Proceedings

DEXA

ARES 2006

The First International Conference on Availability, Reliability and Security

20th-22nd April 2006

Vienna University of Technology, Austria

In Cooperation with

enisa
European Network
and Information
Security Agency

TU WIEN

Technische
Universität
Wien

Vienna
University of
Technology

Oesterreichische
Computer Gesellschaft
Austrian
Computer Society

Published by the IEEE Computer Society
10662 Los Vaqueros Circle
P.O. Box 3014
Los Alamitos, CA 90720-1314

IEEE Computer Society Order Number P2567
Library of Congress Number Pending
ISBN 0-7695-2567-9

ISBN 0-7695-2567-9
90000
9 780769 525679

Proceedings

The First International Conference on Availability, Reliability and Security

ARES 2006

The papers in this book comprise the proceedings of the meeting mentioned on the cover and title page. They reflect the authors' opinions and, in the interests of timely dissemination, are published as presented and without change. Their inclusion in this publication does not necessarily constitute endorsement by the editors, the IEEE Computer Society, or the Institute of Electrical and Electronics Engineers, Inc.

IEEE Computer Society Order Number P2567
ISBN 0-7695-2567-9
ISBN 978-0-7695-2567-9
Library of Congress Number 2006923025

Additional copies may be ordered from:

IEEE Computer Society
Customer Service Center
10662 Los Vaqueros Circle
P.O. Box 3014
Los Alamitos, CA 90720-1314
Tel: + 1 800 272 6657
Fax: + 1 714 821 4641
http://computer.org/cspress
csbooks@computer.org

IEEE Service Center
445 Hoes Lane
P.O. Box 1331
Piscataway, NJ 08855-1331
Tel: + 1 732 981 0060
Fax: + 1 732 981 9667
http://shop.ieee.org/store/
customer-service@ieee.org

IEEE Computer Society
Asia/Pacific Office
Watanabe Bldg., 1-4-2
Minami-Aoyama
Minato-ku, Tokyo 107-0062
JAPAN
Tel: + 81 3 3408 3118
Fax: + 81 3 3408 3553
tokyo.ofc@computer.org

Individual paper REPRINTS may be ordered at: <reprints@computer.org>

Editorial production by Bob Werner
Cover art production by Joe Daigle/Studio Productions
Printed in the United States of America by The Printing House

IEEE
COMPUTER
SOCIETY

IEEE

IEEE Computer Society
Conference Publishing Services
http://www.computer.org/proceedings/

Table of Contents: ARES 2006

First International Conference on Availability, Reliability and Security

Message from the Organizing Committee xv

ARES and Workshops Committees xvi

Invited Talks

Risk Management and Risk Assessment at ENISA: Issues and Challenges 2
Louis Marinos

Model Driven Security 4
David Basin

Session 1: Trust Management

Trust Based Risk Management for Distributed System Security — A New Approach 6
Ching Lin and Vijay Varadharajan

RATING: Rigorous Assessment of Trust in Identity Management 14
Rajarajan Sampath and Deepak Goel

Provably Secure Anonymous Access Control for Heterogeneous Trusts 24
Kilho Shin and Hiroshi Yasuda

Session 2: P2P Systems

A Secure Event Agreement (SEA) Protocol for Peer-to-Peer Games 34
Amy Corman, Scott Douglas, Peter Schachte, and Vanessa Teague

Satisfiability and Trustworthiness of Peers in Peer-to-Peer Overlay Networks 42
Yoshio Nakajima, Kenichi Watanabe, Naohiro Hayashibara, Tomoya Enokido, Makoto Takizawa, and S. Misbah Deen

Tamper-resistant Replicated Peer-to-Peer Storage Using Hierarchical Signatures 50
Alexander Zangerl

Censorship-Resistant and Anonymous P2P Filesharing 58
Regine Endsuleit and Thilo Mie

Session 3: Mobile Network and Pervasive Systems

A Dependable Device Discovery Approach for Pervasive Computing Middleware 66
Sheikh Ahamed, Mohammad Zulkernine, and Suresh Anamanamuri

Single Sign-On Framework for AAA Operations within Commercial Mobile Networks 74
Saber Zrelli and Yoichi Shinoda

A Selector Method for Providing Mobile Location Estimation Services within a Radio Cellular Network 82
Junyang Zhou and Joseph Kee-Yin Ng

Guidelines for Biometric Recognition in Wireless System for Payment Confirmation 90
Leon Grabensek and Sasa Divjak

Session 4: Protocol and Communication

An Extended Verifiable Secret Redistribution Protocol for Archival Systems 100
V.H. Gupta and K. Gopinath

Analysis of Current VPN Technologies 108
Thomas Berger

Integration of Quantum Cryptography in 802.11 Networks 116
Thi Mai Trang Nguyen, Mohamed Ali Sfaxi, and Solange Ghernaouti-Hélie

Availability Constraints for Avionic Data Buses 124
Alban Gabillon and Laurent Gallon

Session 5: Security as Quality of Service

Securing DNS Services through System Self Cleansing and Hardware Enhancements 132
Yih Huang, David Arsenault, and Arun Sood

Personalized Security for E-Services 140
George Yee

Providing Security Services in a Multiprotocol Service Discovery System for Ubiquitous Networks 148
Juan Vera del Campo, Josep Pegueroles, and Miguel Soriano

Towards a Stochastic Model for Integrated Security and Dependability Evaluation 156
Karin Sallhammar, Bjarne Helvik, and Svein Knapskog

Session 6: Networking and Fault Tolerance

A Novel Artificial-Immune-Based Approach for System-Level Fault Diagnosis 166
Mourad Elhadef, Shantanu Das, and Amiya Nayak

Sandboxing in myKlaim 174
René Rydhof Hansen, Christian W. Probst, and Flemming Nielson

Evaluation of Network Robustness for Given Defense Resource Allocation Strategies 182
C.-H. Chen, Y.-L. Lin, Y.-S. Lin, P.-H. Tsang, and C.-L. Tseng

Proxy Oblivious Transfer Protocol 190
Yao Gang and Feng Dengguo

Session 7: Identification and Authentication

Providing Response Identity and Authentication in IP Telephony 198
Feng Cao and Cullen Jennings

Towards a Framework of Authentication and Authorization Patterns for Ensuring Availability in Service Composition 206
Judith E.Y. Rossebø and Rolv Bræk

An Optimal Round Two-Party Password-Authenticated Key Agreement Protocol ______ 216
Maurizio Adriano Strangio

A Method for the Identification of Inaccuracies in Pupil Segmentation ______ 224
Hugo Proença and Luís Alexandre

Availability Enforcement by Obligations and Aspects Identification ______ 229
Frédéric Cuppens, Nora Cuppens-Boulahia, and Tony Ramard

Session 8: High Availability and Dependability

An Integral IT Continuity Framework for Undisrupted Business Operations ______ 240
R.W. Helms, S. van Oorschot, J. Herweijer, and M. Plas

Highly Adaptable Dynamic Quorum Schemes for Managing Replicated Data ______ 245
Oliver Theel and Christian Storm

High Availability Support for the Design of Stateful Networking Equipments ______ 254
Pablo Neira Ayuso, Laurent Lefevre, and Rafael M. Gasca

A Hybrid Network Intrusion Detection Technique Using Random Forests ______ 262
Jiong Zhang and Mohammad Zulkernine

Identifying Intrusions in Computer Networks with Principal Component Analysis ______ 270
Wei Wang and Roberto Battiti

Session 9: Reliability and Availability

Systematic Error Detection for RFID Reliability ______ 280
Sozo Inoue, Daisuke Hagiwara, and Hiroto Yasuura

Feasibility of Multi-Protocol Attacks ______ 287
Cas Cremers

Diversity to Enhance Autonomic Computing Self-Protection ______ 295
Michael Jarrett and Rudolph Seviora

Reliability Forecasting in Complex Hardware/Software Systems ______ 300
Javier Cano and David Rios

Availability Modeling and Analysis on High Performance Cluster Computing Systems ______ 305
Hertong Song, Chokchai "Box" Leangsuksun Raja Nassar,
Narasimha Raju Gottumukkala, and Stephen Scott

Session 10: Security and Privacy Issue

Schedulability Driven Security Optimization in Real-time Systems ______ 314
Man Lin and Laurence Yang

Ensuring Privacy for E-Health Services ______ 321
George Yee, Larry Korba, and Ronggong Song

The Security Issue of Federated Data Warehouses in the Area of Evidence-Based Medicine ______ 329
Nevena Stolba, Marko Banek, and A Min Tjoa

Secrecy Forever? Analysis of Anonymity in Internet-Based Voting Protocols 340
Melanie Volkamer and Robert Krimmer

A Practical Framework for Dynamically Immunizing Software Security Vulnerabilities 348
Zhiqiang Lin, Bing Mao, and Li Xie

Session 11: Security Management

A Study of Security Architectural Patterns 358
David García Rosado, Carlos Gutiérrez, Eduardo Fernández-Medina, and Mario Piattini

Workshop-Based Multiobjective Security Safeguard Selection 366
Thomas Neubauer, Christian Stummer, and Edgar Weippl

Towards a Security Architecture for Vehicular Ad Hoc Networks 374
Klaus Plößl, Thomas Nowey, and Christian Mletzko

Improving Security Management through Passive Network Observation 382
Yohann Thomas, Hervé Debar, and Benjamin Morin

