analyzing these considerations, the deployment and maintenance cost of the solution may increase dramatically, causing, in this way, the failure of the solution.

We shall carry out an analysis in relation to the aforementioned features. For each of the patterns studied, we shall verify whether it completely satisfies the features

raised (F), whether it refers only briefly to these features (P) or whether it neither mentions nor considers them (N).

In Table 1, the vertical columns show the references for the analyzed proposals. These proposals are grouped into several contexts, according to the classification of the studied works of patterns carried out in Section 2. The horizontal rows show the features set out above. In Addition, Figure 1 shows a graphical representation of the analysis performed in Table 1. The following results are related to considerations that should be taken into account when applying security patterns:

Most proposals do not take the impact on the system's other components into account, because they do not consider aspects related to the system's performance after implementing the solution. One proposal makes a slight reference to this consideration [27], but it does not analyze it in depth, that is to say, it speaks about the possible impact on the systems involved, but it does not specify the possible impact on the system's components. Only one proposal fully considers this feature [31].

Table 1. Analysis of Results

		Considerations			
Context of patterns	References	Impact on the other components	Complexity in the deployment	Complexity of use	Complexity of the maintenance
Communications	[27]	P	N	P	P
	[28]	N	N	P	P
	[29]	N	N	P	N
Identity management	[30]	N	N	P	N
	[31]	F	N	N	F
	[32]	N	N	P	N
	[33]	N	N	P	P
Privacy	[34]	N	N	F	N
	[16]	N	N	F	N
	[35]	N	N	F	N
Attacker standpoint	[19]	N	N	N	N
	[36]	N	N	N	N
Trust relationships	[37]	N	N	P	P
	[38]	N	N	N	N
Others	[39]	N	N	P	N
	[40]	N	N	N	P
	[41]	N	N	N	N

None of the proposals consider the complexity that the deployment of the security patterns might entail for the engineers in charge of this work.

With regard to the considerations related to the complexity of security pattern usage, it is possible to observe that a significant amount of the proposals analyzed do not take this consideration into account [41, 31, 19]. A further significant amount of them only make a slight reference to this issue [39, 28, 37], that is to say, they briefly state that the application of the security patterns may have consequences for the people who use them, but they do not provide details on how this increases complexity. Only a few proposals take this consideration fully into account [16, 35, 34].

Finally, in relation to the considerations of complexity in the maintenance of the security pattern when it is applied, it is necessary to emphasize that most proposals ignore this consideration, for example [16, 35, 39, 19]. Some proposals state the need for maintenance of the solution but they do not explain the complexity that this task may imply for the engineers in charge [33, 40, 28]. Only one proposal [31] clearly states the consequences of security pattern implementation at the moment of carrying out maintenance tasks.

The following figure shows a graphical summary of these results.

