



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



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



9 780769 525679

Proceedings

The First International Conference on
Availability, Reliability and Security

ARES 2006

Copyright © 2006 by The Institute of Electrical and Electronics Engineers, Inc.

All rights reserved.

Copyright and Reprint Permissions: Abstracting is permitted with credit to the source. Libraries may photocopy beyond the limits of US copyright law, for private use of patrons, those articles in this volume that carry a code at the bottom of the first page, provided that the per-copy fee indicated in the code is paid through the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

Other copying, reprint, or republication requests should be addressed to: IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, P.O. Box 133, Piscataway, NJ 08855-1331.

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](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
<i>Louis Marinou</i>	
Model Driven Security	4
<i>David Basin</i>	

Session 1: Trust Management

Trust Based Risk Management for Distributed System Security — A New Approach	6
<i>Ching Lin and Vijay Varadharajan</i>	
RATING: Rigorous Assessment of Trust in Identity Management	14
<i>Rajarajan Sampath and Deepak Goel</i>	
Provably Secure Anonymous Access Control for Heterogeneous Trusts	24
<i>Kilho Shin and Hiroshi Yasuda</i>	

Session 2: P2P Systems

A Secure Event Agreement (SEA) Protocol for Peer-to-Peer Games	34
<i>Amy Corman, Scott Douglas, Peter Schachte, and Vanessa Teague</i>	
Satisfiability and Trustworthiness of Peers in Peer-to-Peer Overlay Networks	42
<i>Yoshio Nakajima, Kenichi Watanabe, Naohiro Hayashibara, Tomoya Enokido, Makoto Takizawa, and S. Misbah Deen</i>	
Tamper-resistant Replicated Peer-to-Peer Storage Using Hierarchical Signatures	50
<i>Alexander Zangerl</i>	
Censorship-Resistant and Anonymous P2P Filesharing	58
<i>Regine Endersleit and Thilo Mie</i>	

Session 3: Mobile Network and Pervasive Systems

A Dependable Device Discovery Approach for Pervasive Computing Middleware	66
<i>Sheikh Ahamed, Mohammad Zulkernine, and Suresh Anamanamuri</i>	
Single Sign-On Framework for AAA Operations within Commercial Mobile Networks	74
<i>Saber Zrelli and Yoichi Shinoda</i>	
A Selector Method for Providing Mobile Location Estimation Services within a Radio Cellular Network	82
<i>Junyang Zhou and Joseph Kee-Yin Ng</i>	

Guidelines for Biometric Recognition in Wireless System for Payment Confirmation _____	90
<i>Leon Grabensek and Sasa Divjak</i>	

Session 4: Protocol and Communication

An Extended Verifiable Secret Redistribution Protocol for Archival Systems _____	100
<i>V.H. Gupta and K. Gopinath</i>	

Analysis of Current VPN Technologies _____	108
<i>Thomas Berger</i>	

Integration of Quantum Cryptography in 802.11 Networks _____	116
<i>Thi Mai Trang Nguyen, Mohamed Ali Sfaxi, and Solange Ghernaoui-Hélie</i>	

Availability Constraints for Avionic Data Buses _____	124
<i>Alban Gabillon and Laurent Gallon</i>	

Session 5: Security as Quality of Service

Securing DNS Services through System Self Cleansing and Hardware Enhancements _____	132
<i>Yih Huang, David Arsenaault, and Arun Sood</i>	

Personalized Security for E-Services _____	140
<i>George Yee</i>	

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

Towards a Stochastic Model for Integrated Security and Dependability Evaluation _____	156
<i>Karin Sallhammar, Bjarne Helvik, and Svein Knapskog</i>	

Session 6: Networking and Fault Tolerance

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

Sandboxing in myKlaim _____	174
<i>René Rydhof Hansen, Christian W. Probst, and Flemming Nielson</i>	

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

Proxy Oblivious Transfer Protocol _____	190
<i>Yao Gang and Feng Dengguo</i>	

Session 7: Identification and Authentication

Providing Response Identity and Authentication in IP Telephony _____	198
<i>Feng Cao and Cullen Jennings</i>	

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

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-Bouahia, 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 Seviara

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 Plöbfl, 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 Frohofer, 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-Escó, 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
Davronzhon 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 Biffel

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 Environment:
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 Durrresi, 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
Luis 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
<i>Alfonso Rodriguez, Eduardo Fernández-Medina, and Mario Piattini</i>	
Representing Levels of Abstraction to Facilitate the Secure Multidimensional Modeling _____	678
<i>Rodolfo Villarroel, Emilio Soler, Eduardo Fernández-Medina, Juan Trujillo, and Mario Piattini</i>	
Modeling Permissions in a (U/X)ML World _____	685
<i>Muhammad Alam, Ruth Breu, and Michael Hafner</i>	