Digital Signatures for Modifiable Collections 390
Serge Abiteboul, Bogdan Cautis, Amos Fiat, and Tova Milo

Session 12: Distributed Systems

A System Architecture for Enhanced Availability of Tightly Coupled Distributed Systems 400
Johannes Osrael, Lorenz Froihofer, Karl M. Goeschka,
Stefan Beyer, Pablo Galdámez, and Francesc Muñoz

DeDiSys Lite: An Environment for Evaluating Replication Protocols in
Partitionable Distributed Object Systems 408
Stefan Beyer, Alexander Sánchez, Francesc Muñoz-Escoí, and Pablo Galdámez

Defense Trees for Economic Evaluation of Security Investments 416
Stefano Bistarelli, Fabio Fioravanti, and Pamela Peretti

Proposed Framework for Achieving Interoperable Services between European Public Administrations 424
Amir Hayat, Muhammad Alam, and Thomas Rössler

Gait Recognition Using Acceleration from MEMS 432
Davrondzhon Gafurov, Kirsi Helkala, and Torkjel Søndrol

Session 13: Software Security and Dependability

Making Web Services Dependable 440
Louise Moser, P. Michael Melliar-Smith, and Wenbing Zhao

A Simple Component Connection Approach for Fault Tree Conversion to Binary Decision Diagram 449
John Andrews and Rasa Remenyte

Secure Business Process Management: A Roadmap 457
Thomas Neubauer, Markus Klemen, and Stefan Biffl

Supporting Attribute-Based Access Control with Ontologies ____ 465
Torsten Priebe, Wolfgang Dobmeier, and Nora Kamprath

Diagnosis of Complex Systems Using Ant Colony Decision Petri Nets ____ 473
Calin Ciufudean, Adrian Graur, Constantin Filote, Cornel Turcu, and Valentin Popa

International Symposium on Frontiers in Availability, Reliability and Security (FARES)

Session 1: IP Network and Adhoc Network

A Lightweight Model of Trust Propagation in a Multi-Client Network Environement:
To What Extent does Experience Matter? ____ 482
Marc Conrad, Tim French, Wei Huang, and Carsten Maple

Secure 3G User Authentication in Adhoc Serving Networks ____ 488
Arjan Durresi, Lyn Evans, Vamsi Paruchuri, and Leonard Barolli

Security Analysis for IP-Based Government Emergency Telephony Service ____ 496
Feng Cao and Saadat Malik

Inter-Domains Security Management Model (IDSM) for IP Multimedia Subsystem (IMS) ____ 502
Muhammad Sher, Thomas Magedanz, and Walter T. Penzhorn

Privacy Threats and Issues in Mobile RFID ____ 510
Hyangjin Lee and Jeeyeon Kim

Session 2: Wireless and Sensor Network

A Framework of Survivability Model for Wireless Sensor Network ____ 515
Dong Seong Kim, Khaja Mohammad Shazzad, and Jong Sou Park

Mitigating Denial of Service Threats in GSM Networks ____ 523
Valer Bocan and Vladimir Creţu

Achieving Availability and Reliability in Wireless Sensor Networks Applications ____ 529
Amirhosein Taherkordi, Majid Alkaee Taleghan, and Mohsen Sharifi

Secure Enhanced Wireless Transfer Protocol ____ 536
Jin-Cherng Lin, Yu-Hsin Kao, and Chen-Wei Yang

Session 3: Authentication and Authorization

Quality of Password Management Policy ____ 544
Carlos Villarrubia, Eduardo Fernández-Medina, and Mario Piattini

A Proposal of an Anonymous Authentication Method for Flat-rate Service ____ 551
Yoshio Kakizaki, Hiroshi Yamamoto, and Hidekazu Tsuji

Recovery Mechanism of Online Certificate Chain in Grid Computing ____ 558
MingChu Li, Jianbo Ma, and Hongyan Yao

Session 4: Trust Management and Recovery

PKI Trust Relationships: From a Hybrid Architecture to a Hierarchical Model ____ 563
Cristina Satizábal, Rafael Páez, and Jordi Forné

Recovery Mechanism of Cooperative Process Chain in Grid ____ 571
MingChu Li and Hongyan Yao

Run Time Detection of Covert Channels ____ 577
Naoyuki Nagatou and Takuo Watanabe

Session 5: Secure Information System

Practical Approach of a Secure Management System Based on ISO/IEC 17799 ____ 585
Luís Enrique Sánchez, Daniel Villafranca, Eduardo Fernández-Medina, and Mario Piattini

Testing Complex Business Process Solutions ____ 593
Gerd Saurer, Josef Schiefer, and Alexander Schatten

Deontic Relevant Logic as the Logical Basis for Specifying, Verifying, and Reasoning about Information Security and Information Assurance ____ 601
Jingde Cheng and Junichi Miura

Resource Management *Continuity* with Constraint Inheritance Relation ____ 609
Zude Li, Guoqiang Zhan, and Xiaojun Ye

Session 6: Availability

On the Reliability of Web Clusters with Partial Replication of Contents ____ 617
Jose Daniel Garcia, Jesus Carretero, Felix Garcia,
Alejandro Calderon, Javier Fernandez, and David E. Singh

Reliability Modeling Strategy of an Industrial System ____ 625
Syed Rizwan and Ramachandran KP

Persistent Computing Systems as Continuously Available, Reliable, and Secure Systems ____ 631
Jingde Cheng

Active/Active Replication for Highly Available HPC System Services ____ 639
Christian Engelmann, Stephen L. Scott, Chokchai "Box" Leangsuksun, and Xubin (Ben) He

Session 7: Software Security 1

Towards an Integrated Conceptual Model of Security and Dependability ____ 646
Erland Jonsson

A Comparison of the Common Criteria with Proposals of Information Systems Security Requirements ____ 654
Daniel Mellado, Eduardo Fernández-Medina, and Mario Piattini

Secure and Reliable Java-Based Middleware — Challenges and Solutions ____ 662
Walter Binder

Session 8: Software Security 2

Security Requirement with a UML 2.0 Profile 670
Alfonso Rodriguez, Eduardo Fernández-Medina, and Mario Piattini

Representing Levels of Abstraction to Facilitate the Secure Multidimensional Modeling 678
Rodolfo Villarroel, Emilio Soler, Eduardo Fernández-Medina, Juan Trujillo, and Mario Piattini

Modeling Permissions in a (U/X)ML World 685
Muhammad Alam, Ruth Breu, and Michael Hafner

Session 9: Safety and Security

Application of the Digraph Method in System Fault Diagnostics 693
Emma Kelly and Lisa Bartlett

No Risk is Unsafe: Simulated Results on Dependability of Complementary Currencies 701
Kenji Saito, Eiichi Morino, and Jun Murai

Session 10: E-commerce and E-Government

A Reference Model for Authentication and Authorisation Infrastructures Respecting Privacy and Flexibility in b2c eCommerce 709
Christian Schläger, Thomas Nowey, and Jose A. Montenegro

Achieving Fairness and Timeliness in a Previous Electronic Contract Signing Protocol 717
Magdalena Payeras-Capellà, Josep Lluís Ferrer-Gomila, and Llorenç Huguet-Rotger

Digital Signatures with Familiar Appearance for e-Government Documents: *Authentic PDF* 723
Thomas Neubauer, Edgar Weippl, and Stefan Biffl

Workshop on Dependable and Sustainable Peer-to-Peer Systems (DAS-P2P 2006)

Session 1: Construction of Dependable Overlay Networks

Efficient Link Failure Detection and Localization using P2P-Overlay Networks 732
Barbara Emmert and Andreas Binzenhöfer

Replication Strategies for Reliable Decentralised Storage 740
Matthew Leslie, Jim Davies, and Todd Huffman

Session 2: Security

Multipath Key Exchange on P2P Networks 748
Yuuki Takano, Naoki Isozaki, and Yoichi Shinoda

Defending the Sybil Attack in P2P Networks: Taxonomy, Challenges, and a Proposal for Self-Registration 756
Jochen Dinger and Hannes Hartenstein

Session 3: Social Front

Fair Trading of Information: A Proposal for the Economics of Peer-to-Peer Systems 764
Kenji Saito, Eiichi Morino, and Jun Murai

Ecosystem of Naming Systems: Discussions on a Framework to Induce Smart Space Naming Systems Development 772
Yusuke Doi, Shirou Wakayama, Masahiro Ishiyama, Satoshi Ozaki, Tomohiro Ishihara, and Yojiro Uo

Deriving Ratings through Social Network Structures 779
Omer Rana, Hameeda Alshabib, and Ali ShaikhAli

Workshop on Bayesian Networks in Dependability (BND2006)

Bayesian Networks Implementation of the Dempster Shafer Theory to Model Reliability Uncertainty 788
Christophe Simon and Philippe Weber

Multi-Agent Causal Models for Dependability Analysis 794
Sam Maes and Philippe Leray

Computing Multiple Diagnoses in Large Devices Using Bayesian Networks 799
Véronique Delcroix, Mohamed-Amine Maalej, and Sylvain Piechowiak

Automatically Translating Dynamic Fault Trees into Dynamic Bayesian Networks by Means of a Software Tool 804
Stefania Montani, Luigi Portinale, Andrea Bobbio, and Daniele Codetta-Raiteri

Modelling the Reliability of Search and Rescue Operations within the UK through Bayesian Belief Networks 810
Ashley Russell, John Quigley, and Robert van der Meer

