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

Proceedings

The First International Conference on Availability, Reliability and Security

ARES 2006

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
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
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
Alfonso Rodríguez, 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-Joancomarti, 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

Representing security and audit rules for data warehouses at the logical level by using the Common Warehouse Metamodel

Emilio Soler[1], Rodolfo Villarroel[2], Juan Trujillo[3], Eduardo Fernández-Medina[4] and Mario Piattini[4]
(1) Departamento de Informática. Universidad de Matanzas (Cuba)
Autopista de Varadero km 3. Matanzas. Cuba.
emilio.soler@umcc.cu
(2) Departamento de Computación e Informática. Universidad Católica del Maule (Chile)
Avenida San Miguel 3605 Talca (Chile)
rvillar@spock.ucm.cl
(3) Departamento de Lenguajes y Sistemas Informáticos. Universidad de Alicante (Spain)
C/ San Vicente S/N 03690 Alicante (Spain)
jtrujillo@dlsi.ua.es
(4) Departamento de Informática. Universidad de Castilla-La Mancha (Spain)
Paeso de la Universidad, 4-13071 Ciudad Real (Spain)
{mario.piattini, eduardo.fdzmedina}@uclm.es

Abstract

Data warehouses (DWs) contained high sensitive data, and therefore, it is essential to specify security measures from the early stages of the DW design and enforce them. Access control models for transactional (relational) databases, based on tables, columns and rows, are not appropriate for DWs. Instead, security and audit rules defined for DWs must be specified based on the multidimensional (MD) modeling used to design data warehouses. So far, very few approaches represent security measures in the conceptual modeling of data warehouses form the early stages of a DW project. Moreover, these security measures cannot be directly represented in the relational model for data warehouses, thereby having a semantic gap between the conceptual and logical schemas. In this paper, we present an extension of the relational model to consider security and audit measures represented in the conceptual modeling. To accomplish this, we based on the Relational Package of the Common Warehouse Metamodel (CWM) and extend it to properly represent all security and audit rules defined in the conceptual modelling of data warehouses. Finally, to show the benefit of our approach, we apply our proposal to a health care case study.

1. Introduction

Data Warehouses (DW), Multidimensional (MD) Databases, and On-Line Analytical Processing (OLAP) applications are used in conjunction to form a highly powerful mechanism for discovering crucial business information in strategic decision-making processes.

MD modeling is the foundation of DWs, MD databases and OLAP applications. Sometimes MD models also store information regarding private or personal aspects of individuals, such as identification data, medical data or even religious beliefs or ideologies. In the past few years, various approaches have been proposed for representing the main multidimensional (MD) properties at the conceptual level [3, 4, 7, 8, 17, 18]. Nevertheless, these models do not consider the design of secure MD models for DW. Actually, the Unified Modeling Language (UML) [5] has been widely accepted as the standard object-oriented (OO) modeling language for modeling various aspects of software systems. In [6] the authors presented an approach, based on the UML, to represent main access control and audit rules in the conceptual modeling of data warehouses from the very early stages of a data warehouse project and enforce them in the further design steps.

The standard OMG (Object Management Group) [15] promotes the theory and practice of object-

0-7695-2567-9/06 $20.00 © 2006 IEEE

oriented technology in software development, based on the four-layer metamodel architecture. A model at one layer is used to specify models in the layer above. The four layers are M0 (instances), M1 (system modeling), M2 (metamodeling) and M3 (meta-metamodeling). The metamodel of the UML [5] belongs to M2 layer, from this layer, we can build UML models in the M1 layer, and lately, the UML model instances (i.e. objects) belong to M0 layer. The four-layer architecture is shown in figure 1.

Meta-level	MOF Terms	Examples
M3	meta-metamodel	The MOF model
M2	Metamodel, metametadata	UML metamodel, CWM metamodel
M1	Model, metadata	UML models, CWM metadata
M0	object, data	Modeled systems, warehouse data.

