



Proceedings

DEXA

ARES 2007

The Second International Conference on Availability, Reliability and Security

April, 10th - April, 13th 2007, Vienna University of Technology, Austria

In Cooperation with



[SECURE]
Business Austria
Corporate for Management and Security



**GESTERREICHISCHE
COMPUTER GESELLSCHAFT**
AUSTRIAN
COMPUTER SOCIETY



IEEE Computer Society Conference Publications Operations Committee



CPOC Chair

Phillip Laplante

Professor, Penn State University

Board Members

Mike Hinchey, *Director, Software Engineering Lab, NASA Goddard*

Linda Shafer, *Professor Emeritus, University of Texas at Austin*

Jeffrey Voas, *Director, Systems Assurance Technologies, SAIC*

Thomas Baldwin, *Manager, Conference Publishing Services (CPS)*

IEEE Computer Society Executive Staff

David Hennage, *Executive Director*

Angela Burgess, *Publisher*

IEEE Computer Society Publications

The world-renowned IEEE Computer Society publishes, promotes, and distributes a wide variety of authoritative computer science and engineering texts. These books are available from most retail outlets. Visit the CS Store at <http://www.computer.org/portal/site/store/index.jsp> for a list of products.

IEEE Computer Society Conference Publishing Services (CPS)

The IEEE Computer Society produces conference publications for more than 200 acclaimed international conferences each year in a variety of formats, including books, CD-ROMs, USB Drives, and on-line publications. For information about the IEEE Computer Society's Conference Publishing Services (CPS), please e-mail: tbaldwin@computer.org or telephone +1-714-821-8380. Fax +1-714-761-1784. Additional information about the IEEE Computer Society's Conference Publishing Services (CPS) can be accessed from our web site at: <http://www.computer.org/cps>.

IEEE Computer Society / Wiley Partnership

The IEEE Computer Society and Wiley partnership allows the CS Press *Author's Book* program to produce a number of exciting new titles in areas of computer science and engineering with a special focus on software engineering. IEEE Computer Society members continue to receive a 15% discount on these titles when purchased through Wiley or at: <http://wiley.com/ieeeocs>. To submit questions about the program or send proposals, please e-mail dplummer@computer.org or telephone +1-714-821-8380. Additional information regarding the Computer Society's authored book program can also be accessed from our web site at: <http://www.computer.org/portal/pages/ieeeocs/publications/books/about.html>.

Revised: 17 August 2006



New CPS Online Workspace

An IEEE Online Collaborative Publishing Environment

We're proud to announce the launch of *CPS Online*, a new IEEE online collaborative conference publishing environment designed to speed the delivery of price quotations and provide conferences with anytime access to all of a project's publication materials during production, including the final papers. *CPS Online's* workspace gives a conference the opportunity to upload files through any Web browser, check status and scheduling on a project, make changes to the Table of Contents and Front Matter, approve editorial changes and proofs, and communicate with a CPS editor through discussion forums, chat tools, commenting tools and e-mail.

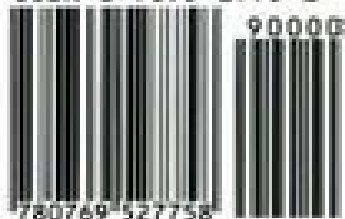
The following is the URL link to the CPS Online Publishing Inquiry Form:
http://www.ieeeconfpublishing.org/cpir/inquiry/cps_inquiry.html



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

IEEE Computer Society Order Number P2775
Library of Congress Number 2007922437
ISBN 0-7695-2775-2

ISBN 0-7695-2775-2



The Second International Conference on Availability, Reliability and Security



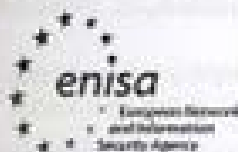
ARES 2007

DEXA

10 - 13 April 2007

Vienna, Austria

In Cooperation with



Technische
Universität
Wien
Vienna
University of
Technology

[SECURE]
Business Austria



ÖSTERREICHISCHE
COMPUTER GESELLSCHAFT
AUSTRIAN
COMPUTER SOCIETY



IEEE

Los Alamitos, California

Washington • Tokyo



Copyright © 2007 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 P2775

ISBN 0-7695-2775-2

ISBN 978-0-7695-2775-8

Library of Congress Number 2007922437

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.apo@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

 THE
COMPUTER
SOCIETY

 IEEE

 CPS

Conference Publishing Services

<http://www.computer.org/proceedings/>

Table of Contents

Second International Conference on Availability, Reliability and Security (ARES 2007)

Message from the Organizing Committee	xvi
ARES and Workshops Committees	xviii

Session 1: Trust Model & Trust Management

Formalising Dynamic Trust Negotiations in Decentralised Collaborative e-Health Systems	3
<i>Oluwafemi Ajayi, Richard Sinnott, and Anthony Stell</i>	
Why Trust is Not Proportional to Risk	11
<i>Bjarnar Solhaug, Dag Elgesem, and Ketil Stølen</i>	
From Trust to Dependability through Risk Analysis	19
<i>Yudistira Asnar, Paolo Giorgini, Fabio Massacci, and Nicola Zannone</i>	
Dynamic Trust Domains for Secure, Private, Technology-assisted Living	27
<i>Jatinder Singh, Jean Bacon, and Ken Moody</i>	
A Hybrid Trust Model for Enhancing Security in Distributed Systems	35
<i>Ching Lin and Vijay Varadharajan</i>	
A Reliable Component-based Architecture for E-Mail Filtering	43
<i>Wilfried N. Gansterer, Andreas G.K. Janecek, and Peter Lechner</i>	

Session 2: Availability, Fault-Tolerant & Recovery

Availability and Performance of the Adaptive Voting Replication Protocol	53
<i>Johannes Osrzel, Lorenz Frohofer, Norbert Chlaupke, and Karl M. Goeschka</i>	
Distributed Stream Processing Analysis in High Availability Context	61
<i>Marcin Gorawski and Pawel Marks</i>	
Implementing Network Partition-aware Fault-tolerant CORBA Systems	69
<i>Stefan Beyer, Francesc D. Muñoz-Escó, and Pablo Galdámez</i>	
Failure Recovery in Cooperative Data Stream Analysis	77
<i>Bin Rong, Fred Douglas, Zhen Liu, and Cathy H. Xia</i>	
A Recovery Protocol for Middleware Replicated Databases Providing GSI	85
<i>J.E. Armendáriz, F.D. Muñoz-Escó, J.R. Juárez, J.R.G. de Mendivil, and B. Kemme</i>	
Revisiting Hot Passive Replication	93
<i>Rubén de Juan-Marin, Hendrik Decker, and Francesc D. Muñoz-Escó</i>	

Session 3: Reputation Management & Trust

Reputation Management Survey <i>Sini Ruohomaa, Lea Kuitvonen, and Eleni Koutroufi</i>	103
Dirichlet Reputation Systems <i>Audun Jøsang and Jochen Haller</i>	112
Compartmented Security for Browsers — Or How to Thwart a Phisher with Trusted Computing <i>Sebastian Gajek, Ahmad-Reza Sadeghi, Christian Stöble, and Marcel Winandy</i>	120
Secure Anonymous Union Computation among Malicious Partners <i>Stefan Bötcher and Sebastian Obermeier</i>	128

Session 4: Privacy & Access Control

A Privacy Enhancing Service Architecture for Ticket-based Mobile Applications <i>Oliver Jorns, Oliver Jung, and Gerald Quirchmayr</i>	139
Privacy in Pervasive Computing and Open Issues <i>Pankaj Bhaskar and Sheikh I. Ahamed</i>	147
Context-dependent Access Control for Contextual Information <i>Christin Groba, Stephan Groß, and Thomas Springer</i>	155
Bytecode Verification for Enhanced JVM Access Control <i>Dongxi Liu</i>	162