Modelling Dependable Systems Using Hybrid Bayesian Networks 817
Martin Neil, Manesh Tailor, David Marquez, Norman Fenton, and Peter Hearty

Workshop on Dependability in Large-scale Service-oriented Systems (DILSOS)

An Architecture for Service Discovery Based on Capability Matching 824
Jaka Močnik and Piotr Karwaczynski

A Declarative Control Language for Dependable XML Message Queues 832
Alexander Böhm, Carl-Christian Kanne, and Guido Moerkotte

Timed Modelling and Analysis in Web Service Compositions 840
Raman Kazhamiakin, Paritosh Pandya, and Marco Pistore

Web Service Discovery, Replication, and Synchronization in Ad-Hoc Networks 847
Lukasz Juszczyk, Jaroslaw Lazowski, and Schahram Dustdar

Evaluating Certification Protocols in the Partial Database State Machine 855
António Sousa, Alfrânio Correia Jr, Francisco Moura, José Pereira, and Rui Oliveira

Workshop: Security in E-Learning (SEL)

A Secure E-Exam Management System ____ 864
Jordi Castellà-Roca, Jordi Herrera-Joancomartí, and Aleix Dorca-Josa

Intra-Application Partitioning in an eLearning Environment — A Discussion of Critical Aspects ____ 872
Elke Franz and Katrin Borcea-Pfitzmann

Access Control in a Privacy-Aware eLearning Environment ____ 879
Elke Franz, Hagen Wahrig, Alexander Boettcher, and Katrin Borcea-Pfitzmann

Adding Security to a Multiagent Learning Platform ____ 887
Carine Webber, Maria de Fátima W. do Prado Lima, Marcos E. Casa, and Alexandre M. Ribeiro

Unlocking Repositories: Federated Security Solution for Attribute and
Policy Based Access to Repositories via Web Services ____ 895
Marek Hatala, Ty Mey (Timmy) Eap, and Ashok Shah

Workshop "Dependability Aspects on Data WArehousing and Mining Applications (DAWAM 2006)

Offline Internet Banking Fraud Detection ____ 904
Vasilis Aggelis

Practical Approaches for Analysis, Visualization and Destabilizing Terrorist Networks ____ 906
Nasrullah Memon and Henrik Legind Larsen

Representing Security and Audit Rules for Data Warehouses at
The Logical Level by Using the Common Warehouse Metamodel ____ 914
Emilio Soler, Juan Trujillo, Rodolfo Villaroel, Eduardo Fernández-Medina, and Mario Piattini

A 2^d-Tree-Based Blocking Method for Microaggregating Very Large Data Sets ____ 922
Agusti Solanas, Antoni Martínez-Ballesté, Josep Domingo-Ferrer, and Josep M. Mateo-Sanz

Using a Bayesian Averaging Model for Estimating the Reliability of Decisions in Multimodal Biometrics ____ 929
Vitaly Schetinin and Carsten Maple

On Efficiency and Data Privacy Level of Association Rules Mining Algorithms within
Parallel Spatial Data Warehouse ____ 936
Marcin Gorawski and Karol Stachurski

Depdendability in Data Mining: A Perspective from the Cost of Making Decisions ____ 944
H. Michael Chung

Workshop on Bioinformatics and Security (BIOS 06)

Grid Infrastructures for Secure Access to and Use of Bioinformatics Data:
Experiences from the BRIDGES Project ____ 950
Richard Sinnott, M. Bayer, A. Stell, and J. Koetsier

The Usability and Practicality of Biometric Authentication in the Workplace ____ 958
Carsten Maple and Peter Norrington

Building an Encrypted File System on the EGEE Grid: Application to Protein Sequence Analysis ____ 965
Christophe Blanchet, G. Deléage, and R. Mollon

Workshop: Information Security Risk Management (ISRM)

The Knowledge Pressure on Risk and Security Managers is Increasing ____ 974
Christer Magnusson, Heidi Olá, and Camilla Silversjö Holmqvist

Validation of IT-Security Measurement Tools ____ 980
Ruedi Baer and Martin Dietrich

Risk Management Approach on Identity Theft in Biometric Systems Context ____ 982
Sabine Delaitre

Workshop "Dependability and Security in e-Government" (DeSeGov 2006)

E-voting: Dependability Requirements and Design for Dependability ____ 988
Jeremy Bryans, Bev Littlewood, Peter Ryan, and Lorenzo Strigini

Defining Criteria for Rating an Entity's Trustworthiness Based on Its Certificate Policy ____ 996
Omar Batarfi and Lindsay Marshall

A Component Based Software Architecture for E-Government Applications ____ 1004
Raphael Kunis, Daniel Beer, and Gudula Rünger

Designing Mutual-aid Model for RAQ (Rarely Asked Question) in e-Government: Practical use of Anonymity ____ 1012
Akiko Orita

Maintaining Data-Integrity in the Back Office Registries of Cities; A Survey on Organizational Barriers and Ways to Address Those ____ 1017
Rob Peters, Marco Meesters, Pim Jörg, Edwin Stuart, and Marcel Hoogwout

Choosing the Right Wireless LAN Security Protocol for the Home and Business User ____ 1025
Carsten Maple, Helen Jacobs, and Matthew Reeve

An Ontology for Secure e-Government Applications ____ 1033
M. Karyda, T. Balopoulos, S. Dritsas, L. Gymnopoulos, S. Kokolakis, C. Lambrinoudakis, and S. Gritzalis

Building Governments in e-Government: Settlement of Trusted e-Oligarchy ____ 1038
Semir Daskapan

Author Index ____ 1045

Message from the Organizing Committee

The idea for this conference came from the colleagues of the various ARES 2006 committees; our goal being to build a bridge amongst the various aspects of system dependability as an integrated concept.

The idea to launch the conference in Austria in the first half of the year 2006 has also to do with Austria's Presidency of the European Union from January to June 2006.

The European Union and the Austrian Governmental Bodies are very keen to bridge the gap between the scientific work and applications in this area — especially in the areas of e-Government.

We are very pleased therefore to have this conference organised in cooperation with ENISA (The European Network and Information Security Agency). ENISA supports the idea of this conference due to the urgent need of research and dissemination of new techniques in this key area.

We hope that the conference will have a real benefit for innovative applications which have to consider the various dependability issues, and furthermore will build a platform for in-depth discussions between researchers in the different areas of Dependability such as Availability, Reliability, and Security.

We received 159 papers from 35 countries for ARES and the Program Committee eventually selected 58 papers, making an acceptance rate of 36.47 percent of submitted papers.

Eight workshops are organised on special topics of ARES, i.e.:

- Workshop on Dependable and Sustainable Peer-to-Peer Systems (DAS-P2P 2006)
- Workshop on Bayesian Networks in Dependability (BND2006)
- Workshop on Dependability in Large-scale Service-oriented Systems (DILSOS)
- Workshop: Security in E-Learning (SEL)
- Workshop "Dependability Aspects on Data WArehousing and Mining Applications" (DAWAM 2006)
- Workshop on Bioinformatics and Security (BIOS 06)
- Workshop: Information Security Risk Management (ISRM)
- Workshop "Dependability and Security in e-Government" (DeSeGov 2006)

As an additional feature of ARES we have invited distinguished scientists for the International Symposium on Frontiers in Availability, Reliability and Security (FARES) to present and discuss special aspects relevant for future applications and research.

We would like to express our gratitude to all program committee members, workshop organisers and committee members and all the external referees who reviewed the papers very thoroughly and in a timely manner.

Due to the high number of submissions and the quality of the submitted papers, the reviewing, and discussion process was an extraordinarily challenging task. In total they have dealt with 232 papers.

Special thanks must be given to Mr. Tho Manh Nguyen for all his support in the organization of the PC-tasks of ARES 2006 and workshop coordination. We would also like to thank all the authors who submitted their papers to ARES 2006.

Finally many thanks to Ms. Christine Tronigger for providing a great deal of support in administering the registrations.

Prof. Norman Revell, Prof. Roland Wagner (Honorary Co-chairs)
Prof. Günther Pernul, Prof. Makoto Takizawa (General Co-chairs)
Prof. Gerald Quirchmayr, Prof. A Min Tjoa (Program Co.-chairs)

ARES and Workshops Committees

Honorary Co-Chairs
Norman Revell, Middlesex University, United Kingdom
Roland Wagner, University of Linz, Austria

General Co-Chairs
Guenther Pernul, University of Regensburg, Germany
Makoto Takizawa, Tokyo Denki University, Japan

Program Co-Chairs
Gerald Quirchmayr, University of Southern Australia, Australia
A Min Tjoa, Vienna University of Technology, Austria

Workshops Co-Chairs
Nguyen Manh Tho, Vienna University of Technology, Austria
Abdelkader Hameurlain, University of Toulouse, France
Leonard Barolli, Fukuoka Institute of Technology (FIT), Japan

International Liaison Chair
Maria Wimmer, University of Koblenz-Landau, Germany
Charles Shoniregun, University of East London, United Kingdom

Publicity Chair
Vladimir Marik, Czech Technical University, Czech Republic

Publication Chair
Monika Lanzenberger, Norwegian University of Science and Technology, Trondheim, Norway

Local Organizing Co-Chairs
Maria Schweikert, Vienna University of Technology, Austria
Markus Klemen, Vienna University of Technology, Austria

