



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

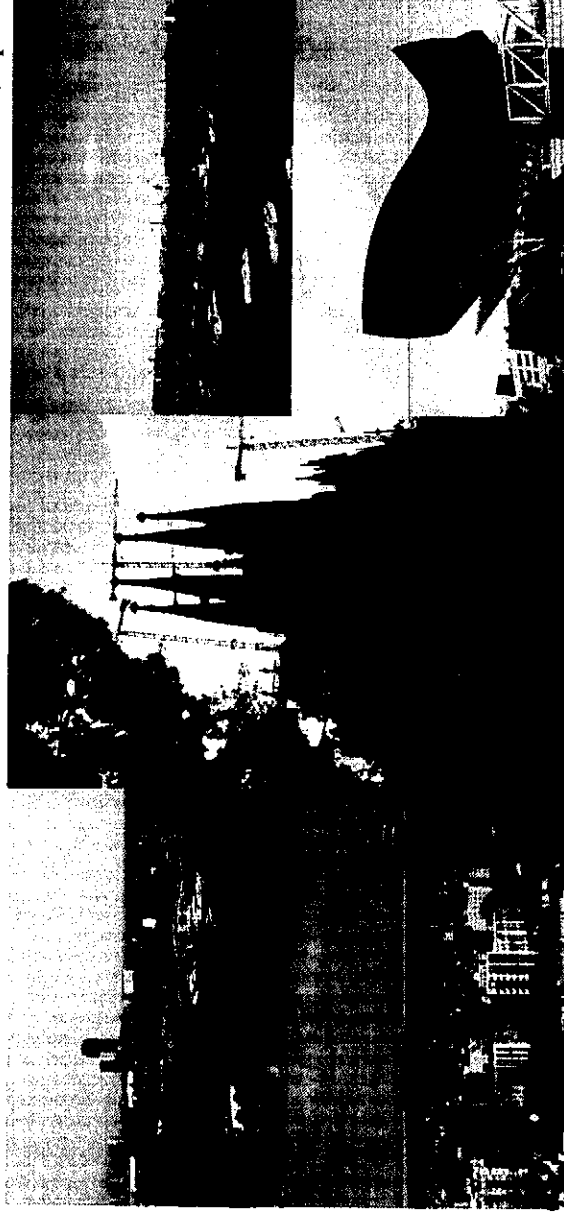
# ARES 2008

## The Third International Conference on Availability, Security and Reliability

### PROCEEDINGS

March 4-7, 2008

Barcelona, Spain



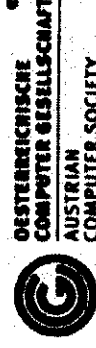
Edited by Stefan Jakoubi, Simon Tjoa, and Edgar R. Weippl

Organised by

**[SECURE]**  
Business Austria



In cooperation with



*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

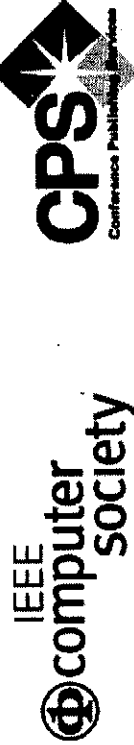
*Additional copies may be ordered from:*

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](mailto: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](mailto:tokyo.ofc@computer.org)

*Individual paper REPRINTS may be ordered at:* <[reprints@computer.org](mailto: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 Grascher, 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 Sahaan*
- 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-Maknawicius, 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*

<b>Session 10: IDS and Models</b>	
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>	
<b>Session 11: Trust, Security and Economics</b>	
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>	
<b>ARES Short Paper Sessions</b>	
<b>Session 1: Applications</b>	
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>	
<b>Session 2: Services and Trust</b>	
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>	
<b>Session 3: Privacy and Safety</b>	
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	<b>Session 6: Crypto and Health</b>	
<b>Session 4: Networks</b>		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 Anspser</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 Lluich 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	<b>Session 7: Models and Networks</b>	
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 Rohv 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	<b>Session 8: IDS</b>	
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
<b>Session 5: Crypto</b>		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		

<b>Session 9: Hardware</b>	
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
<b>Workshop FARES</b>	
<b>Session 1: Miscellaneous</b>	
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
<b>Session 2: Access Control and Algorithms</b>	
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
<b>Session 3: Crypto</b>	
New Self Certified Proxy Digital Signature Scheme based on Elliptic Curve Cryptosystem <i>Youn 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
<b>Session 4: Risk Management</b>	
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  $\Omega$ 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 Artsiom 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>	
<b>Workshop SECSE</b>	
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
<b>Workshop WSDF</b>	
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
<b>Workshop DAWAM</b>	
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
<b>Workshop WAIS</b>	
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

## PSecGCM: Process for the development of Secure Grid Computing based Systems with Mobile devices

David G. Rosado<sup>1</sup>, Eduardo Fernández-Medina<sup>1</sup>, Javier López<sup>2</sup> and Mario Piattini<sup>1</sup>

(1) Group Research Alarcos, Information Systems and Technologies Department UCLM-Indra Research and Development Institute. ESI. University of Castilla-La Mancha Ciudad Real  
{David.GRosado, Eduardo.Fdez-Medina, Mario.Piattini}@uclm.es

(2) Computer Science Department University of Málaga 29071, Málaga, Spain  
jlm@lcc.uma.es

### Abstract

Mobile Grid, in relevance to both Grid and Mobile Computing, is a full inheritor of Grid with the additional feature of supporting mobile users and resources in a seamless, transparent, secure and efficient way. Security of these systems, due to their distributed and open nature, receives great interest. A formal approach to security in the software life cycle is essential to protect corporate resources. However, little thought has been given to this aspect of software development. Due to its criticality, security should be integrated as a formal approach in the software life cycle. A methodology of development for secure mobile Grid computing based systems is defined, that is to say, an engineering process that defines the steps to follow so that starting from the necessities to solve, we can design and construct a secure Grid system with support for mobile devices that is able to solve and cover these necessities.

