



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.

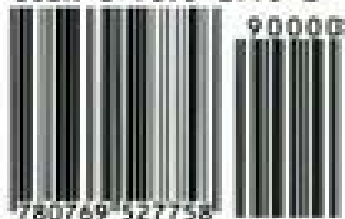
The following is the URL link to the CPS Online Publishing Inquiry Form:
http://www.ieeeconfpublishing.org/cpir/inquiry/cps_inquiry.html



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



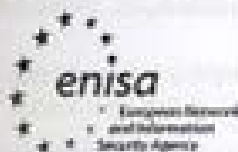
ARES 2007

DEXA

10 - 13 April 2007

Vienna, Austria

In Cooperation with



Technische
Universität
Wien
Vienna
University of
Technology

[SECURE]
Business Austria



OESTERREICHISCHE
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 Osrael, 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 Kuvonen, 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 Böttcher 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 Guiping 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 Slobodan 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>Yijun 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 Msanyila 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

A Framework for the Development of Secure Data Warehouses based on MDA and QVT

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.

esolercu@yahoo.es, http://www.umcc.cu

(2) *Departamento de Lenguajes y Sistemas Informáticos, University of Alicante, Spain*
C/ San Vicente S/N 03690 Alicante, Spain

jtrujillo@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

Data warehouses (DWs) store historical and aggregated information, extracted from multiple heterogeneous, autonomous and distributed sources of information, therefore it is essential to specify security measures from early stages of DW design and to enforce them. Several proposals on DW development have arisen in the last couple of years. However, few approaches represent security measures in the DW conceptual model starting from early stages of development of a DW project. In addition, these security measures cannot be automatically represented at logical level, so heuristic design guides for such transformations have appeared. This paper presents a framework based on Model Driven Architecture (MDA) for the development of secure data warehouses that covers all the phases of design (conceptual, logical and physical) and embeds security measures in all of them. Moreover, transformations between models are clearly and formally established by using Query/View/Transformation (QVT), to obtain consequently a traceability of the security rules from the early stages of development to the final implementation.

1. Introduction

In the last years, there have been several initiatives to include security in the DW design [1-4], many of them being focused on specific aspects related to

access control, multilevel security, federated database applications, commercial tools applications, etc. However, [5, 6] propose an access and audit control model integrated with an Unified Modeling Language (UML) extension, this allowing the development of secure multidimensional models at conceptual level. This proposal is promising, but still it does not cover all the stages of a DW development cycle.

The new standard that addresses the complete life cycle of developing applications by using models in software development is arising: Model Driven Architecture (MDA) [7]. In the MDA technology, the standard for defining transformations is Meta-Object Facility (MOF) 2.0 Query/View/Transformations (QVT) [8].

Current specialized literature comprises several proposals to integrate security with the MDA technology [9-12], but all of them are related with information systems, access control, security services and secure distributed applications, so none of them, is related with the design of secure DWs.

This article proposes a methodological approximation for the development of secure data warehouses using MDA and QVT. This proposal is a natural continuation of our previous work [13] and of the results presented in [5, 6, 14]. Our main objective is the proposal of an architecture that transforms security requirements from the conceptual level up to the logical level.

The rest of this article is structured as follows. Section 2 presents the main aspects related to the MDA

technology and the QVT transformations. Section 3 presents a framework for the development of secure data warehouses, by employing MDA and QVT. Finally, section 4 presents the main conclusions and defines immediate future work.

2 MDA-QVT: an overview

This section summarizes the main characteristics of MDA and of QVT transformations.

MDA promotes the specification of a Platform Independent Model (PIM) that does not contain information specific to the platform or to the technology to be used to develop it. This PIM can be transformed into one or several Platform Specific Models (PSMs) by including platform and development technology specific information. Later, each PSM is implemented into code to be executed on a platform in order to obtain the final software product.

Besides these models, a Computation Independent Model (CIM) is provided by MDA as means of modeling requirements.

QVT specification has a hybrid declarative / imperative nature, with the declarative part being split into two-level architecture [8]: Relations and Core metamodels. In the relations metamodel, the model transformation between model candidates is specified as a set of relations. These relations must hold for a successful model transformation. In the imperative style, a Black-box implementation of operations can be used to allow reuse of existing algorithms or domain specific libraries in certain model transformations. In this paper we focus on the QVT relations.