Program Committee

Jemal Abawajy, Deakin University, Australia
Abiola Abimbola, Napier University, UK
Rafael Accorsi, University of Freiburg, Germany
Alessandro Acquisti, Carnegie Mellon University, USA
John Andrews, Loughborough, University, UK
Lisa Bartlett, Loughborough University, UK
Elisa Bertino, Purdue University, USA
Bharat Bhargava, Purdue University, USA
Stefan Biffl, Vienna University of Technology, Austria
Michael Burmester, Florida State University, USA
Jiannong Cao, Hong Kong Polytechnic University, Hongkong, China
Jordi Castellà-Roca, Rovira i Virgili University of Tarragona
Anirban Chakrabarti, Infosys Technologies, India
Guihai Chen, Nanjing University, China
John A. Clark, University of York, UK
George Davida, University of Wisconsinat Milwaukee, USA
Pierpaolo Degano, Università diPisa, Italia
Robert Deng, Singapore Management University, Singapore
Yvo Desmedt, University College London, UK

Zoran Despotovic, DoCoMo Euro-Labs, Germany
Roger Dingledine, The Free Haven Project, USA
Paolo Donzelli, Office of the Prime Minister, Italy
Jeroen Doumen, University of Twente, Neitherland
Schahram Dustdar, Vienna University of Technology, Austria
Gerhard Eschelbeck, Webroot Inc., USA
Yung-Chin Fang, Dell Corp., USA
Pascal Felber, Université de Neuchâtel, Switzerland
Elena Ferrari, Universita' dell' Insubria, Italy
Jordi Forné, Universitat Politècnica de Catalunya, Spain
Felix C. Freiling, RWTH Aachen University, Germany
Steven Furnell, University of Plymouth, UK
Stephan Groß, Technische Universität Dresden, Germany
Daniel Grosu, Wayne State University, USA
Yong Guan, Iowa State University, USA
Ibrahim Haddad, Concordia University, Canada
Abdelkader Hameurlain, Université Paul Sabatier, France
Marit Hansen, Independent Centre for Privacy Protection Schleswig-Holstein Kiel, Germany
Naohiro Hayashibara, Tokyo Denki University, Japan
Xubin (Ben) He, Tennessee Technological University, USA
Yanxiang He, Wuhan University, China
Rattikorn Hewett, Texas Tech University, USA
Jimmy Huang, York University, Canada
Jan Jürjens, Munich University of Technology, Germany
Erland Jonsson, Chalmers University of Technology, Sweden
Oliver Jorns, ftw. Forschungszentrum Telekommunikation Wien, Austria
Audun Josang, University of Queensland, Australia
Yukiko Kawai, National Institute of Information and Communications Technology, Japan
Dogan Kesdogan, RWTH Aachen Informatik IV, Germany
Hiroaki Kikuchi, Tokai University, Japan
Hong Ong Oak, Ridge National Laboratory, USA
Seungjoo Kim, Sungkyunkwan University, Korea
Christian Kirchsteiger, European Commission
Peter Küng, Credit Suisse, Switzerland
Sy-Yen Kuo, National Taiwan UniversityTaiwan, R.O.C
Marc Lacoste, France Télécom Division R&D., France
Kwok-Yan Lam, Tsinghua University, China
Monika Lanzenberger, Norwegian University of Science and Technology, Trondheim, Norway
Chokchai (Box) Leangsuksun, Louisiana Tech University,USA
Yih-Jiun Lee, Chienkuo Technology University,Taiwan, R.O.C
Chin-Laung Lei, National Taiwan University, R.O.C
Chae Hoon Lim, Sejong University, Korea
Ching Lin, Macquarie University, Australia
Tong Liu, Dell Corp., USA
Javier Lopez, University of Malaga, Spain
Sanlu Lu, Nanjing University, China
Burgazzi Luciano, ENEA, Italy
Jianhua Ma, Hosei University, Japan
Josef Makolm, Federal Ministry of Finance, Austria
Geyong Min, University of Bradford, UK
Yi Mu, University of Wollongong, Australia
Günter Müller, Telematik Universitaet Freiburg, Germany
Junghyun Nam, Sungkyunkwan University, Korea
Tho Manh Nguyen, Vienna University of Technology, Austria
Jesper Buus Nielsen, Aarhus University, Denmark
Flemming Nielson, Technical University of Denmark, Denmark

Juan Gonzalez Nieto, Queensland University of Technology, Australia
Thomas Nowey, University of Regensburg, Germany
Manish Parashar, Rutgers University, USA
Fernando Pedone, Universita della Svizzera Italiana, Switzerland
María S. Pérez-Hernández, Universidad Politécnica de Madrid,Spain
Mario Piattini, University of Castilla La Mancha, Spain
Makan Pourzandi, Ericsson Inc.
Christopher Price, University of Wales Aberystwyth, UK
Philipp Reisner, MD at LINBIT Information Technologies GmbH, Austria
Heiko Rossnagel, Johann Wolfgang Goethe University Frankfurt, Germany
Bimal Roy, Indian Statistical Institute, India
Rei Safavi-Naini, University of Wollongong, Australia
Kenji Saito, Keio University, Japan
Kouichi Sakurai, Kyushu University, Japan
Henrique Santos, Universidade do Minho, Portugal
Stephen L. Scott, Oak Ridge National Laboratory
Jean-Marc Seigneur, University of Geneva, Switzerland
Ahmed Serhrouchni, Telecom Paris, France
Ingrid Schaumüller-Bichl, ITSB Linz, Austria
Charles Shoniregun, University of East London, UK
Amund Skavhaug, Norwegian University of Science and Technology (NTNU), Norway
Neal. A. Snooke, University of Wales Aberystwyth, UK
Ketil Stølen, SINTEF and University of Oslo, Norway
Peter Struss, Technische Universitat and Occ'm Sofwtare, Germany
Tsuyoshi Takagi, FutureUniversity – Hakodate, Japan
Makoto Takizawa, Tokyo Denki University, Japan
A Min Tjoa, Vienna University of Technology, Austria
Jorge Villar, Universitat Politècnica de Catalunya, Spain
Roland Wagner, University of Linz, Austria
Edgar Weippl, Vienna University of Technology, Austria
Chuan-Kun Wu, Chinese Academy of Sciences, China
Cheng-Zhong Xu, Wayne State University, USA
Mariemma I. Yagüe, University of Malaga, Spain
Laurence T. Yang, St.Francis Xavier University, Canada
Alec Yasinsac, Florida State University, USA
George Yee, National Research Council, Canada
Sung-Ming Yen, National Central University, Taiwan, R.O.C
Bill Yurcik, National Center for Supercomputing Applications (NCSA)
Nicola Zannone, University of Trento, Italy
Jianhong Zhang, North China University of Technology, China
Jianying Zhou, Institute for Infocomm Research, Singapore
Huafei Zhu, Institute for Infocomm Research, Singapore

Workshop on Dependable and Sustainable Peer-to-Peer Systems (DAS-P2P 2006)

Workshop Organizers
Yusuke Doi, Toshiba Corporation, Japan
Youki Kadobayashi, Nara Institute of Science and Technology, Japan
Kenji Saito, Graduate School of Media and Governance, Keio University, Japan

Program Committee
Stéphane Bressan, National University of Singapore, Singapore
Bernard Burg, Panasonic Research, USA
Ian Clarke, Freenet Project, UK
Roger Dingledine, The Free Haven Project, USA
Yusuke Doi, Toshiba Corporation, Japan (co-chair)
Claudiu Duma, Linköping University, Sweden
Debojyoti Dutta, University of Southern California, USA
Noria Foukia, University of Otago, New Zealand
Maria Gini, University of Minnesota, USA
Achmad Nizar Hidayanto, University of Indonesia, Indonesia
Sam Joseph, University of Hawaii, USA
Youki Kadobayashi, Nara Institute of Science and Technology, Japan (co-chair)
Anirban Mondal, University of Tokyo, Japan
Akiko Orita, Keio University, Japan
Omer F. Rana, Cardiff University, UK
Kenji Saito, Keio University, Japan (co-chair)
Claudio Sartori, University of Bologna, Italy
Nguyen Manh Tho, Vienna University of Technology, Austria
Sheng Zhong, State University of New York at Buffalo, USA

Workshop on Bayesian Networks in Dependability (BND2006)

Workshop Co-chairs
Stefania Montani, University of Piemonte Orientale
Hichem Boudali, University of Twente

Workshop Committee
Joanne Bechta Dugan, University of Virginia
Marc Bouissou, Electricite' de France
Helge Langseth, Sintef, Norway
Luigi Portinale, University of Piemonte Orientale
John L. Quigley, University of Strathclyde, Glasgow
Luis E. Sucar, Department of Computer Science, INAOE, Puebla, Mexico
Philippe Weber, Université Henri Poincaré, Nancy

Workshop on Dependability in Large-scale Service-oriented Systems (DILSOS 2006)

Program Chairs
Karl M. Göschka, Vienna University of Technology, Austria
Schahram Dustdar, Vienna University of Technology, Austria
Mehdi Jazayeri, University of Lugano, Switzerland