### 1. Introduction

The Grid idea is mainly focused on the remote access to computational resources, thus solving the problem of coordinating the resources shared between virtual, multi-institutional and dynamic organizations. When talking about sharing, we refer not only to files interchange but also to direct access to computers, software, data and other resources that are required by multiple applications in the fields of industry, science or engineering [1].

Mobile Computing is a generic term describing the application of small, portable, and wireless computing and communication devices. The Mobile Computing focuses on the requirement of providing access to information, communications and services everywhere, anytime and by any available means. The technical solutions for achieving this are not always easy to implement [2].

Security has been a central issue in grid computing from the outset, and has been regarded as the most

significant challenge for grid computing [3]. The characteristics of computational grids lead to security problems that are not addressed by existing security technologies for distributed systems [4]. But now the growing size and profile of the grid require comprehensive security solutions as they are critical to the success of the endeavour [5]. So, the grid must have mechanisms and security policies that are in charge of checking out that only authorized users have access to the resources provided by it [6, 7].

In many cases, constrained wireless networks are made up of devices that are physically constrained and therefore have little room for memory, batteries, and auxiliary chips. These constraints introduce significant challenges that have to be addressed in order to maintain a secure network [8]. Security over the mobile platform is more critical due to the open nature of wireless networks. In addition, security is more difficult to implement into a mobile platform due to the limitations of resources in these devices. Therefore, a Grid infrastructure that supports the participation of mobile nodes will play a significant role in the development of Grid computing.

On the other hand, a Grid system is a software that has been developed by means of a certain technology and that fulfills a set of characteristics and own functionalities of the Grid. As it is software, the problems that have arisen and given rise to numerous researches in the last years are those of considering and integrating security into the whole software lifecycle [9, 10]. In addition, if we add the appearance of a new technology where security is fundamental and the advance that mobile computation has experienced in the last years it appears the need to define, consider and develop a methodology of development in which, from the initial state to the final state, all the requirements related to Mobile Grid systems are analyzed and integrated. This process must make it easier for developers the analysis and characterization of all functional and security necessities during all stages of the development cycle of the software based

on Grid technology as well as support the mobile devices.

In this paper, we will begin to construct the foundations of a process or ordered methodology of systematic development that serves as guide for the development of any Grid system with mobile devices, considering all the aspects of security during all phases of development obtaining, as a result, a secure, robust and scalable Mobile Grid system.

In next section, the importance of mobile Grid computing will be described. In section 3, we give a brief overview of the wireless and mobile environment. Section 4 is the main contribution of the paper, and the initial proposal of the process of systematic development to construct a secure Grid system that supports the mobile devices will be stated. We will finish by putting forward our conclusions as well as some research lines for our future work.

### 2. Mobile Grid Computing

At first glance, it seems that the marriage of mobile wireless consumer devices with high-performance grid computing would be an unlikely match [11]. The interest to incorporate mobile devices into Grid systems has arisen with two main purposes. The first one is to enrich users of these devices while the other is that of enriching the own Grid infrastructure. Both sides benefit from this fact since, on the one hand, the Grid offers its services to the mobile users to complete their works in a fast and simple way and on the other hand, the mobile devices offer their limited resources, but million of them, in any place and at any time, endorsed by the fast advance in the yield and capacity that is being carried out in the mobile technology.

There are certain researches in the field of Grid environments with mobile devices [12-14], that deal with the problem and the difficulty to incorporate into the existing Grid systems, mobile devices and terminals that can consume services and share their resources since they are flexible, heterogeneous and limited. This fact makes their incorporation into a fixed platform even more difficult.

Today, the development of wireless technology and mobile devices enables us to access the network service from anywhere at any time [15]. Although mobile devices promote mobile communication and flexible use, they still bring problems such as unpredictable quality of the network, low confidence, limited resources (energy, bandwidth, etc.) and periods of disconnections [16]. Provided that mobile devices have limited computing capacity, the Grid becomes an important computation service provider that enables mobile users to perform complicated jobs [17]. On the

other hand, the performances of current mobile devices have significantly increased, reason why laptops and PDAs can provide aggregated computational capability when gathered in hotspots, forming a Grid on site. This capability can improve the use of Grid applications even in places where this would be imaginary.