Figure 1. The four-layer architecture of OMG

An extension of UML 2.0/OCL profile is presented in [19], which corresponds with a metamodel that allows us to represent the main security and audit measures in the conceptual modeling of data warehouses. According to the four-layer architecture of the OMG, this extended metamodel belongs to the M2 layer and their instances, i.e. secure DW conceptual model belongs to the M1 layer.

There are some proposals to extend security aspects in databases. In [1], authors, inspired by the privacy tenet of the Hippocratic Oath, proposed that the databases that include privacy as a central concern be called Hippocratic databases. Based on this idea, an auditing framework offering efficient methods for managing, auditing, and transmitting electronic health data in a manner that preserves the privacy of individual patients is proposed in [2]. This technology operates as a middleware layer between the database and enterprise applications, although it does not provide a metamodel nor represents secure properties modelled at the conceptual level. Databases in general is out of our goal as we based our proposal in Data Warehouses in order to represent all required security and audit rules in the conceptual modeling of DWs.

The previous work presented in [12] introduced a Model Driven Architecture (MDA) oriented framework for the DW development, choosing the ROLAP (Relational OnLine Analitical Processing) like DBMS and the Platform Specific Model (PSM) is modeled by using the relational metamodel from the CWM [16]. However, none security and audit measures can be modeled in this metamodel, and for that reason, we focus this paper on an extension of the relational model of CWM to consider security and audit rules represented in the conceptual modeling phase. We state that is out of the scope of this paper establish the framework MDA [14] for defining transformations between the considered metamodels.

The rest of this paper is structured as follows. Section 2 presents the main aspects related to secure multidimensional modeling. An extension of the relational metamodel of CWM is presented in section 3. Section 4 presents a health case study and applies our extension for represent at logical level, all security and audit rules defined in the conceptual modeling. Finally, section 5 presents the main conclusions and sketches the immediate future work.

2. Secure Multidimensional Modeling

The main properties of the multidimensional modeling are represented by a UML profile [11], which is based on OO conceptual modeling approach proposed in [17]. The metamodel presented in [11] has been employed in [12] to align the whole DW development process to MDA. This profile does not permit us to represent the secure aspects of the multidimensional modeling for Data Warehouses.

In [19], this previous profile is reused in order to be able to design an MD conceptual model classifying both information and users in order to represent the main security aspects in the conceptual modeling of DWs. Therefore, the profile allows us to classify the security information that will be used in our conceptual modeling of data warehouses. For each element of the model (fact class, dimension class, fact attribute, etc.), is defined its security information, specifying a sequence of security levels, a set of user compartments and a set of user roles. Security constraint is considered to specify security in attributes. The security information and these constraints indicate the security properties that users have to be able to access information. The profile is called Secure Data Warehouses (SECDW), it description is represented as a UML package.

0-7695-2567-9/06 $20.00 © 2006 IEEE

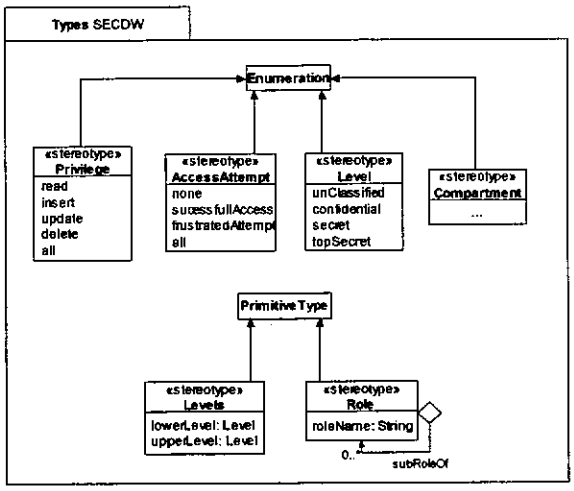

Figure 2. Values associated to new data types

In figure 2, we can observe the new data types incorporated and the values associated to each one of the necessary types. Security levels, roles and organizational compartments can be defined according to the needs of the organization. However, we have considered within the "Level" data type, the typical values associated to security levels.