Session 9: Safety and Security

Application of the Digraph Method in System Fault Diagnostics _____	693
<i>Emma Kelly and Lisa Bartlett</i>	
No Risk is Unsafe: Simulated Results on Dependability of Complementary Currencies _____	701
<i>Kenji Saito, Eiichi Morino, and Jun Murai</i>	

Session 10: E-commerce and E-Government

A Reference Model for Authentication and Authorisation Infrastructures Respecting Privacy and Flexibility in b2c eCommerce _____	709
<i>Christian Schläger, Thomas Nowey, and Jose A. Montenegro</i>	
Achieving Fairness and Timeliness in a Previous Electronic Contract Signing Protocol _____	717
<i>Magdalena Payeras-Capellà, Josep Lluís Ferrer-Gomila, and Llorenç Huguet-Rotger</i>	
Digital Signatures with Familiar Appearance for e-Government Documents: <i>Authentic PDF</i> _____	723
<i>Thomas Neubauer, Edgar Weippl, and Stefan Biffi</i>	

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
<i>Barbara Emmert and Andreas Binzenhöfer</i>	
Replication Strategies for Reliable Decentralised Storage _____	740
<i>Matthew Leslie, Jim Davies, and Todd Huffman</i>	

Session 2: Security

Multipath Key Exchange on P2P Networks _____	748
<i>Yuuki Takano, Naoki Isozaki, and Yoichi Shimoda</i>	
Defending the Sybil Attack in P2P Networks: Taxonomy, Challenges, and a Proposal for Self-Registration _____	756
<i>Jochen Dinger and Hannes Hartenstein</i>	

Session 3: Social Front

Fair Trading of Information: A Proposal for the Economics of Peer-to-Peer Systems _____	764
<i>Kenji Saito, Eiichi Morino, and Jun Murai</i>	
Ecosystem of Naming Systems: Discussions on a Framework to Induce Smart Space Naming Systems Development _____	772
<i>Yusuke Doi, Shirou Wakayama, Masahiro Ishiyama, Satoshi Ozaki, Tomohiro Ishihara, and Yojiro Uo</i>	
Deriving Ratings through Social Network Structures _____	779
<i>Omer Rana, Hameeda Alshabib, and Ali ShaikhAli</i>	

Workshop on Bayesian Networks in Dependability (BND2006)

Bayesian Networks Implementation of the Dempster Shafer Theory to Model Reliability Uncertainty _____	788
<i>Christophe Simon and Philippe Weber</i>	
Multi-Agent Causal Models for Dependability Analysis _____	794
<i>Sam Maes and Philippe Leray</i>	
Computing Multiple Diagnoses in Large Devices Using Bayesian Networks _____	799
<i>Véronique Delcroix, Mohamed-Amine Maalej, and Sylvain Piechowiak</i>	
Automatically Translating Dynamic Fault Trees into Dynamic Bayesian Networks by Means of a Software Tool _____	804
<i>Stefania Montani, Luigi Portinale, Andrea Bobbio, and Daniele Codetta-Raiteri</i>	
Modelling the Reliability of Search and Rescue Operations within the UK through Bayesian Belief Networks _____	810
<i>Ashley Russell, John Quigley, and Robert van der Meer</i>	
Modelling Dependable Systems Using Hybrid Bayesian Networks _____	817
<i>Martin Neil, Manesh Tailor, David Marquez, Norman Fenton, and Peter Hearty</i>	

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

An Architecture for Service Discovery Based on Capability Matching _____	824
<i>Jaka Močnik and Piotr Karwaczynski</i>	
A Declarative Control Language for Dependable XML Message Queues _____	832
<i>Alexander Böhm, Carl-Christian Kanne, and Guido Moerkotte</i>	
Timed Modelling and Analysis in Web Service Compositions _____	840
<i>Raman Kazhamiakin, Paritosh Pandya, and Marco Pistore</i>	
Web Service Discovery, Replication, and Synchronization in Ad-Hoc Networks _____	847
<i>Lukasz Juszczuk, Jaroslaw Lazowski, and Schahram Dustdar</i>	
Evaluating Certification Protocols in the Partial Database State Machine _____	855
<i>António Sousa, Alfrânio Correia Jr, Francisco Moura, José Pereira, and Rui Oliveira</i>	

Workshop: Security in E-Learning (SEL)

