



ARES 2008 - International Conference on Availability, Reliability and Security
The Dependability Conference

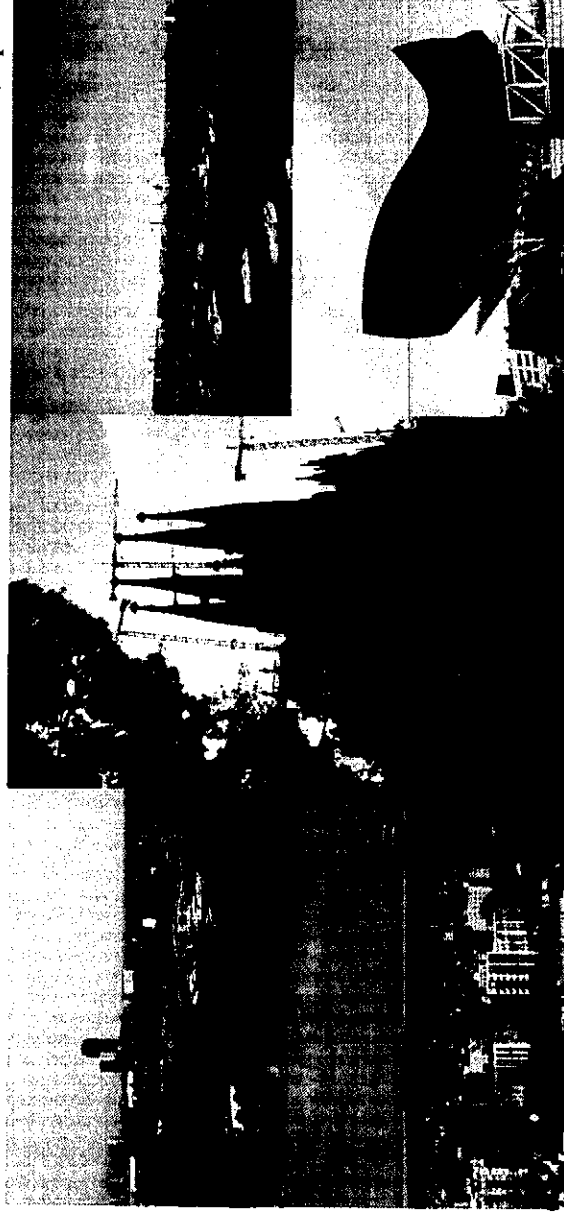
ARES 2008

The Third International Conference on Availability, Security and Reliability

PROCEEDINGS

March 4-7, 2008

Barcelona, Spain



Edited by Stefan Jakoubi, Simon Tjoa, and Edgar R. Weippl

Organised by

[SECURE]
Business Austria



In cooperation with



ÖSTERREICHISCHE
COMPUTER GESELLSCHAFT
AUSTRIAN
COMPUTER SOCIETY

Proceedings of the

The Third International Conference on
Availability, Security, and Reliability

March 4-7, 2008, Barcelona, Spain



Los Alamitos, California
Washington • Tokyo



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 P3102
ISBN 0-7695-3102-4
ISBN 978-0-7695-3102-1
Library of Congress Number 2007909935

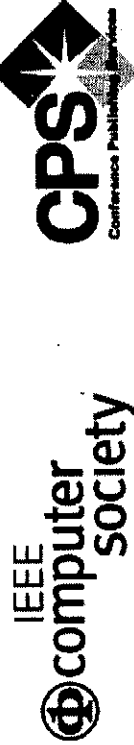
Additional copies may be ordered from:

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

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

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



IEEE Computer Society
Conference Publishing Services (CPS)
<http://www.computer.org/cps>

Table of Contents

The Third International Conference on Availability, Reliability and Security (ARES 2008)

Message from the General Chairs..... **xxi**
Conference Officers..... **xxii**

Keynotes

Security and Privacy Challenges in Location Based Service Environments..... **xxiii**
Vijayalakshmi Athuri
Infrastructure Support for Authorization, Access Control and Privilege Management..... **xxvi**
Günther Pernul

The ASCAA Principles for Next-Generation Role-Based Access Control..... **xxvii**
Ravi Sandhu and Venkata Bhamidipati

ARES Full Paper Sessions

Session 1: Applications

Securing Telehealth Applications in a Web-Based e-Health Portal..... **3**
Qian Liu, Shuo Lu, Yuan Hong, Lingyu Wang, and Rachida Dssouli
Multi-Level Reputation-Based Greylisting..... **10**
Wilfried Gansterer, Andreas Janecek, and Ashwin Kumar
Hardening XDS-Based Architectures..... **18**
Kim Wuyts, Riccardo Scandariato, Geert Claeys, and Wouter Joosen

Session 2: Miscellaneous

Finding Evidence of Antedating in Digital Investigations..... **26**
Svein Yngvar Willassen
FEDC: Control Flow Error Detection and Correction for Embedded Systems without Program Interruption..... **33**
Navid Farazmand, Mahdi Fazeli, and Seyyed Ghasem Miremadi
Economic and Security Aspects of Applying a Threshold Scheme in e-Health..... **39**
Bernhard Riedl, Veronika Grasser, Mathias Kolb, and Thomas Neubauer
Anomaly Based Character Distribution Modeling to Detect SQL Injection Attacks..... **47**
Mehdi Kiani, Andrew Clark, and George Mohay
On the Possibility of Small, Service-Free Disk Based Storage Systems..... **56**
Jehan-François Pâris and Thomas Schwarz
Efficient High Availability Commit Processing..... **64**
Heine Kollveit and Svein-Olaf Hvasshovd

Session 3: Models

- Soundness Conditions for Message Encoding Abstractions in Formal Security Protocol Models..... 72
Alfredo Pironi and Riccardo Sisto
- Towards Formal Specification of Abstract Security Properties..... 80
Antonio Maña and Gimena Pujol
- A Behavioral Model of Ideologically-motivated "Snowball" Attacks 88
Natalia Stakhanova, Oleg Stakhanov, and Ali Ghorbani
- Property Specification and Static Verification of UML Models 96
Igor Siveroni, Andrea Zisman, and George Spanoudakis

Session 4: Database

- Towards Comprehensive Requirement Analysis for Data Warehouses:
Considering Security Requirements 104
*Emilio Soler, Veronika Stefanov, Jose-Norberto Mazón, Juan Trujillo,
Eduardo Fernández-Medina, and Mario Piattini*
- A New Scheme for Distributed Density Estimation Based Privacy-Preserving Clustering 112
Chunhua Su, Jianying Zhou, Feng Bao, Tsyvoshi Takagi, and Kouichi Sakurai
- A Database Replication Protocol Where Multicast Writesets Are Always Committed 120
*José Ramón Juárez-Rodríguez, Enrique Armendáriz-Jitigo,
José Ramón González de Mendivil, and Francesc Daniel Muñoz-Escó*

Session 5: Mobile

- Matching Policies with Security Claims of Mobile Applications..... 128
Natalia Bielova, Marco Dalla Torre, Nicola Dragoni, and Ida Siahaan
- PSecGCM: Process for the Development of Secure Grid Computing based
Systems with Mobile Devices 136
David G. Rosado, Eduardo Fernández-Medina, Javier López, and Mario Piattini
- WATCHMAN: An Overlay Distributed AAA Architecture for Mobile Ad hoc Networks 144
Amir Khakpour, Maryline Laurent-Maknavicus, and Hakima Chaouchi

Session 6: RBAC and Recommender

- Hierarchical Domains for Decentralized Administration of Spatially-Aware RBAC Systems 153
Maria Luisa Damiani, Claudio Silvestri, and Elisa Bertino
- Experimental Demonstration of a Hybrid Privacy-Preserving Recommender System 161
*Esmá Aïmeur, Gilles Brassard, José M. Fernandez,
Flavien Serge Mani Onana, and Zbigniew Rakowski*
- Fast Qualitative Reasoning about Actions for Computing Anticipatory Systems 171
Natsumi Kitajima, Yuichi Goto, and Jingde Cheng

Session 7: Risk Management

- Enhancing Business Impact Analysis and Risk Assessment Applying a
Risk-Aware Business Process Modeling and Simulation Methodolog..... 179
Simon Tjoa, Stefan Jakoubi, and Gerald Quirchmayr
- Defining Secure Business Processes with Respect to Multiple Objectives 187
Thomas Neubauer and Johannes Heurix
- Analysis and Component-based Realization of Security Requirements 195
Denis Hatebur, Maritta Heisel, and Holger Schmidt

Session 8: Networks

- A Framework for Detecting Anomalies in VoIP Networks..... 204
Yacine Bouzida and Christophe Mangin
- Rapid Detection of Constant-Packet-Rate Flows 212
Kuan-Ta Chen and Jing-Kai Lou
- Performance Analysis of Anonymous Communication Channels Provided by Tor..... 221
Andriy Panchenko, Lexi Pimenidis, and Johannes Renner
- Fast Algorithms for Consistency-Based Diagnosis of Firewall Rule Sets 229
Sergio Pozo Hidalgo, Rafael Ceballos, and Rafael Martínez Gasca
- Privacy/Analysis Tradeoffs in Sharing Anonymized Packet Traces: Single-Field Case..... 237
William Yurcik, Clay Woolam, Greg Hellings, Latifur Khan, and Bhavani Thuraisingham

A Distributed Defense Framework for Flooding-Based DDoS Attacks..... 245

- Yonghua You, Mohammad Zulkernine, and Anwar Haque*
- Pure MPLS Technology 253
Liwen He and Paul Boham
- Symmetric Active/Active Replication for Dependent Services..... 260
Christian Engelmann, Stephen L. Scott, Chokchai Leangsuksun, and Xubin He

Session 9: Software

- Statically Checking Confidentiality of Shared-Memory Programs with Dynamic Labels..... 268
Marcus Völz
- A Cause-Based Approach to Preventing Software Vulnerabilities..... 276
David Byers and Nahid Shahmehri
- Integrating a Security Plug-in with the OpenUP/Basic Development Process..... 284
Shanai Ardi and Nahid Shahmehri
- A Novel Testbed for Detection of Malicious Software Functionality 292
Jostein Jensen
- Type and Effect Annotations for Safe Memory Access in C..... 302
Syrine Tlili and Mourad Debbabi