### 3. Wireless and Mobile Computing

One of the main problems of wireless technologies is that the provided bandwidth is, in terms of magnitude, lower than in wired networks and, as a consequence, the signal loss is very frequent and the noise level is influenced by the external conditions. A second aspect is related to mobile devices themselves which are characterized by a scarce amount of resources in terms of CPU, RAM, display, storage and, in particular, the fact that they are equipped with small batteries that limit power consumption and affect both the wireless transmission and the access to services that require a high computational load. Finally, a third aspect that is necessary to consider is user mobility since it causes problems related to signal loss during the movement in a new cell (handoff), to the address management due to the crossing of different administrative domains as well as to the need of adapting services to the real position of the user [18].

Mobile computing is characterized by four constraints: Mobile elements are resource-poor relative to static elements. Mobility is inherently hazardous. Mobile connectivity is highly variable in performance and reliability. Mobile elements rely on a finite energy source. These constraints are not artifacts of current technology, but are intrinsic to mobility. Together, they complicate the design of mobile information systems and require us to rethink traditional approaches to information access [19].

### 4. Methodology of development

#### 4.1. Overview

Our objective is to provide developers with firstly a methodology or development systematic process that will include the complete development of Grid systems of whatever complexity and magnitude, and secondly an architecture that helps them develop a secure Grid system where support for mobile devices is defined.

This systematic engineering process will mainly face two great challenges: On the one hand, to establish a methodology for the secure development of the Grid systems, not only considering the functional needs, but also the non-functional ones, especially security not only of the system to be constructed but

also of the necessities arising when implementing it using the Grid technology. On the other hand, the second challenge to solve is the use of mobile devices in Grid systems, with all the difficulties that constructing a Grid infrastructure that supports mobile devices entails, due to the limitations and characteristics of these devices.

For that reason, having a methodology of development centered in Grid systems, that provides a secure development and supports mobile devices is a great advance in the field of Grid systems and mobile devices. Simultaneously, it supposes a powerful tool for the developers of these systems.

#### 4.2. Development Process Approach

The systematic process of development is an iterative and incremental process. An iterative approach proposes an incremental understanding of the problem through successive refinements and an incremental growth of an effective solution through several versions. Thus, in each iteration of the process, new and necessary characteristics can be added and extended so that a complete final design is obtained. In this first proposal, and following some methodologies like the Unified Process [20], we will present a general vision of the development methodology, leaving a more detailed study for future researches.

The methodology to develop a systematic process will consist of different phases, each one of them will also be divided into stages, and these last ones into activities and tasks. Our methodology will initially consist of 3 phases (see Figure 1). In all phases and stages we must take into account many features associated with grid environments [4] during the life cycle: user population, resources pool, and the group of processes running on different sites are potentially large and dynamic; a user may be associated with different local name spaces or credentials; local authentication, authorization and access control may apply at different sites; individual users may be associated with different local name spaces, credentials and accounts at different sites.

#### 4.4. Stages of the Methodology

**4.4.1. Planning Stage.** Apart from the typical aspects of any planning stage, other aspects related to the mobile grid described here, are taken into account. Security is a much more important factor in planning and maintaining a grid than in conventional distributed computing, where data sharing comprises the bulk of

the activity. It is important to understand exactly which components of the grid must be rigorously secured to detect any kind of attack.

While a grid-based environment may offer many advantages, any given application may not necessarily benefit from a grid. For example, some personal productivity applications are tightly coupled with a user's interface and do not consume a large amount of computing resources. Running them on a grid may not provide significant benefits. However, other applications may be very suited for exploiting a grid. To determine if existing or planned applications that are CPU intensive can take advantage of a grid environment requires many considerations. In this stage, we must describe some aspects to be considered related to the possible applicability of a grid to these applications, for example, to determine whether calculations can be performed parallelly, to consider the amounts of data needed to be sent to the node performing a calculation and the time required to send it, etc. Both portability and the capability to take advantage of virtual resources are key attributes of an application that can take advantage of grid computing.

*Activities:* This stage is composed the following activities (see Figure 2):

- A1: Initial Study. It collects data and organizes them so that they can be used, identifying the objectives, reach and scope of the mobile grid system.
- A2: Identification of Necessities. It identifies the necessities that are due to cover, taking into account the user's necessities, the grid considerations and the limitations of the mobile devices
- A3: Definition of the Virtual Organization. To identify the group of the implied ones that they will take part in the development process, to determine the functions to carry out, and necessary and final products.
- A4: Study of current Mobile Grid systems. It selects and studies the current mobile Grid systems, valuing their characteristics and deficiencies to take them into account in later steps.
- A5: Definition of the technologic mobile Grid Architecture. The administrator should understand the organization's requirements for the mobile grid to better choose the grid and mobile technologies that satisfy those requirements.
- A6: Study of viability. It studies the different solutions alternatives considering the products to develop or use, the necessities, dates, costs, risks, scope and to study the impact of the solution with Grid technology.