A Secure E-Exam Management System _____	864
<i>Jordi Castellà-Roca, Jordi Herrera-Joancomarti, and Aleix Dorca-Josa</i>	
Intra-Application Partitioning in an eLearning Environment — A Discussion of Critical Aspects _____	872
<i>Elke Franz and Katrin Borcea-Pfzmann</i>	
Access Control in a Privacy-Aware eLearning Environment _____	879
<i>Elke Franz, Hagen Wähg, Alexander Boettcher, and Katrin Borcea-Pfzmann</i>	
Adding Security to a Multiagent Learning Platform _____	887
<i>Carine Webber, Maria de Fátima W. do Prado Lima, Marcos E. Casa, and Alexandre M. Ribeiro</i>	
Unlocking Repositories: Federated Security Solution for Attribute and Policy Based Access to Repositories via Web Services _____	895
<i>Marek Hatala, Ty Mey (Timmy) Eap, and Ashok Shah</i>	

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

Offline Internet Banking Fraud Detection _____	904
<i>Vasilis Aggelis</i>	
Practical Approaches for Analysis, Visualization and Destabilizing Terrorist Networks _____	906
<i>Nasrullah Memon and Henrik Legind Larsen</i>	
Representing Security and Audit Rules for Data Warehouses at The Logical Level by Using the Common Warehouse Metamodel _____	914
<i>Emilio Soler, Juan Trujillo, Rodolfo Villaroel, Eduardo Fernández-Medina, and Mario Piattini</i>	
A 2 ^d -Tree-Based Blocking Method for Microaggregating Very Large Data Sets _____	922
<i>Agusti Solanas, Antoni Martínez-Ballesté, Josep Domingo-Ferrer, and Josep M. Mateo-Sanz</i>	
Using a Bayesian Averaging Model for Estimating the Reliability of Decisions in Multimodal Biometrics _____	929
<i>Vitaly Schetin and Carsten Maple</i>	
On Efficiency and Data Privacy Level of Association Rules Mining Algorithms within Parallel Spatial Data Warehouse _____	936
<i>Marcin Gorawski and Karol Stachurski</i>	
Dependability in Data Mining: A Perspective from the Cost of Making Decisions _____	944
<i>H. Michael Chung</i>	

Workshop on Bioinformatics and Security (BIOS 06)

Grid Infrastructures for Secure Access to and Use of Bioinformatics Data: Experiences from the BRIDGES Project _____	950
<i>Richard Sinnott, M. Bayer, A. Stell, and J. Koetsier</i>	
The Usability and Practicality of Biometric Authentication in the Workplace _____	958
<i>Carsten Maple and Peter Norrington</i>	
Building an Encrypted File System on the EGEE Grid: Application to Protein Sequence Analysis _____	965
<i>Christophe Blanchet, G. Deléage, and R. Mollon</i>	

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. Lambrinouidakis, 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 Biffel, 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 Wisconsin Milwaukee, USA
Pierpaolo Degano, Università di Pisa, 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 Rosnagel, 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 Universität und Occ'm Software, 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 Orłowska, 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, Macquarie 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

Jernal 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 eNetherlands, The Netherlands
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 Tor Vergata, 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

Security Requirement with a UML 2.0 Profile

Alfonso Rodríguez

*Departamento de Auditoría e
Informática,
Universidad del Bío Bío,
La Castilla S/N,
Chillán
Chile*
alfonso@ubiobio.cl

Eduardo Fernández-Medina, Mario Piattini

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

Abstract

Business processes are important for companies because they allow us to obtain an advanced marketplace position, and then, these enterprises can optimize and assure the quality of their products and services. Moreover, business processes are important for software developers, because they can capture from them the necessary requirements for software design and creation. At the same time, organizations have been opened and this implies more vulnerability. In spite of all these facts, security is an aspect that has been scarcely dealt with in the business process modeling. In this paper, we summarize our UML 2.0 profile for secure business process modeling through activity diagrams, and we apply this approach to a typical health-care business process.

1. Introduction

Business Processes are considered to be the key point of paradigms as important as BPR (Business Process Reengineering) [1] and BPM (Business Process Management) [2] in the field of business and management. Business Processes are defined as a set of procedures or activities which collectively pursue a business objective or policy goal [3]. Business processes are a good answer to the environment complexity, the speed required by new products and the growing number of involved actors in the activities of the organization.

The introduction of electronic commerce, with the intensive use of communications and information technologies, implies that enterprises not only expand their businesses but also increase their vulnerability.

As a consequence, with the increase of the number of attacks on systems, it is highly probable that sooner or later an intrusion can be successful [4]. This security violation causes losses. For this reason, it is necessary to protect computers and their systems in the best possible way. Best possible security does not necessarily mean absolute security, but a reasonably high security level in relation to the given limitations [5].

The notion of security is often neglected in business process models, which usually concentrate on modeling the process in a way that functional correctness can be shown [6] mainly due to the fact that the expert in the business process domain is not an expert in security [7]. On the other hand, most requirements engineers are not trained at all in security, and the few that have been trained have only been given an overview of security architectural mechanisms such as passwords and encryption rather than a proper training in actual security requirements [8].