Session 10: IDS and Models	
Adaptability of a GP Based IDS on Wireless Networks.....	310
<i>Adetokunbo Makanju, Nur Zincir-Heywood, and Evangelos Milios</i>	
An Intrusion-Tolerant Mechanism for Intrusion Detection Systems.....	319
<i>Liwei Kuang and Mohammad Zulkernine</i>	
Fuzzy Private Matching (Extended Abstract).....	327
<i>Lukasz Chmielewski and Jaap-Henk Hoepman</i>	
Session 11: Trust, Security and Economics	
Navigating in Webs of Trust: Finding Short Trust Chains in Unstructured Networks without Global Knowledge.....	335
<i>Jens-Uwe Bußer, Steffen Fries, Martin Otto, and Peter Hartmann</i>	
Trust Modelling in E-Commerce through Fuzzy Cognitive Maps.....	344
<i>Christian Schlöger and Günther Pernul</i>	
Boosting Markov Reward Models for Probabilistic Security Evaluation by Characterizing Behaviors of Attacker and Defender.....	352
<i>Zonghua Zhang, Farid Nait-Abdesselam, and Pin-Han Ho</i>	
ARES Short Paper Sessions	
Session 1: Applications	
CERTLOC: Implementation of a Spatial-Temporal Certification Service Compatible with Several Localization Technologies.....	363
<i>José María de Fuentes García-Romero de Tejada, Ana Isabel González-Tablas Ferreres, and Arturo Ribagorda Garnacho</i>	
Extending Mixed Serialisation Graphs to Replicated Environments.....	369
<i>Josep M. Bernabé-Gisbert and Francesc D. Muñoz-Escot</i>	
Towards Secure E-Commerce Based on Virtualization and Attestation Techniques.....	376
<i>Frederic Stumpf, Claudia Eckert, and Shane Balfé</i>	
Fuzzy Belief-Based Supervision.....	383
<i>Alexandre Vorobiev and Rudolph Seviora</i>	
Ensuring Progress in Amnesiac Replicated Systems.....	390
<i>Rubén de Juan-Marín, Luis Irín-Briz, and Francesc D. Muñoz-Escot</i>	
Enhancing Face Recognition with Location Information.....	397
<i>R.J. Hulsebosch and P.W.G. Ebben</i>	
A Lazy Monitoring Approach for Heartbeat-Style Failure Detectors.....	404
<i>Benjamin Satzger, Andreas Pietzowski, Wolfgang Trummer, and Theo Ungerer</i>	
Defending On-Line Web Application Security with User-Behavior Surveillance.....	410
<i>Yu-Chin Cheng, Chi-Sung Laih, Gu-Hsin Lai, Chia-Mei Chen, and Tshuhan Chen</i>	
Session 2: Services and Trust	
A Pattern-Driven Security Process for SOA Applications.....	416
<i>Nelly A. Delessy and Eduardo B. Fernandez</i>	
Toward a Dependable Architecture for Highly Available Internet Services.....	422
<i>Ayari Narjess, Pablo Neira Ayuso, Laurent Lefevre, Denis Barbaron, and Rafael Gasca</i>	
Assessing the Reliability and Cost of Web and Grid Orchestration.....	428
<i>Alan Stewart, Maurice Clint, Terry Harmer, Peter Kilpatrick, Ron Perrott, and Joaquim Gabarro</i>	
Application-Oriented Trust in Distributed Computing.....	434
<i>Riccardo Scandariato, Yoram Ofek, Paolo Falcarin, and Mario Baldi</i>	
BlueTrust in a Real World.....	440
<i>Bradley Markides and Marijke Coetsee</i>	
Session 3: Privacy and Safety	
Privacy Preserving Shortest Path Computation in Presence of Convex Polygonal Obstacles.....	446
<i>Ananda Swarup Das, Jitu Kumar Keshri, Kannan Srinathan, and Vaibhav Srivastava</i>	
Privacy Protected ELF for Private Computing on Public Platforms.....	452
<i>Thomas Morris and V.S.S. Nair</i>	

haplog: A Hash-Only and Privacy-Preserved Secure Logging Mechanism <i>Chih-Yin Lin</i>	458	Cluster-based Group Key Agreement for Wireless Ad hoc Networks <i>Elisavet Konstantinou</i>	550
An Improved Zonal Safety Analysis Method and Its Application on Aircraft CRJ200 <i>Li Xiaolei, Tian Jin, and Zhao Tingdi</i>	461	Session 6: Crypto and Health	
Session 4: Networks		A Statistical Algorithm for Linguistic Steganography Detection Based on Distribution of Words <i>Chen Zhi-li, Huang Liu-sheng, Yu Zhen-shan, Li Ling-jun, and Yang Wei</i>	558
A Model for Specification and Validation of Security Policies in Communication Networks: The Firewall Case <i>Ryma Abbassi and Sihem Guemara El Fatmi</i>	467	RTQG: Real-Time Quorum-based Gossip Protocol for Unreliable Networks <i>Bo Zhang, Kai Han, Binoy Ravindran, and E.D. Jensen</i>	564
SPIT Detection and Prevention Method in VoIP Environment <i>He Guang-yu, Wen Ying-You, and Zhao Hong</i>	473	A Secure and Scalable Infrastructure for Inter-Organizational Data Exchange and eGovernment Applications <i>Jan Willemson and Arne Anspær</i>	572
A New Approach to Analysis of Interval Availability <i>Ezzat Kirmant and Cynthia Hood</i>	479	A Security Model and its Application to a Distributed Decision Support System for Healthcare <i>Liang Xiao, Andrew Peet, Paul Lewis, Srimandan Dasmahapatra, Carlos Sáez, Madelina Croitoru, Javier Vicente, Horacio González-Vélez, Magi Lluçh i Ariet, David Dupplaw, and Alex Gibb</i>	578
SFMD: A Secure Data Forwarding and Malicious Routers Detecting Protocol <i>Xiang-he Yang, Hua-ping Hu, and Xin Chen</i>	484	Session 7: Models and Networks	
Fault Effects in FlexRay-Based Networks with Hybrid Topology <i>Mehdi Dehbashi, Yahid Lari, Seyed Ghassem Miremadi, and Mohammad Shokrolah-Shirazi</i>	491	Run-time Information Flow Monitoring based on Dynamic Dependence Graphs <i>Salvador Cavadini and Diego Cheda</i>	586
Securing Wireless Sensor Networks <i>Xun Yi, Mike Faulkner, and Eiji Okamoto</i>	497	Automated Process Classification Framework using SELinux Security Context <i>Pravin Shinde, Priyanka Sharma, and Srinivas Guntupalli</i>	592
SEIF: Secure and Efficient Intrusion-Fault Tolerant Routing Protocol for Wireless Sensor Networks <i>Abdelraouf Ouadjaout, Yacine Challal, Nouredine Lasla, and Miloud Bagaa</i>	503	Using Composition Policies to Manage Authentication and Authorization Patterns and Services <i>Judith E. Y. Rossebo and Roh Bræk</i>	597
The Impact of Flooding Attacks on Network-based Services <i>Meiko Jensen, Nils Gruschka, and Norbert Luttenberger</i>	509	Providing Fault Tolerance in Wireless Backhaul Network Design with Path Restoration <i>Pakorn Leesuthipornchai, Naruemon Wattanapongsakorn, and Chalermpol Charmsripinyo</i>	604
Managing Priorities in Atomic Multicast Protocols <i>Emili Miedes and Francesc D. Muñoz-Escot</i>	514	Session 8: IDS	
Beacon Frame Spoofing Attack Detection in IEEE 802.11 Networks <i>Asier Martínez, Urko Zurutuza, Roberto Uribeetxeberria, Miguel Fernández, Jesús Lizarraga, Ainhoa Serna, and Iñaki Vélez</i>	520	Histogram Matrix: Log File Visualization for Anomaly Detection <i>Adrian Frei and Marc Rennhard</i>	610
An End-to-End Security Solution for SCTP <i>Stefan Lindskog and Anna Brunstrom</i>	526	Context-based Profiling for Anomaly Intrusion Detection with Diagnosis <i>Benferhat Salem and Tabia Karim</i>	618
Session 5: Crypto		A Revised Taxonomy of Data Collection Mechanisms with a Focus on Intrusion Detection <i>Ulf Larson, Erlend Jonsson and Stefan Lindskog</i>	624
An Identity-Based Group Key Agreement Protocol from Pairing <i>Hongji Wang, Gang Yao, and Qingshan Jiang</i>	532	IDRS: Combining File-level Intrusion Detection with Block-level Data Recovery based on iSCSI <i>Youhui Zhang, Hongyi Wang, Yu Gu, and Dongsheng Wang</i>	630
An Authenticated 3-Round Identity-Based Group Key Agreement Protocol <i>Gang Yao, Hongji Wang, and Qingshan Jiang</i>	538	Intrusion Detection for Wormhole Attacks in Ad hoc Networks: A Survey and a Proposed Decentralized Scheme <i>Marianne Azer, Sherif El-Kassas, Abdel Wahab Hassan, and Magdy El-Soudani</i>	636
High Capacity Steganographic Method Based Upon JPEG <i>Adel Almohammad, Robert Hierons, and Gheorghita Ghinea</i>	544		

Session 9: Hardware	
NFC Devices: Security and Privacy <i>Gerald Madlmayr, Josef Langer, Christian Kamtner, and Josef Scharinger</i>	642
Analyzing Fault Effects in the 32-bit OpenRISC 1200 Microprocessor <i>Nima Mehdizadeh, Mohammad Shokrolah Shirazi, and Seyed Ghassem Miremadi</i>	648
Increasing the Performability of Computer Clusters Using RADIC II <i>Guna Santos, Angelo Duarte, Dolores Rexachs, and Emilio Luque</i>	653
A Framework for Proactive Fault Tolerance <i>Geoffroy Vallée, Kulathep Charoenpormwattana, Christian Engelmann, Anand Tikotekar, Chokchai Leangsuksun, Thomas Naughton, and Stephen Scott</i>	659
Workshop FARES	
Session 1: Miscellaneous	
Anti-DDoS Virtualized Operating System <i>Sanjiam Garg and Huzur Saran</i>	667
A Case for High Availability in a Virtualized Environment (HAVEN) <i>Erin Farr, Richard Harper, Lisa Spainhower, and Jimi Xenidis</i>	675
Session 2: Access Control and Algorithms	
A Federated Physical and Logical Access Control Enforcement Model <i>Stéphane Onno</i>	683
Fostering the Uptake of Secure Multiparty Computation in E-Commerce <i>Octavian Catrina and Florian Kerschbaum</i>	693
Efficient Certificate Path Validation and Its Application in Mobile Payment Protocols <i>Rafael Martínez-Peláez, Cristina Sotizábal, Francisco Rico-Novella, and Jordi Forné</i>	701
Avoiding Policy-based Deadlocks in Business Processes <i>Mathias Kohler and Andreas Schaad</i>	709
A Secure High-Speed Identification Scheme for RFID Using Bloom Filters <i>Yasunobu Nohara, Sozo Inoue, and Hiroto Yasuura</i>	717
Session 3: Crypto	
New Self Certified Proxy Digital Signature Scheme based on Elliptic Curve Cryptosystem <i>Youan Xiao</i>	723
Privacy-preserving Protocols for Finding the Convex Hulls <i>Qi Wang, Yonglong Luo and Liusheng Huang</i>	727
A Secure RFID Protocol based on Insubvertible Encryption Using Guardian Proxy <i>Kyosuke Osaka, Shuang Chang, Tsuyoshi Takagi, Kenichi Yamazaki, and Osamu Takahashi</i>	733
Cryptographic Properties of Second-Order Memory Elementary Cellular Automata <i>Ascension Hernández Encinas, Angel Martín del Rey, J.L. Pérez Iglesias, Gerardo Rodríguez Sánchez, and Araceli Queiruga Dios</i>	741
New Efficient and Authenticated Key Agreement Protocol in Dynamic Peer Group <i>Shengke Zeng, Mingxing He, and Weidong Luo</i>	746
Session 4: Risk Management	
Intensive Programme on Information and Communication Security <i>Christian Schläger, Ludwig Fuchs, and Günther Pernul</i>	752
Applications for IT-Risk Management—Requirements and Practical Evaluation <i>Heinz Lothar Grob, Gereon Strauch, and Christian Buddendick</i>	758
Security Analysis of Role-based Separation of Duty with Workflows <i>Rattikorn Hewett, Phongphun Kijsanayothin, and Ashay Thipse</i>	765

Session 5: Databases and Models

- Detecting Suspicious Relational Database Queries 771
Stefan Böttcher, Rita Hartel, and Matthias Kirschner
- Assessing the Value of Enterprise Identity Management (EIdM)—
Towards a Generic Evaluation Approach 779
Denis Royer
- An Ontological Approach to Secure MANET Management 787
Mark Orwat, Timothy Levin, and Cynthia Irvine