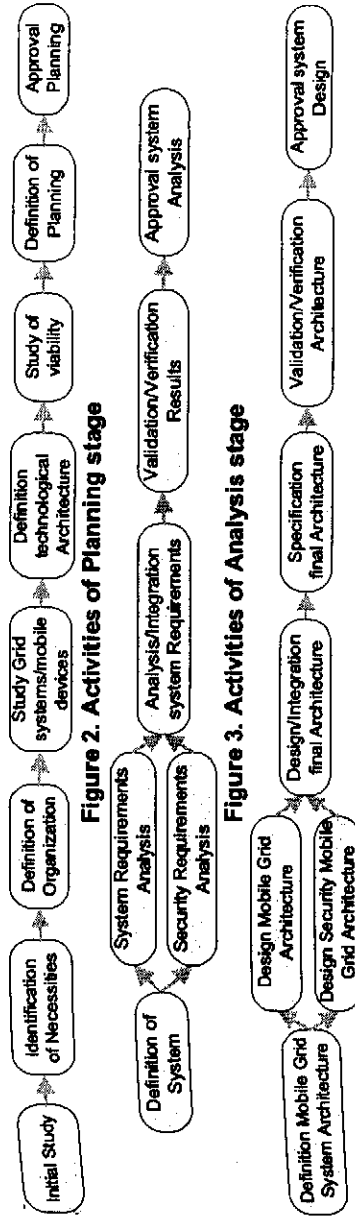


Figure 2. Activities of Planning stage

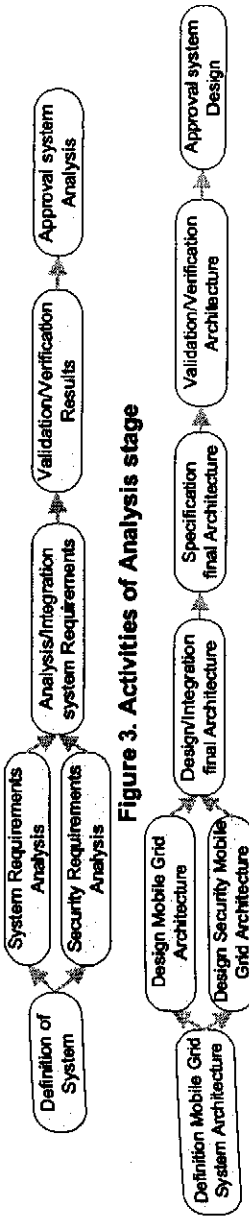


Figure 3. Activities of Analysis stage

Figure 4. Activities of Design stage

▪ A7: Definition of Planning. It defines the plan of the project indicating the objectives and necessities that cover, the implied ones in each stage, intermediate and final obtained results, technical and human resources to use, documentation to elaborate, obtained benefits, etc.

▪ A8: Checking and Approval of the Planning. It reviews the results of the planning as well as those of approving the final result if all the people in charge are in agreement.

*Input Artifacts:* Business description (strategy, principles, goals and drivers), Time limits, Organizational constraints, Budget information, financial constraints, Current architecture/IT system description, Description of developing organization, Description of resources available to the developing organization, Technology specification (Grid computing, wireless and mobile devices)

*Output Artifacts:* Problem description (purpose of scenario), Detailed objectives, Actors and their roles and responsibilities, Project description and scope, Project plan and schedule, Architecture vision, Technical requirements, Refined statements of business goals and strategic drivers, Catalogue of necessities and requirements of system, norms and standards to use, Security necessities for the system, grid environment and mobile devices, work plan structured.

*Techniques, Practices and Reference guides:* Cataloging, Grid design workshops, UML (Diagrams, Use cases, models, etc.), Interviews, project Planning, Study of Cost-benefit, Impact on the Organization, Risk Management, Change Management, Documentation, Tests

*Main Roles:* Customer experts, Project Manager, Business modeler, Project team, Analysts, Security experts, Grid Computing experts, Mobile technology and Mobile devices experts, External entities

**4.4.2. Analysis Stage.** Apart from the typical aspects of any analysis stage, other aspects related to the

mobile grid described here, are taken into account. We should define the most common general security requirements and challenges associated with grids [21]. Among them, we can find the following ones: Authentication; Confidentiality; Integrity; Authorization and access control; Freshness; Scalability; Trust; Single sign-on; Delegation; Privacy; Non-repudiation; Availability; Credentials; Exportability; Interoperability; Integration; Uniform credentials and certification infrastructure. For mobile computing, there are five fundamental requirements for any type of data security, including wireless Authentication, authorization and accounting (AAA); Data integrity; Privacy, Non-repudiation; Security policies. All of these factors are at play in the wireless and mobile device world [22].

Applications and their requirements should be analyzed to understand how they could be designed and developed to reap the benefits of a grid. To properly secure your grid environment, there are many different tools and technologies available. This stage analyzes some of those technologies.

*Activities:* This stage is composed of the following activities (see Figure 3):

- A1: Definition of Mobile Grid System. It describes the system adapting the previous results and limiting the reach of the system to identify standards, norms and tools to use and describe all the relevant information to consider in this stage. It identifies the grid components as well.
- A2: Mobile Grid System Requirements Analysis. It defines and analyzes general both functional and non-functional requirements of the mobile grid system, for example, heterogeneity of the computing resources, geographical and organizational distribution of the resources, scalability, availability, mobile accessibility, mobility restrictions, limited resources, disconnections, QoS, distributed storage, job execution, autonomy, etc.
- A3: Mobile Grid System Security Requirements Analysis. It defines and analyzes the security



requirements of the mobile Grid system, for example, trust, single sign-on, delegation, privacy, non-repudiation, credentials, confidentiality, integrity, authentication, encryption, certificates, keys, etc.

■ A4: Mobile Grid System Requirements Integration. It integrates all the requirements analysis identified in previous stages obtaining a full analysis of all requirements of secure mobile grid system and an analysis model.