Session 5: Failure Detection & Attack Prevention

Automatic Failure Detection with Separation of Concerns <i>P. Hazy and R.E. Seviora</i>	173
A Failure Detection Service for Large-Scale Dependable Wireless Ad-Hoc and Sensor Networks <i>Mourad Elhadef and Azzedine Boukerche</i>	182
Intrusion Detection System for Signal Based SIP Attacks through Timed HCPN <i>Yanlan Ding and Guiqing Su</i>	190
3G-WLAN Convergence: Vulnerability, Attacks Possibilities and Security Management Model <i>Muhammad Sher and Thomas Magedanz</i>	198
Specification and Detection of TCP/IP Based Attacks Using the ADM-Logic <i>Meriam Ben Ghorbel, Mehdi Talbi, and Mohamed Mejri</i>	206
Near Optimal Protection Strategies against Targeted Attacks on the Core Node of a Network <i>Frank Yeong-Sung Lin, Po-Hao Tsang, and Yi-Luen Lin</i>	213

Session 6: Authentication & Authorisation

Errors in Attacks on Authentication Protocols..... <i>Anders Moen Hagalsleffo</i>	223
Effects of Architectural Decisions in Authentication and Authorisation Infrastructures <i>Christian Schläger and Monika Ganslmayer</i>	230
Vulnerability Analysis of EMAP — An Efficient RFID Mutual Authentication Protocol <i>Tieyan Li and Robert Deng</i>	238
Authentication Mechanisms for Mobile Agents <i>Leila Ismail</i>	246
Using SAML and XACML for Complex Authorisation Scenarios in Dynamic Resource Provisioning <i>Yuri Demchenko, Leon Gommans, and Cees de Laat</i>	254
Implicit Authorization for Accessing Location Data in a Social Context..... <i>Georg Treu, Florian Fuchs, and Christiane Dargatz</i>	263

Session 7: Security Algorithm & Framework

Fingerprint Matching Algorithm Based on Tree Comparison Using Ratios of Relational Distances <i>Abinandhan Chandrasekaran and Bhavani Thuraisingham</i>	273
A Reconfigurable Implementation of the New Secure Hash Algorithm <i>M. Zeghida, B. Bouallegue, A. Baganne, M. Machhout, and R. Tourki</i>	281
Applications for Provably Secure Intent Protection with Bounded Input-Size Programs..... <i>J. Todd McDonald and Alec Yasinsac</i>	286
A Framework for the Development of Secure Data Warehouse Based on MDA and QVT..... <i>Emilio Soler, Juan Trujillo, Eduardo Fernández-Medina, and Mario Plattini</i>	294

Session 8: Software Security

Design of a Process for Software Security <i>David Byers and Nahid Shahmehri</i>	301
STEF: A Secure Ticket-based En-Route Filtering Scheme for Wireless Sensor Networks <i>Christoph Krauß, Markus Schneider, Kpatcha Bayarou, and Claudia Eckert</i>	310
A Secure Architecture for the Pseudonymization of Medical Data <i>Bernhard Riedl, Thomas Neubauer, Gemot Goluch, Oswald Boehm, Gert Reinauer, and Alexander Krumboeck</i>	318
Collection of Quantitative Data on Security Incidents <i>Thomas Nowey and Hannes Federrath</i>	325

Session 9: Security Models

Security Vulnerabilities in DNS and DNSSEC <i>Suranjith Arnyapperuma and Chris J. Mitchell</i>	335
---	-----



Secure, Resilient Computing Clusters: Self-Cleansing Intrusion Tolerance with Hardware Enforced Security (SCIT/HES).....	343
<i>David Arsenaull, Arun Sood, and Yih Huang</i>	
Applying a Tradeoff Model (TOM) to TACT.....	351
<i>Raihan Al-EKram, Ric Holt, and Chris Hobbs</i>	
A Pattern System for Security Requirements Engineering.....	356
<i>Denis Halebur, Maritta Heisel, and Holger Schmidt</i>	
Security Requirements for a Semantic Service-oriented Architecture.....	366
<i>Stefan Dürbeck, Rolf Schillinger, and Jan Koller</i>	
Supporting Compliant and Secure User Handling — A Structured Approach for In-House Identity Management.....	374
<i>Ludwig Fuchs and Günther Pernul</i>	

Session 10: Miscellaneous Security Techniques

A New Classification Scheme for Anonymization of Real Data Used in IDS Benchmarking.....	385
<i>Vidar Evenrud Seeberg and Siobodan Petrović</i>	
Static Evaluation of Certificate Policies for GRID PKIs Interoperability.....	391
<i>Valentina Casola, Nicola Mazzocca, Jesus Luna, Oscar Manso, Manel Medina, and Massimiliano Rak</i>	
Towards an Ontology-based Risk Assessment in Collaborative Environments Using the SemanticLIFE.....	400
<i>Mansoor Ahmed, Amin Anjomshoaa, Tho Manh Nguyen, and A Min Tjoa</i>	
Universally Composable Three-party Key Distribution.....	408
<i>TingMao Chang, YueFei Zhu, Jin Zhou, and YaJuan Zhang</i>	

Session 11: eAuction & eVoting Protocol

An Efficient eAuction Protocol.....	417
<i>Brian Curtis, Josef Pieprzyk, and Jan Seruga</i>	
Enhancing the Security of Local Danger Warnings in VANETs — A Simulative Analysis of Voting Schemes.....	422
<i>Benedikt Ostermaier, Florian Dötzer, and Markus Strassberger</i>	
A Practical Verifiable e-Voting Protocol for Large Scale Elections over a Network.....	432
<i>Orhan Cetinkaya and Ali Doganaksoy</i>	

Session 12: Dependability in Distributed & Ubiquitous Computing

Decoupling Constraint Validation from Business Activities to Improve Dependability in Distributed Object Systems.....	443
<i>Lorenz Frohofer, Johannes Osrail, and Karl M. Goeschka</i>	
Dependability Aspects of Ubiquitous Computing.....	451
<i>Lu Yan and Kaisa Sere</i>	
Concurrency Control Using Subject- and Purpose-Oriented (SPO) Scheduler.....	454
<i>Tomoya Enokido and Makoto Takizawa</i>	

Session 13: Anomaly & Intrusion Detection

Comparing Classifier Combining Techniques for Mobile-Masquerader Detection.....	465
<i>Oleksiy Mazhels and Seppo Puuronen</i>	
Process Profiling Using Frequencies of System Calls.....	473
<i>Surekha Mariam Varghese and K. Poulose Jacob</i>	
Terrorist Networks Analysis through Argument Driven Hypotheses Model.....	480
<i>D.M. Akbar Hussain</i>	

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

Session 1: Fault-Tolerant & Availability

High Availability for Network Management Applications.....	493
<i>Prabhu S. and Venkat R.</i>	
RWAR: A Resilient Window-consistent Asynchronous Replication Protocol.....	499
<i>Yanlong Wang, Zhanhua Li, and Wei Lin</i>	
Fault-Tolerant Semi-Passive Coordination Protocol for a Multi-Actuator/Multi-Sensor Model.....	506
<i>Keiji Ozaki, Naohiro Hayashibara, Tomoya Enokido, and Makoto Takizawa</i>	

Session 2: Access Control

Realizing Fine-Granular Read and Write Rights on Tree Structured Documents.....	517
<i>Franz Kollmann</i>	
Access Control Model for Web Services with Attribute Disclosure Restriction.....	524
<i>Vipin Singh Mewar, Subhandu Aich, and Shamik Surai</i>	
Aggregating and Deploying Network Access Control Policies.....	532
<i>Joaquin G. Alfaro, Frédéric Cuppens, and Nora Cuppens-Boulahia</i>	

Session 3: Authentication

Secure Spatial Authentication Using Cell Phones.....	543
<i>Arjan Durresi, Vamsi Paruchuri, Mimoza Durresi, and Leonard Baroli</i>	
Broadcast Authentication Protocol with Time Synchronization and Quadratic Residues Chain.....	550
<i>Bogdan Groza</i>	
A Secure Key Exchange and Mutual Authentication Protocol for Wireless Mobile Communications.....	558
<i>Yjun He, Nan Xu, and Jie Li</i>	
Improved Client-to-Client Password-Authenticated Key Exchange Protocol.....	564
<i>Gang Yao, Dengguo Feng, and Xiaoxi Han</i>	



Session 4: Real-Time System & Sensor Network

Adaptation Mechanisms for Survivable Sensor Networks against Denial of Service Attacks	575
<i>Dong Seong Kim, Chung Su Yang, and Jong Sou Park</i>	
Models for Automatic Generation of Safety-Critical Real-Time Systems	580
<i>Christian Buckl, Matthias Regensburger, Alois Knoll, and Gerhard Schrott</i>	
A Near-Real-Time Behaviour Control Framework	588
<i>Bastian Preindl and Alexander Schatten</i>	