Session 6: Models

- Reliability Analysis using Graphical Duration Models 795
Roland Donat, Laurent Bouillaut, Patrice Aknin, and Philippe Leray
- From Omega to Ω P in the Crash-Recovery Failure Model with Unknown Membership 801
Mikel Larrea and Cristian Martin
- Policy-based Group Organizational Structure Management using an Ontological Approach 807
Mario Anzués-García and Luz A. Sánchez-Gálvez
- A Systematic Review and Comparison of Security Ontologies 813
Carlos Blanco, Joaquín Lasheras, Rafael Valencia-García, Eduardo Fernández-Medina, Ambrosio Toval, and Mario Piattini
- Context Ontology for Secure Interoperability 821
Céline Coma, Nora Cuppens-Boulahia, Frédéric Cuppens, and Ana Rosa Cavalli

Session 7: Passwords and Services

- On the Security of VSH in Password Schemes 828
Kimmo Halunen, Pauli Rikula, and Juha Rönning
- Sustaining Web Services High-Availability Using Communities 834
Zakaria Maamar, Quan Z. Sheng, and Djamal Benslimane
- Distributed Information Retrieval Service for Ubiquitous Services 842
Takeshi Tsuchiya, Marc Lihan, Hirokazu Yoshinaga, and Keiichi Koyanagi

Session 8: Software

- A Lightweight Security Analyzer inside GCC 851
Davide Pozza and Riccardo Sisto
- Dynamic Maintenance of Software Systems at Runtime 859
Habib Seifzadeh, Mostafa Kermani, and Mohsen Sadighi
- Software Security: A Vulnerability Activity Revisit 866
Mohammad Ali Hadavi, Hossein Shirazi, Hasan Mokhtari Sangchi, and Valid Saber Hamishagi

Session 9: Trust

- Making Multi-Dimensional Trust Decisions on Inter-Enterprise Collaborations 873
Sini Ruohomaa and Lea Kivronen
- A Survey on Trust and Reputation Schemes in Ad Hoc Networks 881
Mariamme Azer, Sherif El-Kassas, Abdel Wahab Hassan, and Magdy El-Soudani

Workshop WPA

- Privacy-Preserving Recommendation Systems for Consumer Healthcare Services 889
Stefan Katzenbeisser and Milan Peirković
- Detecting Bots Based on Keylogging Activities 896
Yusuf Al-Hammadi and Uwe Aickelin
- A Comprehensive Approach for Context-dependent Privacy Management 903
Mike Bergmann, Thomas Springer, Elke Franz, and Christin Groba
- Traceable Quantitative Risk Assessment Applied to Investment Decision for Local Backups 911
Steffen Weiss, Martin Wahl, Michael Tieleman, and Klaus Meyer-Wegener
- Quantitative Assessment of Enterprise Security System 921
Ruth Breu, Frank Innerhofer-Oberperfer, and Artiom Yautsiukhin
- Clustering Oriented Architectures in Medical Sensor Environments 929
Eleni Kloudatou, Elisavet Konstantinou, Georgios Kambourakis, and Stefanos Gritzalis
- An Initial Model and a Discussion of Access Control in Patient Controlled Health Records 935
Lillian Røstad
- Secure Team-Based EPR Access Acquisition in Wireless Networks 943
Sigurd Eskeland and Vladimir Oleshchuk
- VEA-bility Security Metric: A Network Security Analysis Tool 950
Melanie Tupper and A. Nur Zimeir-Heywood
- Towards an Architecture for Balancing Privacy and Traceability in Ubiquitous Computing Environments 958
Stefan G. Weber, Andreas Heinemann, and Max Mühlhäuser

Workshop PSAI

GOST-28147 Encryption Implementation on Graphics Processing Units.....	967
<i>Victor Korobitsin and Sergey Ilyin</i>	
Intelligent Video Surveillance Networks: Data Protection Challenges.....	975
<i>Fanny Coudert and Jos Dumortier</i>	
Intrusion Detection with Data Correlation Relation Graph.....	982
<i>Amin Hassanzadeh and Babak Sadeghian</i>	
A Critique of <i>k</i> -Anonymity and Some of Its Enhancements.....	990
<i>Josep Domingo-Ferrer and Vicenç Torra</i>	
Cluster-Specific Information Loss Measures in Data Privacy: A Review.....	994
<i>Vicenç Torra and Susana Ladra</i>	
Hierarchical Trust Architecture in a Mobile Ad-Hoc Network Using Ant Algorithms.....	1000
<i>Cristina Sattizábal, Jordi Forné, Rafael Martínez-Peláez, and Francisco J. Rico-Novella</i>	
Representation and Reasoning on ORBAC: Description Logic with Defaults and Exceptions Approach.....	1008
<i>Narhimene Boustia and Aicha Mokhtari</i>	
Using Non-Adaptive Group Testing to Construct Spy Agent Routes.....	1013
<i>Georgios Kalogridis and Chris Mitchell</i>	
A Bayesian Approach for on-Line Max Auditing.....	1020
<i>Gerardo Canfora and Bice Cavallo</i>	
Detection of Malcodes by Packet Classification.....	1028
<i>Irfan Ahmed and Kyung-suk Lee</i>	
Performance of a Strategy Based Packets Forwarding in Ad Hoc Networks.....	1036
<i>Marcin Serechynski, Pascal Bouvry, and Mieczysław Kłopotek</i>	
Bayesian Additive Regression Trees-Based Spam Detection for Enhanced Email Privacy.....	1044
<i>Saeed Abu-Nimeh, Dario Nappa, Xinlei Wang, and Suku Nair</i>	
AntTrust: A Novel Ant Routing Protocol for Wireless Ad-hoc Network Based on Trust between Nodes.....	1052
<i>Carlos Aguilar Melchor, Bousad Ait Salem, Philippe Gaborit, and Karim Tamime</i>	
A Post-processing Method to Lessen <i>k</i> -Anonymity Dissimilarities.....	1060
<i>Agusti Solanas, Glòria Pujol, Antoni Martínez-Ballesté, and Josep Maria Mateo-Sanz</i>	
Improving Techniques for Proving Undecidability of Checking Cryptographic Protocols.....	1067
<i>Zhiyao Liang and Rakesh Verma</i>	
A Preliminary Investigation of Skype Traffic Classification Using a Minimalist Feature Set.....	1075
<i>Duffy Angevine and A. Nur Zincir-Heywood</i>	

Workshop APE

Partial Disclosure of Searchable Encrypted Data with Support for Boolean Queries.....	1083
<i>Yasuhiro Ohtaki</i>	
Secure and Privacy-Friendly Logging for eGovernment Services.....	1091
<i>Karel Wouters, Koen Simoens, Danny Lathouwers, and Bart Preneel</i>	
The REM Framework for Security Evaluation.....	1097
<i>Flora Amato, Valentina Casola, Antonino Mazzeo, and Valeria Vittorini</i>	
Static Validation of Licence Conformance Policies.....	1104
<i>René Rydhof Hansen, Flemming Nielson, Hanne Riis Nielson, and Christian W. Probst</i>	
Towards Practical Security Monitors of UML Policies for Mobile Applications.....	1112
<i>Fabio Massacci and Katsiaryna Naliuka</i>	
Synthesis of Local Controller Programs for Enforcing Global Security Properties.....	1120
<i>Fabio Martinelli and Ilaria Matteucci</i>	
Weighted Datalog and Levels of Trust.....	1128
<i>Stefano Bistarelli, Fabio Martinelli, and Francesco Santini</i>	
Negotiation of Usage Control Policies—Simply the Best?.....	1135
<i>Alexander Pretschner and Thomas Walter</i>	
Workshop SECSE	
Security Requirement Engineering at a Telecom Provider.....	1139
<i>Albin Zuccato, Viktor Endersz, and Nils Daniels</i>	
Identifying Security Aspects in Early Development Stages.....	1148
<i>Takao Okubo and Hidehiko Tanaka</i>	
Using Security Patterns to Combine Security Metrics.....	1156
<i>Thomas Heyman, Riccardo Scandariato, Christophe Huygens, and Wouter Joosen</i>	
Secure Software Design in Practice.....	1164
<i>Per Håkon Meland and Jostein Jensen</i>	
Covering Your Assets in Software Engineering.....	1172
<i>Martin Gilje Jaatun and Inger Anne Tøndel</i>	
A Non-Intrusive Approach to Enhance Legacy Embedded Control Systems with Cyber Protection Features.....	1180
<i>Shangping Ren and Kevin Kwiat</i>	
Towards Incorporating Discrete-Event Systems in Secure Software Development.....	1188
<i>Sarah Whittaker, Mohammad Zulkernine, and Karen Rudie</i>	
How to Open a File and Not Get Hacked.....	1196
<i>James Kupsch and Barton Miller</i>	

Design of an FDB based Intra-domain Packet Traceback System <i>Hiroaki Hazezama, Yoshihide Matsumoto, and Youki Kadobayashi</i>	1313
An Independent Evaluation of Web Timing Attack and its Countermeasure <i>Yoshitaka Nagami, Daisuke Miyamoto, Hiroaki Hazezama, and Youki Kadobayashi</i>	1319
Secure Spatial Authentication for Mobile Stations in Hybrid 3G-WLAN Serving Networks <i>Arjan Durresi, Mimoza Durresi, and Leonard Barolli</i>	1325
Privacy-Preserving Distributed Set Intersection <i>Qingsong Ye, Huaxiong Wang, and Christophe Tartary</i>	1332
Examination of Forwarding Obstruction Attacks in Structured Overlay Networks <i>Yo Mashimo, Shintaro Ueda, Yasutaka Shinzaki, and Hiroshi Shigeno</i>	1340
A Novel Approach for Multiplication over $GF(2^m)$ in Polynomial Basis Representation <i>Abdulah Abdulah Zadeh</i>	1346
Workshop WSDF	
Wi-Fi Network Signals as a Source of Digital Evidence: Wireless Network Forensics <i>Benjamin Turnbull and Jill Slay</i>	1355
Improving the Analysis of Lawfully Intercepted Network Packet Data Captured for Forensic Analysis <i>Jill Slay, Benjamin Turnbull, and Joshua Broadway</i>	1361
Recovery of Encryption Keys from Memory Using a Linear Scan <i>Christopher Hargreaves and Howard Chivers</i>	1369
Proposal for Efficient Searching and Presentation in Digital Forensics <i>Jooyoung Lee</i>	1377
Secure Steganography in Compressed Video Bitstreams <i>Bin Liu, Fenlin Liu, Chunfang Yan, and Yifeng Sun</i>	1382
Considerations Towards a Cyber Crime Profiling System <i>Kweku Arthur, Martin Olivier, Hein Yenter, and Jan H.P. Eloff</i>	1388