3 A framework for the development of secure data warehouses

This section integrates MDA and QVT with the multidimensional modeling of secure data warehouses. Subsections 3.1 and 3.2 introduce an Secure Multidimensional PIM (SMD PIM) and an Secure Multidimensional PSM (SMD PSM). In subsection 3.3 we define QVT relations that allow us to represent at logical level all security and audit requirements captured at the stage of conceptual modeling of the secure data warehouses. We do not comment on the way the code is obtained, as it is out of our scope.

Figure 1 illustrates through a diagram the Secure Multidimensional MDA architecture for the development of secure data warehouses. The upper part presents the CIM that defines the requirements for the DW. It represents a perspective on the DW

within its business environment, so it plays an important role in reducing the gap between those who are experts in the domain and their requirements and those who are experts in the design and development of the DW which needs to satisfy the requirements.

By means of the transformation T_1 in Figure 1 we obtain the Secure Multidimensional PIM, which is located at conceptual level. The T_2 transformation derives the Secure Multidimensional PSM (SMD PSM). This transformation is not unique, as other secure PSMs are possible. This is why on the left hand side of the area corresponding to the logical level a secure relational platform is represented, while on the right hand side of the same area any other secure platform is represented.

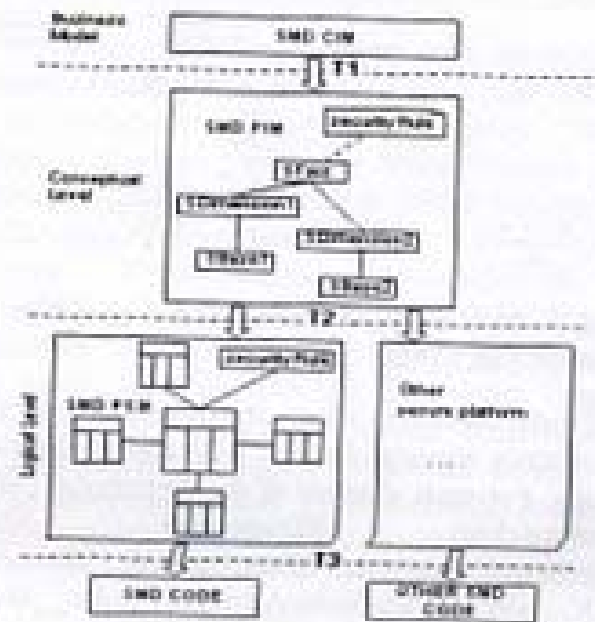


Figure 1. A framework for the development of secure data warehouses

Starting from each SMD PSM code is derived for the target platform. This code is called Secure Multidimensional Code, (SMD Code) and is represented in the lower part of Figure 1. It is to be noted how the security restriction defined using OCL (represented as an UML note) is transformed from the conceptual level to the logical level by means of T_2 , and later transformed in code by means of T_3 .

3.1 Definition of the SMD PIM

The UML profile presented in [6], called Secure Data Warehouse (SECDW), allows us to represent the main security requirements for the conceptual modeling of the DW. Figure 2 represents the SECDW metamodel, while omitting certain attributes to make the metamodel more comprehensible.

As security requirements are modeled in this PIM, it is therefore denominated as SMD PIM (Secure Multidimensional PIM). The main characteristics of this metamodel are the many-to-many relations between facts and specific dimensions, degenerated dimensions, the multiple classifications and the alternative path of hierarchy, as well as non-strict and complete hierarchies. The UserProfile metaclass contains information on each user's right of access to the multidimensional model.