The SECDW profile incorporates four types of stereotypes. We can see in figure 3 that: Secure class, secure data warehouses stereotypes and attribute

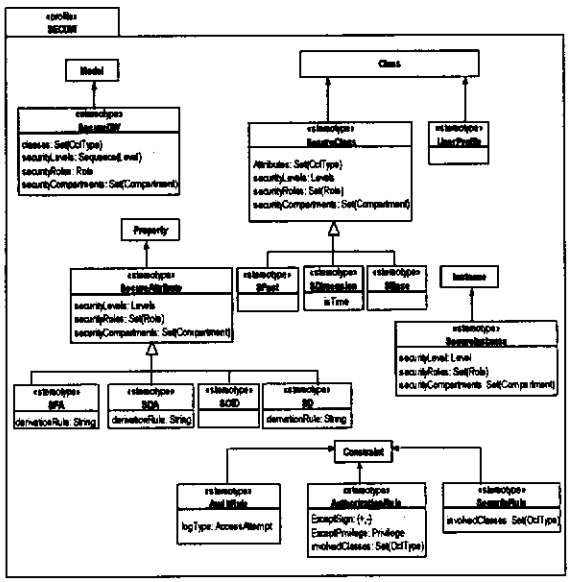

Figure 3. New stereotypes

stereotypes. For representing security constraint, there are authorization rules and audit rules and finally, user profile stereotype. We need to take into consideration that the tagged values are associated to each one of the stereotypes. For example, 'SecureDW' stereotype has the following values associated: Classes, Security Levels, SecurityRoles and SecurityCompartments.

The defined tagged values are applied to certain components that are especially particular to MD modeling, allowing us to represent them in the same model and in the same diagrams that describe the rest of the system. The tagged values will represent the sensitivity information of the different elements of the MD modeling (fact class, dimension class, base class, attributes, etc.), and they will allow us to specify security constraints depending on this security information and on the value of attributes of the model.

In order to define well-formedness rules a set of an inherent constraint are specified. The rules are grouped as follows: correct value of tagged values, security information of instances, relationship between security information of classes and their attributes, categorization of dimensions, classification hierarchies, derived attribute and combination of dimensions.

The main feature of the considered SMD modeling (Secure Multidimensional Modeling) are the many-to-many relationship relationships between facts and one specific dimension, degenerated dimensions, multiple classification and alternative path hierarchies, and the non strict and complete hierarchies. In this approach, the structural properties of MD modeling are represented by means of a UML class diagram in which the information is clearly organized into facts and dimensions. These facts and dimensions are represented by secureFact and secureDimension classes respectively.

SecureFact classes are defined as composite classes in shared aggregation relationships of n secureDimension classes. The minimum cardinality in the role of the secureDimension classes is 1 to indicate that every fact must always be related to all the dimensions. The many-to-many relationships between a secureFact and a specific secureDimension are specified by means of the cardinality 1...n in the role of the corresponding dimension class.

A secureFact is composed of measures or SecureFactAttributes. By default, all measures in the secureFact class are considered to be additive. For non-additive measures, additive rules are defined as constraints and are included in the secureFact class. Furthermore, derived measures can also be explicitly represented (indicated by /) and their derivation rules are placed between braces near the fact class. Our approach also allows the definition of identifying attributes in the secureFact class (stereotype SOID).

With respect to secureDimensions, each level of a classification hierarchy is specified by a secureBase

class. An association of secureBase classes specifies the relationship between two levels of a classification hierarchy. The only prerequisite is that these classes must define a Directed Acyclic Graph (DAG) rooted in the secureDimension class (DAG restriction is defined in the stereotype secureDimension). The DAG structure can represent both multiple and alternative path hierarchies. Every secureBase class must also contain an identifying secureAttribute OID (SOID) and a secureDescriptor attribute (SD). All constraints (AuditRule, AuthorizationRule and SecurityRule) are modeled using UML notes. The class called UserProfile will contain information of all users entitled to access to the multidimensional model.