Organizational Chair
Martin Treiber, Vienna University of Technology, Austria

Program Committee
Marco Aiello, University of Trento, Italy
Mikio Aoyama, Nanzan University, Japan
Luciano Baresi, Politecnico di Milano, Italy
Boualem Benatallah, UNSW, Australia
Sara Bouchenak, University of Grenoble I, France
Sjaak Brinkkemper, Univ. of Utrecht, Netherlands
Tevfik Bultan, University of California, USA
Fabio Casati, HP, USA
Malu Castellanos, Hewlett-Packard, USA
Gianpaolo Cugola,, Italy
Harmke de Groot,, Netherlands
Asuman Dogac, METU, Turkey
Dieter Fensel, DERI, Ireland
Gianluigi Ferrari, University of Pisa, Italy
Jacqueline Floch, Sintef, Norway
Kary Fraemling, Helsinki University of Technology, Finland
Claude Godart, INRIA, France
Paul Grefen, Eindhoven Uni. of Technology, Netherlands
John Grundy, University of Auckland, New Zealand
Mohand-Said Hacid, Universite Claude Bernard Lyon, France
Manfred Hauswirth, EPFL, Switzerland
Alfons Kemper, TU Muenchen, Germany
Bernd Kraemer, University of Hagen, Germany
Frank Leymann, University of Stuttgart, Germany
Ozelin Lopez, ATOS Origin, Spain
Brahim Medjahed, University of Michigan, USA
Joachim Nern, Aspasia Systems, Germany
Beng Chin Ooi, National University of Singapore, Singapore
Maria Orlowska, UQ, Australia
Aris M. Ouksel, University of Illinois at Chicago, USA
Mike Papazoglou, Tilburg Univ., Netherlands
Jose Pereira, Universidade do Minho, Portugal
Barbara Pernici, Politecnico di Milano, Italy
Marco Pistore, Universita di Trento, Italy
Dimitris Plexousakis, FORTH, Greece
Alexander Romanovsky, University of Newcastle, UK
Anne-Marie Sassen, European Commission, EU
Vladimiro Sassone, University of Sussex, UK
Ian Sommerville, Lancaster University, UK
Jianwen Su, UCSB, USA
Katia Sycara, Carnegie Mellon University, USA
Stefan Tai, IBM Watson, USA
Paolo Traverso, ITC, Italy
Elena Troubitsyna, Aabo Akademi, Finland
Wil van der Aalst, Eindhoven University of Technology, Netherlands

Jos van Hillegersberg, Univ. of Twente, Netherlands
Steve Vinoski, IONA, USA
Martin Wirsing, Ludwig-Maximilians-University Munich, Germany
Jian Yang, Macuquarie University, Australia
Gianluigi Zavattaro, University of Bologna, Italy

Workshop: Security in E-Learning (SEL)

Program Chair
Edgar Weippl, Vienna University of Technology, Austria

Program Committee
Elke Franz, Dresden University of Technology, Germany
Gerald Quirchmayr, University of South Australia, Australia
Tomaz Klobucar, Jozef Stefan Institute, Slovenija
Günther Pernul, University of Regensburg, Germany

Workshop "Dependability Aspects on Data WArehousing and Mining Applications" (DAWAM 2006)

Organizer Co-chairs
Jimmy Huang, York University, Canada
Josef Schiefer, Senactive IT-Dienstleistungs GmbH, Austria
Nguyen Manh Tho, Vienna University of Technology, Austria

Program Committee
Jemal Abawajy, Deakin University, Australia
Aijun An, York University, Canada
Pawan Chowdhary, IBM T J Watson Research Center, USA
LiWu Chang, Naval Research Laboratory, USA
Josep Domingo-Ferrer, Rovira i Virgili University of Tarragona, Spain
Elena Ferrari, University of Insubria at Como, Italy
Ulrich Flegel, University of Dortmund, Germany
Tyrone Grandison, IBM Almaden Research, USA
Jimmy Huang, York University, Canada
Jun-Jang (JJ) Jeng, IBM T.J. Watson Research Center, USA
Hillol Kargupta, University of Maryland, Baltimore County, USA and Agnik, LLC
Zongwei Luo, University of Hong Kong, Hong Kong
Taneli Mielikäinen, University of Helsinki, Finland
Tho Manh Nguyen, Vienna University of Technology, Austria
Daniel E. O'Leary, University of Southern California, USA
Stanley Oliveira, Embrapa Information Technology, Brazil
Arnon Rosenthal, MITRE Corporation, USA
Josef Schiefer, Senactive IT-Dienstleistungs GmbH, Austria
Ben Soh, La Trobe University, Australia
David Taniar, Monash University, Australia
Juan Trujillo, University of Alicante, Spain
Vassilios S. Verykios, University of Thessaly, Greece
Justin Zhan, University of Ottawa, Canada
Sheng Zhong, State University of New York at Buffalo, USA

Workshop on Bioinformatics and Security (BIOS 06)

Workshop Chairs
Küng Josef, University of Linz, FAW Austria
Mazuran Petra, FAW, Austria
Wagner Roland, University of Linz, FAW Austria

Program Committee
Eisenacher Martin, University of Münster, Germany
Hochreiter Sepp, TU Berlin, Germany
Hof Sonja, (DWS) AG,Switzerland
Kramer Stefan, TUM, Germany
Marik Vladimir, Technical University Prag, Czech
Mazuran Petra, FAW, Austria
Palkoska Jürgen, FAW Austria
Retschitzegger Werner, University of Linz, Austria
Revell Norman, Middlesex University, UK
Tjoa A Min, Technical University of Vienna, Austria

Workshop: Information Security Risk Management (ISRM)

Workshop Chairs
Professor Dr. D. Karagiannis, University of Vienna, Austria
Dr. L. Marinos, ENISA, Greece

Program Committee
M. Dietrich, BSG Unternehmensberatung, Switzerland
M. Hoevers, ECP-NL, Platform voor eNetherland, The Netherland
K. Kalmelid, Swedish Emergency Management Agency, Sweden
S. Lebel, Dir. Centrale de la Sécurité des Systèmes d'information, France
Prof. Dr. G. Müller, Telematik, Univ. of Feiburg, Germany
M. Rohde, European Commission, DG Information Society and Media, Belgium
Dr. I. Schaumüller-Bichl, IT Security Consultant, Austria

Workshop "Dependability and Security in e-Government" (DeSeGov 2006)

Workshop Chairs
A Min Tjoa, Vienna University of Technology, Austria
Erich Schweighofer, University of Vienna, Austria

Program Committee
Peggy Agouris, University of Maine, USA
Yigal Arens, USC/Columbia University Digital Government Research Center, USA
Jon Bing, University of Oslo, Norway
Fernando Galindo, University of Zaragoza, Spain
Dieter Klumpp, Alcatel SEL Foundation, Germany
Robert Krimmer, Vienna University of Economics and Business Administration, Austria
Scott F. Midkiff, Virginia Polytechnic Institute and State University,USA
Enrico Nardelli, University of Rome TorVergata, Italy
Tho Manh Nguyen, Vienna University of Technology, Austria
Erich Schweighofer, University of Vienna, Austria
Efthimios Tambouris, CERTH/ITI, Greece
A Min Tjoa, Vienna University of Technology, Austria
Greg B. White, The University of Texas at San Antonio, USA
Maria A. Wimmer, University of Koblenz, Germany

A Study of Security Architectural Patterns

David G. Rosado[1], Carlos Gutiérrez[2], Eduardo Fernández-Medina[1] y Mario Piattini[1]
(1) 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
{David.GRosado, Eduardo.Fdez-Medina, Mario.Piattini}@uclm.es
(2) STL. Calle Manuel Tovar 9, 28034 Madrid, Spain
carlos.gutierrez@stl.es

Abstract.

Security and reliability issues are rarely considered at the initial stages of software development and are not part of the standard procedures in development of software and services. Security patterns are a recent development as a way to encapsulate the accumulated knowledge about secure systems design, and security patterns are also intended to be used and understood by developers who are not security professionals. In this paper, we will compare several security patterns to be used when dealing with application security, following an approach that we consider important for measuring the security degree of the patterns, and indicating a fulfilment or not of the properties and attributes common to all security systems.

1. Introduction

A good percentage of the software deployed in industrial/commercial applications is of poor quality and contains numerous flaws that can be exploited by attackers [1, 2]. There are many reasons for this and there is no doubt that we have a serious problem, every day the press reports of attacks to web sites or databases around the world, resulting in millions of dollars in direct or indirect losses [3]. Security is a very important aspect of any computing system, and has become a serious problem since institutions have opened their databases to the Internet [4-6]. Most web systems in current use have not been designed with security in mind and patches have failed to make them more resistant to attacks [7]. It is important to develop systems where security has been considered at all stages of design and at all architectural levels, which not only satisfy their functional specifications but also satisfy security and other non-functional requirements [8, 9].

There is very little work concerning the full integration of security and systems engineering from the earliest phases of software development. Although several approaches have been proposed for some integration of security, there is currently no comprehensive methodology to assist developers of security sensitive systems. Lack of support for security engineering in those approaches for software systems development is usually seen as a consequence of: i) security requirements being generally difficult to analyse and model, and ii) developers lacking expertise in secure software development [10, 11].

Security patterns are proposed as a means of bridging the gap between developers and security experts. Security patterns are intended to capture security expertise in the form of worked solutions to recurring problems. The first person who used the pattern approach was Christopher Alexander [12], and in his book he indicated that each pattern describes a problem which occurs over and over again in our environment, and then states the core of the solution to that problem, in such a way that you can use this solution a million times over, without ever doing it the same way twice.

This paper will study a set of security patterns that help us to implement security requirements in the applications design. They are patterns that guide the systems design to make them more secure in a comfortable and efficient way. The rest of the paper is organized as follows: In section 2, we will define a template to define patterns and we will study a set of patterns to make the comparison. Then, we will describe the comparison framework that we have used

0-7695-2567-9/06 $20.00 © 2006 IEEE

and we will perform the patterns comparison. Finally, we will put forward our conclusions.