Rules of Thumb for Developing Secure Software: Analyzing and Consolidating Two Proposed Sets of Rules <i>Holger Peine</i>	1204
Workshop DAWAM	
Adaptive Data Integrity through Dynamically Redundant Data Structures <i>Vincenzo De Florio and Chris Blondia</i>	1213
ISEDS: An Information Security Engineering Database System Based on ISO Standards <i>Daisuke Horie, Shoichi Morimoto, Noor Azimah, Yuichi Goto, and Jingde Cheng</i>	1219
Privacy Aspects of eHealth <i>Daniel Slamang and Christian Stingl</i>	1226
Adaptive Voting Algorithms for Reliable Dissemination of Data in Sensor Networks <i>Kaliappa Ravindran, Jiang Wu, Kevin Kwiat, and Ali Sabbir</i>	1234
Risk as Dependability Metrics for the Evaluation of Business Solutions: A Model-driven Approach <i>Yudistira Asnar, Rocco Moretti, Maurizio Sebastianis, and Nicola Zannone</i>	1240
Implementing Multidimensional Security into OLAP Tools <i>Carlos Blanco, Eduardo Fernández-Medina, Juan Trujillo, and Mario Piattini</i>	1248
Detecting Key Players in 11-M Terrorist Network: A Case Study <i>Nasrullah Memon and David L. Hicks</i>	1254
Privacy Preserving Support Vector Machines in Wireless Sensor Networks <i>Dong Seong Kim, Muhammad Anwarul Azim, and Jong Sou Park</i>	1260
An Image Encryption System by Cellular Automata with Memory <i>Farhad Maleki, Ali Mohades, S. Mehdi Hashemi, and Mohammed Ebrahim Shiri</i>	1266
Workshop WAIS	
Insider-secure Signcryption KEM/Tag-KEM Schemes without Random Oracles <i>Chik How Tan</i>	1275
Internet Observation with ISDAS: How Long Does a Worm Perform Scanning? <i>Tomohiro Kobori, Hiroaki Kikuchi, and Masato Terada</i>	1282
Electronic Voting Scheme to Maintain Anonymity in Small-scale Election by Hiding the Number of Votes <i>Tsukasa Endo, Isao Echizen, and Hiroshi Yoshiura</i>	1287
Enocoro-80: A Hardware Oriented Stream Cipher <i>Dai Watanabe, Kota Ideguchi, Jun Kitahara, Kenichiro Muto, Hiroki Furuichi, and Toshinobu Kaneko</i>	1294
Cryptanalysis and Improvement of an 'Improved Remote Authentication Scheme with Smart Card' <i>Marko Hölbl and Tatjana Welzer</i>	1301
Effective Monitoring of a Survivable Distributed Networked Information System <i>Paul Rubel, Michael Atighetchi, Partha Pal, Martin Fong, and Richard O'Brien</i>	1306

Workshop SREIS

Alignment of Misuse Cases with Security Risk Management.....	1397
<i>Raimundas Matulevičius, Nicolas Mayer, and Patrick Heymans</i>	
Information Stream Based Model for Organizing Security	1405
<i>Bernhard Thalheim, Sabah Al-Fedaghi, and Khaled Al-Sagabi</i>	
Security Requirements Variability for Software Product Lines	1413
<i>Daniel Mellado, Eduardo Fernandez-Medina, and Mario Piattini</i>	
Transforming Security Requirements into Architecture	1421
<i>Koen Yskout, Riccardo Scandariato, Bart De Win, and Wouter Joosen</i>	
Modelling Security Properties in a Grid-based Operating System with Anti-Goals	1429
<i>Alvaro Arenas, Benjamin Aziz, Juan Bicarregui, Brian Matthews, and Erica Y. Yang</i>	
Annotating Regulations Using Cerno: An Application to Italian Documents—Extended Abstract.....	1437
<i>Nicola Zeni, Nadzeya Kiyavitskaya, James R. Cordy, Luisa Mich, and John Mylopoulos</i>	
Goal-Oriented, B-Based Formal Derivation of Security Design Specifications from Security Requirements.....	1443
<i>Riham Hassan, Shawn Bohner, Sherif El-Kassas, and Mohamed Eltoweissy</i>	
Analysis of Security Requirements for Cryptographic Voting Protocols (Extended Abstract).....	1451
<i>Orhan Cetinkaya</i>	

Author Index..... **1457**

Chair's Message

The Third International Conference on Availability, Reliability and Security (ARES 2008 – The International Dependability Conference) brings together researchers and practitioners in the area of dependability. ARES 2008 highlights the various aspects of dependability, with special focus on the crucial linkage between availability, reliability and security.

ARES aims at a full and detailed discussion of research issues in the field of dependability as an integrative concept that covers amongst others availability, safety, confidentiality, integrity, maintainability and security and their different areas of applications.

This conference emphasizes the interplay between foundations and practical issues of dependability in areas such as information systems, e-government, m-government, location-based services, ubiquitous computing, and autonomous computing.

This years ARES conference is devoted to the critical examination and research challenges of the various aspects of Dependable Computing and the definition of a future road map.

We are very happy to welcome three well-known keynote speakers:

- Prof. Ravi Sandhu (Executive Director, Institute for Cyber-Security Research (ICSR) and Latcher Brown Endowed Chair in Cyber-Security, University of Texas, San Antonio)
- Prof. Vijay Atluri (Management Science and Information Systems Department, Rutgers University)
- Prof. Günther Pernul (Department of Information Systems, University of Regensburg)

From over 200 submissions we have selected the 44 best for a presentation as full paper. In addition, several workshops and short papers show ongoing research projects and offer interesting starting points for discussions.

We wish all participants an enjoyable conference and interesting discussions.

Edgar R. Weippl, Secure Business Austria, Vienna University of Technology
Gerald Quirchmayr, University of Vienna and University of South Australia

Jill Slay, University of South Australia

Conference Officers

Honorary Co-Chairs

Roland Wagner, University of Linz, Austria

General Co-Chairs

Guenther Pernul, University of Regensburg, Germany
Makoto Takizawa, Tokyo Denki University, Japan

Program Co-Chairs

Gerald Quirchmayr, University of South Australia, Australia
Jill Slay, University of South Australia, Australia
Edgar Weippl, Vienna University of Technology / Secure Business Austria, Austria

Workshops Co-Chairs

Leonard Barolli, Fukuoka Institute of Technology (FIT), Japan
A Min Tjoa, Vienna University of Technology, Austria

Organizing Chair

Fatos Xhafa, Technical University of Catalonia, Spain

International Liaison Co-Chairs

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

Publicity Chair

Vladimir Marik, Czech Technical University, Czech Republic

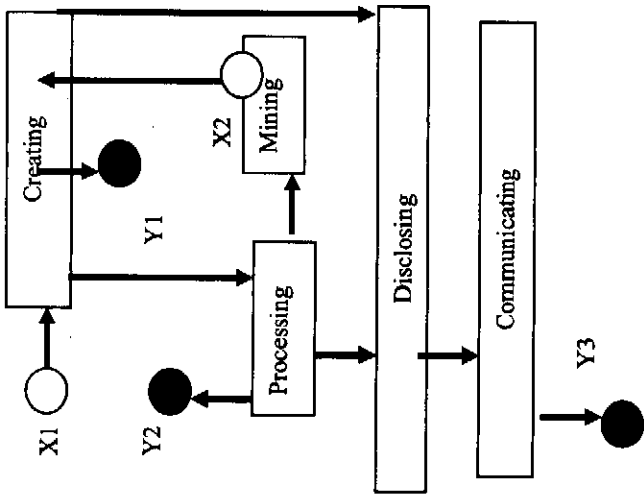


Figure 12. Entry and exit points for internally generated data.

VIII. CONCLUSION

One of the important aspects of security organization is to establish a framework to identify significant security points where policies and procedures are declared. The (information) security infrastructure comprises entities, processes, and technology. All are participants in handling information, which is the item that needs to be protected. Our approach is to identify information stream as the principal focus of security consideration. It is based on identifying points of transformation in the flow of information as the pivots around which security organization is built.

Currently, there is an implicit understanding of such a method. For example, in a computer system critical security posts are built around a core set of functionalities such as access control of stored information, internal processes, logon accounts, external communication connections, etc. Inside a single system (e.g., database security) security functions are unsystematically allocated according to information type, operation type, output type (e.g., mining), etc. The information stream model introduces a general coherent blueprint of security-significant posts that complements identification of security-related controls.

Security Requirements Variability for Software Product Lines

Daniel Mellado
Ministry of Work and Social
Affairs; Social Security IT
Department, Madrid, Spain
Daniel.Mellado@alu.uclm.es

Eduardo Fernández-Medina
University of Castilla La-
Mancha, Alarcos Research
Group, Information Systems
and Technologies
Department, Spain.
Eduardo.FdezMedina@uclm.es

Mario Piattini
University of Castilla La-
Mancha, Alarcos Research
Group, Information
Systems and Technologies
Department, Spain.
Mario.Piattini@uclm.es

Abstract

Software product line engineering has proven to be one of the most successful paradigms for developing a diversity of similar software applications and software-intensive systems at low costs, in short time, and with high quality, by exploiting commonalities and variabilities among products to achieve high levels of reuse. At the same time, due to the complexity and extensive nature of product line development, security and requirements engineering are critical success factors in the development of a software product line. However, most of the current product line practices in requirements engineering do not adequately address the security requirements engineering. Therefore, in this paper we will propose a security requirements decision model driven by security standards along with a security variability model to manage the variability of the security requirements related artefacts. The aim of this approach is to deal with security requirements from the early stages of the product line development in a systematic way, in order to facilitate the conformance to the most relevant security standards with regard to the management of security requirements, such as ISO/IEC 27001 and ISO/IEC 15408.

products [24].

Security is a cross-cutting concern in software intensive systems and should consequently be subject to careful requirements analysis and decision making. Moreover, in SPL engineering, security is one of the most important attributes concerning quality, given that a weakness in security can cause problems throughout all the products of a product line. Specifying requirements for a SPL is a challenging task [24], and specifying security quality requirements for a SPL is even more challenging due to the varying security properties required in different products. Therefore, the discipline known as Security Requirements Engineering is a very important part of the SPL development process for the achievement of secure SPL and products, because it provides techniques, methods, standards and systematic and repeatable procedures for tackling SPL security requirement issues throughout the SPL development lifecycle both to ensure the definition of security quality requirements and to manage variability of security properties. Nevertheless, software engineering methodologies and standard proposals of SPL engineering have traditionally ignored security requirements and security variability issues.

In the last few years, it has been a spectacular growing of security standards and security requirements related proposals, such as [3, 6-8, 14, 18, 20, 21, 27]. Recently, several attempts have also been made for defining SPL architectures for security, as those of [1, 5, 9], although they are more oriented to the software solution than to security requirements. Thus, neither of the proposals provides a systematic approach to manage and trace security requirements, with the aim of including security requirements variability in the models of a SPL. In addition, after

1. Introduction

In search for improved software quality and high productivity, software product line (SPL) based development has become the most successful approach in the reuse field, because it can help us significantly reduce time-to-market as well as development costs [2, 4], by maximizing software reuse and managing variability, which also assists in achieving software of high quality and maintaining a desired quality level of

REFERENCES

[1] Al-Fedaghi, S. Aspects of Personal Information Theory, 7th, The Seventh Annual IEEE Information Assurance Workshop (IEEE-IAW), West Point, NY: United States Military Academy, June 20-23, 2006.
 [2] Al-Fedaghi, S., Personal Information Model for P3P, W3C Workshop on Languages for Privacy Policy Negotiation and Semantics-Driven Enforcement, 17 and 18 October 2006, Ispra/Italy.
 [3] Beaugard, J. MODELING INFORMATION ASSURANCE, Thesis, Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio, March 2001. <http://www.iwar.org.uk/iwar/resources/usaf/maxwell/students/2001/aift-gor-ens-01m-03.pdf>
 [4] Blain, B. The Story of the Information Chain Theory, 2001 The Edwardsville Journal of Sociology, Volume 1. <http://www.siu.edu/SOCIOLOGY/journal/blain.htm>
 [5] Commission of European Communities. Information technology security evaluation criteria, version 1.2, 1991.
 [6] Hafiz M., and Johnson, R. Security Patterns and their Classification <https://netfiles.uiuc.edu/mhafiz/www/ResearchandPublications/sepataclassify.pdf>
 [7] Maconachy, W., Schou, C., Ragsdale D. and Welch, D. A Model for Information Assurance: An Integrated Approach, Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, United States Military Academy, West Point, NY, 5-6 June.
 [8] McCumber, John. "Information Systems Security: A Comprehensive Model". Proceedings 14th National Computer Security Conference, National Institute of Standards and Technology, Baltimore, MD, October 1991.
 [9] McCumber, J. "Application of the comprehensive INFOSEC Model: Mapping the Canadian Criteria for Systems Certification, Unpublished Manuscript, February 1993.
 [10] Tomhave, B. Alphabet Soup: Making Sense of Models, Frameworks, and Methodologies, 8/16/2005. http://falcon.secureconsulting.net/professional/papers/Alphabet_Soup.pdf

analyzing most of them in [23], we also concluded that neither of them facilitates the SPL products security certification against the most relevant international security standards with respect to the management of security requirements (such as mainly ISO/IEC 15408 [11], ISO/IEC 27001 [13] and ISO/IEC 17799 [12]).