The metamodel associated with the SECDW profile allows representing security aspect for multidimensional modeling, which belong to M2 layer in the mentioned four-layer architecture. According to [19], the security aspects secureFact, secureDimension, secureBase are represented with the same icons from classes stereotypes inherited from the

Management	Warehouse Process				Warehouse Operation		
Analysis	Transformation	OLAP		Data Mining	Information Visualization		Business Nomenclature
Resource	Object	Relational		Record	Multidimensional		XML
Foundation	Business Information		Data Types	Expressions	Keys and Indexes	Software Deployment	Type Mapping
Object Model	Core			Behavioral	Relationships		Instance

Figure 4. CWM metamodel layering and its packages

proposal stated in [13], but adding to them a letter "S", indicating that it is a secure class. All constraints (AuditRule, AuthorizationRule and SecurityRule) are modeled using UML notes. An instance of the SECDW metamodel is shown in section 4.

3. Secure Relational Modeling of Data Warehouses

In this section we outline the relational metamodel of Common Warehouse Metamodel (CWM) [16]. For representing MD models at logical level there are some proposals, depending of concrete kind of a specific DBMS (ROLAP, MOLAP or HOLAP). But, according to Kimball [9] the most common representation for MD models is on relational platforms, i.e. ROLAP systems. In the literature, we can find several proposals of relational metamodels, however, we based our approach in CWM [16], which is being accepted more and more as the standard metamodel. The main purpose of the CWM is to enable easy interchange of warehouse and business intelligence metadata between warehouse tools, warehouse platforms and warehouse metadata repositories in distributed heterogeneous environments. CWM is based on three key industry standards:

- UML - Unified Modeling Language, an OMG modeling standard.
- MOF - Meta Object Facility, an OMG metamodeling and metadata repository standard.
- XMI - XML Metadata Interchange, an OMG metadata interchange standard.

The UML standard defines a rich, object oriented modeling language that is supported by a range of graphical design tools. The MOF standard defines an extensible framework for defining models for metadata, and providing tools with programmatic interfaces to store and access metadata in a repository. The XMI standard allows metadata to be interchanged as streams or files with a standard format based on XML. CWM has been designed to conform to the "MOF model", it belong to the M2 layer metamodel, we refer the reader to figure 1 for further details on the different metamodel layers of the CWM.

In [13] the authors showed in details the organization of CWM. CWM is organized in 21 separate packages which they were grouped into five stackable layers by means of similar roles. See figure 4.

From the organization represented in figure 4, we will mainly focus our work on the Resource layer and, more precisely, on the Relational package as a relational metamodel to describe that represent metadata of relational data resources. The resource layer describes the structure of data resources that act as either sources or targets of a CWM-mediated interchange. The Relational package describes data accessible through a relational interface such as a native RDBMS, ODBC, or JDBC. The Relational package is based on the [SQL] standard section concerning RDBMS catalogs. The container Catalog,

is intended to cover all the tables a user can use in a single statement. A catalog contains schemas which themselves contain tables. Tables are made of columns which have an associated data type [16].

The Relational package defines a container Schema, which is a collection of tables. A ColumnSet represents any form of relational data. A Table is a cataloged version of a ColumnSet, which contains Columns. A ForeignKey associates columns from one table with columns of another table. PrimaryKey class

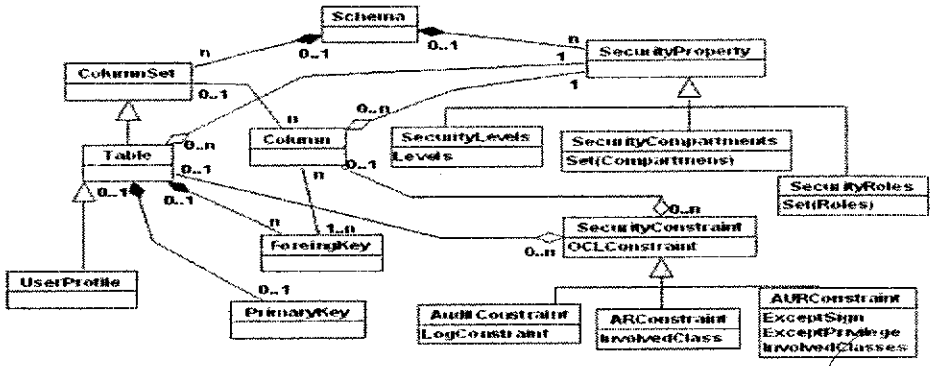

Figure 5. Secure Relational Modeling for Data Warehouse

inherits from the UniqueConstraint. PrimaryKey and ForeingKey metaclasses are owner by Table metaclass.