2. Template and Security Architectural Patterns Selected

A software pattern can be described through a set of properties (a template) such as name, problem, solution and so on. These templates allow authors to define new patterns, but respecting this structure [13].

In this section, a template will be defined composed of the following properties (based on [14, 15]): i) *Intent*: It describes what the pattern does, which its rationale and intent are, and what particular design issue it addresses. ii) *Context*: It describes the context of the problem. iii) *Problem*: It gives a statement of the problem that this pattern solves. iv) *Description*: A scenario that illustrates a design problem. v) Solution: To give a statement of the solution to the problem. vi) *Consequences*: To describe the trade-offs and results when we use the pattern. vii) *Known uses*: Examples of the patterns found in real systems viii) *Related patterns*: To list other related patterns that use this pattern as a reference.

Once the template has been defined, we are join to present some of the most important security architectural patterns, analyzing characteristics and find out the degree of security that they supply to the systems that use them. These patterns are as follows [13, 16-18] : 1) Authorization Pattern; 2) RBAC Pattern (Role-Based Access Control); 3) Multilevel Security Pattern; 4) Reference Monitor Pattern; 5) Virtual Address Space Access Control; 6) Execution Domain Pattern; 7) SAP Pattern (Single Access Point),; 8) Check Point Pattern; y 9) Session Pattern.

There are many others security patterns that, due to space constraints we can not described with detail, but we can find more information in [13, 17-22].

2.1. Authorization Pattern

i) *Intent*: It describes who is authorized to access the resources systems. ii) *Context*: Any computational environment where there are active entities that request resources whose access must be controlled. iii) *Problem*: The permissions granted for security subjects that have access to protected objects need to be explicitly indicated. On the contrary, any subject could access any resource. iv) *Description*: To structure the different access policies, we distinguish between active entities (subjects) and passive resources (protection objects). v) *Solution*: The Authorization structure (see Figure 1) can be captured from classes and relationships or associations. The active entities are represented by the *Subject* class and the passive resources (or resources to be protected) are represented the by *Object* class. The relationship between subject and object describes what subject is authorized to access certain objects (*Rights*). vi) *Consequences*: The solution is independent of the resources to be protected. The subjects can be executions of processes, users, roles and group of users; the objects to be protected can be transactions, memory area, I/0 devices, files or other resources of the operating system and the type of access can be reading, writing, execution or methods in higher level objects. vii) *Known uses*: It is the basis for the access control systems of most commercial products as Unix, Windows, Oracle and others. viii) *Related patterns*: The RBAC pattern shown later is a specialization of this pattern.

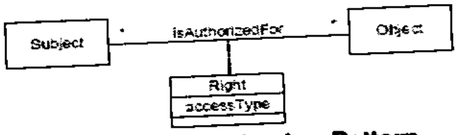

Figure 1. Authorization Pattern.

2.2. RBAC Pattern

i) *Intent*: To control the access resources only based on the subject role. ii) *Context*: Any environment where we need to control the access to computing resources and where users can be classified according to their jobs and tasks. iii) *Problem*: It is necessary to assign rights and permissions (central authority) in an appropriate way for users to be able to access the protected objects. iv) *Description*: It improves the administration by using roles that can be assigned to individual users or groups. We may need to have hierarchies of roles, with inheritance of rights. A role may be assigned to individual users or to groups of users. v) *Solution*: It extends the idea of the *Authorization* pattern by translating roles as subjects. A basic model for RBAC is shown in Figure 2. User and Role classes describe registered users and predefined roles, respectively. Users are assigned to roles, roles are given rights according to their functions and the *Right* association class defines the types of access that a user within a role is authorized to apply to the protection object. The combination Role, Protection Object and Rights is an instance of the Authorization pattern. vi) *Consequences*: When introducing roles, the administrative effort is reduced because there is no need of assigning rights to individuals. The roles structure let us manage big groups as well as reduce rules. vii) *Known uses*: RBAC is implemented in Sun's

2567-9/06 $20.00 © 2006 IEEE

J2EE, Microsoft's Windows 2000, IBM's WebSphere, and Oracle, among others.

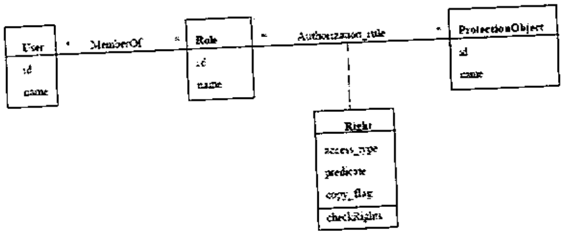

Figure 2. RBAC Pattern.

2.3. Multilevel Security Pattern

i) *Intent*: It provides a mechanism of access management in a system with several levels of security classification. ii) *Context*: It is applicable to systems that need to provide several security levels. iii) *Problem*: How to decide access in an environment with security classifications. iv) *Description*: In many systems, data integrity and confidentiality need to be guaranteed. This model would be able to be used in any architecture level and it provides a structure that allows us to have differente security levels for both subjects and objects. v) *Solution*: To represent the structure of Multilevel Security, there must be an instance of the class Subject Clasification for each subject and an instance of the class Object Classification for each object (see Figure 3). These instances are used to add levels and objects security categories to a subject. vi) *Consequences*: It facilitates the administrative work in an environment that requires the classification of subjects and objects. The multilevel security can be expensive since subjects and objects need to be classified into certain levels of sensitiveness. vii) *Known uses:* The model has been used by several military-sponsored projects and in a few commercial products, including DBMSs (Informix) and operating systems (Pitbull [23] and HP's Virtual Vault [24]). viii) *Related patterns*: The concept of roles can also be applied here.

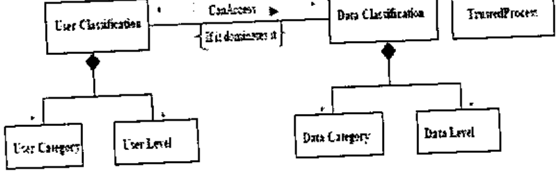

Figure 3. Multilevel Security Pattern

2.4. Reference Monitor Pattern

i) *Intent*: To make it possible that all authorizations are fulfilled when a process requires resources. ii) *Context*: A multiprocess environment making petitions by resources. iii) *Problem*: If the defined authorizations are not fulfilled, processes can execute all kind of illegal actions, for instance, any user could read any file. iv) *Description*: To define authorization rules is not enough; these rules must be imposed when a process makes a petition to a resource. There are many implementations and we need an abstract execution model. v) *Solution*: To define an abstract process that intercepts all petitions from resources and confirms them. Figure 4 shows us a class diagram in which we can see a Reference Monitor. Authorization rules indicate a collection of authorization rules organized as ACLs (access control lists) vi) *Consequences*: If all petitions are intercepted, we can assure that they fulfil the rules. The specific implementations are necessary for any kind of resource. To check each petition can mean a performance loose. vii) *Known uses*: Most modern operating systems implement this concept, e.g., Solaris 9, Windows 2000, AIX, and others. The Java Security Manager is another example. viii) *Related patterns*: This pattern is a special case of the *Checkpoint* pattern (section 2.9).

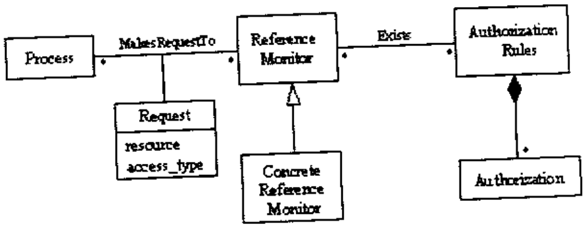

Figure 4. Reference Monitor Pattern.

2.5. Virtual Address Space Access Control Pattern

i) *Intent*: To control the access by processes to specific areas of their virtual address space (VAS) according to a set of predefined access types. ii) *Context*: Multiprogramming systems with a variety of users. Processes executing on behalf of these users must be able to share memory areas in a controlled way. Each process is executed in its own address space. iii) *Problem*: Processes must be controlled when they access memory, otherwise they could overwrite areas from other processes or gain access to private information. iv) *Description*: There is a variety of structures of virtual memory addresses space: some systems use a separate set, others an only level address space. Furthermore, VAS can be divided into users and operating system. We would like to control the access to all these kinds in a uniform way. This implies that an implementation of the solution will require specific hardware architecture. However, the solution must be independent of the hardware. v) *Solution*: To divide VAS into segments corresponding to logical units within the programs. To use descriptors to indicate access rights such as the beginning address of the accessible segment, the limit of the accessible segment and the type of allowed access (reading, writing, executing). Figure 5 shows a diagram to indicate the solution to the class. A process (*Process* class) must have a descriptor (*Descriptor* class) to access a segment in the VAS. vi) *Consequences*: This pattern provides a protection of the required segment because a process cannot access a segment without an own descriptor. If all resources are outlined in a virtual address space, the pattern can control the access to any kind of resource, including files. The solution is dependent of the hardware. In systems that use separate address spaces it is necessary to add an extra identifier to the descriptor registers to indicate the address space number. vii) *Known uses*: IBM S/38, IBM S/6000, Intel X86 [25], and Intel Pentium use some type of descriptors for memory access control. The operating systems in these machines must use this approach for memory management. viii) *Related patterns*: This pattern is a direct application of the Authorization pattern to the processes' address space.