Session 5: RFID Techniques & Applications

RFID Security Issues in Military Supply Chains	599
<i>Qinghan Xiao, Cam Boulet, and Thomas Gibbons</i>	
The Cost of Preserving Privacy: Performance Measurements of RFID Pseudonym Protocols	606
<i>Jens Mache and Chris Allick</i>	
Mobile Phone Based RFID Architecture for Secure Electronic Payments Using RFID Credit Cards	610
<i>Geethapriya Venkataramani and Srividya Gopalan</i>	

Session 6: Secure Solution & Applications

A Modular Architecture for Secure and Reliable Distributed Communication	621
<i>C.M. Jayalath and R.U. Fernando</i>	
Security Oriented e-Infrastructures Supporting Neurological Research and Clinical Trials	629
<i>Anthony Stell, Richard Sinnott, Oluwafemi Ajayi, and Jipu Jiang</i>	
Securing Medical Sensor Environments: The CodeBlue Framework Case	637
<i>Georgios Kambourakis, Eleni Kliaoudatou, and Stefanos Gritzalis</i>	
A Set of QVT Relations to Transform PIM to PSM in the Design of Secure Data Warehouses	644
<i>Emilio Soler, Juan Trujillo, Eduardo Fernández-Medina, and Mario Piattini</i>	

Session 7: Security Issue in Business Management

Agent Alliances: A Means for Practical Threshold Signature	655
<i>Regine Endsuleit and Christoph Amma</i>	
Protecting Online Transactions with Unique Embedded Key Generators	663
<i>Martin Boesgaard and Erik Zenger</i>	
A Research Agenda for Autonomous Business Process Management	670
<i>Thomas Neubauer, Gernot Goluch, and Bernhard Riedl</i>	

Session 8: Web, XML, Content Management

Secure Web Application Development and Global Regulation.....	681
<i>William Bradley Glisson, L. Milton Glisson, and Ray Welland</i>	
Query Assurance Verification for Dynamic Outsourced XML Databases.....	689
<i>Viet Hung Nguyen, Tran Khanh Dang, Nguyen Thanh Son, and Josef Küng</i>	
A Reflection-based Framework for Content Validation.....	697
<i>Lars-Heige Netland, Yngve Espelid, and Khalid A. Mughal</i>	

Session 9: Security Policies & Techniques

Web Engineering Security: Essential Elements.....	707
<i>William Glisson and Ray Welland</i>	
Designing a Security Policy According to BS 7799 Using the OCTAVE Methodology.....	715
<i>Paulina Januszkiewicz and Marek Pyka</i>	
CSP-based Firewall Rule Set Diagnosis Using Security Policies.....	723
<i>S. Pozo, R. Ceballos, and R.M. Gasca</i>	
CASSIS — Computer-based Academy for Security and Safety in Information Systems.....	730
<i>Gernot Goluch, Andreas Ekelhart, Stefan Fenz, Stefan Jakoubi, Bernhard Riedl, and Simon Tjoa</i>	

Session 10: Trust Management & Trust Model

Trust in Global Computing Systems as a Limit Property Emerging from Short Range Random Interactions.....	741
<i>V. Liagkou, E. Makri, P. Spirakis, and Y.C. Stamatiou</i>	
A Trust Overlay Architecture and Protocol for Enhanced Protection against Spam.....	749
<i>Jimmy McGibney and Dmitri Botvich</i>	
HICI: An Approach for Identifying Trust Elements — The Case of Technological Trust Perspective in VBEs.....	757
<i>Simon Samwel Msanjila and Hamideh Afsarmanesh</i>	
A Semantic and Time Related Recommendation-Feedback Trust Model.....	765
<i>Lin Zhang, Feng Xu, Yuan Wang, and Jian Lv</i>	

Session 11: Miscellaneous Applications

AsmLSec: An Extension of Abstract State Machine Language for Attack Scenario Specification.....	775
<i>Mohammad Raihan and Mohammad Zulkernine</i>	
Error Modeling in RF-based Location Detection (EMLD) for Pervasive Computing Environments.....	783
<i>Niraj Swami and Sheikh I. Ahamed</i>	
A Performance Model to Cooperative Itinerant Agents (CIA): A Security Scheme to IDS.....	791
<i>Rafael Pérez, Cristina Sotizábal, and Jordi Forné</i>	

On the Assessment of the Interaction Quality of Users with Cerebral Palsy.....	799
<i>C. Mauria, T. Granollers, and A. Solanas</i>	
Research and Design of Mobile Impeachment System with Semi-cryptonym.....	806
<i>Chaobo Yang and Ming Qi</i>	
Efficient Malicious Agreement in a Virtual Subnet Network.....	812
<i>Shu-Ching Wang, Shyl-Ching Liang, Kuo-Qin Yan, and Guang-Yan Zheng</i>	

Second International Workshop Dependability Aspects on Data Warehousing and Mining Applications (DAWAM 2007)

Extended RBAC-Based Design and Implementation for a Secure Data Warehouse.....	821
<i>Bhavani Thuraisingham and Srinivasan Iyer</i>	
Application of QVT for the Development of Secure Data Warehouses: A Case Study.....	829
<i>Emilio Solar, Juan Trujillo, Eduardo Fernández-Medina, and Mario Piattini</i>	
Protecting Private Information by Data Separation in Distributed Spatial Data Warehouse.....	837
<i>Marcin Gorawski and Jakub Bularz</i>	
Applying a Flexible Mining Architecture to Intrusion Detection.....	845
<i>Marcello Castellano, Giuliano Bellone de Grecis, Giuseppe Mastronardi, Angela Aprile, and Flaviano Fiorino</i>	
An Application of Learning Problem in Anomaly-based Intrusion Detection Systems.....	853
<i>Veselina G. Jecheva and Evgeniya P. Nikolova</i>	
Detecting Critical Regions in Covert Networks: A Case Study of 9/11 Terrorists Network.....	861
<i>Nasrullah Memon, Kim C. Kristoffersen, David L. Hicks, and Henrik Legind Larsen</i>	
Access Control and Integration of Health Care Systems: An Experience Report and Future Challenges.....	871
<i>Lillian Røstad, Øystein Nytra, Inger Anne Tandef, and Per Håkon Meland</i>	
A Collaborative Inter Data Grids Strong Semantic Model with Hybrid Namespace.....	878
<i>Dalia El-Mansy and Ahmed Sameh</i>	
Reliability Markov Chains for Security Data Transmitter Analysis.....	886
<i>Calin Ciufudean, Bianca Satco, and Constantin Filote</i>	

2nd International Workshop Dependability and Security in e-Government (DeSeGov 2007)

Requirements and Evaluation Procedures for eVoting.....	895
<i>Melanie Volkamer and Margaret McGaley</i>	
Towards Secure E-Elections in Turkey: Requirements and Principles.....	903
<i>Orhan Cetinkaya and Deniz Cetinkaya</i>	
On Coercion-Resistant Electronic Elections with Linear Work.....	908
<i>Stefan G. Weber, Roberto Araújo, and Johannes Buchmann</i>	
A Security Model and Architecture for Multichannel E-Government Systems.....	917
<i>MariaGrazia Fugini</i>	

eTVRA, a Threat, Vulnerability and Risk Assessment Method and Tool for eEurope.....	925
<i>Judith E. Y. Rossebe, Scott Cadzow, and Paul Sijben</i>	
Framework for Information Sharing Across Multiple Government Agencies under Dynamic Access Policies	934
<i>K. Bhoopalam, K. Maly, R. Mukkamala, and M. Zubair</i>	
Secure Distributed Dossier Management in the Legal Domain	941
<i>Martijn Wamier, Frances Brazier, Martin Apistola, and Anja Oskamp</i>	
Building a Dependable Messaging Infrastructure for Electronic Government.....	948
<i>Elsa Estevez and Tomasz Janowski</i>	

Workshop on Foundations of Fault-tolerant Distributed Computing (FOFDC 2007)