Is clear that every main relational property can be represented in the relational metamodel of CWM, but; nevertheless, to the best of our knowledge never this package has been employed to represent at logical level all security and audit rules defined in the conceptual modeling of data warehouse.

We only use part of the relational CWM metamodel for our purposes; which allow us to represent tables, columns, primary keys and foreign keys. However, for representing security and audit measures in the metamodel, we need to add some metaclasses. We based our extensions in assurance security at the model, table, attribute and users levels. The Schema metaclass aim the security at the model level. SecurityProperty metaclass inherit from the Constraint (from Core) metaclass and specializes as SecurityLevels, SecurityCompartments and SecurityRoles metaclasses. Furthermore, for representing security constraints, authorization rules and audit rules in the metamodel we add AUDconstraint class, ARconstraint class and AURconstraint class, which inherit from SecurityConstraint. For specify constraints depending on particular information of a user or a group of users, we introduce the userProfile metaclass. Finally, we need add associations of Table and Column metaclasses with the metaclasses introduced in order to establish security in attributes and tables. For express the constraints (AuditRule, AuthorizationRule and SecurityRule) modeled in SECDW metamodel using notes, we need to add a new attribute OCLConstraint in the SecurityConstraint metaclass.

In figure 5 we show part of the relational CWM metamodel extended. We can observe the relationships between classes. We have omitted the attributes in classes and the cardinality of the typical operations from UML to do better understood the figure. We clarify that before specifying the model, we have data and rules which come from the conceptual level. The application of the modeling technique over the dynamicity of rules and mostly at runtime is out of the scope of this paper.

The extension considered of part of the CWM relational metamodel allows us representing security and audit measures at logical level, which has been represented in the conceptual modeling of data warehouse, i.e. in SECDW metamodel. Our new metamodel will be called Secure Relational Data Warehouse (SECRDW). The container Schema is a collection of ColumnSet and SecurityProperties. A ColumnSet represents any form of relational data. A Table is a cataloged version of a ColumnSet, which contains Columns. A ForeignKey associates columns from one table with columns of another table. Primarykey class inherited from the UniqueConstraint. PrimaryKey and ForeingKey is owner by Table metaclass. The metamodel not only inherit all properties from Relational package, it also incorporate the data types showed in figure 2, from section 2. We do not consider all details in the metamodel in order to clarify it. The SECRDW metamodel belong to the M2-layer of OMG (see fig.1). An instance of the SECRDW metamodel being a part of the CWM

metadata, i.e. contains tables with columns, which may have primary and foreign key. An object table may contain some SecurityProperty(SecurityLevels,SecurityCompartments or SecurityRoles), which will be represented in the heading of the Table class. The same is valid for columns, but in this case, SecurityProperty (i.e., SecurityLevels, Security Compartments or SecurityRoles) are modeled join with the own column. Instances of SecurityContraints metaclass are modeled using notes, which may be associated with Table and Column.

When we built a model instance of the SECRDW metamodel we obtain the logical design phase. In order to convert the data gathered during the logical design phase we need a physical design process. We can choice, for example, the DBMS Oracle 9i and we will be able to obtain SQL code in an easy and straightforward way from SECRDW models. According to MDA framework [19], we can consider transformations between SECDW and SECRDW metamodels in order to establish a solution for the semantic gap between conceptual and logical schemas in the multidimensional modeling of data warehouses, but this consideration are out of the scope of this paper.