■ A5: Validation and Verification of Results. During the course of some designs the requirements can change at the last minute or may go undiscovered. Requirements also have a way of changing when you least expect them to, so it is always a good idea to validate them before you proceeding.

■ A6: Approval of System Analysis. It validates the obtained results and the analysis. It approves the analysis of the system.

*Input Artifacts:* Output artifacts of the Planning stage, the Validation report and the modifications (of the construction stage), Business domain, Use cases models, Use cases of security models, Reports of threats and risks, List of Requirements and Security Requirements (of generic system, of Grid systems and of mobile devices), Specific standards, Policies of security, Manuals, System Constraints.

*Output Artifacts:* Catalogue of requirements and security requirements of the system on a Grid environment with mobile devices, Specification of Requirements and Security requirements of the final system, Analysis model, Report of analysis validation, Report of failures or errors found.

*Techniques, Practices and Reference guides:* Meeting and interviews, UML, UMLSec, cost-benefit analysis, abuse cases, tree of threats, security use cases.

*Main Roles:* Project Manager, Business modeler, Requirements engineer, Security requirement engineer, Systems Analyst, Security Analyst, Risk expert, System Architect, Security Architect, Grid Computing expert, Mobile technology and mobile devices expert.

**4.4.3. Design Stage.** Apart from the typical aspects of any design stage, other aspects related to the mobile grid described here, are taken into account. The participants and users of the grid can be members of several real and virtual organizations. The grid can help in enforcing security rules among them along with implementing policies, which can resolve priorities for both resources and users. Many or most of the grid middleware, technologies, and system components are probably new to many people within the design team and it is always a good idea to hear firsthand experience. Once the functional and non-functional requirements are known, the architect should readily be able to select the type of grid and the best topology

required to satisfy the majority of the business requirements.

Given that grid solutions are adaptable to meet the needs of various business problems, different types of grids are designed to meet specific usage requirements and constraints. Any design will require a basic set of system management tools to help determine availability and performance within the grid. A design without these tools is limited in how much support and information can be provided about the health of the grid infrastructure. The storage possibilities are endless within a grid design. How that storage will be secured, backed up, managed, and replicated are some of the questions that the grid design will try to answer. In this world of mobile broadband, IT managers have several primary concerns about wireless security. Namely, they want to make certain that their current, wired networks remain secure, and they want to ensure that only authorized and authenticated users are accessing that network [22].

*Activities:* This stage is composed of the following activities (see Figure 4):

■ A1: Definition of the Mobile Grid System Architecture. It describes the generic architecture, elements, grid components, subsystems, security services, mechanisms, patterns, etc. Besides, it describes the generic Mobile Grid architecture and its technological environment.

■ A2: Design of the Mobile Grid System Architecture. It designs and analyzes the mobile grid architecture obtaining an architecture that covers all the necessities of the system (generic, grid and mobile necessities).

■ A3: Design of the Security Mobile Grid Architecture. It designs and analyzes the security mobile grid architecture obtaining a security architecture that covers all the security necessities of the system (security generic, security grid and security mobile).

■ A4: Integration and Design of the final Architecture. It designs and analyzes the resulting architecture relating and integrating the previous architectures to obtain a final architecture of reference that covers all the necessities of the secure mobile Grid system.

■ A5: Specification of the final Architecture. It specifies the final architecture in a coherent way, by precisely describing the grid components, elements and relations and all the details of the designed architecture, using some ADL, design models and views and points of view with security aspects.

■ A6: Validation and Verification of the final Architecture. It verifies that in the designed architecture, all the elements that appear to be correct are justified and it validates that the design covers the initial necessities of the system.

■ A7: Approval of the System Design. It presents and approves the design of the final architecture.

*Input Artifacts:* Output artifacts of Analysis stage, Best practices, Technological environment, reference architecture, security architecture, design constraints, grid characteristics and mobile functionalities.

*Output Artifacts:* Architecture design, Description of the architecture, Specification of the architecture with ADL, Detailed specification of components, elements, relations, etc., Design models, Report of fulfillment of requirements in the architecture, Report of validation of design.

*Techniques, Practices and Reference guides:* Walkthroughs, Design Patterns, Security patterns, UML, UMLSec, Revisions, Monitoring, Documentation.

*Main Roles:* Project Manager, Systems Analyst, Security Analyst, Risk expert, Security developer, System Architect, Security Architect, Security Designer, Integrator Engineer, Grid Computing expert, Mobile technology and mobile devices expert.

**4.4.4. Construction Stage.** Apart from the typical aspects of any construction stage, other aspects related to the mobile grid described here, are taken into account. The degree of security involved is based on the type of grid topology as well as on the data that the security will be protecting. The security requirements for a grid design within a bank will be completely different from those of an academic institution doing research. Grids can be built in all sizes, ranging from just a few machines in a department to groups of machines organized as a hierarchy spanning the world. We must define the grid system topologies (intragrid, extragrid or intergrid) that we are aimed at building as a means for identifying the necessary technical, infrastructural, and other middleware components and subsystems for a grid infrastructure. The infrastructure represents the physical hardware and software components used to interconnect different grid computers. These components help support the information flow between grid systems and provide the basic set of services for connectivity, security, performance availability, and management. While

many of these infrastructure components supply basic functionality to the grid, many others are optional. It will be up to you to decide on the requirements and how well these components match up to the needs of your design. There are numerous software-based ways to safeguard mobile devices, virtual private networks (VPNs), firewalls, on-device data encryption software and device management solutions, to name just a few.