In this paper, we will present a proposal for the management of the security requirements variability as an extension of our already presented Security Requirements Engineering Process for Software Product Lines (SREPLLine) [22], where it was only described the process and its workflows without explaining the security variability management nor the model that is supported by the Security Resources Repository. Therefore the aim of this approach is to deal with the security requirements artefacts variability from the early stages of the product line development in a systematic and intuitive way, in order to facilitate the conformance of SPL products to the most relevant security standards with regard to the management of security requirements, such as ISO/IEC 27001 and ISO/IEC 15408 (Common Criteria). To this end, we will propose a security requirements decision model driven by security standards in order to assist in the SPL products security certification as well as a security variability model to manage the variability and traceability of the security requirements related artefacts of the SPL and its products.

The rest of the paper is structured as follows. In section 2 we will present our Security Requirements Engineering Process for software Product Lines (SREPLLine). Next, in section 3, we will explain our proposal for the security requirements variability management in SREPLLine. Finally, in section 4, we will discuss our contributions and future work.

2. Overview of SREPLLine: security requirements engineering process for software product lines

The Security Requirements Engineering Process for software Product Lines [22] (SREPLLine) is an add-in development process model of an organization providing it with a security requirements engineering approach.

SREPLLine is a security features or security goals based process which is driven by risk and security standards (concretely ISO/IEC 27001 and Common Criteria) that deals with security requirements and their related artefacts from the early stages of SPL

development in a systematic and intuitive way especially adapted for SPL based development. It is based on the use of the latest security requirements techniques, such as security use cases [6] or misuse cases [27], as well as the integration of the Common Criteria (CC) components and ISO/IEC 27001 controls into the SPL lifecycle in order to facilitate SPL products security certification. Moreover, our proposed process suggests using a method to carry out the risk assessment which conforms to ISO/IEC 13335, specifically it uses Magerit [19] for both SPL risk assessment and SPL products risk assessment. Furthermore, SREPLLine has the aim of minimizing the necessary security standards knowledge as well as security expert participation during SPL products development. To this end, it provides a Security Core Assets Repository to facilitate the security artefacts reuse and to implement the security variability model and the security requirement decision model, that assist in the management of the variability and traceability of the security requirements related artefacts of the SPL and its products.

Our process is composed of two subprocesses with their respective activities: Product Line Security Domain Requirements Engineering subprocess and Product Line Security Application Requirements Engineering subprocess. These subprocesses cover the four basic phases of requirements engineering according to [15]: requirements elicitation; requirements analysis and negotiation; requirements documentation; and requirements validation and verification. At least, they have to be performed for each iteration of the Domain or Application Requirements Engineering Process of the SPL respectively.

3. Security requirements variability management

As the existing variability management approaches address functional variability instead of security requirements variability, in SREPLLine we will propose a Security Core Assets Repository to support the security variability model and the security requirement decision model described below in order to assist in security requirements and their related artefacts reuse, as well as in the management of commonalities and variabilities of security requirements artefacts and their traceability links in the SPL lifecycle. In essence, it is a knowledge repository with a structure to support holistic security requirements reasoning in SPL.

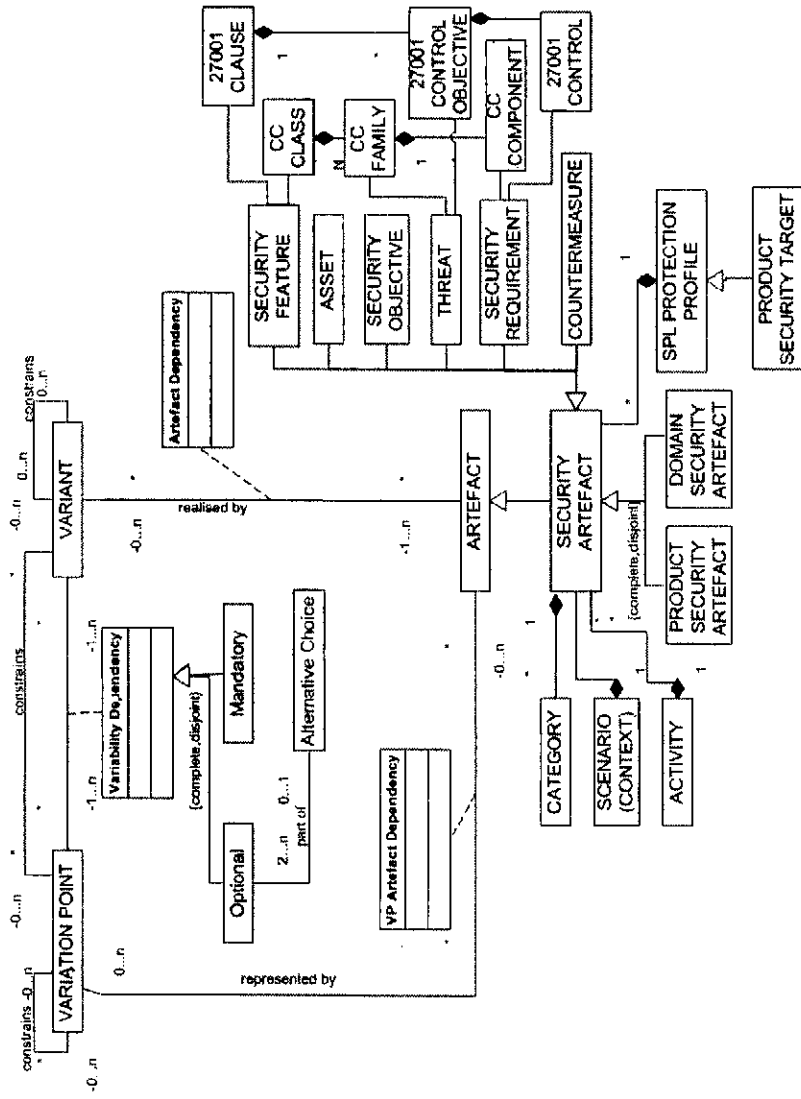


Fig. 1 Security variability meta-model

3.1. Security variability model

Our proposed Security Variability Model, which will be shown in Fig. 1 is based on the Reusable Assets Specification (RAS), adopted as OMG standard [25] and extends the orthogonal variability model of Pohl et al.[26] as well. Besides, it is part of the Security Requirement Decision Model. This variability model relates the defined variability to other software development models such as feature models, use case models, design models and test models. Thus, it is easier to adopt it in the SPL development methodology of an IT-department. Furthermore, it provides a cross-cutting view of the security variability across all security development artefacts and assists in keeping the different views of variable security requirements artefacts consistent.

The basic elements of our security variability model are defined in the meta model using UML 2 as shown in Fig. 1. The three main elements of the orthogonal variability model [26] are 'variation point' and 'variant' and 'artefact' classes.

The association class 'variability dependency' relates a variation point to at least one variant and vice

versa, and it could be either a mandatory or an optional relationship. The mandatory variability dependency states that a variant is required for a variation point to which it is related. This does not imply that this variant has to be included in all SPL applications. A mandatory variant is part of an application only if the related variation point is part of it. The optional variability dependency states that a variant related to the variation point can be part of a particular SPL application but does not need to be part of it. The alternative choice groups a set of variants which are related through an optional variability dependency to the same variation point and defines the range for the amount of optional variants to be selected for this group.

The 'variant to variation point constrains dependency' describes a relationship between a variant and a variation point where the selection of a variant requires or excludes the consideration of a variation point. A 'variant constraint dependency' describes a relationship between two variants, so that the selection of a variant requires or excludes the selection of another variant independent of the variation points the variants are associated with. Similarly, a 'variation

point constraint dependency' describes a relationship between two variation points, where a variation point requires or excludes the consideration of another variation point in order to be realised.

In addition, it is also important to relate the variability defined in the variability model to software artefacts specified in other models. Thereby, the meta-model depicted in Fig. 1 contains the class 'artefact' that represents any kind of development artefact. Particular development artefacts are sub-classes of the 'artefact' class, such as 'security artefact' which is a specialization of an artefact. A development artefact can but does not have to be related to one or several variants, but a variant must be related to at least one development artefact. Moreover, a development artefact can but does not have to be related to one or several variation points and vice versa.

Therefore, the Security Core Assets Repository, proposed in SREPPLine [22], must be integrated into the SPL core assets repository to facilitate these traceability links between the SPL variability model and the different types of security artefacts and the other development artefacts.

As it is depicted in Fig. 1, the 'security artefact' class has a complete and disjoint specialization relationship where any security artefact has to be a product security artefact or a SPL domain security artefact. Each 'security artefact' has to be part of the related artefacts of a development activity, but a development activity can but does not have to be related to one or several security artefacts. Similarly, a security artefact has to be part of a scenario (it has to have a context), although a scenario can but does not have to be related to one or several security artefacts. Furthermore, a security artefact can but does not have to be categorized. The 'category' class helps us avoid semantic problems and assists in reusing security artefacts, even in applying security patterns. It is a key class for the security requirement decision model, because it guides us throughout the categories to identify the security artefacts. Moreover, the class 'security artefact' has as version' as a mandatory attribute in order to facilitate the security artefacts versions traceability and variability, as there could be products with different versions of the same security artefacts.

Finally, in Fig. 1 we have represented the security standards variability, by integrating the Common Criteria (CC) elements, and the ISO/IEC 27001 controls into the security variability model. These security standards elements are related to the categories of some particular security artefacts

(security features, threats and security requirements) with the aim of assisting in the SPL or SPL products certification against these standards and making their reasoning easier.

3.2. Security requirement decision model

We treat security artefacts as a natural source of variability among the products or SPL artefacts. In order to capture and manage knowledge related to security requirements we propose a security requirement decision model for SPL engineering, which will be shown in a different figure (Fig. 2) to make its comprehension easier.

This model facilitates the security requirements related artefacts reasoning and the security standards conformance. It supports capturing, specifying and reasoning about security requirements for both SPL and SPL members.

In terms of security requirements, this model has as a prime objective to construct systems (products) that carefully balance the risk with the impact on SPL members, that is, with the economical impact of implementing the countermeasures related to these security requirements. The proposed model is not, however, intended to be a tool for risk assessment, but a validated methodology which conforms ISO/IEC 13335 [10], such as Magerit [19] is proposed to support this process.