A Universal Construction for Concurrent Objects	959
<i>Rachid Guerraoui and Michel Raynal</i>	
FCPre: Extending the Arora-Kulkarni Method of Automatic Addition of Fault-Tolerance.....	967
<i>Bastian Braun</i>	
On the Implementation of the Omega Failure Detector in the Crash-Recovery Failure Model	975
<i>Cristian Martin, Mikel Larrea, and Ernesto Jiménez</i>	
Self-Diagnosing Wireless Mesh and Ad-Hoc Networks Using an Adaptable Comparison-Based Approach	983
<i>Mourad Elhadef, Azzedine Boukerche, and Hisham Elkadiki</i>	
Self-Stabilization as a Foundation for Autonomic Computing.....	991
<i>Olga Brukman, Shlomi Dolev, Yinnon Haviv, and Reuven Yagel</i>	
On Programming Models for Service-Level High Availability	999
<i>C. Engelmann, S.L. Scott, C. Leangsuksun, and X. He</i>	

First International Workshop on Secure Software Engineering (SecSE 2007)

Using Privacy Process Patterns for Incorporating Privacy Requirements into the System Design Process	1009
<i>Christos Kalloniatis, Evangelia Kavakli, and Stefanos Gritzalis</i>	
How Can the Developer Benefit from Security Modeling?.....	1017
<i>Shanai Ardi, David Byers, Per Håkon Meland, Inger Anne Tendel, and Nahid Shahmehri</i>	
AProSec: An Aspect for Programming Secure Web Applications	1026
<i>Gabriel Hermosillo, Roberto Gomez, Lionel Seinturier, and Laurence Duchien</i>	
Empirical and Statistical Analysis of Risk Analysis-Driven Techniques for Threat Management	1034
<i>Koen Buyens, Bart De Win, and Wouter Joosen</i>	
Secure Software Development through Coding Conventions and Frameworks	1042
<i>Takao Okubo and Hidehiko Tanaka</i>	

Pastures: Towards Usable Security Policy Engineering	1052
<i>Sergey Bratus, Alex Ferguson, Doug McIlroy, and Sean Smith</i>	
Security Objectives within a Security Testing Case Study	1060
<i>Kaarina Karppinen, Reijo Savola, Mikko Rapeli, and Esa Tikka</i>	
CppTest: A Prototype Tool for Testing C/C++ Programs	1066
<i>Chengying Mao and Yansheng Lu</i>	
A Novel Approach to Building Secure Systems	1074
<i>Dragan Vidakovic and Dejan Simic</i>	

Workshop on "Modeling, Designing, and Testing Correct, Secure, and Dependable Event-Based System" (EBITS 2007)

Exception Handling in an Event-Driven System	1085
<i>Jan Ploski and Wilhelm Hasselbring</i>	
Issues in Testing Dependable Event-based Systems at a Systems Integration Company	1093
<i>Armin Beer and Matthias Heindl</i>	
Optimizing Events Traffic in Event-based Systems by Means of Evolutionary Algorithms	1101
<i>Jiri Kubalik and Richard Mordinyi</i>	
Event-based Monitoring of Open Source Software Projects	1108
<i>Dindin Wahyudin and A. Min Tjoa</i>	
Using Space-based Computing for More Efficient Group Coordination and Monitoring in an Event-based Work Management System	1116
<i>Marcus Mor, Richard Mordinyi, and Johannes Riemer</i>	
Indexing and Search of Correlated Business Events	1124
<i>Roland Vecera, Szabolcs Rozsnyai, and Heinz Roth</i>	

First International Workshop on Advances in Information Security (WAIS 2007)

An Approach for Adaptive Intrusion Prevention Based on The Danger Theory	1135
<i>Alexander Krizhanovsky and Alexander Marasanov</i>	
A Human-Verifiable Authentication Protocol Using Visible Laser Light	1143
<i>Rene Mayrhofer and Martyn Welch</i>	
Insider-secure Hybrid Signcryption Scheme without Random Oracles	1148
<i>Chik How Tan</i>	
ZeroBio — Evaluation and Development of Asymmetric Fingerprint Authentication System Using Oblivious Neural Network Evaluation Protocol	1155
<i>Kei Nagai, Hiroaki Kikuchi, Wakaha Ogata, and Masakatsu Nishigaki</i>	
A Policy Language for the Extended Reference Monitor in Trusted Operating Systems	1160
<i>Hyung Chan Kim, R.S. Ramakrishna, Wook Shin, and Koichi Sakurai</i>	

Analysis on Bleichenbacher's Forgery Attack.....	1167
<i>Tetsuya Izu, Masahiko Takenaka, and Takeshi Shimoyama</i>	
A New Method for Reducing the Revocation Delay in the Attribute Authentication	1175
<i>Yoshio Kakizaki and Hidekazu Tsuji</i>	
Efficient Multiparty Computation for Comparator Networks.....	1183
<i>Koji Chida, Hiroaki Kikuchi, Gembu Morohashi, and Keiichi Hirota</i>	
Pseudo-Voter Identity (PVID) Scheme for e-Voting Protocols.....	1190
<i>Orhan Cetinkaya and Ali Doganaksoy</i>	
Attacks are Protocols Too	1197
<i>Anders Moen Hagalsieffo</i>	
Evaluation Function for Synthesizing Security Protocols by Means of Genetic Algorithms	1207
<i>Luis Zarza, Josep Pegueroles, and Miguel Soriano</i>	
On the Use of One-Way Chain Based Authentication Protocols in Secure Control Systems	1214
<i>Bogdan Groza and Toma-Leonida Dragomir</i>	
Bypassing Data Execution Prevention on Microsoft Windows XP SP2.....	1222
<i>Nenad Stojanovski, Marjan Gušev, Danilo Gligorski, and Svein J. Knapskog</i>	
A Security Framework for RFID Multi-Domain System.....	1227
<i>Dong Seong Kim, Taek-Hyun Shin, and Jong Sou Park</i>	

Workshop on "Security in E-Learning" (SEL)

E-Learning 2.0 = e-Learning 1.0 + Web 2.0?.....	1235
<i>Martin Ebner</i>	
Blended Learning Technology in Information Security Management Courses.....	1240
<i>Gerald Quirchmayr</i>	
Defining a Trusted Service-oriented Network Environment.....	1245
<i>Emmanuel A. Adigun and J.H.P. Eloff</i>	
Designing a Cryptographic Scheme for e-Surveys in Higher-Education Institutions.....	1251
<i>Alan Ward, Jordi Castellà-Roca, and Aleix Dorca Josa</i>	
Author Index	1256

Message from the Organizing Committee

Security, Reliability and Availability of IT systems and infrastructures have for over two decades been core research areas in the field of IT Security. Recent strategic research foci, especially in the European Union, have renewed the interest in the area and are setting the stage for very interesting and challenging developments, in areas ranging from the use of IT for increasing security in general, to the security of critical IT infrastructures and legal, economic and social issues. That is why ARES 2007, like ARES 2006 before, is again designed to serve as a bridge and discussion forum for researchers and practitioners.

We are therefore very pleased to have this conference for a second time 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 scientific research and the dissemination of new techniques in these areas.

We hope that this years ARES conference will again have a significant 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 have received 212 competed, on time submitted papers amongst over 250 abstract submissions from 43 countries for ARES 2007 and the Program Committee eventually selected 59 papers, making an acceptance rate of 27,83 % of submitted papers.

Seven workshops are organised on special topics of ARES, i.e.-

- Workshop "Dependability Aspects on Data Warehousing and Mining applications" (DAWAM 2007)
- Workshop "Dependability and Security in e-Government" (DeSeGov 2007)
- Workshop "Foundations of Fault-tolerant Distributed Computing" (FOFDC 2007)
- Workshop "Secure Software Engineering" (SecSE 2007)
- Workshop "Modeling, Designing, and Testing Correct, Secure, and Dependable Event-Based System" (EBITS 2007).
- Workshop "Advances in Information Security" (WAIS 2007)
- Workshop: Security in E-Learning (SEL 2007)

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 profoundly and in a timely manner. Due to the high number of submissions and the high quality of the submitted papers, the reviewing, and discussion process was an extraordinarily challenging task.

Special thanks must be given to Dr. Tho Manh Nguyen for all his essential support in the organization of the PC-tasks of ARES 2007. We would also like to thank all the authors who submitted their papers to ARES 2007 as their contributions built the basis of this year's excellent technical program. Many thanks go to Ms. Gabriela Wagner for her invaluable support with administrative issues.