For business process modeling, there are several languages and notations [9]. However, BPMN (Business Process Modeling Notation) and UML (Unified Modeling Language) are considered the main standards [10].

The most important change of UML 2.0 version with respect to the previous ones has been that of the activity diagrams which improve the business process representation. Our work considers a UML 2.0 profile that allows us to incorporate security requirements into activity diagrams from the perspective of the business analyst. This will make it possible to perform independent specifications of the implementation, thus

favouring the use of MOF (Meta Object Facility) and MDA (Model Driven Architecture).

The remainder of this paper is structured as follows. Section 2 briefly summarizes the background and related works, section 3 shows the most important aspects of UML 2.0 activity diagrams. In section 4 we will propose a UML 2.0 profile to represent security requirements from the business analyst's perspective. In section 5, we present an example to show our proposal and in section 6 our conclusion is drawn.

2. Background and Related Work

In spite of the importance of security for business processes, we have found out two problems. The first one is that modeling has not been adequate since, generally, those who specify security requirements are requirements engineers that have accidentally tended to use architecture specific restrictions instead of security requirements [8]. And in the second place, security has been integrated into an application in an ad-hoc manner, often during the actual implementation process [6], during the system administration phase [11] or it has been considered like outsourcing [12].

A way to model security considering several perspectives is presented in [7]. Authors take into consideration the following perspectives: *static*, about the processed information security, *functional*, from the viewpoint of the system processes, *dynamic*, about the security requirements from the life cycle of the objects involved in the business process, *organizational*, used to relate responsibilities to acting parties within the business process and the *business processes* perspective, that provides us with an integrated view of all perspectives with a high degree of abstraction.

On the other hand, functional security requirements tend to vary depending on the kind of application. This cannot be said about security requirements since any application at the highest level of abstraction will tend to have the same basic kinds of valuable and potentially vulnerable assets [13].

The research works related to security specifications carried out by business domain experts are; (i) scarce [6, 7, 14], (ii) oriented to transaction security [15], (iii) directly oriented to information systems in general [16] or (iv) thought for security and software engineers. [12]. And research works related to UML 2.0 extensions and business processes refer to aspects of the business such as Customer, kind of Business Process, Goal, Deliverable and Measure [17], Data Warehouse and its relation to business process dynamic structures [18] or they add semantics to the activities considering organizational aspects that allow

us to express resource restrictions during the execution of an activity [19].

We have previously presented an approach for integrating security requirements into business process modeling through the BPMN (Business Process Modeling Notation) [20]. There were considered security requirements significant for the business analysts and having a clear meaning for security experts. But unfortunately, BPMN is not much used in the business process research community. In addition, the last UML version, improve the representation the business process.

3. UML 2.0 Activity Diagrams

Activity diagrams are the UML 2.0 elements used to represent business processes and workflows [19, 21]. In UML previous versions, expressivity was limited and this fact confused users that did not use the orientation to objects as an approach for modeling. Now, it is possible to support flow modeling across a wide variety of domains [22]. Activities are redesigned to use a Petri-like semantics instead of state machines. Among other benefits, this widens the number of flows that can be modeled, especially those that have parallel flows [23].

UML 2.0 is divided into structural and behavioral specifications, that is, models of the static and dynamic aspects of a system. Behavior models specify how the structural aspects of a system change over time. UML has three behavior models: activities, state machines, and interactions. Activities focus on the sequence, conditions, and inputs and outputs for invoking other behaviors, state machines show how events cause changes of object state and invoke other behaviors, and interactions describe message-passing between objects that causes invocation of other behaviors [24].

An activity specifies the coordination of executions of subordinate behaviors, using a control and data flow model. The subordinate behaviors coordinated by these models may be initiated for several reasons. Firstly, they can be initiated because other behaviors in the model finish executing; in the second place, due to the fact that, objects and data become available, or finally, because there are events that occur external to the flow. The flow of execution is modeled as activity nodes connected by activity edges. A node can be the execution of a subordinate behavior, such as an arithmetic computation, a call to an operation, or manipulation of object contents. Activity nodes also include flow of control constructs, such as synchronization, decision, and concurrency control. Activities may form invocation hierarchies invoking other activities, ultimately resolving to individual

actions [23]. The graphical notation of an activity is a combination of nodes and connectors that allow us to form a complete flow. A complete explanation can be found in [22-28].

4. UML 2.0 profile for the modeling of secure business process

The Profiles package contains mechanisms that allow meta-classes from existing meta-models to be extended to adapt them for different purposes. This includes the ability to tailor the UML meta-model for different platforms (such as J2EE or .NET) or domains (such as real-time or business process modeling). The profiles mechanism is consistent with the OMG Meta Object Facility (MOF) [23].