As a starting point we used the goals/soft-goals [3] and feature models and their correlations in order to take into consideration functional and non-functional requirements, concretely security requirements. To express the intentions of a system, goal models as well as feature models can be used, and in most cases define similar information [26]. Therefore, the interest of starting from goal/softgoal model comes from the fact that it allows us to decide (if the traceability links are carefully established) what security features are needed to reach the selected security goals and which is the optimal set of security features/goals of a determined priority in the context of the different scenarios of the SPL that provides the rationale of the selection. This supposes a rise in the abstraction level of the variants selection process, making the selection in the requirements level instead of in the design level [17].

In addition, within this model we characterize a SPL as a set of 'variation points' which are represented by 'features' or 'goals', and each goal can be achieved by lots of concrete ways, which are represented as 'scenarios'.

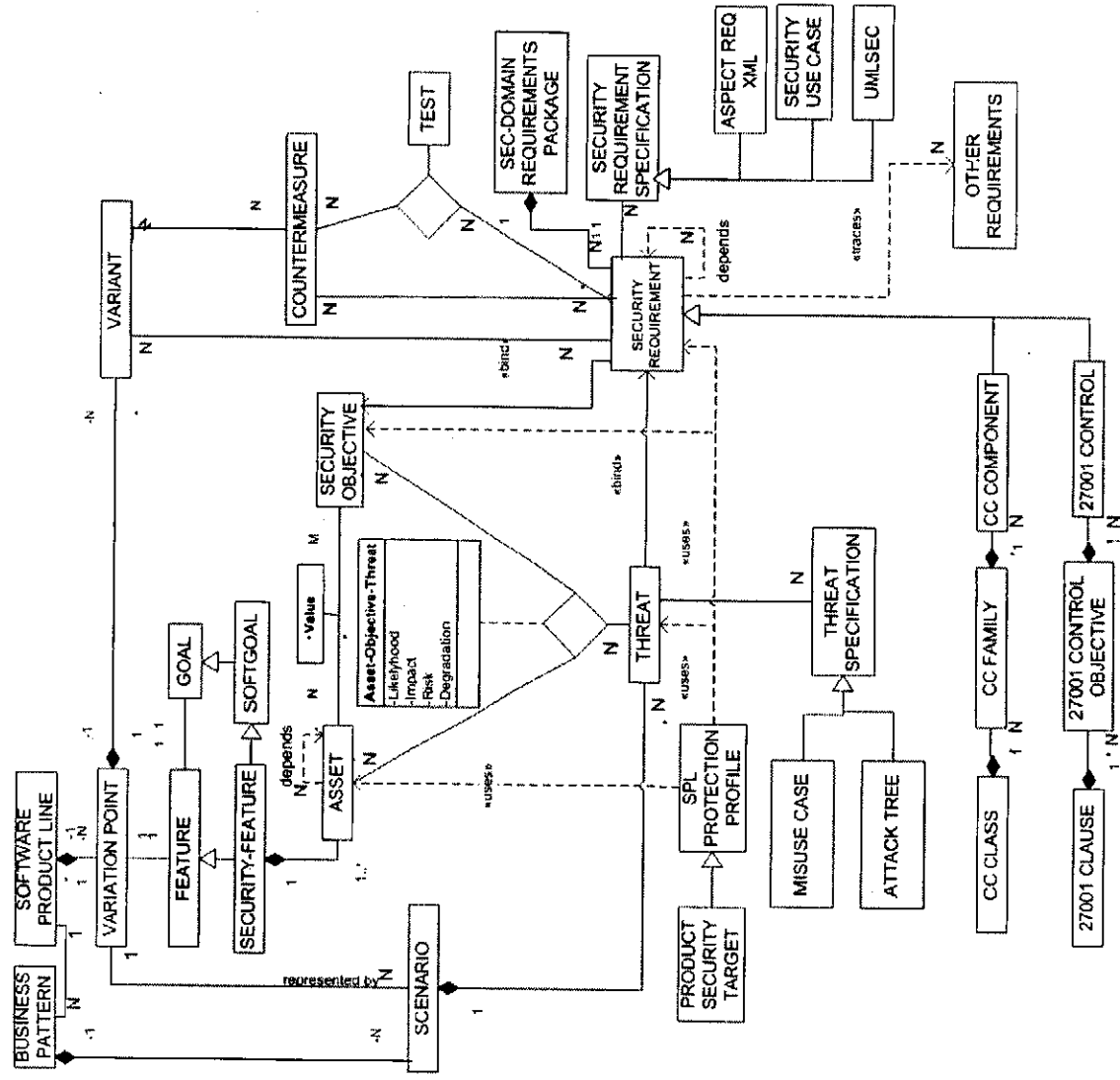


Fig. 2 Security requirement decision meta-model

The security core concepts that this model deals with are as follows: security feature, asset, security objective, threat, security requirement and SPL protection profile. Other supplementary security concepts include: risk, impact, degradation, likelihood, countermeasures and security standards concepts (CC and ISO/IEC 27001 concepts).

Security features are those features that describe security characteristics of the system which correspond with the security goals that the system under consideration should achieve. Thereby, a group of assets will be involved in the achievement of each security feature.

These assets are the resources in the information

systems of the SPL or related to them that are necessary for the organization to operate correctly and achieve their goals. And there will be different categories or types of assets (such as the environment, information systems, services, components and information or data). Moreover, there could be dependencies between assets. Also, an asset, as it is shown in Fig. 1, is a class which inherits from the 'security artefact' class, so it can be a 'variation point'. Each asset will have different related security objectives (or security dimensions) with the corresponding assigned value (following a standardized scale from 0 to 10 according to the risk methodology called Magerit [19]) which is agreed by

the stakeholders, who have also to reach an agreement about the common and optional assets. The valuation of each asset is given in each security objective and it is propagated through the dependencies tree assets, therefore only the higher assets in the dependency tree have to be explicitly valued.

The security objectives or security dimensions are the objectives which must be achieved in order to protect the organization business goals. Following Magerit [19], the security objectives/dimensions managed by the model can only be the following ones: integrity, confidentiality, availability, authenticity of service users, authenticity of data origin, accountability of service use and accountability of data access. Throughout the selected category/ies of the asset, this model could propose security objectives related to these categories to assist in the security objectives identification and valuation for each asset.

Furthermore, the assets are exposed to threats which can prevent the security objective from being achieved. Not all threats affect all assets nor all their security objectives so the common and optional ones have to be identified. In addition, there is a certain relationship between the category of the asset and what could happen to it. Thus, throughout the selected category/ies of the asset this model could propose threats or categories of threats related to these categories of assets to assist in the common and optional threats identification and valuation. To calculate the impact of each threat, the value of the assets of each security objective along with the degradation caused by the threat are taken into account. To estimate the risk, the impact and the likelihood of occurrence of the threat are taken into account. Then, the risk is classified in a range from 0 (negligible) to 5 (very high) (according to Magerit [19] scale).

Each type (category) of asset and depending on their associated categories of threats will have related a category or categories of security requirements that could mitigate the impact or reduce the likelihood of these threats. This mechanism facilitates the elicitation of the common and optional security requirements of the SPL as well as the security requirements instantiation in the products. Moreover, there could be dependencies between security requirements, so there could be security requirements packages structured by the security dimension of the requirements, that is, they are a group of security requirements that work together in order to mitigate the same threats and satisfy similar security objectives of the assets. However, there still could be groups of requirements,

as textual requirements by using aspect-XML specification [16].

The orthogonal variability model, in which our approach is based on, allows us to relate the different places at which the variability is defined to each other. In fact, starting from a changed artefact, other artefact affected by the change can be found by following the relationship with the associated variant and from the variant with the other associated artefact. Thereby, the variability of the security artefacts of the security decision model is clearly and unambiguously documented throughout the artefact dependencies of the security variability model.

4. Conclusions

Security requirements issues are extremely important in SPL because a weakness in security can cause problems throughout the lifecycle of a line. Although there have been several attempts to fill the gap between requirements engineering and SPL requirements engineering, there is not a systematic approach available for defining security quality requirements and managing the variability of them and their related security artefacts to the models of a SPL.

In [22] we only described the SREPLLine process and its workflows but it was not explained the management of the security variability nor the model that is supported by the Security Resources Repository. Therefore, the contribution of this work is that of providing, as an extension to SREPLLine [22], an holistic approach for the systematic management of the security requirements variability from the early stages of the product line development, in order to facilitate the conformance of the SPL products to the most relevant security standards with regard to the management of security requirements, such as ISO/IEC 27001 and ISO/IEC 15408 (Common Criteria). Our proposal defines a security requirements decision model driven by security standards in order to assist in the SPL security requirements definition and to facilitate products security certification. Moreover, it is proposed a security variability model to manage the variability and traceability of the security requirements related artefacts of the SPL and its products.

SREPLLine [22] together with the extension proposed in this paper is a suitable approach especially for SPL where security is a key quality issue. This is due to the broader impact of the existence or non-existence of specific security goals on all SPL

members, as well as to the level of management of variable security features required for the diversity of market segments.

Finally, further work is also required to develop a CARE (Computer Aided Requirements Engineering) tool to support SREPLLine and the Security Resources Repository, and to assist in the complex management and maintainability of the variability and traceability relations. Furthermore, we will carry out a refinement of our approach by proving it with a real case study to validate and deeply illustrate SREPLLine, with the aim of providing an holistic framework for security requirements engineering in SPL.

5. Acknowledgments

This paper is part of the ESFINGE (TIN2006-15175-C05-05), DSMD (TIN2005-25866-E) and ELEPEs (TIN2006-27690-E) projects of the Ministry of Education and Science (Spain), and of the MISTICO (PBC-06-0082) and DIMENSIONS (PBC-05-012-2) projects of the Consejería de Ciencia y Tecnología de la Junta de Comunidades de Castilla-La Mancha and the FEDER.