Norman Revell, *Middlesex University, United Kingdom*

Roland Wagner, *University of Linz, Austria*

Honorary Co-Chairs

Günther Pernul, *University of Regensburg, Germany*

Makoto Takizawa, *Tokyo Denki University, Japan*

General Co-Chairs

Gerald Quirchmayr, *University of Southern Australia, Australia*

A Min Tjoa, *Vienna University of Technology, Austria*

Program Co-Chairs

Application of QVT for the Development of Secure Data Warehouses: A case study

Emilio Soler¹, Juan Trujillo², Eduardo Fernández-Medina³ and Mario Piattini³

(1) *Departamento de Informática, University of Matanzas, Cuba*

Autopista de Varadero km 3, Matanzas, Cuba.

emilio.soler@umcc.cu, <http://www.umcc.cu>

(2) *Departamento de Lenguajes y Sistemas Informáticos, University of Alicante, Spain*

C/ San Vicente S/N 03690 Alicante, Spain

trujillo@dlsi.ua.es, <http://www.dlsi.ua.es>

(3) *Grupo ALARCOS, Departamento de Tecnologías y Sistemas de Información*

Centro Mixto de Investigación y Desarrollo de Software UCLM-Soluziona

University of Castilla-La Mancha

Paseo de la Universidad, 4 - 13071 Ciudad Real, Spain

{eduardo.fdzmedina, mario.piattini}@uclm.es, <http://www.uclm.es>

Abstract

It is a crucial aspect for the development of Data Warehouses (DW) because they contain sensitive information. The application of the Model Driven Architecture (MDA) in the secure modeling of DW's obtaining the secure logical scheme from the conceptual model. In this paper, we apply the Query/View/Transformations (QVT) language to the development of a secure DW by means of a case study. We introduce the case study related to a typical sanitary system. Afterwards, with the application of a set of QVT relations, we transform all the captured security and audit requirements from the multidimensional conceptual model of the DW, to the relational model, by means of the construction of a secure logical model. From this scheme it turns out easier to obtain code for a specific platform that implements security and audit aspects.

Introduction

Dimensional modeling (MD) is the foundation of Data Warehouses (DWs), MDOLAP and On-Line Analytical Processing (OLAP) applications. These applications are used in order to form a highly powerful mechanism covering crucial business information in order to support decision-making processes.

These systems store historical information which is obtained from multiple, heterogeneous, autonomous and distributed data sources, thereby, the survival of

the organizations depends on the correct management, security and confidentiality of the information [1]. The information security is a serious requirement which must be given careful thought to, not as an isolated aspect, but as an present element in all stages of the lifecycle development, from requirement analysis to implementation and maintenance [2]. Therefore, it is crucial to specify confidentiality measures in the MD modelling process, and to enforce them.

The Unified Modeling Language (UML) profile presented in [3] allows us to specify the main aspects of security in a MD model. In [4] we present an extension of the relational package of the Common Warehouse Metamodel (CWM) that allow us to specify at the logical level all the considered security and audit measures in the conceptual modeling of DWs. These two proposals are integrated under the Model Driven Architecture (MDA) framework [5], to establish a secure platform independent model (secure PIM) and a secure platform specific model (secure PSM), as well as a set of Query/View/Transformations (QVT) relations for the modeling of secure DWs. Hereby we propose a solution to the semantic gap between advanced conceptual data models and relational or multidimensional implementations of data cubes [6].

In this work we apply a set of QVT relations to the development of a secure DW. The case study presented is related to a sanitary typical system. The considered multidimensional conceptual model is transformed into a relational logical scheme and from this we explain how to obtain code for a target platform. To this aim, we use a secure multidimensional PIM (SMD PIM)

and a secure multidimensional PSM (SMD PSM) as well as the relations defined in [5].

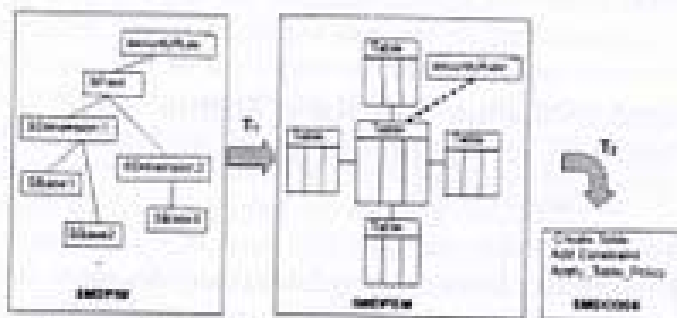


Figure 1. General transformation scheme

The diagram in Figure 1 illustrates a reduced approximation of the Secure Multidimensional MDA architecture [5]. On the left hand side the Secure Multidimensional conceptual scheme, i.e., SMD PIM, is presented. By means of the transformation T_1 we obtain the relational logical scheme, i.e., SMD PSM, represented in the centre of Figure 1. If we choose a SGBD that implements security aspects, then SMD PSM is transformed according to T_2 into code for the target platform. This code is called the Secure Multidimensional Code (SMD Code). The Figure illustrates how the security constraint defined by means of a securityRule [3, 4] (represented as an UML note) is transformed from the conceptual level to the logical level by employing T_1 , and later transformed into code with the T_2 transformation.

The rest of this paper is structured as follows. Section 2 begins introducing the case of study related to a typical sanitary system. It follows an explanation of the conceptual multidimensional modeling to introduce the secure PIM, this section finishes with the application of the QVT transformations to obtain the secure PSM. Finally, section 3 draws the main conclusions and outlines our immediate future work.

2. Case study

In this section, we apply the QVT transformations to the development of a secure DW related to a typical sanitary system. We have omitted some details to make the case of study more understandable. The example is an extended version of [4].

2.1 Introduction to the case study

A hospital desires to automate the incomes of the patients as well as to keep million of complex records treatments realized to patients. A sanitary system manipulates highly confidential information, so it is

mandatory to build a DW that contemplate a way security requirements (see Figure 2)

The Admission class keeps information about patients that enter to one or more hospitals. In the data of the patient and its diagnosis are used the classes, Diagnosis, Patient, Time, Diagnosis_Group and City. The class UserProfile contains information of all the users that will have access to the system. In order to store the information of the patient and diagnosis are necessary the Diagnosis, Patient, Diagnosis_Group and City classes. The UserProfile class contains information of all the users who have access to the system.

We have used the following security levels: confidential, secret and topSecret. User roles of Health (including Doctor and Nurse subroles) and nonHealth (including Maintenance and Administration subroles) have been defined. The root of hierarchical roles tree is HospitalEmployee. In example we have not considered organization compartments.

2.2 Conceptual multidimensional modeling

Figure 2 shows a secure MD model that includes a fact class (Admission), three dimensions (Diagnosis, Patient and Time), five base classes (DataD, Diagnosis_Group, DataP, City, and DataT) and a UserProfile class. The Admission fact class (SFact stereotype) contains all the individual admissions of patients in one or more hospitals. It can be accessed by all the users who have security levels secret or topSecret -labeled value SecurityLevel (SL)-, and perform health or administrative roles -tagged value SecurityRoles (SR)-. Be observed that the attribute cost only can be accessed by users who play administrative role - tagged value SR-. The database DataP contains the information of the patients in the hospital and can be accessed by all the users who have security level secret - tagged value SL-, and health or administrative roles -t value SR-.