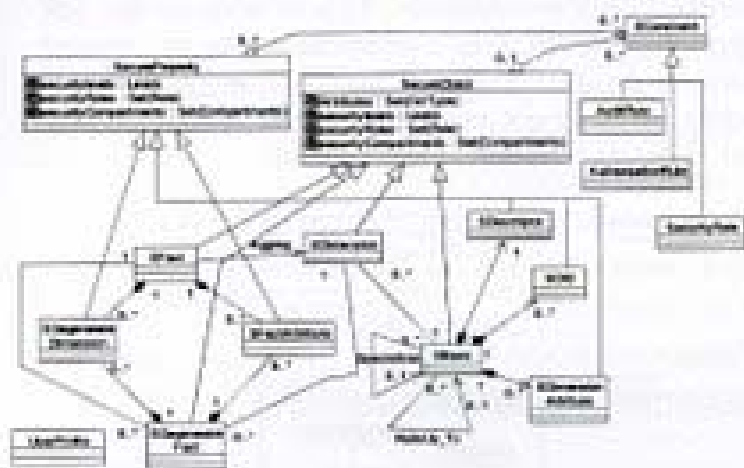


Figure 2. The SECDW metamodel used in the design of SMD PIM

The metamodel also allows the representation of the main security aspects for the DW multidimensional modeling. For each element of the metamodel (SFact, SDegenerateFact, SDimension, SBase, SDegenerateDimension, SFactAttribute, SDescriptor, SOID and SDimensionAttribute), its security information is defined by means of a sequence of security levels (SecurityLevels), a set of user categories (SecurityCompartment) and a set of user roles (SecurityRoles). Additionally these classes have security constraints (SConstraint) to indicate the security level and the rights conceded to a user to accede to certain information. For example, an authorization rule (AuthorizationRule) can represent an interdiction to specific users to access certain information. The access type can depend on the value of certain attributes contained in several classes. This fact can be captured in the model by means of a security rule (SecurityRule). If a user tries to accede to information for which his access is denied, then this fact can be modeled with an audit rule (AuditRule). These restrictions are defined using an Object Constraint Language (OCL) extension [15] and represented at model level with an UML note associated to the corresponding class.

More details on this profile can be found in [5, 6].

3.2 Definition of the SMD PSM

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 [8] assures that the most common representation is a relational platforms, i.e., on ROLAP systems.

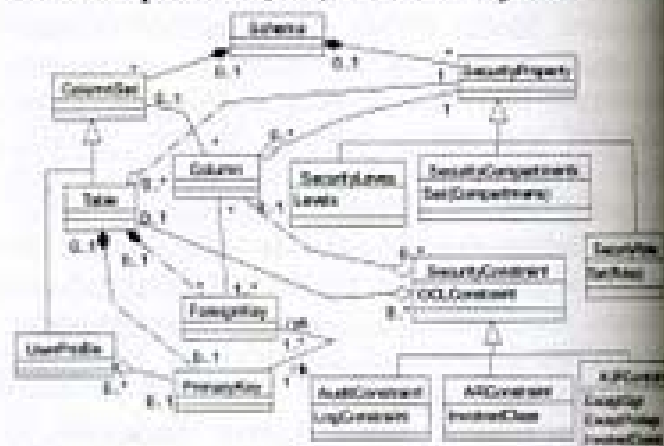


Figure 3. The SECDW metamodel used in the design of the SMD PSM

Our PSM is described in [17], starting from the relational Common Warehouse Metamodel (CWM), that allows us to model the security and other aspects represented at logical level in DW modeling. This metamodel is called the Secure Relational Data Warehouse (SECRDW).

Figure 3 presents the SECRDW metamodel that will be designated in the following as PSM. In order to distinguish the security aspects it comprises, it will be called the Secure Multidimensional PSM (SMD PSM). With this metamodel we can represent Table, Columns, primary and foreign keys, etc. The Schema container allows the security at model level. Its SecurityProperty and SecurityConstraint metaclass are associated with the Table and Column metaclass respectively, and they establish security for attributes and tables. In addition SecurityConstraint allows us to express the constraints (AuditRule, AuthorizationRule and SecurityRule) modelled through the UML notes of the Secure DW (SECDW) metamodel, i.e., in PIM. The UserProfile metaclass specifies restrictions on particular information corresponding to a user or user group.

3.3 QVT transformations of the SMD PIM to SMD PSM

Figure 4 employs the textual notation to establish the main transformations, i.e., the SMD PIM to SMD PSM transformation. The keyword *top* preceding the relations specifies that those relations will never be needed by other relations throughout the transformation. Each one of these relations has its own name and where clauses corresponding pre and post-conditions to be satisfied.

```

Transformation SMD To SREL(SMD: SECOW)
SREL: SECROW)
key Table(name, Schema);
key Column(name, owner);
key UserProfile(name, Schema);
key PrimaryKey(name, owner);
key ForeignKey(name, owner);
key SecurityProperty(name, owner);
key SecurityConstraint(name, owner);
top relation SecureDW2Schema()
top relation UserProfile2RUserProfile()
top relation SFact2Table()
top relation SDegenerateFact2Table()
top relation SDimension2Table()
Association SFact with SDimension
top relation AssocSF_2DFKey()
Association SDegenerateFact with SDimension
top relation AssocSDF_2DFKeyFK()
Association SDegenerateFact with SFact
top relation AssocSDF_2DFKey()