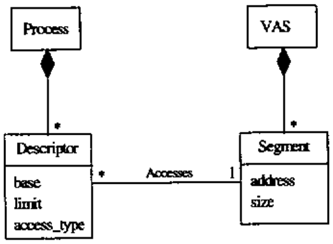

Figure 5. Virtual Address Space Access Control Pattern.

2.6. Execution Domain Pattern

i) *Intent*: Define an execution environment for processes, indicating explicitly all the resources a process can use during its execution, as well as the type of access for the resources. ii) *Context*: A process executes on behalf of a user, group, or role (a subject). A process must have access rights to use the resources defined for its subject during execution. The set of access rights given to a process define its execution domain. At times the process may also need to enter other domains to perform its work; for example, to extract a statistical value (avg, mean) from a file in another user's domain. iii) *Problem*: Restricting a process to a specific set of resources is a basic step to control malicious behaviour. Otherwise, unauthorized processes could destroy or modify information in files or databases with obvious results or could interfere with the execution of other processes. iv) *Description*: There is a need to restrict the actions of a process during its execution; otherwise it could perform illegal actions. Resources typically include memory and I/O devices, but can also be system data structures and special instructions. A process needs the flexibility to create multiple domains and to enter inner domains for specific purposes. v) *Solution*: Attach to the process a set of descriptors that represent the rights of the process. In Figure 6, class Domain represents domains and in conjunction with the Composite pattern it describes nested domains. Operation enter in class Domain lets a process enter a new domain. A domain includes a set of descriptors that define rights for resources. vi) *Consequences*: It could be applied to describe access to any type of resource if the resource is mapped to a specific memory address. The model does not restrict the implementation of domains. It has extra complexity and special hardware is needed. In capability systems the descriptors are part of the process code and are enabled during execution. vii) *Known uses*: The Plessey 250 and the IBM S/6000 running AIX [26] are good examples of the use of this pattern. The Java Virtual Machine defines restricted execution environments in a similar way [27].

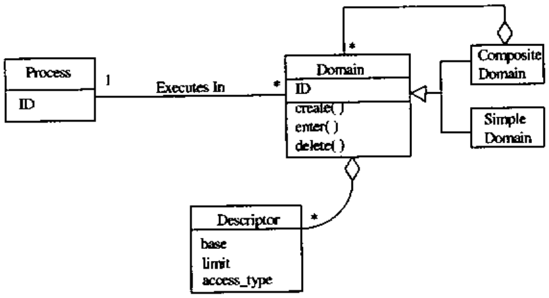

Figure 6. Execution Domain Pattern

2.7. Session Pattern

i) *Intent*: To provide us with an environment where a user's rights can be restricted and controlled. ii) *Context*: Any environment where we need to control the access to computing resources. iii) *Problem*: Depending on the context, for example, within a certain application, a user will only activate a subset of the authorizations he/she has. This will avoid that users use their rights wrongly (for instance, to accidentally delete certain files). In this way, if an attacker endangers a process, the damage potential is reduced. iv) *Description*: In many systems, global information is necessary in several points. To overcome this problem, Session objects that provide the necessary information are used. v) *Solution*: Figure shows us elements of a class diagram session. A subject can be in several sessions at the same time and it has a limited lifetime. When we start a session (for example, when registering ourselves), a user only activates a set of authorization contexts assigned to him/her, then, only the necessary rights are available within this session. The *Subject* class describes an active entity that accesses the system and asks for resources. The *AuthorizationContext* class describes a set of contexts of executions or active rights that the user has in a given interaction. vi) *Consequences*: Each session gains all privileges that are necessary to carry out the desired tasks. Thus, damage will be potentially reduced when a session is in danger because only an activated subset of authorization can be wrongly used. vii) *Known uses*: This concept appears in many computational environments, e.g. RBAC use sessions as defined by this pattern. UNIX ftp and telnet services use a Session for keeping track of requests and restricting user actions. viii) *Related patterns*: Session is an alternative to a Singleton [10] in a multi-threaded, multi-user, or distributed environment. SAP validates a user through Check Point (sections 2.8 and 2.9). It gets a Session in return if the user validation is acceptable.

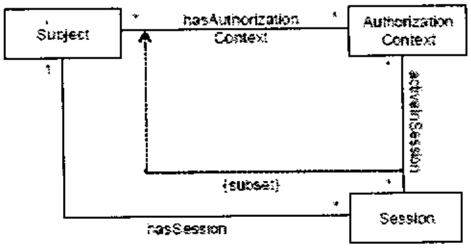

Figure 7. Session Pattern.

2.8. Single Access Point Pattern (SAP)

i) *Intent*: The SAP pattern defines a simple interface for all communications performed with entities external to the system. ii) *Context*: SAP can be applied to self-contained systems that need to communicate with external entities. iii) *Problem*: A security model is difficult to confirm when it has multiple main, back and lateral doors to come in the application. iv) *Description*: The application of a SAP pattern avoids that external entities are directly communicated with components of the system. All input traffic is carried out through a channel, where the supervision can be easily performed and this channel will collect information about occurred access petitions, their origins and authorization information. It will generate actions or transmit data to parts inside the system. v) *Solution*: SAP represents the only connection of the system with outside (see Figure 8). All incoming communication petitions are taken to the SAP instance that works as a mediator. If certain policies need to be imposed, all petitions should be sent to a *Check Point* class before they are transmitted to their addresses. vi) *Consequences*: SAP will provide a good place to capture register information as well as to carry out authorization tasks. The undesirable modification of data can be avoided with efficient checks that let us access the system. vii) *Known uses*: UNIX telnet and Windows NT login application use SAP for logging into the system. These systems also create the necessary Roles for the current Session. viii) *Related patterns*: SAP validates the user's login information through a Check Point and uses that information to initialize the user's Roles and Session. A Singleton [10] could be used for the login class especially if you only allow the user to have one login session started or only log into the system once.

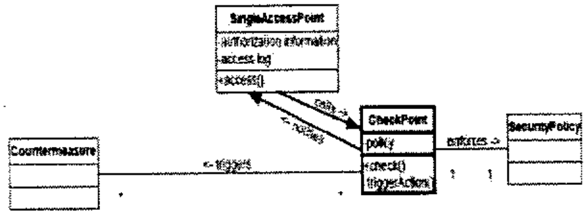

Figure 8. SAP Pattern and Check Point Pattern

2.9. Check Point Pattern

i) *Intent*: It states a structure to check the incoming petitions. If it finds violations, this pattern is in charge of taking the appropriate countermeasures. ii) *Context*: *Check Points* are applicable to any relevant security communication. iii) *Problem*: To avoid a disauthorized access, it is crucial to check who and how is interacting within a system and take measures if it is necessary. iv) *Description*: It needs to take any kind of action, if there are mistakes depending on the seriousness. v) *Solution*: A *Check Point* is a component that analyzes all petitions and messages. A SAP is predestined to be combined with a Check Point for all messages to be supervised (see Figure 8). It implements a method to check messages according to the current security policy. It gives place to actions that could be necessary to protect the system against attacks. vi) *Consequences*: Its application can benefit the system confidentiality, if the checking algorithm is correct. Undesirable

0-7695-2567-9/06 $20.00 © 2006 IEEE

modifications can be filtered if the checking algorithm is able to detect those attacks. Complex checking routines can make both the system and the message interchange work slower. vii) *Known uses*: The login process for an ftp server uses Check Point. viii) *Related patterns*: Single Access Point is used to insure that *Check Point* gets initialized correctly and that none of the security checks are skipped. Roles are often used for Check Point's security checks and could be loaded by *Check Point*. *Check Point* usually configures a *Session* and stores the necessary security information in it. It can also interact with the *Session* to get the user's Role during the authorization process.

3. Comparative Framework

In this section, we will put forward a comparison based on certain criteria that we consider important for security with the purpose of distinguishing all properties and characteristics of all previous patterns as well as showing a general vision of the subject. There are some comparisons [13] of patterns with certain criteria or security principles [28]. Some of these defined criteria are based on the works of Babar [29] and Firesmith [30], in which they select the most commonly used attributes and security properties in the security dominion. The security properties considered to make our comparison are the following: *Authentication*: It must be validated the identity of customers to frustrate any unauthorized access. *Authorization*: This attribute defines the access privileges of entities to different resources and services of a system. *Integrity*: To guarantee that data and communications will not be compromised by active attacks. *Confidentiality*: The guarantee that information is not accessed by unauthorized parts. *Attacker detection*: To be able to detect and register access or modification intents in the system coming from unauthorized users. *No-Repudiation*: It prevents that certain participant in certain interaction can deny to have participated in it. *Auditability*: To keep a log of user's or other system's interaction with a system and it helps detect potential attacks. *Maintainability*: It facilitates the introduction or modification of the security policy during the software development life cycle. *Availability*: It assures that authorized users can use the resources when they are required. *Reliability*: It assures the system operations due to failures or configuration mistakes. Besides, it assures the system availability even when the system is being attacked. *Error management*: A system must provide a robust error management mechanism.

Also, we consider some criteria to evaluate patterns as they are: *Performance*: It indicates the impact of the pattern on the functioning of a system. *Implementation cost*: Costs accompanying the pattern use. *Security degree*: It indicates the security level that the pattern has for the function it fulfils, that is, the more security properties the pattern covers, the more security degree will have.