*Activities:* This stage is composed of the following activities (see Figure 5):

■ A1: Environment Preparation. It assures that all the tools and equipment are available for the construction of the mobile grid system.

■ A2: Implementation of the Mobile Grid System Architecture. It identifies the significant components of the architecture and implements these components using the means available, mechanisms and services, as many of the Grid technology as of the mobile devices.

■ A3: Implementation of the Security Mobile Grid Architecture. It implements the grid components or security elements of the architecture using not only the tools available from the technological platform Grid but also from well-known software tools of security.

■ A4: Integration and Implementation of the final Mobile Grid Architecture. It integrates all the components implemented in the previous stages to give rise to the construction of a stable architecture and that can be proven.

■ A5: Design and Execution of tests. It designs and defines the tests verifying that the requirements, the grid components and the complete system are correct. The different tests and results will be handled, so that it is possible to go back to the previous stages if defects important to be fixed appear.

■ A6: Evaluation of tests. It analyzes the test results and evaluates them according to the awaited results. It also determines the reach of the possible modifications, costs, resources, etc.

■ A7: Elaboration of Manuals and Documentation. It elaborates the necessary documentation necessary to provide the user with. Furthermore, it deals with the preparation and formation of the user, the definition

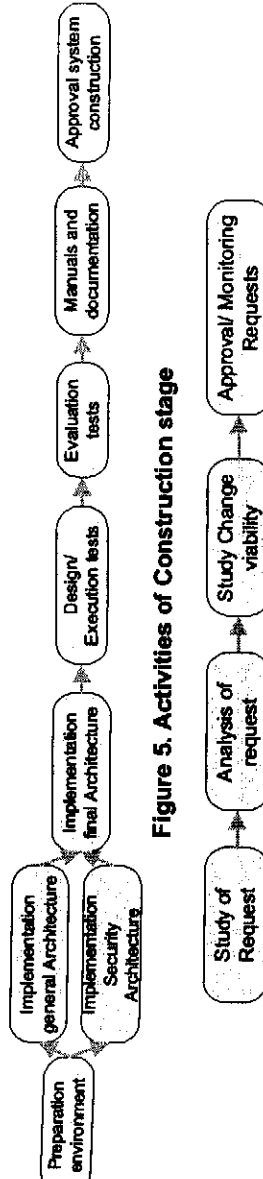


Figure 5. Activities of Construction stage



Figure 6. Activities of Maintenance stage

of the delivery formats, supports, etc.

- A8: Approval of System Construction. It approves and accepts the constructed system studying the results obtained in the previous stages and making sure that the system is correct and stable to be given to the user.

**Input Artifacts:** Output artifacts of the Design stage, specification of technological environment, implementation standards, grid and wireless and mobile technology, security mechanisms and procedures test environments, relevant technical requirements.

**Output Artifacts:** Built Secure Grid system with mobile devices, Result of tests, Report of test evaluation, documentation and manual of user, Plan of trainers, Evaluation of errors and changes.

**Techniques, Practices and Reference guides:** Tests, revisions, Implementation methods, security verification, Monitoring

**Main Roles:** Test Engineer, Trainers, Technical team, Systems Analyst, Security Analyst, Security expert, Security developer, Integrator Engineer, Programmers, Architects Team, Grid Computing expert, Mobile technology and mobile devices expert.

**4.4.5. Maintenance Stage.** Apart from the typical aspects of any maintenance stage, other aspects related to the mobile grid described here are taken into account. A plan of maintenance of the system for its later modification is defined according to the new necessities of the client. Once the system has been put into the hands of the end users, often we have to face questions that require an additional development to fit the system, to correct some non detected problems or to finalize some characteristics that had been postponed. Depending on the received request of maintenance, we must study the viability of the proposed change to identify which part of the system is affected and who must take part in its correction, being this change able to be accepted or denied depending on the reach of it.

**Activities:** This stage is composed of the following activities (see Figure 6):

- A1: Study of Requests. It studies the change request and defines a system of control and request registry.
- A2: Analysis of Requests. It analyzes the request to establish the reach to carry out the request. It allocates the people in charge and studies the possible solutions. Also, it determines if the request is accepted or rejected.
- A3: Study of Change Viability. It studies the modifications to carry out, defining the resources, personnel, cost and time affected by the request and evaluating the propose complexity of the change and solutions.

- A4: Approval and Monitoring of Requests. It establishes a request monitoring plan. The changes will be made and if the results of the previous activities are favourable and the people in charge agree, the request will be approved.

**Input Artifacts:** Output artifacts of the construction stage and maintenance request.

**Output Artifacts:** Report of impact of change, Acceptance or rejection of the request, Personnel, cost and time required, List of elements to change.

**Techniques, Practices and Reference guides:** Monitoring, Cost/benefit analysis, Estimation of resources, personnel and time, Interviews and meeting.