```

Figure 4. Textual notation for the SMDPIM to SMDPSM transformation

3.3.1. The SFact to Table transformation

Figure 5 illustrates the SFact2Table relation in its graphical notation. There is a table corresponding to SFact and having the same name. This table has a column with a name (specified in the where clause), which is also the primary key of the table. The security information represented with tagged values in the SFact is transformed into objects associated to the table. This security information is modeled at logical level as the *where* clause of the SFact table. The SFact2Table relation is satisfied only when the SecureDW2Schema pre-condition is satisfied, therefore ensuring that the table will be contained in Schema.

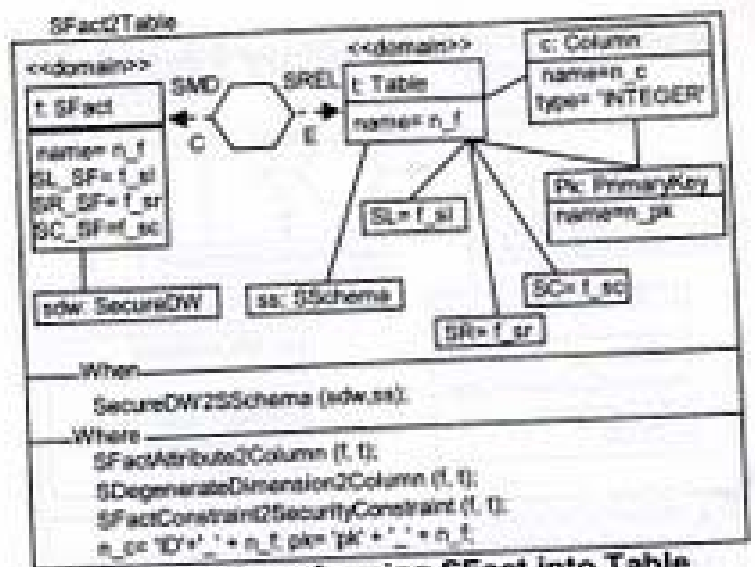


Figure 5. Transforming SFact into Table

The SFact attributes together with their security information and constraints are transformed according to the relations SFactAttribute2Column (if the attribute's type is FactAttribute) or SDegenerateDimension2Column (if the attribute is of type SDegenerateDimension).

Every SFactAttribute involved in the SFactAttribute2Column relation inherits security information and restrictions from the SecureProperty class, as the latter contains the SConstraint class. For this reason SFactAttribute2Column transforms not only attributes into columns, but also all the associated security information that SFactAttribute contains at conceptual level.

3.3.2. The SFactConstraint to Security Constraint transformation

SFact contains tagged values that inherit security restrictions of SecureClass. These security restrictions are transformed in table security restrictions by SFactConstraint2SecurityConstraint (see Figure 6), the resulting restrictions being modeled as *where* clauses.

Figure 6 illustrates the graphical notation provided by QVT to define the SFactConstraint2SecurityConstraint relation, certain attributes are omitted to make it more comprehensible. When the relation is applied, the constraints AuditRule, AuthorizationRule and SecurityRule transform themselves into AuditConstraint, ARConstraint and AURConstraint respectively, but associated to the table that represents the SFact. It is to be noted that this relation's where clause employs OCL to ensure that the "s_icst" attribute corresponds to the tables that represent the involvedTables attribute of the ARConstraint restriction.

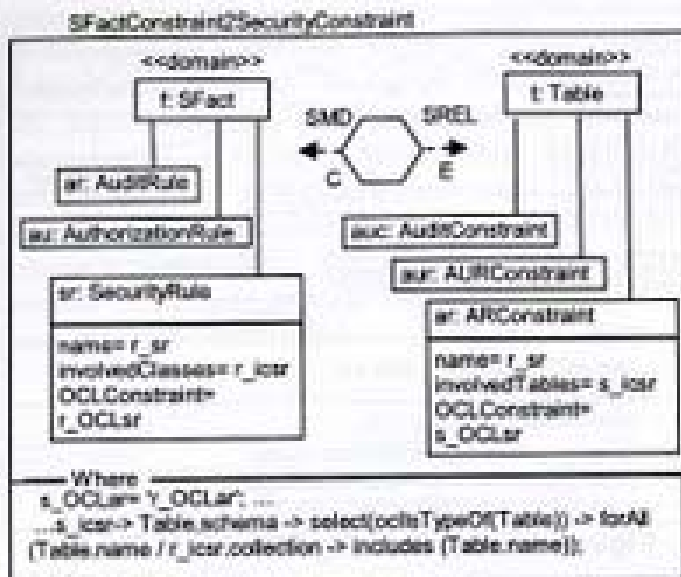


Figure 6. Graphical notation of the transformation of SFactConstraint into SecurityConstraint