6. References

- [1] J. L. Arciniegas, J. C. Dueñas, J. L. Ruiz, R. Cerón, J. Bermejo, and M. A. Oltra, "Architecture Reasoning for Supporting Product Line Evolution: An Example on Security," in *Software Product Lines: Research Issues in Engineering and Management*, T. Kähkölä and J. C. Dueñas, Eds.: Springer, 2006.
- [2] J. Bosh, *Design & Use of Software Architectures*: Pearson Education Limited, 2000.
- [3] L. Chung, B. Nixon, E. Yu, and J. Mylopoulos, *Non-Functional Requirements in Software Engineering*: Kluwer Academic Publishers, 2000.
- [4] P. Clements and L. Northrop, *Software Product Lines: Practices and Patterns*: Addison-Wesley, 2002.
- [5] T. E. Faegri and S. Hallsteinsen, "A Software Product Line Reference Architecture for Security," in *Software Product Lines: Research Issues in Engineering and Management*, T. Kähkölä and J. C. Dueñas, Eds.: Springer, 2006.
- [6] D. G. Firesmith, "Engineering Security Requirements," *Journal of Object Technology*, vol. 2, pp. 53-68, 2003.
- [7] P. Giorgini, H. Mouratidis, and N. Zannone, "Modelling Security and Trust with Secure Tropos," in *Integrating Security and Software*

- Engineering: *Advances and Future Visions*, H. Mouratidis and P. Giorgini, Eds.: Idea Group Publishing, 2007, pp. 160-189.
- [8] C. B. Haley, R. Laney, J. D. Moffett, and B. Nuseibeh, "Arguing Satisfaction of Security Requirements," in *Integrating Security and Software Engineering: Advances and Future Visions*: Idea Group Publishing, 2007.
- [9] A. Immonen, "A Method for Predicting Reliability and Availability at the Architecture Level," in *Software Product Lines: Research Issues in Engineering and Management*, T. Käkälä and J. C. Dueñas, Eds.: Springer, 2006.
- [10] ISO/IEC, "ISO/IEC 13335 Information technology - Security techniques - Management of information and communications technology security - Part 1: Concepts and models for information and communications technology security management," 2004.
- [11] ISO/IEC, "ISO/IEC 15408:2005 Information technology - Security techniques - Evaluation criteria for IT security, (Common Criteria v3.0)," 2005.
- [12] ISO/IEC, "ISO/IEC 17799 Information technology - Security techniques - Code of practice for information security management," 2005.
- [13] ISO/IEC, "ISO/IEC 27001 Information technology -- Security techniques -- Information security management systems -- Requirements," 2006.
- [14] J. Jürjens, "UMLsec: extending UML for secure systems development," *UML 2002 - The Unified Modeling Language. Model Engineering, Languages, Concepts, and Tools. 5th International Conference*, vol. LNCS 2460, pp. 412-425, 2002.
- [15] G. Kotonya and I. Sommerville, *Requirements Engineering Process and Techniques*: John Wiley & Sons, 2000.
- [16] C. Kuloor and A. Eberlein, "Aspect-Oriented Requirements Engineering for Software Product Lines," presented at Proceedings of the 10th IEEE International Conference and Workshop on the Engineering of Computer-Based Systems (ECBS'03), 2003.
- [17] M. A. Laguna and B. Gonzalez-Baixauli, "Goals and MDA in Product Line Requirements Engineering," Department of Computer Science, University of Valladolid, Valladolid (Spain) GIRO-2005-01, 2005.
- [18] L. Liu, E. Yu, and J. Mylopoulos, "Security and Privacy Requirements Analysis within Social Setting," 11th IEEE International Requirements Engineering Conference, 2003.
- [19] F. López, M. A. Amutio, J. Candau, and J. A. Mañas, *Methodology for Information Systems Risk Analysis and Management*: Ministry of Public Administration, 2005.
- [20] J. McDermott and C. Fox, "Using Abuse Case Models for Security Requirements Analysis," presented at Annual Computer Security Applications Conference, Phoenix, Arizona, 1999.
- [21] N. R. Mead, "Identifying Security Requirements Using the Security Quality Requirements Engineering (SQUARE) Method," in *Integrating Security and Software Engineering: Advances and Future Visions*, H. Mouratidis and P. Giorgini, Eds.: Idea Group Publishing, 2007.
- [22] D. Mellado, E. Fernandez-Medina, and M. Piatini, "SREPLINE: Towards a Security Requirements Engineering Process for Software Product Lines," *9th International Conference on Enterprise Information Systems (ICEIS 2007). 5th International Workshop on Security In Information Systems (WOSIS-2007)*, pp. 220-232, 2007.
- [23] D. Mellado, E. Fernández-Medina, and M. Piatini, "A Comparison of the Common Criteria with Proposals of Information Systems Security Requirements," *First International Conference on Availability, Reliability and Security (ARES'06)*, pp. 654-661, 2006.
- [24] E. Niemelä and A. Immonen, "Capturing quality requirements of product family architecture," in *Information & Software Technology*, vol. 49, 2007, pp. 1107-1120.
- [25] OMG (Object_Management_Group), "Reusable Assets Specification (RAS)," ptc/04-06-06, 2004.
- [26] K. Pohl, G. Böckle, and F. v. d. Linden, *Software Product Line Engineering. Foundations, Principles and Techniques*. Berlin Heidelberg: Springer, 2005.
- [27] G. Sindre and A. L. Opdahl, "Eliciting security requirements with misuse cases," *Requirements Engineering 10*, vol. 1, pp. 34-44, 2005.

Author Index

The Third International Conference on Availability, Reliability and Security (ARES 2008)

Abbassi, Ryma.....	467	Blondia, Chris.....	1213
Abu-Nimeh, Saeed.....	1044	Bohner, Shawn.....	1443
Almed, Irfan.....	1028	Botham, Paul.....	253
Aickelin, Uwe.....	896	Böttcher, Stefan.....	771
Almeur, Esma.....	161	Bouillaut, Laurent.....	795
Aknin, Patrice.....	795	Boustia, Narhimene.....	1008
Al-Fedaghi, Sabah.....	1405	Bouvy, Pascal.....	1036
Al-Hammadi, Yousof.....	896	Bouzida, Yacine.....	204
Almohammad, Adel.....	544	Bræk, Rolv.....	597
Al-Saqabi, Khaled.....	1405	Brassard, Gilles.....	161
Amato, Flora.....	1097	Breu, Ruth.....	921
Angevine, Duff.....	1075	Broadway, Joshua.....	1361
Ansper, Arne.....	572	Brunstrom, Anna.....	526
Anzures-García, Mario.....	807	Buddendick, Christian.....	758
Ardi, Shanai.....	284	Bußer, Jens-Uwe.....	335
Arenas, Alvaro.....	1429	Byers, David.....	276
Ariet, Magi Lluch i.....	578	Canfora, Gerardo.....	1020
Armendáriz-Iñigo, Enrique.....	120	Casola, Valentina.....	1097
Arthur, Kweku.....	1388	Catrina, Octavian.....	693
Asnar, Yudistira.....	1240	Cavadini, Salvador.....	586
Atighetchi, Michael.....	1306	Cavalli, Ana Rosa.....	821
Ayuso, Pablo Neira.....	422	Cavallo, Bice.....	1020
Azer, Marianne.....	636, 881	Ceballos, Rafael.....	229
Azim, Muhammad Anwarul.....	1260	Cetinkaya, Orhan.....	1451
Azimah, Noor.....	1219	Challal, Yacine.....	503
Aziz, Benjamin.....	1429	Chang, Shuang.....	733
Bagaa, Miloud.....	503	Chaouchi, Hakima.....	144
Baldi, Mario.....	434	Charnsripinyo, Chalermpol.....	604
Balfe, Shane.....	376	Charoenpomwattana, Kulathap.....	659
Bao, Feng.....	112	Cheda, Diego.....	586
Barbaron, Denis.....	422	Chen, Chia-Mei.....	410
Barolli, Leonard.....	1325	Chen, Kuan-Ta.....	212
Benslimane, Djamel.....	834	Chen, Tsuhan.....	410
Bergmann, Mike.....	903	Chen, Xin.....	484
Bernabé-Gisbert, Josep M.....	369	Cheng, Jingde.....	171, 1219
Bertino, Elisa.....	153	Cheng, Yu-Chin.....	410
Bicarregui, Juan.....	1429	Chivers, Howard.....	1369
Bielova, Nataliia.....	128	Chmielewski, Łukasz.....	327
Bistarelli, Stefano.....	1128	Claeys, Geert.....	18
Blanco, Carlos.....	813, 1248	Clark, Andrew.....	47

Clint, Maurice 428
 Coetzee, Marijke 440
 Coma, Céline 821
 Cordy, James R. 1437
 Coudert, Fanny 975
 Croitoru, Madalina 578
 Cuppens, Frédéric 821
 Cuppens-Boulahia, Nora 821
 Damiani, Maria Luisa 153
 Daniels, Nils 1139
 Das, Ananda Swarup 446
 Dasmahapatra, Srinandan 578
 Debbabi, Mourad 302
 Dehbashi, Mehdi 491
 Delessy, Nelly A. 416
 Dios, Araceli Queiruga 741
 Domingo-Ferrer, Josep 990
 Donat, Roland 795
 Dragoni, Nicola 128
 Dssouli, Rachida 3
 Duarte, Angelo 653
 Dumortier, Jos 975
 Dupplaw, David 578
 Durrési, Arjan 1325
 Durrési, Mimoza 1325
 Ebben, P.W.G. 397
 Echizen, Isao 1287
 Eckert, Claudia 376
 El-Kassas, Sherif 636, 881, 1443
 Eloff, Jan H.P. 1388
 El-Soudani, Magdy 636, 881
 Eltoweissy, Mohamed 1443
 Encinas, Ascension Hernández 741
 Endersz, Viktor 1139
 Endo, Tsukasa 1287
 Engelmann, Christian 260, 659
 Eskeland, Sigurd 943
 Falcarin, Paolo 434
 Farazmand, Navid 33
 Farr, Erin 675
 Fatmi, Sihem Guemara El 467
 Faulkner, Mike 497
 Fazeli, Mahdi 33
 Fernandez, Eduardo B. 416
 Fernandez, José M. 161
 Fernández, Miguel 520
 Fernández-Medina, Eduardo 104,
 136, 813, 1248
 Fernandez-Medina, Eduardo 1413

Ferreres, Ana Isabel González-Tablas 363
 Florio, Vincenzo De 1213
 Fong, Martin 1306
 Formé, Jordi 701, 1000
 Franz, Elke 903
 Frei, Adrian 610
 Fries, Steffen 335
 Fuchs, Ludwig 752
 Furuichi, Hiroki 1294
 Gabarró, Joaquim 428
 Gaborit, Philippe 1052
 Gansterer, Wilfried 10
 Garg, Sanjam 667
 Garnacho, Arturo Ribagorda 363
 Gasca, Rafael Martínez 229
 Gasca, Rafael 422
 Ghinea, Gheorghita 544
 Ghorbani, Ali 88
 Gibb, Alex 578
 González-Vélez, Horacio 578
 Goto, Yuichi 171, 1219
 Grascner, Veronika 39
 Gritzalis, Stefanos 929
 Grob, Heinz Lothar 758
 Groba, Christin 903
 Gruschka, Nils 509
 Gu, Yu 630
 Guang-Yu, He 473
 Guntupalli, Srinivas 592
 Hadavi, Mohammad Ali 866
 Halunen, Kimmo 828
 Hamishagi, Vahid Saber 866
 Han, Kai 564
 Hansen, René Rydhof 1104
 Haque, Anwar 245
 Hargreaves, Christopher 1369
 Harmer, Terry 428
 Harper, Richard 675
 Hartel, Rita 771
 Hartmann, Peter 335
 Hashemi, S. Mehdi 1266
 Hassan, Abdel Wahab 636, 881
 Hassan, Riham 1443
 Hassanzadeh, Amin 982
 Hatebur, Denis 195
 Hazeyama, Hiroaki 1313, 1319
 He, Liwen 253
 He, Mingxing 746
 He, Xubin 260

Kerschbaum, Florian 693
 Keshri, Jitu Kumar 446
 Khakpour, Amir 144
 Khan, Latifur 237
 Kiani, Mehdi 47
 Kijisanayothin, Phongphun 765
 Kikuchi, Hiroaki 1282
 Kilpatrick, Peter 428
 Kim, Dong Seong 1260
 Kirmani, Ezzat 479
 Kirschner, Matthias 771
 Kitahara, Jun 1294
 Kitajima, Natsumi 171
 Kiyavitskaya, Nadzeya 1437
 Klaoudatou, Eleni 929
 Klopotek, Mieczyslaw 1036
 Kobori, Tomohiro 1282
 Kohler, Mathias 709
 Kolb, Mathias 39
 Kollveit, Heine 64
 Konstantinou, Elisavet 550, 929
 Korobitsin, Victor 967
 Koyanagi, Keiichi 842
 Kuang, Liwei 319
 Kumar, Ashwin 10
 Kupsch, James 1196
 Kutvonen, Lea 873
 Kwiat, Kevin 1180, 1234
 Ladra, Susana 994
 Lai, Gu-Hsin 410
 Laihi, Chi-Sung 410
 Langer, Josef 642
 Lari, Vahid 491
 Larrea, Mikel 801
 Larson, Ulf 624
 Lasheras, Joaquin 813
 Lasla, Noureddine 503
 Lathouwers, Danny 1091
 Laurent-Maknavicius, Maryline 144
 Leangsuksun, Chokchai 260, 659
 Lee, Jooyoung 1377
 Leesutthipornchai, Pakorn 604
 Lefevre, Laurent 422
 Leray, Philippe 795
 Levin, Timothy 787
 Lewis, Paul 578
 Lhee, Kyung-suk 1028
 Liang, Zhiyao 1067
 Lihan, Marc 842