4. A case study applying the SECRDW metamodel

In this section, we apply our extension of relational metamodel of CWM in the context of a typical health-care system. We have considered a reduced example in order to focus our attention in the security and audit measures. The example is a reduced version from [19], which represents an instance of the SECMW metamodel.

Figure 6 shows us the secure multidimensional model Hospital whose patient admission is composed of a fact class named Admission, dimension classes called Diagnosis, Patient and Time, and base classes named Diagnosis_group of Patient Dimension. Additionally, in this modeling, an additional class called UserProfile is considered, that will contain information of all users entitled to access to this multidimensional model.

We have used the following security levels: Confidential, Secret and topSecret. User roles Health (including Doctor and Nurse subroles) and NonHealth (including Maintenance and Administrative subroles) have been defined. The root of this hierarchical roles tree is HospitalEmployee. In this example, we have not considered organizational compartments.

1. The security level of each instance of Admission is defined by a security constraint specified in the model. If the value of the description attribute of the Diagnosis_group to which diagnosis belongs is cancer or AIDS, the security level –tagged value SL- of this admission will be top secret, otherwise secret. This constraint is only applied if the user makes a query whose information comes from Diagnosis dimension or Diagnosis_group base classes, together with Patient dimension –tagged value involvedClasses-. Therefore, a user who has secret security level could obtain the number of patients with cancer for each city, but never if information of Patient dimension appears in the query.
2. For confidentiality reasons, we could deny access to admission information to users whose working area is different than the area of a particular admission instance. This is specified by another exception in Admission fact class, considering a condition and the tagged values involvedClasses, exceptSign.
3. The tagged value logType has been defined for Admission class, specifying the value frustratedAttempts. This stereotype specifies that the system has to record, for future audit, the situation in which a user tries to access information whose type is 'primary diagnosis' of this fact class, and so where the system denies it because of lack of permission.
4. The security level –tagged value SL- of each instance of Admission can also depend on the value of cost attribute, which indicates the price of the admission service. In this case, the constraint is only applicable to queries that contain information of the Patient dimension –tagged value involvedClasses-.
5. User can be denied access to data of patients who have been treated before the date of initial contract of the staff in the health area. This stereotype is specified with an exception in the Admission class, considering a condition and InvolvedClasses and ExceptSign tagged values.
6. Patients could be special users of the system. In this case, it could be possible that patients access their own information as patients (for instance, for querying their personal data). This constraint is specified by using the exceptSign tagged value in the Patient class.

In order to represent at logical level the model represented in figure 6, we present the logical schema for representing security and audit measures from the transformation process from a secure multidimensional model to the relational model, by using the star schema

[9]. In figure 7 we show the Data Warehouse logical schema, which represents the logical model of the DW. In order to avoid a cluttered diagram, we only display four tables, only the attributes of admission table and by means of the note from UML we represent an ARConstraint, which correspond with label number 4 in figure 6.