Many patterns fulfil security properties without constraints; others are only fulfilled according to certain conditions, as it can be seen in table 1. The majority of patterns are based on guaranteeing access control, supplying confidentiality and in some cases, also integrity and reliability, but they do not take into account properties as important as error management, flexibility or maintenance, etc. In table 2, we can see the use of these patterns in the software development to allow us to increase or to reduce the performance of the global application. For example, "—a" means that the pattern can reduce performance because there are many users in the system and it is complex to manage and implement the pattern with many users. There are patterns with a high degree of security (see Table 3) but they are complex patterns. Then, if we want to have a system with a high degree of security, they will be also more complex systems, affecting their performance.

Table 1. Comparative table for the security criteria

	Authentication	Authorization	Integrity	Confidentiality	Attackers detection	No-Repudiation	Auditability	Maintainability	Availability	Reliability	Error management
Authoriz.		0		0	1			0	0		
RBAC		0		0	1			0	0		
Multilevel		0	5	6	1				0	0	
Reference Monitor		0	7	7	1				0	7	
Virtual Address		0	7	7	1				0		
Execution Domain		0	7	7	1				0	4	
SAP	0	0	2	0	0	0	0		0	0	0
Check Point	0	0	2	2	0	0			0	0	0
Session		0	0	0	1			3	0	4	

0. Always fulfilled. 1. Only detection. 2. Efficient check algorithm. 3. First step development. 4. Subset of the authorizations activated. 5. Biba model. 6. Bell LaPadula model. 7. To process level.

0-7695-2567-9/06 $20.00 © 2006 IEEE

Developers (not security experts) can find many security patterns but it is very difficult to determine which pattern is better to be used or which pattern guarantees certain degree of security. For this reason, we find a lack of a method or a flexible model of security architectures that guarantees security of the system in many aspects and that guides developers in the right way for the implementation of security into their systems, according to the specific requirements of them [31].

Table 2. Comparative table of the performance

	Performance		
Authorization	—[a]	+[e]	Virtual Address
RBAC	+[c]	—[f]	Execution Domain
Multilevel	—[d]	—[b]	SAP
Reference Monitor	—	—[b]	Check Point
Session	+c		

+: Increase. — : Reduce. Conditions: a) Many users. b) Complex checks. c) Efficient implementation. d) Evaluation access rights. e) If it uses Reference Monitor. f) Domains management

Table 3. Comparative table for the evaluation criteria

	Implem. Cost	Security degree
Authorization	L	M
RBAC	M	M
Multilevel	H	H
Reference Monitor	H	H
Virtual Address	L	M
Execution Domain	M	H
SAP	H	H
Check Point	H	H
Session	H	H

L: Low M: Medium H: High

4. Conclusions and Future Work

Patterns are a promising proposal towards security, useful to build and evaluate systems. Security patterns help us keep in mind non-functional security requirements at the beginning of the design. In the critical applications of security, it is extremely important to avoid mistakes, since we must guarantee the security of such applications and provide all operations and interactions that are performed in the application with a high level of security. Therefore, the use of security patterns is important to develop a secure system.

A software architecture constructed in this way is more reusable and extensible than an architecture defined directly from the requirements or where patterns are applied later. It is clear that combinations of patterns are extensible because of the possibility of replacing a pattern with another concrete realization of the same pattern. They are reusable because of the possibility of replacing several of the used patterns to fit the requirements of a new application.

There are many patterns with different purposes, reason why developers must combine many patterns to establish a high degree of security within the system but they have the problem of choosing which pattern must be used and deciding which pattern will better adapt to the system security requirements.

Our future work will be studying the different security architectures existing in the systems design together with defining a method to specify flexible security architectures that can be easily adapted to systems with very different security requirements as well as guarantee security using security patterns.

5. Acknowledgements

This research is part of the following projects: DIMENSIONS (PBC-05-012-2) financed by FEDER and by the "Consejería de Ciencia y Tecnología de la Junta de Comunidades de Castilla-La Mancha" (Spain), RETISTIC (TIC2002-12487-E) and CALIPO (TIC2003-07804-C05-03) granted by the "Dirección General de Investigación del Ministerio de Ciencia y Tecnología" (Spain).

6. References

[1] E. B. Fernandez, "An Overview of Internet Security", presented at World's Internet and Electronic Cities Conference (WIECC 2001), Kish Island, Iran, 2001.

[2] A. Toval, J. Nicolás, B. Moros, and F. García, "Requirements Reuse for Improving Information Systems Security: A Practitioner's Approach", *Requirements Engineering Journal*, vol. 6, pp. 205-219, 2001.

[3] D. Dennings, "Reflections on cyberweapons controls", *Computer Security*, vol. 16, pp. 43-53, 2000.

[4] A. Ghosh, C. Howell, and J. Whittaker, "Building software securely from the ground up", *IEEE Software*, vol. 19, pp. 14-17, 2002.

[5] E. Ferrari and B. Thuraisingham, "Secure Database Systems in: M. Piattini, O. Díaz," in *Advanced Databases: Technology Design*. Artech House, 2000

[6] P. Devanbu and S. Stubblebine, "Software engineering for security: a roadmap in: A. Finkelstein", *The Future of Software Engineering, ACM Press*, pp. 227-239, 2000.

[7] A. Boulanger, "Catapults and grappling hooks: The tools and techniques of Information warfare", *IBM Sys.*, vol. 37, pp. 106-114, 1998.

[8] ISACF, "Information Security Governance," in *Guidance for Boards of Directors and Executive Management*. USA: Information Systems Audit and Control Foundation, 2001

[9] E. B. Fernandez, "Metadata and authorization patterns", Departament of Computer Science and Eng., Florida Atlantic University TR-CSE-00-16, May 2000 2000.

[10] D. G. Firesmith, "Engineering Security Requirements", *Journal of Object Technology*, vol. 2, pp. 53-68, 2003.

[11] J. H. Saltzer and M. D. Schroeder, "The protection of information in computer systems", presented at Proceedings of the IEEE, 1975.

[12] C. Alexander, S. Ishikawa, and M. Silverstein, *A pattern language: towns, builings, construction*. New York: Oxford University Press, 1977.

[13] R. Wassermann, "Using Security Patterns to Model and Analyze Security Requirements", 032.04/E, 9th March 2004.

[14] AGCS, "AG Communication System. Template Pattern", 1996.

[15] E. Gamma, R. Helm, R. Johnson, and J. Vlissides, *Design Patterns: Elements of Reusable Object-Oriented Software*: Addison-Wesley, 1994.

[16] E. B. Fernandez, "Patterns for Operating Systems Access Control", presented at 9th Conference on Pattern Languages of Programs, PLoP 2002, Allerton Park, Illinois, USA, 2002.

[17] E. B. Fernandez and R. Pan, "A pattern language for security models", presented at 8th Conference on Pattern Languages of Programs, PLoP 2001, Allerton Park, Illinois, USA, 2001.

[18] J. Yoder and J. Barcalow, "Architectural Patterns for Enabling Application Security", presented at 4th Conference on Patterns Language of Programming, PLop 1997, Monticello, Illinois, USA, 1997.

[19] E. B. Fernandez and J. C. Sinibaldi, "More patterns for operating systems access control", presented at 8th European Conference on Pattern Languages of Programs (EuroPlop'2003), Irsee, Germany, 2003.

[20] E. B. Fernandez, M. L. Petrie, N. Seliya, and A. Herzberg, "A Pattern Language for Firewalls", presented at 10th Conference on Pattern Languages of Programs (PLoP'2003), Allterton Park, Monticello, Illinois, 2003.

[21] E. B. Fernandez, "Two patterns for web services security", presented at The 2004 International Symposium on Web Services and Applications, Las Vegas, Nevada, USA, 2004.

[22] S. Lehtoren and J. Pärssinen, "Pattern Language for Cryptographic Key Management", presented at 7th European Conference on Pattern Languages of Programs (EuroPlop'2002), Irsee, Germany, 2002.

[23] Argus Systems Group, "Trusted OS Security: Principles and practice," 2001 http://www.argus-systems.com/product/white_paper/pitbull/oss/2.shtml.

[24] HP, "Hewlett Packard Corp.,Virtual Vault," http://www.hp.com/security/products/virtualvault.

[25] R. E. Childs Jr., J. Crawford, D. L. House, and R. N. Noyce, "A processor family for personal computers", presented at Proceedings of the IEEE, 1984.

[26] N. A. Camillone, D. H. Steves, and K. C. Witte, "AIX operating system: A trustworthy computing system," in *IBM RISC System/6000 Technology*, 1990, pp. 168-172

[27] S. Oaks, *Java Security*, 2nd ed: O'Reilly Media, Inc., 2001.

[28] J. Viega and G. McGraw, *Building Secure Software - How to Avoid Security Problems the Right Way.*, 1st ed: Addison-Wesley, 2002.

[29] M. A. Babar, X. Wang, and I. Gorton, "Supporting Security Sensitive Architecture Design", presented at QoSA-SOQUA 2005, 2005.

[30] D. G. Firesmith, "Specifying Reusable Security Requirements", *Journal of Object Technology*, vol. 3, pp. 61-75, 2004.

[31] C. Gutiérrez, E. Fernández-Medina, and M. Piattini, "Towards a Process for Web Services Security", presented at WOSIS'05, Miami, Florida, USA, 2005.

0-7695-2567-9/06 $20.00 © 2006 IEEE