The Address attribute can be only accessed by users who have an administrative role -tagged value SR- and attributes-. City base class contains the information of cities, and it allows us to group patients by cities. City base class can be accessed by all users who has confidential security level -tagged value SL-. DataD base contains the information of each user diagnosis and can be accessed by users who have a health role -tagged value SR-, and have secret security level -tagged value SL-. Finally Diagnosis_group contains a set of general groups of diagnosis. Each group can be related to several diagnoses, but a diagnosis will be always related to a group. Diagnosis_group can be accessed by all users who have confidential security

SL- tagged value SL-. Some security constraints have been specified by using the previously defined constraints, stereotypes and tagged values:

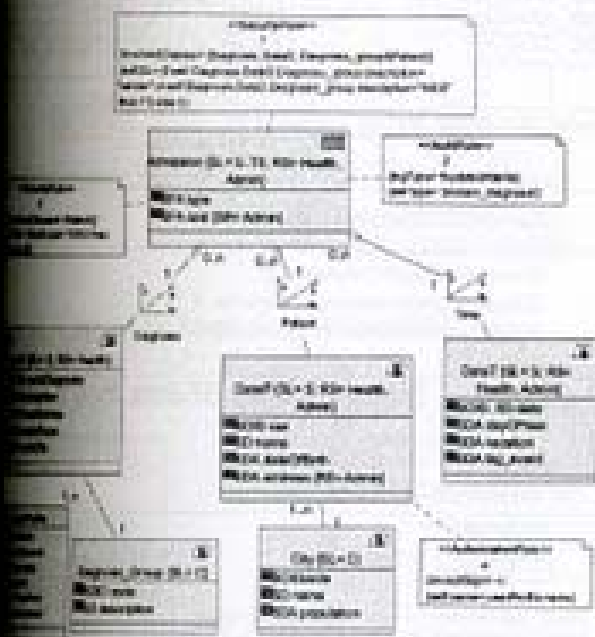


Figure 2. Example of secure multidimensional modeling

The security level of each instance of Admission is defined by a security constraint specified in the model. If the value of the SDescription 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 DataP base -tagged value involvedClasses-. Therefore, a user who has secret security level could obtain the number of patients with cancer for each city, but never its information of DataP base appears in the query.

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 its fact class, and so where the system denies it because of lack of permission.

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 DataP base -tagged value involvedClasses-.

4. Patient 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 DataP class.

The privilege that is considered in these exception is read, but we have not specified it in the model (the default value of exceptPrivilege tagged value is Read).

In Figure 2 we have represented an instance of the PIM, that we have been called Secure Multidimensional PIM (SMD PIM) [5]. In this model the Admission class represents a SFact, whereas Diagnosis, Patient and Time represent SDimension classes. In this example we do not consider SDegenerateFact. Diagnosis_Group and City represent SBase classes. In these classes we can model security requirements, for that reason, by means of notes of UML [7] we represent the AuditRule, AuthorizationRule and SecurityRule classes, in this way we establish security rules in the multidimensional conceptual model. At the attribute level the security is established by means of the SFactAttribute, SOID, SDescriptor and SDimensionAttribute classes.

2.3 QVT relations to obtain the PSM

A platform specific model (PSM) is a system view from the perspective of the platform. A PSM combines the specification of the PIM with the details that specify how the system uses a certain type of platform [8]. In the design of databases and data warehouses, the conceptual modeling provides the PIM, and the logical modeling the PSM. In multidimensional modeling, the logical level is designed according to the specific properties of the SGBD (Relational Online Analytical Processing, ROLAP, Multidimensional Online Analytical Processing, MOLAP or Hybrid Online Analytical Processing, HOLAP). Still, Kimball [9] assures that the most common representation is on relational platforms, i.e., on ROLAP systems.

The SMD PSM allows us to represent at the relational level the security requirements that were represented in the conceptual modeling of the DW. In this model we can represent tables, columns, primary and foreign keys, etc. Thus, we can establish security in attributes and tables. By means of UML notes [7] we express the security constraints that were modelled at the conceptual level.

In order to establish the transformation between SMD PIM and SMD PSM we consider the QVT declarative approach [10].

The main transformation contains relations of the type top-level. In each relation, we specify pre and post-conditions that should satisfy the relation by means of the clauses *when* and *where*. In Figure 3 we have represented the main transformation. The first relation in executing is SecuredW2SSchema, with it, all levels of security: confidential, secret and topsecret, as well as all the hierarchical roles tree is transformed into their equivalent ones of SSchema. The UserProfile2RUserProfile relation transforms the UserProfile class into a table belonging to SSchema that will have the same name of UserProfile. The relation that follows, i.e., SFact2STable is shown in its graphical notation in Figure 4, by means of this relation each SFact jointly with its security properties is transformed into a table that will contain the same information of security.



Figure 3. SMD PIM to SMD PSM transformation

The clause *where* invokes to the relations that must be executed. In Figure 5, we are going to show how the attributes of SFact are transformed into SColumns of the table that represents the SFact, so that, each column will contain the security information of its corresponding attribute in the SFact.

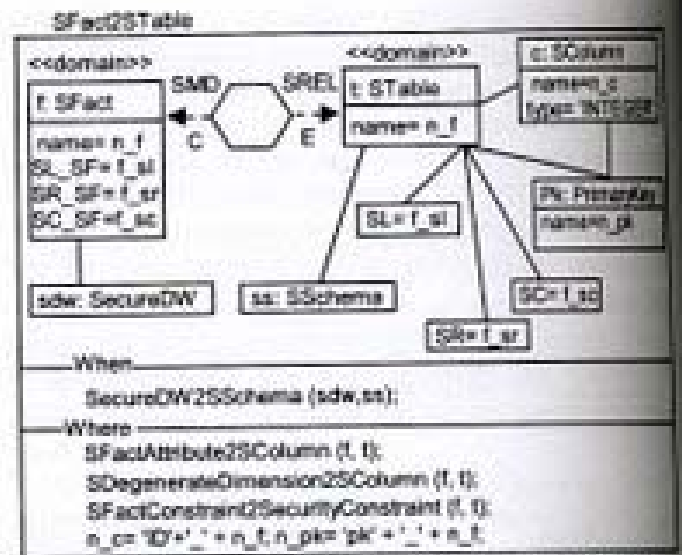


Figure 4. Transforming SFacts into STables

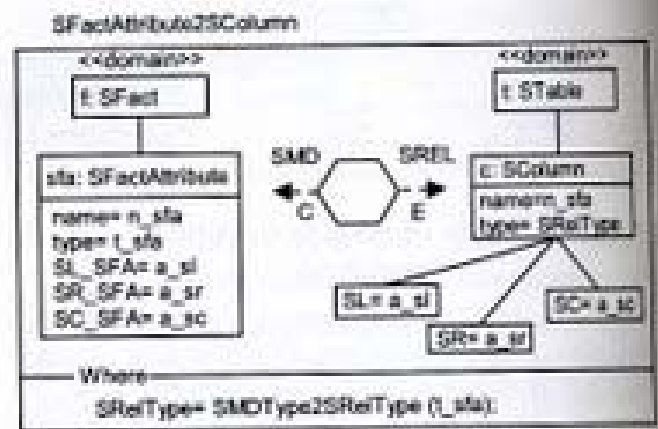


Figure 5. Transforming SAttributes into SColumns

In Figure 6 we show the result of applying the SFact2STable relation to our case study. The SFact Admission is transformed into a table of the model SMD PSM, i.e., in the Admission table, that will have a primary key, as well as the security properties securityLevel and securityRole.

Figure 7 shows the result of applying the SFactAttribute2SColumn relation, as a consequence, the Admission table will contain the columns respectively type and cost of type string and float. The column cost will have associated the security property securityRole. Also in Figure 7, the associated requirements of security to the Admission table are modeled in the heading of the table, according to the SECROW metamodel[4].

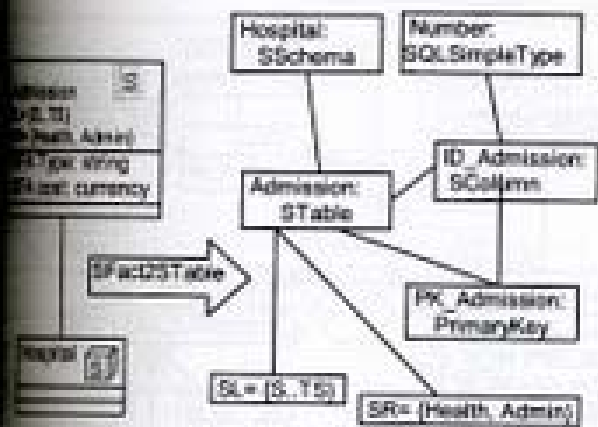


Figure 6. Applying SFact2STable

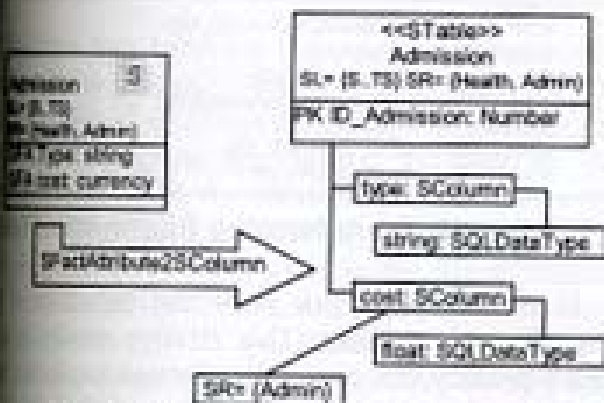


Figure 7. Applying SFactAttribute2SColumn

set, the relations that appear in the clause where SFact2STable must be executed. First the generateDimension2SColumn relation should be used, but in our case we don't have many-to-many relationship between the SFact Admission and dimensions. For that reason we will not define this relation.