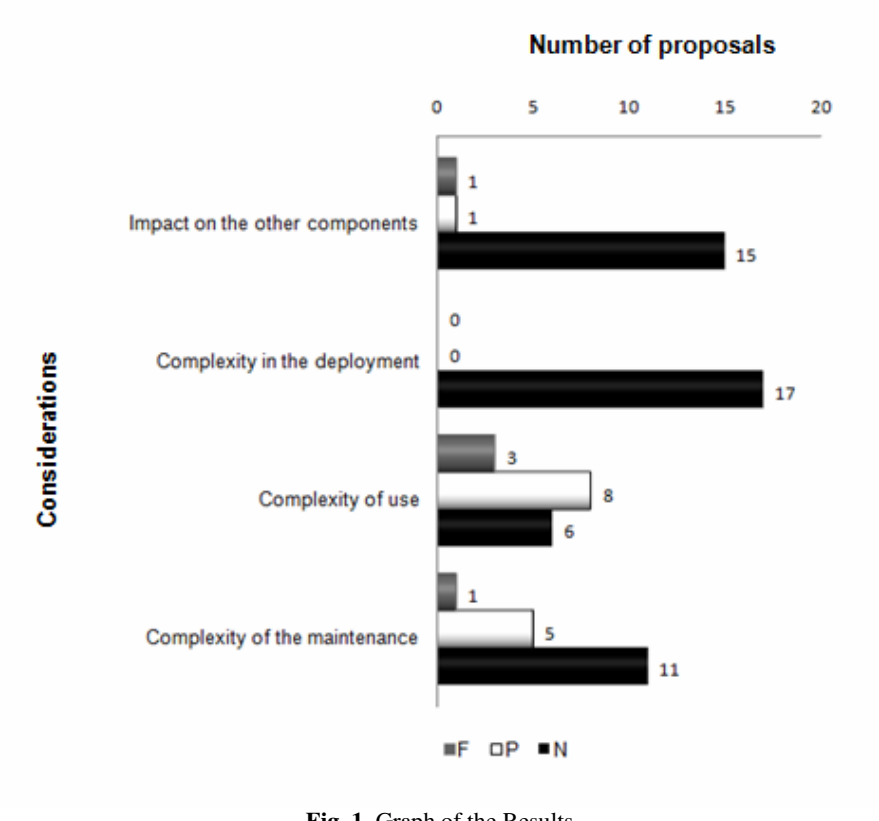

Fig. 1. Graph of the Results

As we have already stated, the main objective of this work is to verify whether the security patterns that exist in the literature can be used for the analysis and design of secure architectures in the field of security engineering in real and complex systems.

As it can be seen from the results, most of the currently described security patterns do not take into account the most important aspects related to the system into which they are introduced. Although these patterns, in their description, include a section called “uses known” which shows that they have been proven, it is not exposed in any section how to implement this solution methodologically within a real and complex system. This section is essential for the development of secure architectures in the field of security engineering, since it provides a clear vision of how to use patterns to add security to an organization's systems. In relation to this, after carrying out this analysis, we have detected a clear differentiation between two types of security patterns particularly concentrating on the security environment to which they can be applied. On the one hand, there are those security patterns which are orientated towards the development of security mechanisms [38]. On the other hand, we can find those security patterns which are orientated towards analyzing and designing secure architectures using the mechanisms previously developed [39]. Once this clear differentiation in the type of pattern had been detected, in this analysis we also detected that the majority of current security patterns are designed to support the development of security mechanisms, such as a secure access system [25] or a secure authentication system [10]. This type of security patterns may be very useful for those security engineers who work to develop this type of mechanisms for large companies (Oracle, Microsoft, IBM, Google, Cisco, etc.) and also for other small and medium enterprises, but they are not applicable to other security engineering sectors, which analyze and design secure architectures within the organizations in which they work. This is due to the fact that the security mechanisms which are incorporated into the architecture of real systems are developed by organizations that are specialized in the development of this kind of artifacts. These mechanisms are then purchased by other companies. For this reason, security patterns should be evolved in order to improve the deployment of these security mechanisms in organizations’ technological architectures.

In order to complete current security patterns and make them more applicable to security architectures design, this type of patterns should overcome a set of shortcomings which involve:

- Specifying in the solution how they should be integrated within a real and complex system.
- Detailing the impact that the implementation of the solution will have on the other components in the system.
- Detailing the business processes, the architecture and the number of physical and logical elements of which the information system is comprised.
- Considering the complexity and difficulties that a security engineer may encounter when deploying the solution.
- Considering the complexity of use that the solution will have for the final user.
- Considering how the management and maintenance tasks are performed.

If these shortcomings were to be included in security patterns, these patterns could be improved in order to facilitate the implementation of security mechanisms to support the analysis and design of security architectures in real and complex environments.