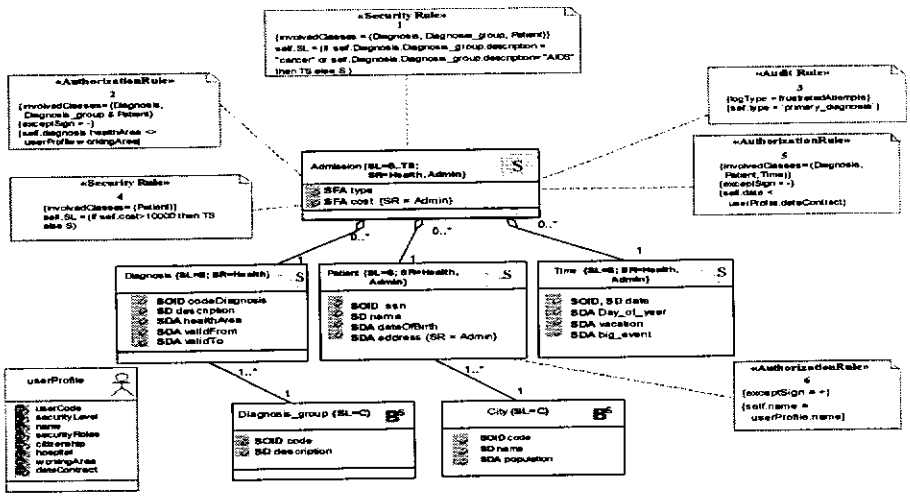

Figure 6. Example of secure multidimensional modeling

We note in figure 7 that Admission table appears with the icon of the stereotype inside the typical representation of a class in UML, whereas three tables are adorned with the stereotype <<Table>>. Admission table contain *SecurityLevels* and SecurityRoles object in its heading class. Additionally note in the SFAcost column the SecurityRole object join with it A associate note with Admission table represent an ARConstraint, note the information of OCLConstraint and involvedClass attributes.

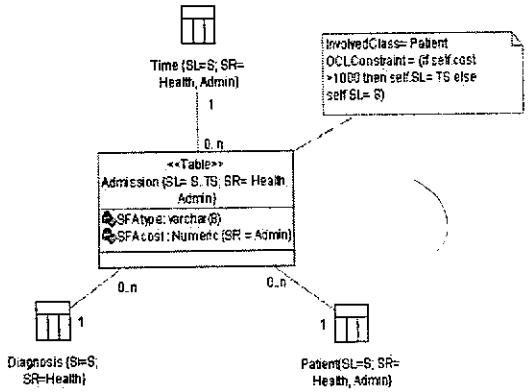

Figure 7. Star schema representing a instance of SECRDW metamodel at logical level

In order to obtain code for specific platform we choose Oracle 9i DBMS which allows us to implement multilevel databases and has a component named Oracle9i Label Security (OLS) [10]. OSL allows us to specify labeling functions and predicates that are triggered when an operation is executed, and which define the value of security labels according to a condition. We omit the creation of tables and only display on security aspect. Table 1 (1) shows an example by which we implement the security constraint labeled with label number 4 in figure 6. If the value of Cost column is greater than 10000 then the security label will be composed of TopSecret security level and Health and Admin user roles, else the security label will be composed of Secret security level and the same user roles. Table 1 (2) shows how to link this labeling function with Admission table.

Table 1. Example for implement security aspect in OSL.

```
(1) CREATE FUNCTION Which_Cost (Cost: Integer)
Return LBACSYS.LABC_LABEL
As MyLabel varchar2(80)
Begin
If Cost > 10000 then MyLabel:= ' TS::Health, Admin';
else MyLabel:= ' S::Health, Admin'; end if;
Return TO_LBAC_DATA_LABEL('MyPolicy',
MyLabel);
End;
(2) APPLY_TABLE_POLICY ('MyPolicy',
'Admission', 'Scheme', , 'Which_Cost')
```

5. Conclusion and Future Work

In this paper, we have presented an extension of the relational metamodel of the Common Warehouse Metamodel in order to represent security and audit measures in the logical modeling of data warehouses. This approach complements our previous works in which we used an Access Control and Audit model and a UML profile for the conceptual modeling of secure data warehouses. In this way, in the approach presented in this paper we can represent all security measures considered at the conceptual level in the further logical modeling of data warehouses, thereby avoiding the semantic gap in the specification of secure measures at the conceptual and logical level.

We plan to include the dynamicity of rules and mostly at runtime in our modeling approach in the future. Our immediate future work consists on the formal specification of all the required transformations between the conceptual and the logical models by using the Query-View-Transformation (QVT), thereby aligning our approach with the Model Driven Architecture. In this way, we will be able to specify all transformations in a formal language, thereby avoiding an arbitrary definition of these rules.

Acknowledgements

This work has been partially supported by the METASIGN project (TIN2004-00779) from the Spanish Ministry of Education and Science, by the DADASMECA project (GV05/220) from the Regional Government of Valencia, and by the DIMENSIONS (PBC-05-012-1) DADS project (PBC-05-012-2) from the Regional Science and Technology Ministry of Castilla -La Mancha (Spain).