UML profiles consist of *Stereotypes*, *Constraints* and *Tagged Values*. A *stereotype* is a model element defined by its name and by the base class which it is assigned to. *Constraints* are applied to the stereotype with the purpose of indicating limitations (e.g. pre or post conditions, invariants). They can be expressed in natural language, programming language or through OCL (Object Constraint Language). *Tagged values* are additional meta-attributes assigned to a stereotype, specified as name-value pairs.

Our proposal allows business analysts to specify security requirements in the business process through activity diagrams. Later on, these requirements will be transformed, by the security experts, into technical specifications that including details necessary for their implementation. In this paper, we will only study the first part. Figure 1 shows the definition of stereotypes.

The main stereotype «*ActivitySecurityElement*» is an abstract class created from *Element* (from *Kernel*) to contain security specifications of security auditing and

security requirements type (see Table 2). The stereotype «*ActivitySecurityElement*» has not a specific notation since it will be defined in the subclasses. It has a composition relationship with the *Activity* class and an association with *ActivityGroup*, *ActivityNode* and *ActivityEdge* classes (see Figure 2).

The «*ActivitySecurityRequirement*» stereotype has been extended with the «*SecurityAuditing*» and «*SecurityRequirement*» stereotypes (see Table 2). «*SecurityAuditing*» and «*SecurityRequirement*» specifications are related. This means that «*SecurityAuditing*» can only be specified if any of the «*SecurityRequirement*» subclasses has been specified. However, «*SecurityRequirement*» subclasses can be specified without «*SecurityAuditing*» specification.

The security requirements derived from the «*SecurityRequirement*» stereotype (See Table 3) will complement the proposed notation by adding it letters that will allow us to identify the type of requirement that is specified. Any of the security requirements derived from «*SecurityRequirement*» can be specified in a complementary way, that is, any of them can be specified for an element of an *Activity Diagram*.

Tagged Values for the stereotypes derived from «*SecurityRequirement*» have not been specified. However, it is possible to add as *Comment* an abstract level of representation of the criticality of this requirement using the concept high/medium/low.

Table 1 shows the security requirements, obtained from the taxonomy proposed in [13], which have been represented in specifications of our profile and in the activity diagram elements on which they can be applied.

Table 1: Security Requirements and Activity Diagram Elements

Security Requirements	UML 2.0 element for containment in activity diagrams						
	ActivityGroup			ActivityNode		ActivityEdge	
	Activity	Activity Partition	Interruptible Activity Region	Action	Data Store	Control Flow	Object Flow
Access Control	✓	✓	✓				
Attack/Harm Detection	✓	✓	✓	✓			✓
Integrity		✓	✓		✓		✓
Nonrepudiation						✓	
Privacy		✓					

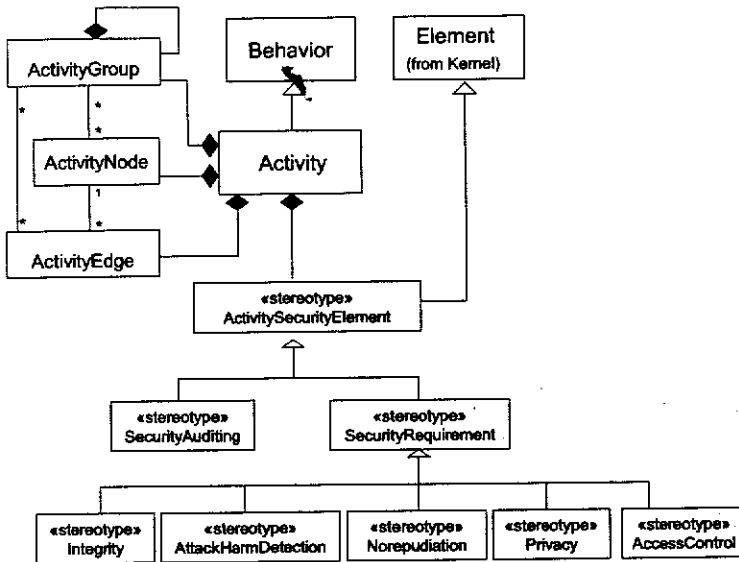


Figure 1. Stereotype for security elements

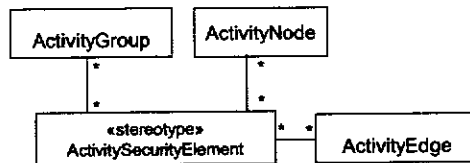


Figure 2. Association relation for «ActivitySecurityElement»

Table 2. Description of «ActivitySecurityElement» class and subclasses








Name	ActivitySecurityElement	
Base Class	Element (from Kernel)	
Description	Abstract class containing audit specifications and security requirements	
Name	SecurityAuditing	Notation 
Base Class	ActivitySecurityElement	
Description	Element related to the business process security specification. It is used to indicate that it is necessary to register the security events with the purpose of them to be audited later on.	
Constrains	It is valid only if it is specified at least one SecurityRequirement. It can be complemented with Comment	
Name	SecurityRequirement	Notation 
Base Class	ActivitySecurityElement	
Description	It can contain business process security requirements specifications. It must be specialized to indicate the required security type.	
Constrains	It must be specified in some of its specializations that this element has to be according to Table 1 restrictions.	