5 Conclusions and Future Work

In this work, an analysis has been carried out to verify the applicability of security patterns in the analysis and design of secure architectures in real complex systems. To do this, we have first synthesized a set of proposals that describe security patterns extracted from a systematic review that we performed previously. We have then analyzed their applicability in the field of information security engineering to develop secure architectures. A number of shortcomings in the description of current patterns have subsequently been observed. Finally, a discussion has been presented in which we have attempted to refine the current patterns so that they can be used by information security engineers to design security within real systems. The main shortcoming that we have found is that security patterns, presented as useful guidelines for information security engineers, do not currently satisfy the engineers' actual needs when creating secure architectures. We have detected that this is because most of these patterns do not reflect the potential impact of the deployment of the solution on the various components involved in a system; they do not consider the complexity of the implementation of the pattern for the engineers in charge of this task; they ignore the complexity of using the system when the patterns are applied; and, they do not consider the complexity of maintaining the solution, implemented in the form of a pattern, by the engineers in charge of security in the systems. Therefore, and after stating the detected shortcomings, we have shown the features that should be incorporated into security patterns to make them useful for the analysis and design of secure architectures in real and complex systems.

At present, we are working on the definition of security patterns to enable them to be used in the analysis and design of secure architectures in real environments. These security patterns will be based on real cases obtained from our own experience together with that of some security experts in the field of information security engineering. We are also working on the development of a methodology with which to solve security issues in the field of information security engineering, and we are additionally working on the development of a methodology to guide both experts and non-experts in the analysis and design of security architectures.

Acknowledgements

This research has been carried out within the framework of the following projects: MODEL-CAOS (TIN2008-03582/TIN), ESPIA (TIN2007-67078) financed by the Spanish Ministry of Education and Science, QUASIMODO (PAC08-0157-0668), SISTEMAS (PII2I09-0150-3135) and SEGMENT (HITO-09-138) financed by the "Viceconsejería de Ciencia y Tecnología de la Junta de Comunidades de Castilla-La Mancha" and the FEDER and BUSINESS (PET2008-0136) financed by the "Ministerio de Ciencia e Innovación (CDTI)" (Spain), and IDONEO (PAC08-0160-6141),

financed by the “Consejería de Ciencia y Tecnología de la Junta de Comunidades de Castilla-La Mancha”.

References

1. The Open Web Application Security Project, OWASP (2010), http://www.owasp.org
2. Halkidis, S.T., Tsantalis, N., Chatzigeorgiou, A., Stephanides, G.: Architectural Risk Analysis of Software Systems Based on Security Patterns. IEEE Transactions on Dependable and Secure Computing, 129–142 (2008)
3. Alexander, C., Ishikawa, S., Silverstein, M.: A Pattern Language: Towns, Buildings, Constructions. Oxford University Press, Oxford (1977)
4. Fernández, E.B.: Security patterns and secure systems design. In: ACM Southeast Regional Conference (2007)
5. Fernandez, E., Washizaki, H., Yoshioka, N., Kubo, A., Fukazawa, Y.: Classifying Security Patterns. In: Progress in WWW Research and Development, pp. 342–347 (2008)
6. Fernandez, E.B., Wu, J., Larrondo-Petrie, M.M., Shao, Y.: On building secure SCADA systems using security patterns. In: Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies, Oak Ridge, Tennessee (2009)
7. Maña, A., Serrano, D., Ruiz, J.F., Armenteros, A., Crespo, B.G.N., Muñoz, A.: Development of Applications Based on Security Patterns. In: Second International Conference on Dependability, DEPEND 2009, pp. 111–116 (2009)
8. Kienzle, D.M., Elder, M.C., Tyree, D., Edwards-Hewitt, J.: Security patterns repository, version 1.0 (2006)
9. Rosado, D.G., Gutiérrez, C., Fernández-Medina, E., Piattini, M.: Security patterns and requirements for internet-based applications. Internet Research: Electronic Networking Applications and Policy (2006)
10. Schumacher, M., Fernandez-Buglioni, E., Hybertson, D., Buschmann, F., Sommerlad, P.: Security Patterns: Integrating Security and Systems Engineering. Wiley, Chichester (2006)
11. Yskout, K., Heyman, T., Scandariato, R., Joosen, W.: An inventory of security patterns. Technical Report CW-469, Katholieke Universiteit Leuven, Department of Computer Science (2006)
12. Fernandez, E.B., Washizaki, H., Yoshioka, N.: Abstract security patterns. In: Proceedings of the 15th Conference on Pattern Languages of Programs, Nashville, Tennessee (2008)
13. Okubo, T., Tanaka, H.: Web security patterns for analysis and design. In: Proceedings of the 15th Conference on Pattern Languages of Programs, Nashville, Tennessee (2008)
14. Ortega-Arjona, J. L., Fernandez, E. B.: The secure blackboard pattern. In: Proceedings of the 15th Conference on Pattern Languages of Programs, Nashville, Tennessee (2008)
15. Serenity Project - System Engineering for Security & Dependability (2010), http://www.serenity-project.org
16. Schumacher, M.: B. Example Security Patterns and Annotations. In: Schumacher, M. (ed.) Security Engineering with Patterns. LNCS, vol. 2754, pp. 171–178. Springer, Heidelberg (2003)
17. Garzás, J., Piattini, M.: Object Oriented Microarchitectural Design Knowledge. IEEE Software, 28–33 (2005)