4. Conclusions and Future Work

This paper introduces a new framework for the development of secure data warehouses based on MDA and QVT. The application of QVT transformation rules to the SMD PIM allows the development of different SMD PSMs, thus facilitating the representation at a logical level of all security and audit requirements captured at earlier stages of DW design. Afterwards, each SMD PSM can be directly converted into code.

The main contributions of this paper are: the development of DWs is reduced to creating an SMD PIM starting from an SMD CIM and its corresponding QVT relations, the time and effort invested in the development of DWs are shortened, the transition between different models and the final implementation is guaranteed, we reach interoperability, portability, adaptability and reusability by employing MDA technology.

Our immediate future work consists in studying the possibility to represent security requirements for Data Warehouses, and establish a transformation between secure CIM and SMD PIM.

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 DADS project (PBC-05-012-2) from the Regional Science and Technology Ministry of Castilla -La Mancha (Spain).

References

- [1] R. Kirkgoze, N. Katic, M. Stolda, and A. M. Tjoa, "A Security Concept for OLAP. (DEXA97)," Toulouse, France.
- [2] N. Katic, G. Quirchmayr, J. Schiefer, M. Stofa, and A. M. Tjoa, "A Prototype Model for DW Security Based on Metadata," (DEXA98), Vienna, Austria, 1998.
- [3] T. Priebe and G. Pernul, "Towards OLAP Security Design - Survey and Research Issues," (DMDW00), Sweden.
- [4] A. Rosenthal and E. Sciore, "View Security as the Basis for DW Security," (DMDW'00), Sweden, 2000.
- [5] E. Fernandez-Medina, J. Trujillo, R. Villarroel, and M. Piattini, "Access control and audit model for the multidimensional modeling of data warehouses," *DSS*, vol. 42, pp. 1270-1289, 2006.
- [6] R. Villarroel, E. Fernandez-Medina, and M. Piattini, "UML 2.0/OCL Extension for Designing Secure DW," *Journal of Research and Practice in IT*, vol. 38, 2006.
- [7] J. Miller and J. Mukerji, "MDA Guide Version 1.0.1," 2003.
- [8] OMG, "MOF 2.0 Query/View/Transformation."
- [9] C.C. Burt, B.R. Bryant, R.R. Rajc, A.M. Olson, and M. Auguston, "Model Driven Security: Unification of Authorization Models for Fine-Grain Access Control" (EDOC'03), 2003.
- [10] D. Basin, J. Deser, and T. Lodderstedt, "Model Driven Security: From UML models to access control infrastructures," ETH, Zürich 4 - September 2003.
- [11] S.N. Sivanandam and G.R. Karpagam, "A Novel approach for Implementing Security services," *Academy Open Internet Journal*, vol. 13, 2004.
- [12] U. Lang and R. Schreiner, "OpenPMF: a Model-Driven Security Framework for Distributed Systems," (ISSIS, Berlin, Germany, 2004.
- [13] J.-N. Mazon, J. Trujillo, M. Serrano, and M. Piattini, "Applying MDA to the development of data warehouses" (DOLAP'05), Bremen, Germany, 2005.
- [14] E. Fernandez-Medina, Juan Trujillo, Rodolfo Villarroel, and M. Piattini, "Developing secure DW with a UML extension," *IS*, vol. Article In Press, Corrected Proof.
- [15] E. Fernandez-Medina and M. Piattini, "Extending OCL for Secure Database Design," (UML'04), Lisboa, Portugal.
- [16] R. Kimball and M. Ross, *The Data Warehouse Toolkit*, 2 edition ed: John Wiley, 2002.
- [17] E. Soler, R. Villarroel, J. Trujillo, E. Fernandez-Medina, and M. Piattini, "Representing security and audit rules in DW at the logical level by using the CWM", (ARE'06), Vienna, Austria, 2006.