Lin, Chih-Yin	458	Miremedi, Seyed Ghassem	491, 648	Piattini, Mario	104, 136, 813, 1248, 1413	Schlager, Christian	344, 752
Linskog, Stefan	526, 624	Miremedi, Seyyed Ghassem	33	Pjetzowski, Andreas	404	Schmidt, Holger	195
Ling-jun, Li	558	Mitchell, Chris	1013	Pimenidis, Lexi	221	Schwarz, Thomas	56
Liu, Bin	1382	Miyamoto, Daisuke	1319	Pironti, Alfredo	72	Scott, Stephen L.	260
Liu, Fenlin	1382	Mohades, Ali	1266	Pozza, Davide	851	Scott, Stephen	659
Liu, Qian	3	Mohay, George	47	Preneel, Bart	1091	Sebastianis, Maurizio	1240
Liu-sheng, Huang	558	Mokhtari, Aicha	1008	Pretschner, Alexander	1135	Seifzadeh, Habib	859
Lizarraga, Jesus	520	Moretti, Rocco	1240	Probst, Christian W.	1104	Seredynski, Marcin	1036
López, Javier	136	Morimoto, Shoichi	1219	Pujol, Grimena	80	Serna, Ainhoa	520
Lou, Jing-Kai	212	Morris, Thomas	452	Pujol, Gloria	1060	Seviora, Rudolph	383
Lu, Shuo	3	Mühlhäuser, Max	958	Quirchmayr, Gerald	179	Shahmehri, Nahid	276, 284
Luo, Weidong	746	Muñoz-Escóí, Francesc D.	369, 390, 514	Rakowski, Zbigniew	161	Sharma, Priyanka	592
Luo, Yonglong	727	Muñoz-Escóí, Francesc Daniel	120	Ravindran, Binoy	564	Sheng, Quan Z.	834
Luque, Emilio	653	Muto, Kenichiro	1294	Ravindran, Kaliappa	1234	Shigeno, Hiroshi	1340
Luttenberger, Norbert	509	Mylopoulos, John	1437	Ren, Shangping	1180	Shinde, Pravin	592
Maamar, Zakaria	834	Nagami, Yoshitaka	1319	Renner, Johannes	221	Shinzaki, Yasutaka	1340
Madlmayr, Gerald	642	Nair, Suku	1044	Rennhard, Marc	610	Shirazi, Hossein	866
Makanju, Adetokunbo	310	Nair, V.S.S.	452	Rexachs, Dolores	653	Shirazi, Mohammad Shokrolah	648
Maleki, Farhad	1266	Nait-Abdesselam, Farid	352	Rey, Angel Martin del	741	Shiri, Mohammed Ebrahim	1266
Maña, Antonio	80	Nalinuka, Katsiaryna	1112	Rico-Novella, Francisco	701	Shokrolah-Shirazi, Mohammad	491
Mangin, Christophe	204	Nappa, Dario	1044	Rico-Novella, Francisco J.	1000	Siahaan, Ida	128
Markides, Bradley	440	Narjess, Ayari	422	Riedl, Bernhard	39	Silvestri, Claudio	153
Martin, Cristian	801	Naughton, Thomas	659	Rikula, Pauli	828	Simoens, Koen	1091
Martinelli, Fabio	1120, 1128	Neubauer, Thomas	39, 187	Röning, Juha	828	Sisto, Riccardo	72, 851
Martinez, Asier	520	Nielson, Fleming	1104	Rosado, David G.	136	Siveroni, Igor	96
Martinez-Ballesté, Antoni	1060	Nielson, Hanne Riis	1104	Rossebo, Judith E.Y.	597	Slamanig, Daniel	1226
Martinez-Peláez, Rafael	1000	Nohara, Yasunobu	717	Røstad, Lillian	935	Slay, Jill	1355, 1361
Martinez-Peláez, Rafael	701	O'Brien, Richard	1306	Royer, Denis	779	Solanas, Agusti	1060
Mashimo, Yo	1340	Ofek, Yoram	434	Rubel, Paul	1306	Soler, Emilio	104
Massacci, Fabio	1112	Ohtaki, Yasuhiro	1083	Rudie, Karen	1188	Spainhower, Lisa	675
Mateo-Sanz, Josep Maria	1060	Okamoto, Eiji	497	Ruohomaa, Simi	873	Spanoudakis, George	96
Matsumoto, Yoshihide	1313	Okubo, Takao	1148	Sabbir, Ali	1234	Springer, Thomas	903
Matteucci, Ilaria	1120	Oleshchuk, Vladimir	943	Sadeghian, Babak	982	Srinathan, Kannan	446
Matthews, Brian	1429	Olivier, Martin	1388	Sadighi, Mohsen	859	Srivastava, Vaibhav	446
Matulevičius, Raimundas	1397	Onana, Flavien Serge Mani	161	Sáez, Carlos	578	Stakhanov, Oleg	88
Mayer, Nicolas	1397	Onno, Stéphane	683	Sakurai, Kouichi	112	Stakhanova, Natalia	88
Mazón, Jose-Norberto	104	Orwat, Mark	787	Salem, Benferhat	618	Stefanov, Veronika	104
Mazzeo, Antonino	1097	Osaka, Kyosuke	733	Salem, Boussad Ait	1052	Stewart, Alan	428
Mehdizadeh, Nima	648	Otto, Martin	335	Sánchez, Gerardo Rodriguez	741	Stingl, Christian	1226
Meland, Per Håkon	1164	Quadjaut, Abdelraouf	503	Sánchez-Gálvez, Luz A.	807	Strauch, Gereon	758
Melchor, Carlos Aguilar	1052	Pal, Partha	1306	Sangchi, Hasan Mokhtari	866	Stumpf, Frederic	376
Mellado, Daniel	1413	Panchenko, Andriy	221	Santini, Francesco	1128	Su, Chunhua	112
Memon, Nasrullah	1254	Páris, Jehan-François	56	Santos, Guna	653	Sun, Yifeng	1382
Mendivil, José Ramón González de	120	Park, Jong Sou	1260	Saran, Huzur	667	Takagi, Tsuyoshi	112, 733
Meyer-Wegener, Klaus	911	Peet, Andrew	578	Satizábal, Cristina	701, 1000	Takahashi, Osamu	733
Mich, Luisa	1437	Peine, Holger	1204	Satzger, Benjamin	404	Tamine, Karim	1052
Miedes, Emili	514	Pernul, Günther	344, 752	Scandariato, Riccardo	18, 434, 1156, 1421	Tan, Chik How	1275
Milios, Evangelos	310	Perrott, Ron	428	Schaad, Andreas	709	Tanaka, Hidehiko	1148
Miller, Barton	1196	Petković, Milan	889	Scharinger, Josef	642	Tartary, Christophe	1332

Notes

Tejada, José María de Fuentes		
García-Romero de	363	911
Terada, Masato	1282	1301
Thalheim, Bernhard	1405	1188
Thipsc, Aashay	765	26
Thuraisingham, Bhavani	237	572
Tielemann, Michael	911	1421
Tikotekar, Anand	659	237
Tingdi, Zhao	461	1091
Tjoa, Simon	179	1234
Tlili, Syrène	302	18
Töndel, Inger Anne	1172	675
Torra, Vicenç	990, 994	578
Torre, Marco Dalla	128	723
Toval, Ambrosio	813	461
Trujillo, Juan	104, 1248	733
Trumler, Wolfgang	404	1382
Tsuchiya, Takeshi	842	1429
Tupper, Melanie	950	484
Turnbull, Benjamin	1355, 1361	532, 538
Ueda, Shintaro	1340	717
Ungerer, Theo	404	921
Uribeceberria, Roberto	520	1332
Valencia-García, Rafael	813	497
Vallée, Geoffroy	659	473
Vélez, Iñaki	520	842
Venter, Hein	1388	1287
Verma, Rakesh	1067	245
Vicente, Javier	578	1421
Vittorini, Valeria	1097	237
Völp, Marcus	268	1346
Vorobiev, Alexandre	383	1240
Wahl, Martin	911	746
Walter, Thomas	1135	1437
Wang, Dongsheng	630	564
Wang, Hongji	532, 538	630
Wang, Hongyi	630	352
Wang, Huaxiong	1332	558
Wang, Lingyu	3	558
Wang, Qi	727	112
Wang, Xinlei	1044	Zincir-Heywood, A. Nur 950, 1075
Watanabe, Dai	1294	Zincir-Heywood, Nur 310
Wattanapongsakorn, Naruemon	604	Zisman, Andrea 96
Weber, Stefan G.	958	Zuccato, Albin 1139
Wei, Yang	558	Zulkernine, Mohammad 245, 319, 1188
		Zurutuza, Urko 520

CPOC Chair

Chita R. Das
Professor, Penn State University

Board Members

Mike Hinchey, *Director, Software Engineering Lab, NASA Goddard*
Paolo Montuschi, *Professor, Politecnico di Torino*
Jeffrey Voas, *Director, Systems Assurance Technologies, SAIC*
Suzanne A. Wagner, *Manager, Conference Business Operations*
Wenping Wang, *Associate Professor, University of Hong Kong*

IEEE Computer Society Executive Staff

Angela Burgess, *Executive Director*
Alicia Stickley, *Senior Manager, Publishing Services*
Thomas Baldwin, *Senior Manager, Meetings & Conferences*

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 250 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: cps@computer.org or telephone +1-714-821-8380. Fax +1-714-761-1784. Additional information about *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 *Authored 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/ieeecs>. To submit questions about the program or send proposals, please e-mail jwilson@computer.org or telephone +1-714-816-2112. 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/ieeecs/publications/books/about.html>

Revised: 21 January 2008

CPS Online is our innovative online collaborative conference publishing system designed to speed the delivery of price quotations and provide conferences with real-time access to all of a project's publication materials during production, including the final papers. The **CPS Online** workspace gives a conference the opportunity to upload files through any Web browser, check status and scheduling on their project, make changes to the Table of Contents and Front Matter, approve editorial changes and proofs, and communicate with their CPS editor through discussion forums, chat tools, commenting tools and e-mail.

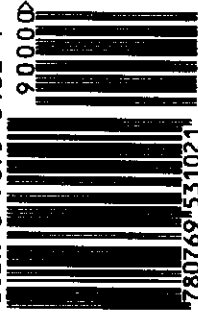
The following is the URL link to the **CPS Online** Publishing Inquiry Form:
http://www.ieeeconpublishing.org/cpir/inquiry/cps_inquiry.html



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

IEEE Computer Society Order Number P3102
Library of Congress Number 2007909935
ISBN 0-7695-3102-4

ISBN 0-7695-3102-4



9 780769 531021