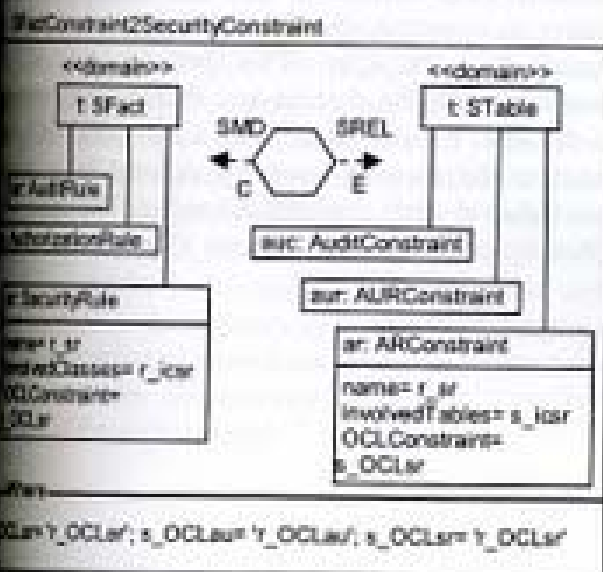


Figure 8. SFactConstraint2SecurityConstraint

Figure 8 presents the definition of the SFactConstraint2SecurityConstraint relation, which guarantees that all the constraints associated with the SFact are transformed in constraints associated with the table, just as it can be seen in Figure 9. The SECROW metamodel [4], assures that these constraints are modelled at the logical level by means of notes associated with table.

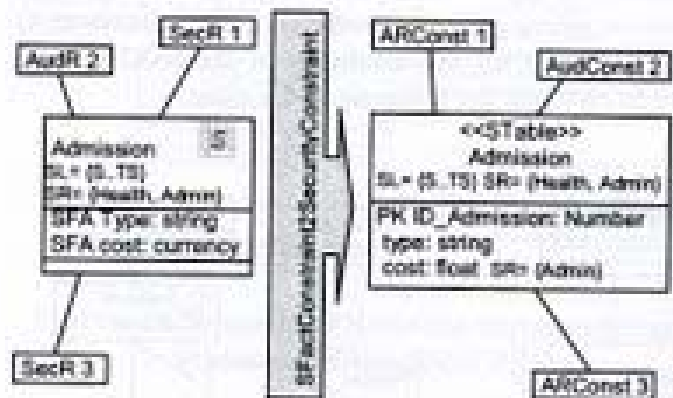


Figure 9. Applying SFactConstraint2SecurityConstraint

Continuing with the main transformation that appears in the Figure 3, it now corresponds to apply the SDgenerateFact2STable relation, which does not appear because all the relations between the SFact Admission and the dimensions are many-to-one. In Figure 10 we show the definition of the SDimension2STable relation.

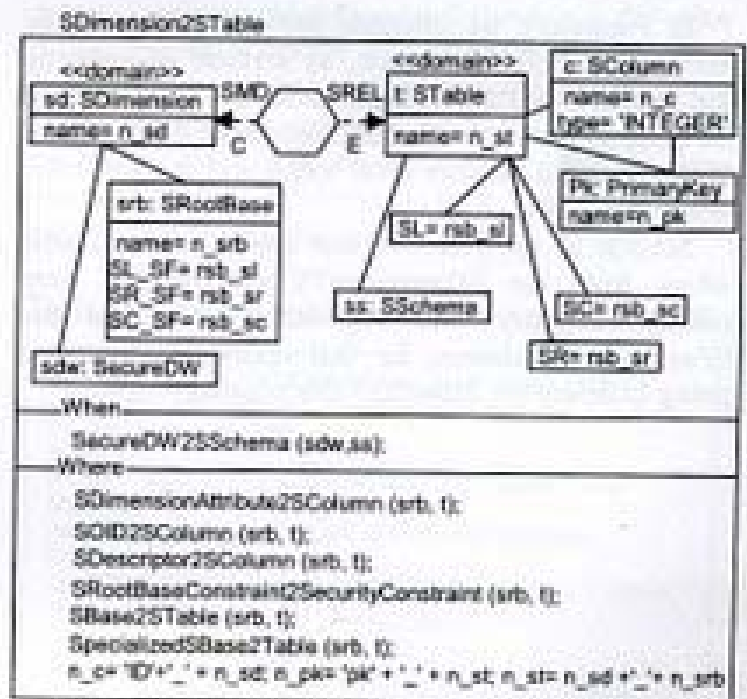


Figure 10. Transforming SDimension into STable

In multidimensional modeling the dimensions do not have attributes [10], for this reason, when the *SDimension2STable* relation is executed, a table is created whose name is merged with the names from dimension and rootBase respectively. The rootBase is the only *SBase* associated with the *SDimension*. All the associated security information with the rootBase is transformed in security properties of the table and by means of the execution of the relations that appear in the clause *where* of the *SDimension2STable* relation, is guaranteed that all the attributes of the rootBase are going to conform the columns of the table.

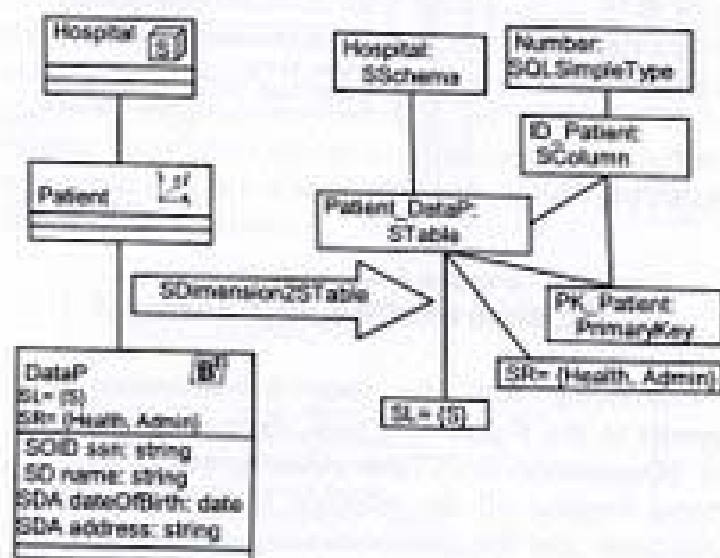


Figure 11. Applying *SDimension2STable*

In Figure 11 we illustrate the application of the *SDimension2STable* relation, as a result of applying this relation, the *Patient_DataP* table is created, with all the security properties that has associated the rootBase, in this case the security level secret and the user roles health and admin.

Several of the relations that appear in the clause *where* from the *SDimension2STable* relation keep certain similarity with the defined ones for the *SFact2STable* relation, for that reason; next we are going to define the *SBase2STable* relation

SBase2STable

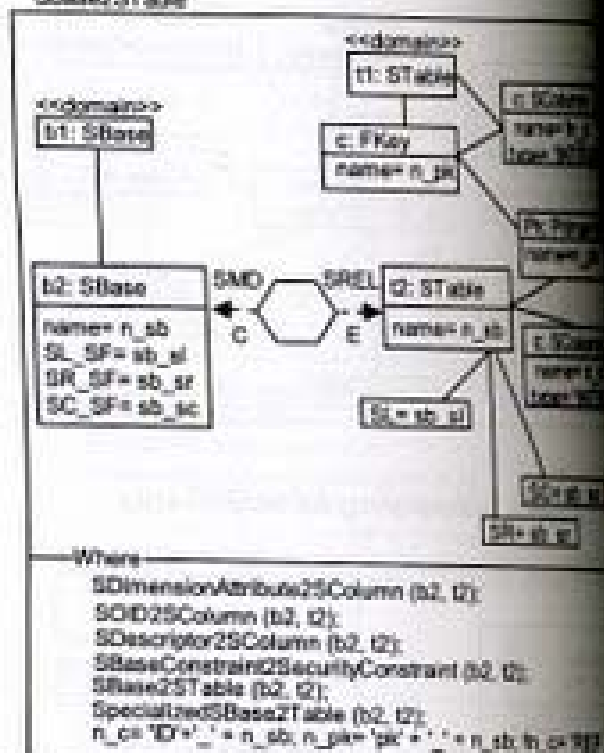


Figure 12. Transforming *SBase* into *STable*

In the Figure 12 we show the definition of the *SBase2STable* relation. This relation creates a table with a primary key, as well as a foreign key in the table that receives as parameter when it is invoked; in this case the primary key and the foreign key will be used for guaranteeing that the tables form a part of a one-to-many between the *SBases*. In the clause *where* this relation is called again, as well as the *SpecializedSBase2STable* relation to assure that the tables cover the whole hierarchy of bases that conform the dimension.