18. Anwar, Z., Yurcik, W., Johnson, R.E., Hafiz, M., Campbell, R.H.: Multiple design patterns for voice over IP (VoIP) security. In: 25th IEEE International Performance, Computing, and Communications Conference, IPCCC 2006 (2006)
19. Fernandez, E. B., Yoshioka, N., Washizaki, H.: Modeling Misuse Patterns. In International Conference on Availability, Reliability and Security, ARES 2009, pp. 566–571 (2009)
20. Moral-Garcia, S., Ortiz, R., Vela, B., Garzás, J., Fernández-Medina, E.: Patrones de Seguridad: ?'Homogéneos, validados y útiles. In: RECSI XI, Tarragona, Spain (submit accepted)
21. Fernandez, E.B., Pernul, G., Larrondo-Petrie, M.M.: Patterns and Pattern Diagrams for Access Control. In: Furnell, S.M., Katsikas, S.K., Lioy, A. (eds.) TrustBus 2008. LNCS, vol. 5185, pp. 38–47. Springer, Heidelberg (2008)
22. Sarmah, A., Hazarika, S.M., Sinha, S.K.: Security Pattern Lattice: A Formal Model to Organize Security Patterns. In: Bhowmick, S.S., Küng, J., Wagner, R. (eds.) DEXA 2008. LNCS, vol. 5181, pp. 292–296. Springer, Heidelberg (2008)
23. Heyman, T., Yskout, K., Scandariato, R., Joosen, W.: An Analysis of the Security Patterns Landscape. In: Proceedings of the Third International Workshop on Software Engineering for Secure Systems (2007)
24. Washizaki, H., Fernandez, E.B., Maruyama, K., Kubo, A., Yoshioka, N.: Improving the Classification of Security Patterns. In: 20th International Workshop on Database and Expert Systems Application, DEXA 2009, pp. 165–170 (2009)
25. Fernandez, E.: Security Patterns and Secure Systems Design. In: Dependable Computing, pp. 233–234 (2007)
26. Kitchenham, B.: Guideline for performing Systematic Literature Reviews in Software Engineering. Version 2.3. University of Keele (Software Engineering Group, School of Computer Science and Mathematics) and Durham (Department of Conputer Science) (2007)
27. Fernandez, E.B., Pelaez, J.C., Larrondo-Petrie, M.M.: Security Patterns for Voice over IP Networks. In: International Multi-Conference on Computing in the Global Information Technology, ICCGI 2007, pp. 33–33 (2007)
28. Chavhan, N.A., Chhabria, S.A.: Multiple design patterns for voice over IP security. In: Proceedings of the International Conference on Advances in Computing, Communication and Control, Mumbai, India (2009)
29. Fernandez, E.B., Ortega-Arjona, J.L.: The Secure Pipes and Filters Pattern. In: 20th International Workshop on Database and Expert Systems Application, DEXA 2009, pp. 181–185 (2009)
30. Delessy, N., Fernandez, E.B., Larrondo-Petrie, M.M.: A Pattern Language for Identity Management. In: International Multi-Conference on Computing in the Global Information Technology, ICCGI 2007, p. 31 (2007)
31. Cuevas, A., El Khoury, P., Gomez, L., Laube, A.: Security Patterns for Capturing Encryption-Based Access Control to Sensor Data. In: Second International Conference on Emerging Security Information, Systems and Technologies, SECURWARE 2008, pp. 62–67 (2008)
32. Morrison, P., Fernandez, E.B.: The credentials pattern. In: Proceedings of the 2006 conference on Pattern languages of programs, Portland, Oregon (2006)
33. Fernandez, E.B., Pernul, G.: Patterns for session-based access control. In: Proceedings of the 2006 conference on Pattern languages of programs, Portland, Oregon (2006)
34. Lobato, L.L., Fernandez, E.B., Zorzo, S.D.: Patterns to Support the Development of Privacy Policies. In: International Conference on Availability, Reliability and Security, ARES 2009, pp. 744–749 (2009)