Table 3. «SecurityRequirement» Subclasses

Name	Integrity	Notation 
Base Class	SecurityRequirement	
Description	It establishes the degree of protection of intentional and non authorized corruption for components (data, hardware, personnel, and/or software)	
Constrains	It can only be specified in the diagram elements indicated in Table 1.	
Name	AccessControl	Notation 
Base Class	SecurityRequirement	
Description	It establishes the need to define and/or intensify the access control mechanisms to restrict access to certain components in an activity diagram.	
Constrains	It can only be specified in the diagram elements indicated in Table 1.	
Name	Nonrepudiation	Notation 
Base Class	SecurityRequirement	
Description	It establishes the need to avoid the denial of any aspect of the interaction.	
Constrains	It can only be specified in the diagram elements indicated in Table 1.	
Name	Privacy	Notation 
Base Class	SecurityRequirement	
Description	It indicates the degree to which non authorized parts are avoided to obtain sensitive information.	
Constrains	It can only be specified in the diagram elements indicated in Table 1.	
Name	AttackHarmDetection	Notation 
Base Class	SecurityRequirement	
Description	It indicates the degree to which the attempt or success of attacks or damages is detected, registered and notified.	
Constrains	It can only be specified in the diagram elements indicated in Table 1.	

5. Example

Our illustrative example (see Figure 3) describes a typical business process for the admission of patients in a health-care institution. In this example, the business analyst identified the following Activity Partition: *Patient* (individual who receives medical care and who must fill out an admission request), *Administration Area* (which is a top partition that is divided in two middle partitions), where the Medical

Institution records details about costs and insurances, and finally, the *Medical Area* (divided into *Medical Evaluation* and *Exams*) where pre-admission tests, exams, evaluations and complete clinical data collecting are carried out.

Security requirements are included in this business process. The business analyst has considered many aspects of security. These requirements will be considered in the next step when the business process transformed into most concrete models.