**Main Roles:** Customers experts, Project Manager, Maintenance Team, Analysts, Requirements engineer, Designers team.

## 5. Conclusions

The Grid connects groups of PCs, storage units and nets, allowing research centers and enterprises to dynamically assign resources according to the business necessities. These resources are distributed on the net in a transparent way but keeping a high security level and a correct management policy that takes into consideration technical as well as economic parameters. It is a new computation paradigm, a shared model that allows not only communication and storage but also information processing all over the world. In this new shared model, security plays an essential role for the success of this new paradigm, assuring access to the resources, the information, the users and the organizations that put their resources at the disposition of the world.

It is difficult to incorporate, safely existing mobile devices into the Grid, so that the impact is minimum and transparent to the user. At the moment, there are many technologies and tools available that cause that the Grid applications are secure, but at the time of incorporating mobile devices (PDA, mobile telephones, etc.) the possibilities of implementing security are reduced, mainly due to the limitations of these mobile devices and to their technologies (wireless, WAP, etc.).

There are numerous referring studies to incorporate security into the whole life cycle of software in order to obtain an end product that fulfills the required security requirements. In the case of the life cycle of a mobile Grid system, the same situation occurs; it is necessary to incorporate security from the first stages of development, by defining a process or a methodology that, besides developing a mobile Grid system, incorporates all aspects of Grid security and mobile devices into the life cycle and obtains,

consequently, a secure end product. That's the reason why the necessity to elaborate and define a process of development of a system based on Grid and mobile technology and, considering the peculiarities and necessities of this type of systems arises. This process must always be flexible, scalable and dynamic, so that it adapts to the necessities, always changing, of the Grid systems.

As future work we will analyze in depth the proposed methodology, making a special effort in describing each stage in detail and defining a scenario or study case where we apply our methodology obtaining a real mobile grid system.

## 6. Acknowledgment

This research is part of the following projects: MISTICO (PBC-06-0082) financed by FEDER and by the "Consejería de Educación y Ciencia de la Junta de Comunidades de Castilla-La Mancha" (Spain), and ESFINGE (TIN2006-15175-C05-05) granted by the "Dirección General de Investigación del Ministerio de Educación y Ciencia" (Spain).

## 7. References

- [1] Foster, I., Kesselman, C., and Tuecke, S., "The Anatomy of the Grid: Enabling Scalable Virtual Organizations". *7th International Euro-Par Conference Manchester on Parallel Processing*, 15(3): 2001, 1 - 4.
- [2] Litke, A., Skoutas, D., and Varvarigou, T. "Mobile Grid Computing: Changes and Challenges of Resource Management in a Mobile Grid Environment". In *5th International Conference on Practical Aspects of Knowledge Management (PAKM 2004)*, December 2004.
- [3] Humphrey, M., Thompson, M.R., and Jackson, K.R., "Security for Grids". *Lawrence Berkeley National Laboratory Paper LBNL-54853*: 2005.
- [4] Foster, I., Kesselman, C., Tsudik, G., and Tuecke, S. "A Security Architecture for Computational Grids". In *5th ACM Conference on Computer and Communications Security*. San Francisco, USA: ACM Press 1998, pp. 83-92.
- [5] Kostopoulos, G., Sklavos, N., and Koufopavlou, O., "Cap. 10. State-of-the-Art Security in Grid Computing", in *Security in Distributed, Grid, Mobile, and Pervasive Computing*, Auerbach Publications, Editor: The University of Alabama, Tuscaloosa, USA. 2007, p. 440.
- [6] Crampton, J. and Lim, H.W., "Role Signatures for Access Control in Grid Computing". pp. 19, 2007.
- [7] Pearlman, L., Welch, V., Foster, I., and Kesselman, C. "A Community Authorization Service for Group Collaboration". In *IEEE 3rd International Workshop on Policies for Distributed Systems and Networks 2002*.
- [8] Bradford, P.G., Grizzell, B.M., Jay, G.T., and Jenkins, J.T., "Cap. 4. Pragmatic Security for Constrained Wireless Networks", in *Security in Distributed, Grid, Mobile, and Pervasive Computing*, Auerbach Publications, Editor: The University of Alabama, Tuscaloosa, USA. 2007, p. 440.

- [9] Baskerville, R., "Information systems security design methods: implications for information systems development". *ACM Computing Surveys*, 25(4): 1993, 375 - 414.

[10] Anderson, R., Security Engineering - A Guide to Building Dependable Distributed Systems: John Wiley&Sons. p. 640, 2001.

[11] Phan, T., Huang, L., and Dulan, C. "Challenge: Integrating Mobile Wireless Devices Into the Computational Grid". In *8th annual international conference on Mobile computing and networking (MobiCom'02)*. Atlanta, Georgia, USA: ACM Press 2002, pp. 271 - 278.

[12] Guan, T., Zaluska, E., and Roure, D.D. "A Grid Service Infrastructure for Mobile Devices". In *First International Conference on Semantics, Knowledge, and Grid (SKG 2005)*. Beijing, China. 2005.

[13] Jameel, H., Kalim, U., Sajjad, A., Lee, S., and Jeon, T. "Mobile-To-Grid Middleware: Bridging the gap between mobile and Grid environments". In *European Grid Conference EGC 2005*. Amsterdam, The Netherlands: Springer, February 14-16 2005, pp. 932-941.