In Figure 13 we illustrate the application of the *SBase2STable* relation to our case study. When this relation is executed, the *City* table is created with a primary key *PK_City*. This primary key is associated with the foreign key that is also created in the *STable* *Patient_DataP*. The *City* table will be associated with the security property defined by the *securityLevel* with confidential value. The final result is that the tables *City* and *Patient_DataP* are related.

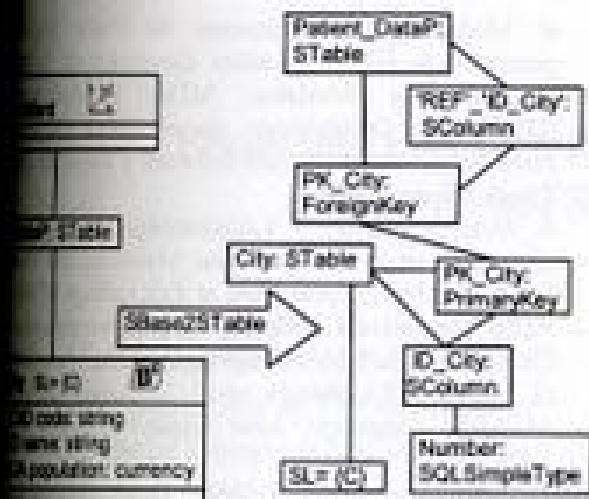


Figure 13. Applying SBase2STable

The first four relations that appears in the clause of the SBase2STable relation guarantee the information of all SBase attributes in columns of the table that represents the SBase, as well as the information of all the constraints associated to the table in constraints associated to the table that represents the SBase. The calls to the SBase2STable specializedBase2STable relations permit to cover all the hierarchy of bases that forms the dimension. The SpecializedBase2STable relation has certain similarity with the SBase2STable relation, for that reason we are not going to define it.

To complete the case study only remains apply the AssocSDF_SD2FKey, AssocSDF_SF2FKey and AssocSDF_SF2FKey relations, which enable to establish relationships between SFact and the dimensions, between the SDgenerateFact and the dimensions and between the SFact and the generateFact. In our case only proceeds to establish relations between the SFact Admission and the dimensions, therefore we do not have generateFact. As consequence, when the AssocSDF_SD2FKey relation is applied, then three primary keys are created in the Admission table. These establish the relationships between the Admission table with the Diagnosis_DataP, Patient_DataP and Time_DataT tables.

In Figure 14 we have omitted the attributes in some tables, as well as the primary keys and the foreign key to make the scheme snowflake more understandable. We observed how the security constraints have been added at the logical level.

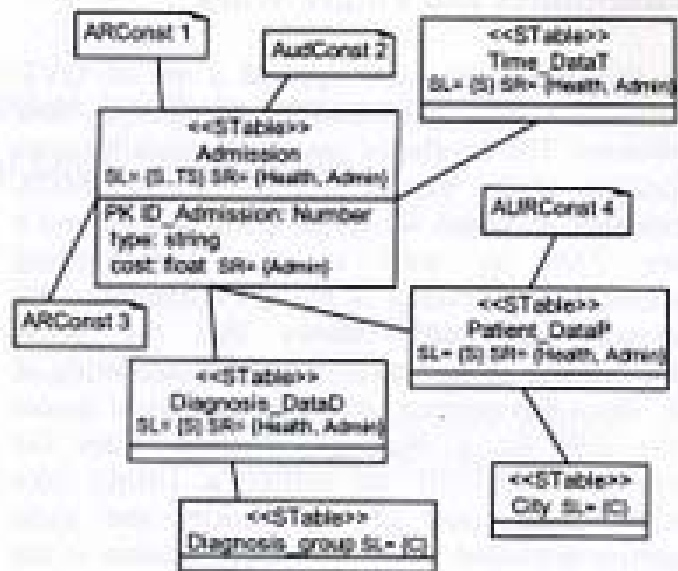


Figure 14 Snowflake schema representing an instance of the SMD PSM

In order to obtain code for a specific platform we choose Oracle 9i DBMS which allows us to implement multilevel databases and has a component named Oracle9i Label Security (OLS) [11]. OLS 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. To illustrate the possibilities of OLS we will only focus on the ARConstraint labeled with label number 3 in Figure 14. Table 1 (1) shows how by means of the creation of a function and the use of security labels we can define the following: 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. Implementing security aspect in OSL

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

3. Conclusions and Future Work

In this paper we have applied a set of QVT relations to the development of secure data warehouses. The developed case study constitutes an application of the Secure Multidimensional MDA architecture, in which we define a secure PIM and a secure PSM as well as the corresponding transformation by means of the QVT standard. The developed case study shows that the MDA framework can be applied to the secure modeling of DWs, since this permits to obtain the logical model of the DW for a relational platform from the conceptual model. If we utilize a DBMS like Oracle9i, then many of the security and audit properties modelled in the snowflake schema at the logical level can be transformed into code, in this way, we show that is possible to automate all the design process of secure DWs, which turns out to be a saving of time for the developers.

Our immediate future work consists of studying the possibility of implementing the QVT relations by using the capacity that offers some case tools.

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] G. Dhillon and J. Backhouse, "Information Systems Security Management in the New Millenium," *Communications of the ACM*, vol. 43 (7), 2000.
- [2] P. Devanbu and S. Stubblebine, "Software Engineering for Security: a Roadmap," presented at The Future of Software Engineering, Limerick, Ireland, 2000.
- [3] R. Villarroel, E. Fernández-Medina, and M. Piattini, "A UML 2.0/OCL Extension for Designing Secure Data Warehouses," *Journal of Research and Practice in Information Technology*, vol. 38, 2006.
- [4] E. Soler, R. Villarroel, J. Trujillo, E. Fernández-Medina, and M. Piattini, "Representing Security and Audit Rules for Data Warehouses at the Logical Level by using the Common Warehouse Metamodel," presented at First International Conference on Availability, Reliability and Security (ARES'06), Vienna, Austria, 2006.
- [5] E. Soler, J. Trujillo, E. Fernández-Medina, and M. Piattini, "Un Conjunto de Transformaciones QVT para

- el Modelado De Almacenes de Datos Seguros presented at III Taller sobre Desarrollo de Software Dirigido por Modelos. MDA y Aplicaciones (DSDM'06). Desarrollado en el marco de las Jornadas de Ingeniería del Software y Bases de Datos Sitges, España, 2006.
- [6] S. Rizzi, A. Abelló, J. Lechtenböcker, and I. Toghiani, "Research in Data Warehouse Modeling and Design: Dead or Alive?," presented at Proceedings of the 1st ACM international workshop on Data warehousing and OLAP (DOLAP'06), Arlington, Virginia, USA, 2006.
- [7] G. Booch, J. Rumbaugh, and I. Jacobson, *The Unified Modeling Language: User Guide*. Addison-Wesley, 1999.
- [8] J. Miller and J. Mukerji, "MDA Guide Version 1.0.1", 2003.
- [9] R. Kimball and M. Ross, *The Data Warehouse Toolkit*, 2 edition ed: John Wiley, 2002.
- [10] QVT, "OMG 2nd Revised Submission: MOF to MOF Query/Views/Transformations," 2006.
- [11] J. Levinger, "Oracle Label Security. Administrator's guide. Release 2.0 (9.2)," 2002.