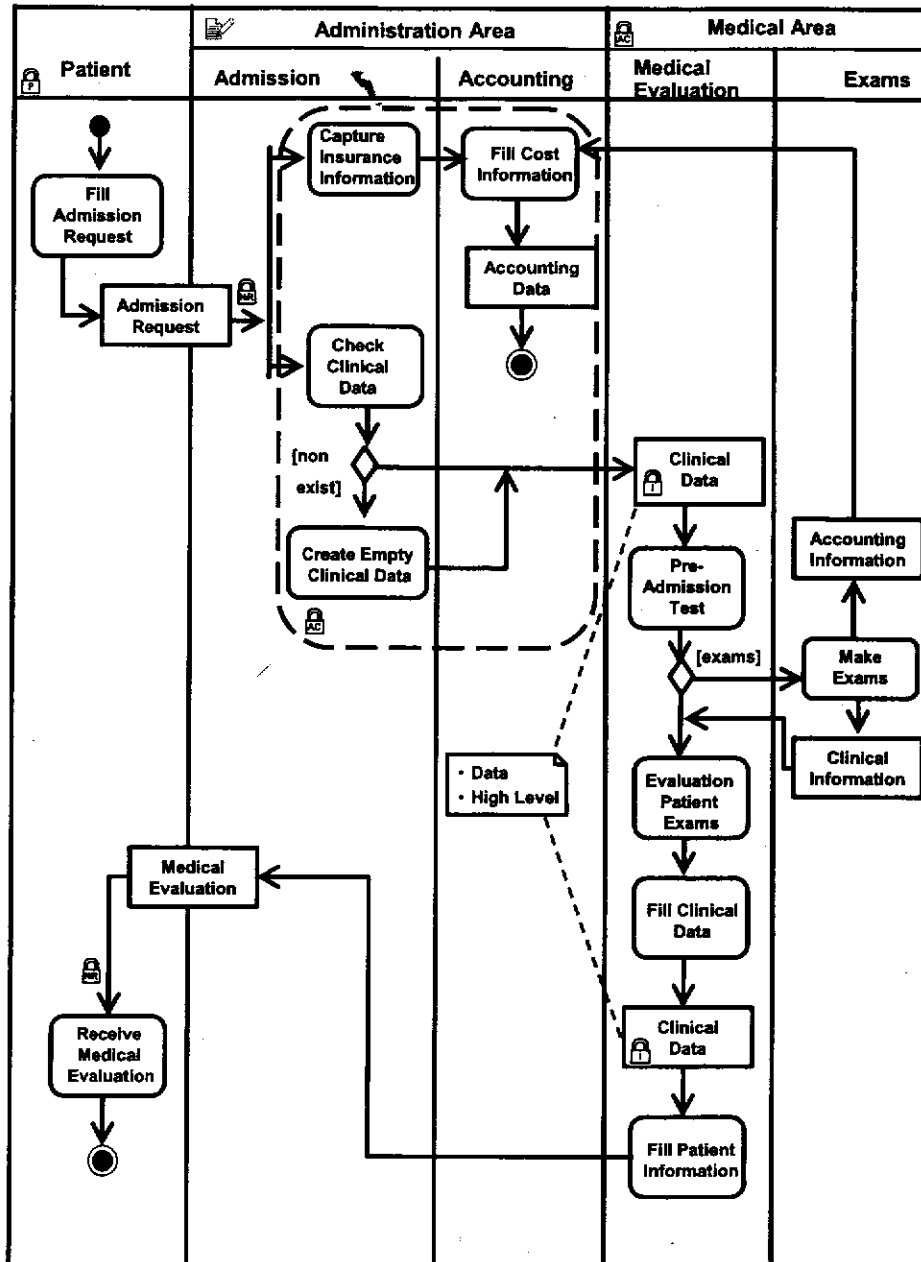


Figure 3. Business Process: Admission of Patients in a Medical Institution

The business analyst has specified «Privacy» over the Activity Partition "Patient", with the aim of prevent the disclosure of sensitive information about the Patient. «Nonrepudiation» has been defined over the control flow that goes from the action "Fill Admission Request" to the actions "Capture Insurance Information" and "Check Clinical Data" with the aim of avoiding the denial of the "Admission Request" reception. Non Repudiation

has been defined also over the control flow between Actions "Fill Patient Information" and "Receive Medical Evaluation". «AccessControl» has been defined over the Interruptible Activity Region. This specification involves all activities; that are, "Capture Insurance Information", "Check Clinical Data" and "Fill Cost Information". Acces Control has been also specified over the Activity Partition "Medical Area" which implies that Access Control is applicable to all

its Activity Partitions which are "Medical Evaluation" and "Exams", and also over all Actions. Moreover, «Integrity» has been assigned to the Data Store "Clinical Data". This specification is over the data with high protection degree. Finally, «Security Auditing» has been specified over the "Administration Area". Its to mean that all the security events defined into the Activity Partition must be register for future security auditing

In spite of the fact that security requirements must have a concrete expression in the business process implementation, we think that this is a first stage that should be defined.

6. Conclusions and Ongoing Work

The strong relationship between companies performance and the quality of their business processes make companies to pay more attention to the way in which business processes are modeled. At the same time, modeling languages have been improved and nowadays, they allow us to capture the essence of the business more precisely. However, security is a business aspect that has not been very studied in the business process modeling. Generally, the process itself together with its technological implementation have been privileged. In this paper, we have presented a UML 2.0 extension that allows us to incorporate security requirements into the business process modeling, thus increasing the expressive ability of activity diagrams. The next step should be that of applying a MDA approach to transform the model (including the security requirements) to most concrete models (i.e. execution models). Therefore, future work must be oriented to enrich the security requirements specifications, improving the UML profile specification to complement it with Well-Formedness Rules and OCL. In addition, it will be necessary to incorporate the viewpoint of the security expert into security requirements specifications in order to make implementation possible.

Acknowledgements

This research is part of the following projects: DIMENSIONS (PBC-05-012-1), supported by FEDER and the "Consejería de Ciencia y Tecnología de la Junta de Comunidades de Castilla-La Mancha", Competisoft (granted by CYTED) and RETISTIC (TIC2002-12487-E) granted by the "Dirección General de Investigación del Ministerio de Ciencia y Tecnología" (Spain).