[14] Kwok-Yan, L., Xi-Bin, Z., Siu-Leung, C., Gu, M., and Jia-Guang, S., "Enhancing Grid Security Infrastructure to Support Mobile Computing Nodes". *Lecture Notes in Computer Science*, 2908/2003: 2004, 42-54.

[15] Bruneo, D., Scarpa, M., Zaia, A., and Puliafito, A. "Communication paradigms for mobile grid users". In *3rd IEEE/ACM International Symposium on Cluster Computing and the Grid (CCGRID'03)*. 12-15 May 2003, pp. 669 - 676.

[16] Forman, G.H. and Zahorjan, J., "The Challenges of Mobile Computing". *IEEE Computer*, 27(4): 1994.

[17] Trung, T.M., Moon, Y.-H., Youn, C.-H., Cho, J.-J., and Jeong, S.-J. "A Gateway Replication Scheme for Improving the Reliability of Mobile-to-Grid Services". In *IEEE International Conference on e-Business Engineering (ICEBE'05)* 2005.

[18] Puliafito, A., Bruneo, D., and Scarpa, M., "Mobile Middleware: Definition and Motivations", in invited chapter in *Mobile Middleware*, P. Bellavista and A. Corradi, Editors, CRC Press: London. 2006, p. 1377.

[19] Satyanarayanan, M. "Fundamental Challenges in Mobile Computing". In *Symposium on Principles of Distributed Computing* 1996, pp. 1-7.

[20] Kruchten, P., The Rational Unified Process: An Introduction. 2nd ed: Addison-Wesley. p. 320, 2000.

[21] Vivas, J.L., López, J., and Montenegro, J.A., "Cap. 12. Grid Security Architecture: Requirements, fundamentals, standards, and models", in *Security in Distributed, Grid, Mobile, and Pervasive Computing*, Auerbach Publications, Editor: Tuscaloosa, USA. 2007, p. 440.

[22] Trusted Computing Group Administration, *Securing Mobile Devices on Converged Networks*, 2006.



# 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, Duffly.....	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	Charnripinyo, 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	Shugeno, 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	Spanhower, 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
Mích, Luísa	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	Weiss, Steffen
Terada, Masato	1282	Welzer, Tajana
Thalheim, Bernhard	1405	Whittaker, Sarah
Thipsc, Aashay	765	Willassen, Svein Yngvar
Thuraisingham, Bhavani	237	Willemson, Jan
Tielemann, Michael	911	Win, Bart De
Tikotekar, Anand	659	Woolam, Clay
Tingdi, Zhao	461	Wouters, Karel
Tjoa, Simon	179	Wu, Jiang
Tlili, Syrène	302	Wuyts, Kim
Töndel, Inger Anne	1172	Xenidis, Jimi
Torra, Vicenç	990, 994	Xiao, Liang
Torre, Marco Dalla	128	Xiao, Youan
Toval, Ambrosio	813	Xiaolei, Li
Trujillo, Juan	104, 1248	Yamazaki, Kenichi
Trumler, Wolfgang	404	Yan, Chunfang
Tsuchiya, Takeshi	842	Yang, Erica Y
Tupper, Melanie	950	Yang, Xiang-he
Turnbull, Benjamin	1355, 1361	Yao, Gang
Ueda, Shintaro	1340	Yasuura, Hiroto
Ungerer, Theo	404	Yautsiukhin, Artsiom
Uribeceberria, Roberto	520	Ye, Qingsong
Valencia-García, Rafael	813	Yi, Xun
Vallée, Geoffroy	659	Ying-You, Wen
Vélez, Iñaki	520	Yoshinaga, Hirokazu
Venter, Hein	1388	Yoshiura, Hiroshi
Verma, Rakesh	1067	You, Yonghua
Vicente, Javier	578	Yskout, Koen
Vittorini, Valeria	1097	Yurcik, William
Völp, Marcus	268	Zadeh, Abdulah Abdulah
Vorobiev, Alexandre	383	Zamone, Nicola
Wahl, Martin	911	Zeng, Shengke
Walter, Thomas	1135	Zeni, Nicola
Wang, Dongsheng	630	Zhang, Bo
Wang, Hongji	532, 538	Zhang, Youhui
Wang, Hongyi	630	Zhang, Zonghua
Wang, Huaxiong	1332	Zhen-shan, Yu
Wang, Lingyu	3	Zhi-li, Chen
Wang, Qi	727	Zhou, Jianying
Wang, Xinlei	1044	Zincir-Heywood, A. Nur
Watanabe, Dai	1294	Zincir-Heywood, Nur
Wattanapongsakorn, Naruemon	604	Zisman, Andrea
Weber, Stefan G.	958	Zuccato, Albin
Wei, Yang	558	Zulkernine, Mohammad
		Zurutuza, Urko

**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](mailto: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](mailto: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.

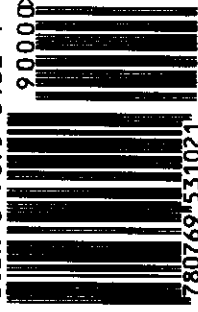
The following is the URL link to the **CPS Online** Publishing Inquiry Form:  
[http://www.ieeeconpublishing.org/cpir/inquiry/cps\\_inquiry.html](http://www.ieeeconpublishing.org/cpir/inquiry/cps_inquiry.html)



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