References

[1] R Agrawal, R. Bayardo, C. Faloutsos, J. Kiernan, R. Srikant. "Auditing Compliance with a Hippocratic Database". Proc. Of the 30 th Int'l Conf. on Very large Databases, Toronto, Canada, August 2004.

[2] R. Agrawal, J. Kiernan, R.Srikant and Y. Xu."Hippocratic Databases" Proc. Of the 28 th Intçl Conf. on Very Large Databases, Hong Kong, China, August 2002.

[3] A. Abelló, J. Samos, and F. Saltor, YAM2 (Yet Another Multidimensional Model): An Extension of UML, in: International Database Engineering & Applications Symposium (IDEAS 2002), IEEE Computer Society, (Edmonton, Canada, 2002).

[4] M. Blaschka, C. Sapia, G. Höfling, and B. Dinter, Finding your way through Multidimensional Data Models, in: 9th Intl. Conference on Database and Expert Systems Applications (DEXA'98): Springer-Verlag (Vienna, Austria, 1998).

[5] G. Booch, J. Rumbaugh, and I. Jacobson, The Unified Modeling Language, User Guide, Addison-Wesley (Redwood city, CA, 1999).

[6] Eduardo Fernández-Medina, Juan Trujillo, Rodolfo Villarroel and Mario Piattini: Access Control and Audit Model for the Multidimensional Modeling of Data Warehouses. Accepted for publication in the Decision Support Systems journal (article in press).

[7] M. Golfarelli, D. Maio, and S. Rizzi, The Dimensional Fact Model: A Conceptual Model for Data Warehouses, International Journal of Cooperative Information Systems, 7(2-3) (1998).

[8] B. Husemann, J. Lechtenborger, and G. Vossen, Conceptual Data Warehouse Design, in: Proceedings of the 2nd. International Workshop on Design and Management of Data Warehouses, Technical University of Aachen (RWTH), (Stockholm, Sweden, 2000).

[9] R. Kimball and M. Ross, The Data Warehousing Toolkit. 2 edn., John Wiley (2002).

[10] J. Levinger, Oracle Label Security. Administrator's guide. Release 2.0 (9,.2). 2002: http://www.csis.gvsu.edu/generalInfo/Oracle/network.920/a96578.pdf

[11] S. Luján-Mora, J. Trujillo, and I.Y. Song, Extending the UML for Multidimensional Modeling, in: 5th International Conference on the Unified Modeling Language (UML 2002): Springer-Verlag. LNCS 2460 (Dresden, Germany, 2002).

[12] Jose-Norberto Mazon, Juan Trujillo, Manuel Serrano, Mario Piattini: Applying MDA to the development of data warehouses. DOLAP 2005: 57-66

[13] Enrique Medina, Juan Trujillo: A Standard for Representing Multidimensional Properties: The Common Warehouse Metamodel (CWM). ADBIS 2002: 232-247

[14] OMG, Model Driven Architecture (MDA). Object management Group, ormsc/2001-07-01, July 2001.

[15] Object Management Group, http://www.omg.org/

[16] Object Management Group (OMG), Common Warehouse Metamodel (CWM), Version 1.1, March 2003, http://www.omg.org/docs/formal/03-03-02.pdf

[17] J. Trujillo, M. Palomar, J. Gómez, and I.Y. Song, Designing Data Warehouses with OO Conceptual Models, IEEE Computer, special issue on Data Warehouses, 34) (2001).

[18] N. Tryfona, F. Busborg, and J. Christiansen, starER: A Conceptual Model for Data Warehouse Design, in: ACM 2nd International Workshop on Data Warehousing and OLAP (DOLAP'99): ACM (Missouri, USA, 1999).

[19] Rodolfo Villarroel, Eduardo Fernández-Medina, Juan Trujillo, Mario Piattini: Towards a UML 2.0/OCL extension for designing Secure Data Warehouses. WOSIS 2005: 217-228

0-7695-2567-9/06 $20.00 © 2006 IEEE