35. Romanosky, S., Acquisti, A., Hong, J., Cranor, L.F., Friedman, B.: Privacy patterns for online interactions. In: Proceedings of the 2006 conference on Pattern languages of programs, Portland, Oregon (2006)
36. Fernandez, E., Pelaez, J., Larrondo-Petrie, M.: Attack Patterns: A New Forensic and Design Tool. In: Advances in Digital Forensics III, pp. 345–357 (2007)
37. Fischer, T., Sadeghi, A.R., Winandy, M.: A Pattern for Secure Graphical User Interface Systems. In: 20th International Workshop on Database and Expert Systems Application, DEXA 2009, pp. 186–190 (2009)
38. Sorniotti, A., El Khoury, P., Gomez, L., Cuevas, A., Laube, A.: A Security Pattern for Untraceable Secret Handshakes. In: SECURWARE 2009. Third International Conference on Emerging Security Information, Systems and Technologies, pp. 8–14 (2009)
39. Fernandez, E.B., Fonoage, M., VanHilst, M., Marta, M.: The Secure Three-Tier Architecture Pattern. In: International Conference on Complex, Intelligent and Software Intensive Systems, CISIS 2008, pp. 555–560 (2008)
40. Fernandez, E.B., Sorgente, T., Larrondo-Petrie, M.M.: Even more patterns for secure operating systems. In: Proceedings of the 2006 conference on Pattern languages of programs, Portland, Oregon (2006)
41. Spanoudakis, G., Kloukinas, C., Androutsopoulos, K.: Towards security monitoring patterns. In: Proceedings of the 2007 ACM symposium on Applied computing, Seoul, Korea (2007)
42. Schumacher, M.: Security Patterns - Security Patterns - Just another Way to Share Best Practices (2003), https://www.sdn.sap.com
43. Dougherty, C., Sayre, K., Seacord, R.C., Svoboda, D., Togashi, K.: Secure Design Patterns. Technical Report, CMU/SEI-2009-TR-010, ESC-TR-2009-010 (2009)
44. Kienzle, D.M., Elder, M.C., Tyree, D.S., Edwards-Hewitt, J.: Security patterns template and tutorial (2002)
45. The Open Group, Guide to Security Patterns - Arquitectural Patterns (2010), http://www.opengroup.org/architecture/togaf7-doc/arch/p4/patterns/patterns.htm
46. Moral-García, S., Ortiz, R., Moral-Rubio, S., Vela, B., Garzás, J., Fernández-Medina, E.: A New Pattern Template to Support the Design of Security Architectures. In: The Second International Conferences of Pervasive Patterns and Applications (submit-accepted, 2010)