References

- [1] D. Grant, "A wider view of business process reengineering", *Communications of the ACM (CACM)*, Vol. 45 (2), pp. 85-90, 2002.
- [2] W.M.P. van der Aalst, A. H. M. t. Hofstede, and M. Weske, "Business Process Management: A Survey", presented at International Conference on Business Process Management (BPM 2003), Eindhoven, The Netherlands., 2003.
- [3] WfMC, "Workflow Management Coalition: Terminology & Glossary." 1999.
- [4] G. Quirchmayr, "Survivability and Business Continuity Management", presented at ACSW Frontiers 2004 Workshops., Dunedin, New Zealand, 2004.
- [5] A. Zuccato, "Holistic security requirement engineering for electronic commerce", *Computers & Security*, Vol. 23 (1), pp. 63-76, 2004.
- [6] M. Backes, B. Pfitzmann, and M. Waider, "Security in Business Process Engineering", presented at International Conference on Business Process Management, Eindhoven, The Netherlands., 2003.
- [7] G. Herrmann and G. Pernul, "Viewing Business Process Security from Different Perspectives", presented at 11th International Bled Electronic Commerce Conference "Electronic Commerce in the Information Society". Slovenia., 1998.
- [8] D. Firesmith, "Engineering Security Requirements", *Journal of Object Technology*, Vol. 2 (1), January-February, pp. 53-68, 2003.
- [9] G. M. Giaglis, "A Taxonomy of Business Process Modelling and Information Systems Modelling Techniques", *International Journal of Flexible Manufacturing Systems*, Vol. 13 (2), pp. 209-228, 2001.
- [10] Mega, "Business process Modeling and Standardization," 2004.
- [11] T. Lodderstedt, D. Basin, and J. Doser, "SecureUML: A UML-Based Modeling Language for Model-Driven Security", presented at UML 2002 - The Unified Modeling Language, 5th International Conference., Dresden, Germany., 2002.
- [12] A. Maña, D. Ray, F. Sánchez, and M. I. Yagüe, "Integrando la Ingeniería de Seguridad en un Proceso de Ingeniería Software", presented at Actas de la VIII Reunión Española de Criptología y Seguridad de la Información, RECSI'04, Leganés, Madrid. España, 2004.

- [13] D. Firesmith, "Specifying Reusable Security Requirements", *Journal of Object Technology*, Vol. 3 (1), January-February., pp. 61-75, 2004.
- [14] A. Maña, J. A. Montenegro, C. Rudolph, and J. L. Vivas, "A business process-driven approach to security engineering", presented at 14th. International Workshop on Database and Expert Systems Applications (DEXA). Prague, Czech Republic., 2003.
- [15] A. W. Röhm, G. Herrmann, and G. Pernul, "A Language for Modelling Secure Business Transactions", presented at 15th. Annual Computer Security Applications Conference., Phoenix, Arizona., 1999.
- [16] T. Tryfonas and E. A. Kiountouzis, "Perceptions of Security Contributing to the Implementation of Secure IS", presented at Security and Privacy in the Age of Uncertainty, IFIP TC11 18th International Conference on Information Security (SEC2003), Athens, Greece., 2003.
- [17] B. List and B. Korherr, "A UML 2 Profile for Business Process Modelling", presented at 1st International Workshop on Best Practices of UML (BP-UML 2005) at the 24th International Conference on Conceptual Modeling (ER 2005), Klagenfurt, Austria, 2005.
- [18] V. Stefanov, B. List, and B. Korherr, "Extending UML 2 Activity Diagrams with Business Intelligence Objects", presented at 7th International Conference on Data Warehousing and Knowledge Discovery (DaWaK2005), Copenhagen, Denmark, 2005.
- [19] A. Kalnins, J. Barzdins, and E. Celms, "UML Business Modeling Profile", presented at Thirteenth International Conference on Information Systems Development, Advances in Theory, Practice and Education, Vilnius, Lithuania, 2004.
- [20] A. Rodriguez, E. Fernández-Medina, and M. Piattini, "Towards an integration of Security Requirements into Business Process Modeling", presented at Proceedings of the Third International Workshop on Security In Information Systems, WOSIS 2005, In conjunction with ICEIS 2005, Miami, USA, 2005.
- [21] H. Podeswa, *B.O.O.M.: Business Object-Oriented Modeling for Business Analysts*, 2005.
- [22] C. Bock, "UML 2 Activity and Action Models", *Journal of Object Technology*, Vol. 2 (4), July-August, pp. 43-53, 2003.
- [23] Object Management Group, "Unified Modeling Language: Superstructure," version 2.0, formal/05-07-04, 2005.
- [24] C. Bock, "UML 2 Activity and Action Models, Part 2: Actions", *Journal of Object Technology*, Vol. 2 (5), September-October, pp. 41-56, 2003.
- [25] C. Bock, "UML 2 Activity and Action Models, Part 3: Control Nodes", *Journal of Object Technology*, Vol. 2 (6), November-December, pp. 7-23, 2003.
- [26] C. Bock, "UML 2 Activity and Action Models, Part 4: Object Nodes", *Journal of Object Technology*, Vol. 3 (1), January-February, pp. 27-41, 2004.
- [27] C. Bock, "UML 2 Activity and Action Models, Part 5: Partitions", *Journal of Object Technology*, Vol. 3 (7), July-August, pp. 37-56, 2004.
- [28] C. Bock, "UML 2 Activity and Action Models, Part 6: Structured Activities", *Journal of Object Technology*, Vol. 4 (4), May-June, pp. 43-66, 2005.